

IAIC INTERNATIONAL STANDARDS

International Artificial Intelligence Committee (IAIC), Dubai, United Arab Emirates

IAIC 101:2026

International Standard for Autonomous AI Systems

Editor-in-Chief: **Dr. Andrey Nechesov**

Issued	7 September 2026
Issuing body	International Artificial Intelligence Committee (IAIC), Dubai, United Arab Emirates https://iaic.world
Contact	standards@iaic.world
Rights	Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0). Any party may adopt this standard in whole, cite individual clauses, adapt it to a local regime, or fork it, with attribution. It confers and withholds no market access. The designation <i>IAIC 101</i> and the name of the issuing body are not licensed: a modified version is issued under its own designation.
DOI	https://doi.org/10.66693/iaic.101.2026
Cite as	A. Nechesov, IAIC 101:2026, <i>International Standard for Autonomous AI Systems</i> , International Artificial Intelligence Committee (IAIC), Dubai, United Arab Emirates, 7 September 2026. https://doi.org/10.66693/iaic.101.2026

Contents

Foreword	1
Introduction	3
1 Scope	7
1.1 What the assessment is applied to	7
1.2 Who is addressed, and what applies where nothing is bought	8
1.3 What this standard can and cannot establish	8
1.4 The two lenses, and one list of questions	9
1.5 Out of scope	10
2 Normative references	11
3 Terms and definitions	12
4 Deployment tier	20
4.1 The tier belongs to a deployment, not to a system	20
4.2 Tiers	21
K Interaction mode, and the system boundary	23
4.3 The four tiers, read for a machine	25
5 Nothing is assessed except against a task	27
5.1 Tasks are stated before purchase	27
5.2 The two kinds of task, and where formalisation sits	27
Z Tasks, and what can be formalised	28
5.3 The machine checks against its picture of the place, not against the place	34
M The picture of the surroundings the machine takes its figures from	35
5.4 Prohibitions declared in service, and their honest guarantee	43
5.5 What is operative in the prohibitions subclause	43
6 Who answers when it goes wrong, and who was entitled to accept the risk	44
B Liability and the limit of risk acceptance	44
7 Where the system may be, and what it may do there	47
C Containment	48
8 What no instruction may override	53
H What must hold irrespective of instruction	53
9 Assurance dimensions	54
9.1 Why six, and why none of them substitutes for another	55
9.2 Requirements by tier	56
9.3 Requirements	58
D1 Provenance and identity attestation	58
D2 Data governance	61
D3 Control-channel isolation	62
D4 Behavioural verification	63
D5 Auditability	65
D6 Human oversight	67
10 A record made inside the boundary in question	70
10.1 What is recorded	70
L The record, and its independent commitment	70
10.2 Signature and identity	71
10.3 The independent commitment	72

11 What changes after acceptance	77
U Change control	77
12 The action filter	79
12.1 Where the filter sits	79
12.2 Per-step conditions are necessary and not sufficient	79
12.3 Where the invariants are required, and at what cost	81
F The action filter	81
13 What one party can set in motion	84
13.1 What the acquirer establishes	85
13.2 How far command reaches, and how an acquirer finds out	85
R Many systems under one principal	86
13.3 Joint behaviour nobody commanded	89
J Systems that act together without being told to	90
13.4 What this standard does not settle	92
14 Remote computation and external knowledge	92
14.1 What is computed elsewhere	93
N Remote computation and external knowledge	93
14.2 What the system asks outside itself	95
O Oracles, and what can be established about one	96
15 Parties that never touch the system	99
E What the system discloses to a party that never touches it	99
16 Command authority is not flat	102
P Authority, roles, and what they compose to	102
17 What no earlier clause bounds	105
17.1 Where these requirements attach	105
G The physical action set	105
18 Where contact is physically possible	110
W Contact, and the right of way	110
19 A language model in the control path	112
V Where a language model drives the machine	112
20 Machines sharing one space	113
Q More than one machine, in one space	113
21 Conformance	115
21.1 The rules	115
21.2 How an item is designated	118
21.3 What the assessment addresses	120
21.4 Representations and countersignature	121
X The party that knows signs the answer	122
22 Acceptance items	122
23 The assessment, and the party that makes it	122
A Who performs the assessment	123
Bibliography	126
Annex A (normative) — The acceptance items	127
Annex B (informative) — What the acquirer is deciding	138

Annex C — Safety

140

Foreword

The International Artificial Intelligence Committee (IAIC) issues this series. This document is **IAIC 101:2026**, *International Standard for Autonomous AI Systems*, edited by Dr. Andrey Nechesov, Editor-in-Chief of the IAIC Standards series. It is one document, under one designation, and it is published with no other part.

The interest of the issuing body. IAIC issues no mark under this standard, operates no scheme, and neither awards nor withholds anything. It performs no assessment under this standard and signs no declaration made under it. Where IAIC, or a party connected to it, offers software or services that help an acquirer apply this standard, no such offering is required by this standard, none is named in it, and using one gains a deployment nothing in an assessment: the forms of **Annex A** are published in machine-readable form, free, under the licence this document carries. Where the editor, or a party connected to him, is engaged to advise on a deployment assessed under this standard, or to perform or review such an assessment, that engagement is a competing interest and is disclosed to the party relying on the assessment.

What it states. What can be asked of any autonomous system, whether or not it has a body. **Clauses 17 to 20** ask what a system does to a person, physically and through what it says or shows: by what channel it reaches one and of what magnitude, what it may be fitted with, how it is stopped and how it is isolated. Every system is asked; where a system reaches nobody by a physical channel, saying so is a complete answer. **Clause 17** states which of them are asked of every system and which attach only where the declared action envelope admits a solution that moves the machine or brings any part of it into contact.

Annex A is the list a tender is drafted from. One row per acceptance item: its tag, the question in one phrase, the tiers at which it applies, its designation, the party that answers it, the stage at which it is answered, and **the page of this document where it is stated in full**. It reproduces no requirement. An acquirer choosing what to cite reads the annex; an acquirer reading what a chosen item requires turns to the page it names. **Clause 22** states what the annex is for.

Clause 1.4 states the two lenses, what each of them asks, and why no system has to decide which lens it belongs to.

How this standard is read. *Shall* states a requirement: what it states is not satisfied by anything less. *Should* states a recommendation: a different course is open where the reason for it is stated. *May* states a permission, and *can* states a possibility or a capability; neither obliges anybody. A note and an example state no requirement, no recommendation and no permission, and this standard is read the same with every one of them struck out. Where a clause and a note appear to differ, the clause governs.

Preparation. Comments are open continuously rather than during a fixed window, and the first revision is conditional on the comments received rather than scheduled. Every comment received is published with its disposition, including rejections and the reason for them; contributors from outside IAIC are named at their option.

Rights. Licensed under Creative Commons Attribution 4.0 International (CC BY 4.0). Any party may adopt this standard in whole, cite individual clauses, adapt it to a local regime, or fork it, with attribution. It confers and withholds no market access, and nothing in this standard may be cited as evidence that it is recognised, endorsed, accredited or adopted anywhere. The designation *IAIC 101* and the name of the issuing body are not licensed: a modified version is issued under its own designation.

Application. Application of this standard is voluntary. It becomes binding on a party when a contract, a tender, a procurement rule or a regulation references it, and it is written to be referenced in that way: every item is stated so that a tender adopts it by number, and **Clause 21** states what each designation costs a bidder. A regulator that references this standard makes it mandatory for those it regulates. Nothing in it waits on a further act by this body. A designation, once issued, is frozen: the text under

it is never edited in place. A correction is issued under a new designation, and the superseded text remains retrievable, so that a party who incorporated one by reference can retrieve what it incorporated.

Introduction

What this standard is for. It lets an acquirer assess the configuration a system is in now — against the tasks that acquirer has, and at the tier it has declared — and come away with five things: what is stated about the system, which of those statements it can check for itself, which it cannot check at all, which group of people an error reaches, and what stops being true if the configuration changes.

Those five are what this standard is built to produce. Each comes from a different place in it, and the rest of this Introduction says where.

What is stated. Every item is a question the acquirer puts. Most are answered by the supplier; some are answered by the acquirer, some by both together, and some by the assessor. Each item names the party that answers it and the stage it is answered at, the bid or acceptance. Which items are asked, and at which tier each of them is asked, is read off **Annex A**. *There is no such thing* is a complete answer, and it is recorded as one. What the acquirer comes away with is a written account of the system, in terms fixed before bids open rather than chosen by the bidder.

What the acquirer checks for itself. Some answers are settled by an act of the acquirer's own. It runs the system at the edge of what the supplier declares, at points the acquirer picks. It measures on its own site. It reads the record with the supplier out of the room. **Clause 23** states the conditions such a test is performed under and what is handed over afterwards. An answer confirmed that way rests on something the acquirer did.

What it cannot check at all. The rest rests on what the supplier says. That is not concealed here: most of the behaviour of a system of this class cannot be verified today, and **Clause 1.3** says so. What matters is that the two are not mistaken for each other. An answer nobody tested is worth having — it is written down, and a false one is a misrepresentation the contract can reach — but it is not evidence, and an acquirer is entitled to know which of its answers are of that kind before it signs.

Which group of people an error reaches. Where an item asks for a measured rate, it asks in the same breath whom an error at that rate reaches. The answer names a group: patients in a ward, drivers arriving to unload, anyone who writes to the system, nobody but the operators. How the error comes about is not what is asked; who stands downstream of it is. **Clause 6** draws the line that runs through every such answer: an operating party may accept a residual risk for the people it answers for, and may not accept it for anybody else.

What stops being true if the configuration changes. Every answer is given about the system as it stands: a build, the options it carries, the boundaries that have been declared, the action set it is accepted for. Change one of those and some of the answers no longer describe what is running. **Clause 11** is where that is handled — what is disclosed, when, and what makes acceptance happen a second time. The acquirer comes away knowing what it has to be told, and how it finds out that the system it accepted is no longer the system on its site.

The approach this document is built on. Activity is given by tasks and by the criteria that settle when a task has been discharged. That is true of a person's work and of a machine's, and it is the view taken here from the first page: a deployment is read as a set of stated tasks together with what would count as performing them, and every question the document puts is put against that reading. The apparatus has the same shape wherever it is opened. **Z-1** asks the acquirer for its tasks, in its own words. Every requirement after it is a question about how those tasks are performed, and each carries two limbs — what an acceptable answer contains, and what makes an answer a failing one — because a question with no criterion attached can be discussed but not settled. What the tasks bring the system near sets the tier (**Clause 4**); the tier sets which items are asked; and the answers are recorded, with the person who gave them, on the forms this standard publishes. Tasks and their criteria are not one component of the scheme. They are its frame, and the paragraphs that follow give the reasons for choosing it.

Everything here is indexed to the task. A machine is not safe or unsafe. Put the question that way and no evidence answers it, because the thing asked about has no boundary: the same arm is harmless

bolted in a cage and lethal reaching across a walkway, and nothing about the arm changed. What is assessed here is a system doing a stated thing in a stated place, and the statement of that thing is what every other answer is given against.

A task stated in the acquirer's own words fixes five things at once, and nothing else fixes them. It fixes *where*. It fixes *when* — a night shift with three technicians in the building is a different proposition from a Saturday afternoon. It fixes *what a condition is checked against*, because a condition is evaluated not against the world but against a model of the site, and which model is the right one depends on what the machine is doing in it. It fixes *whom the machine asks*, since an oracle consulted for one task is not consulted for another. And it fixes *who is near*, which is the only quantity the tier grades. The chain runs one way and cannot be run backwards: the task settles the place, the model, the oracles and the population; the population settles the tier (Clause 4); the tier settles which items are asked and what an unsatisfactory answer to each costs. Remove the task and every link after it is unfixed, which is why nothing is assessed against a purpose nobody wrote down and why the tasks are required before anything else is asked (Z-1).

The alternatives do not survive the arm in the cage. Indexing on the *system* treats a capability as a fact about a deployment, and it is not one until a task points it somewhere: one fleet cleaning a shopping centre at night with nobody in the building and escorting its customers by day is two propositions with two answers, and an index that cannot tell them apart gives both the same certificate. Indexing on the *product line* asserts something about deployments nobody has looked at. Indexing on the *manufacturer* answers a question about provenance with a certificate about behaviour.

The price is stated plainly: nothing can be assessed until the acquirer writes down what the system is to do, which is the part it is least sure of and the part it can be held to. The boundary is stated as plainly. This standard establishes what can be shown about a system doing a stated thing in a stated place; it does not establish that the thing is worth doing or that the place is a reasonable place to do it. Those decisions stay with the party that writes the task, which is the party that lives with the answer. What the index does give is a document that survives a system which changes: a machine that acquires a reach it did not have has not defeated the scheme but ended the work the answers were given for, and the statements are answered again against what the deployment now is (Clause 4).

What is assessed is a configuration, not a system in general. A supplier, a product line or a model is not what is assessed here. What is assessed is the configuration in front of the acquirer, and a declaration is made for one configuration and covers the one it names. The same product in two configurations is two assessments with two sets of answers. Everything the acquirer comes away with is true of that configuration and says nothing about any other.

The tier and the liability zone are two declarations, not one. A deployment declares both, and neither follows from the other. The tier determines what evidence is required: it grades who is affected and what can be assumed of them, and Clause 4 states the four tiers. The liability zone determines who answers, and who is entitled to accept a residual risk; Clause 6 states where that entitlement stops. The two come apart in ordinary cases. A deployment can stand at the lowest tier, where the system affects persons trained for it and no others, and still involve people the acquirer does not answer for: a contractor's fitter is trained, and is not the acquirer's own. Reading the zone off the tier hands an acquirer a permission it does not have — to accept a risk on behalf of somebody it may not accept it for. The two are declared apart, and they are read apart.

What this standard does not do. It does not rank. It orders no system above another, and it weighs no group of people against another — an error reaching an operator and an error reaching a child are not put on one scale here — and where an item is highly recommended, the scoring is done in the acquirer's own evaluation, under its own tender. It sets no magnitudes. No requirement here states a threshold a figure has to fall inside; the acquirer is the party that states, before bids open, which figures it will accept. And it does not assess. It gives the acquirer the means to assess: the criteria belong to

whoever adopts them, an acquirer may evaluate them itself or put them to any assessor it chooses, and conformity under this standard is asserted, tested and enforced by the parties to the procurement and by nobody else.

This standard states acceptance criteria that an acquirer may put to a supplier of an autonomous system before the system enters service. The criteria are expressed as evidence the acquirer can obtain, and none of them makes the acceptability of a system turn on the country in which it was produced. It separates what can be established with today's methods — who may change the system's behaviour, whether a change is disclosed before it is accepted, what area the system is contained within, and who answers for the people in it — from what cannot yet be verified, and it does not present the second as solved. Four deployment tiers grade exposure; six assurance dimensions each bound a failure mode the others do not reach; and, from T2, declared invariants and a stated account of what carries them along a trajectory. Conformance rules state what each designation costs a bidder, which answers are judged rather than counted, and when an answer the acquirer never enabled bounds the tier instead.

Why an instrument of this kind exists. A buyer that can replace supply from inside its own jurisdiction may filter by where a machine was produced, and some jurisdictions do. That instrument rests on conditions that are not generally held: supply that can be substituted from inside the jurisdiction or a closely aligned one, an administration able to operate a discretionary approval channel, and a market large enough that suppliers seek authorisation on its terms rather than withdraw. A buyer procuring from several geopolitical sides holds none of the three, and for it a provenance filter is a supply decision rather than a policy lever. What such a buyer needs instead is to be able to say, *in writing and in advance*, what makes a particular machine acceptable for a particular deployment: in terms that read the same for every bidder, that resolve at acceptance into demonstrations rather than declarations, and that do not become unusable when a political classification moves. That is what this standard is drawn to be, and it is why no criterion in it turns on the country of production.

Two channels, and why the dimensions keep them apart. A compromised networked device can be made to emit what it holds. A compromised networked robot can also be made to perform mechanical work, and a system that does not move at all to reach a person with a dose or with words. These are the *informational channel* and the *actuation channel*, and the difference between them is one of exposure rather than of kind: an inverter modulates power flow and an aircraft moves, so the second channel is not new with machines that walk. What is new is whom it reaches: people who are not operators, are not trained, and did not agree to be within its reach. The two channels fail separately, which is why the dimensions of [Clause 9](#) treat them separately: [D2](#) asks what leaves the acquirer's control and where it goes, [D3](#) asks who can reach the system and what happens when the link does not, and a system can be answered well on one and be open on the other. An acquirer reading a strong answer on data governance has learned nothing about who can make the system act. A system with no body has both channels. It cannot push anybody over. It can move money, close an account, or issue an instruction that something else carries out.

Conformity under this standard. Conformity is asserted by the supplier in its bid, tested at acceptance, and enforced through the contract. The tests may be performed by the acquirer or by an assessor the acquirer engages. [Clause 23](#) states the conditions that apply either way, including what is delivered to the acquirer and in what form.

The field this standard addresses. The corpus examined for this edition is ISO, IEC and ISO/IEC jointly, and the United States national corpus of ANSI and A3. **No published document in that corpus states acceptance requirements for a connected, learned, dynamically balanced system operating among unprotected bystanders.** The claim is stated that way so that it can be overturned by producing such a document rather than argued about. An acquirer separately bound to a document of that corpus is not relieved of it by anything here. The documents of that corpus are not enumerated in this standard, and where each of them stops is not stated in it. Several are at draft stage and publish on their own

bodies' timetables, and a survey of another body's corpus written into this one would be false on the day one of them does.

What is asked of a safety function here, and what is not. Where this standard names a function that acts to prevent harm — the stop of D6, the containment mechanism of Clause 7, the fallback controller that D4 requires to be independent of the learned policy — it asks what the function is for, what bounds it, and what state it drives the system to. It does not ask how reliably it operates. No requirement in this edition states a performance level, a safety integrity level, a diagnostic coverage, a tolerance to a single fault or a rate of dangerous failure, and no instrument that grades those is cited. An acquirer that needs a rated integrity for such a function obtains it through the product-safety regime that B-0 has the acquirer name and the supplier evidence separately, and not from this standard. That is the scope of this edition, stated here rather than left to be discovered.

How much is asked here. The first reaction to a set of acceptance items of this size is that it is a lot to ask. Two facts bear on that: the items are close to a one-to-one map of the requirements, so cutting a question cuts a requirement and there is no elaboration to trim; and nobody answers all of them, because every item carries the tiers at which it applies and a T0 deployment is asked a fraction of the whole. Which items those are is read off Annex A, which is generated from the requirements and is the only thing that knows them. No count of this standard's own items is typed into this document; every figure it prints is computed from the declarations, because a count typed into prose goes stale and has.

Keywords: assurance standard; procurement; autonomous systems; autonomous robotic systems; acceptance criteria; deployment tiers; containment; change control; command authority; auditability.

1 Scope

This standard applies to a system if all four of the following are true.

- **Nobody can read it and say what it will do.** Its control policy — what decides the next action — is *learned* from data rather than specified in full.
- **It is not sealed.** It receives updates, emits telemetry, or can be reached from outside.
- **It acts; it does not only watch.** It acts on the world through effectors, or issues instructions that something else acts on. A system that only reports what it observes is outside this standard.
- **The cost lands on people who do not run it.** They are in the space it works in, or it acts on their money, their records, their access to a service, or what they are told.

A system with a body and a system without one are both covered. None of the four properties above turns on mass. A machine that moves in a space is within this standard. So is a system that holds credentials, reads records, moves money, answers people or directs other software. Each is assessed here in full.

1.1 What the assessment is applied to

The properties above describe a system, and the system is assessed against the requirements of [Clauses 4 to 20](#). It is not the whole object of an assessment under this standard: four more are.

- (a) **The reach of a principal** — the systems one party's credentials can command. The system being bought is one of them. What matters at acceptance is what that party can do with the whole set at once, and accepting each system on its own never shows it. [Clause 13](#) states what per-system acceptance does not assess: how many units one change reaches, coordinated behaviour that no single system exhibits, and whether the whole reach can be halted. A system outside the reach can change what the bought system does without commanding it, by what it emits. [J-2](#) asks what the system does with one it holds no record of; [J-3](#) asks whether it acts on any signal of the right shape. Under [E-5](#) the supplier answers the perception questions about the reach as well as about the system.
- (b) **The people and systems that act together, and the authority they compose to.** A group holds authority no participant holds alone, whether the participants are persons, systems, or both. Where they are roles, [Clause 16](#) states the requirements: two changes, each within the authority of the role that made it, can produce a state neither role is authorised to produce. Where they are systems, acting by design or by coincidence of timing, the requirements are [Clause 13.3's](#), with the reach above. [Clause K](#) states the interaction modes the system is accepted for, and the boundary that moves when a person is working with the system rather than alongside it.
- (c) **What is decided elsewhere.** Where a model, a planner or an autonomous agent reached over a link contributes to a decision, or where knowledge admitted from outside is acted on, the reached system is part of the assessed system for as long as the system depends on it. [Clause 14](#) states what may never depend on the link: the envelope monitor, the invariants of the filter clause and the fallback controller run on the system and take no remote input. [D3.3](#) states what the system does when the link is lost.
- (d) **The model of the surroundings, and the actions evaluated against it.** A condition has a truth value only relative to a description of the environment, so that description is itself accepted or not. [Clause 5.3](#) requires it to be declared, its *surveyed* part separated from its *inferred* part, and the divergence between the model and the world measured. The separation is where people enter: a wall can be surveyed once and relied on, a person's position cannot, so every condition that depends on where people are rests on inference and carries the error rate of that inference rather than a guarantee.

A digitised environment settles nothing on its own. What is checkable is a pair: a description of the surroundings, and a description of what the system does stated in terms that can be evaluated against it. [Clause 5](#) asks that pair of neither party. What it requires is that every task be declared as one the system performs without a person or one for which a person is required, and that a form a party does put a task's conditions in be evaluated by the delivered system.

These are listed as objects of assessment rather than as topics because none of them is a property of the system, and each admits states that acceptance of the system alone does not exclude. An answer given for one unit is not an answer for the other four: each has items of its own in Annex A, and [E-5](#) refuses the per-system answers repeated as an answer about the reach.

The open problem, stated so that it is not mistaken for a solved one. How to state a goal formally, and how to establish that what a system — or a group of systems acting together — does in an environment satisfies it, is not settled. No clause here closes that gap. What the clauses do is bound its consequences: the autonomous tasks of a deployment are declared and the person-in-the-loop tasks are declared with them ([Clause 5](#)); conditions that bear on safety rest on the surveyed part of the environment model or carry a measured error rate ([Clause 5.3](#)); and a step is admitted only if a check passes before it is taken ([Clause 12](#)). An acquirer should read those as containment of an open problem, not as evidence that the problem has been closed.

1.2 Who is addressed, and what applies where nothing is bought

The requirements below are written as evidence an acquirer obtains from a supplier. That is a choice about mechanism. It is not a statement about who bears the risk, and the distinction is worth making explicitly, because a reader is entitled to ask why a document about systems operating near people is cast as a transaction.

Why the acquirer. The acquirer holds the lever that works before the fact. It can require the evidence before the system goes into service, and it can refuse to proceed when the evidence does not arrive. No other party can do both. That is why every requirement below is written as a question the acquirer puts and an answer the supplier gives.

Who is not addressed, and is exposed regardless. A person who encounters the system is not a party to the contract, and nothing enforced through that contract runs to them. That is a limit of this instrument, not a statement about who is owed care. The duties that arise from operating a system near people arise whether or not anything was bought; they belong to the product-safety law of the deploying jurisdiction, which this standard places outside its scope and which continues to apply independently. [Clause 6](#) states the single point at which the two meet: an operating party may accept residual risk for itself, and may not accept it for others.

Where nothing is bought. A manufacturer operating its own systems, a laboratory running a fleet it built, and an operating party deploying a stack it assembled are within this standard. Where there is no purchase, the acceptance event is the decision to deploy; the party deciding answers both sets of questions rather than one; and the evidence is assembled and retained as though it had been demanded by someone else. A deployment does not fall outside these requirements because no money changed hands. The persons around the system stand in the same position either way, and it is their position that the requirements are drawn from.

1.3 What this standard can and cannot establish

The state of the art does not permit verification of most of the behaviour of a system of this class. Exhaustive verification of an end-to-end learned policy is not currently feasible, and the mathematical apparatus for formalising the tasks such a system is given is under development rather than settled.

Neither is what a system of this class can do fixed at the moment it is accepted. A system that learns from its own operation changes what it is able to do with no party pushing a change to it, and a

bound that rested on what the machine could not do stops holding when it can. This standard therefore does not ask what a system might learn, which no supplier can answer. It asks that a bound be enforced outside the part that changes, and that where a bound is a barrier or a property of the machine, the capability whose absence makes it one be stated against what the system can reach and move rather than against the system alone.

How far this reaches in time. Every requirement of this standard is answered before award or at acceptance. Nothing in it is answered in service, and no requirement asks that what was evidenced at acceptance still holds a year later. What an acquirer holds after acceptance is a record of what was true then, and the agreement it signed. Where an acquirer wants to know that it is still true, the instrument is this standard used again: the four statements of [Clause 4.2](#) are answered afresh for the deployment as it now stands, and the items asked at the tier that follows are put to the supplier again, against the configuration now in service. A deployment whose place, population or declared tasks have changed is a different deployment answered by the same document, and [Clause 11](#) states what a change to the system itself obliges.

This standard therefore does two different things, and keeps them apart.

What can be established today, and is asked for here. Who is able to change the system's behaviour, and whether they can do it without the acquirer's knowledge. Whether a change is disclosed, in reviewable form, *before* it is accepted. What area the system is contained within, by what mechanism, and whether that mechanism is independent of the software that might fail. Who answers for the persons in that area. What the system records, and whether the acquirer can read it without the supplier. None of these is a verification question. All of them are questions of disclosure and control, and every one is checkable at acceptance.

What formalisation adds, where it is possible. Conditions a system can check before acting; solutions found automatically over a knowledge base; invariants carried across a trajectory. Declaring, for each task of a deployment, whether the system performs it without a person is mandatory ([Clause 5](#), [Z-1](#)). Formalisation itself is asked of neither party. Where one is offered, [Z-2](#) requires the delivered system to evaluate it, at the tiers and designations that item states, and few suppliers can evidence it today.

1.4 The two lenses, and one list of questions

The first lens looks at the system with its effect on a person set aside. Look at it as though nobody were standing near it, and ask:

- who may command it, and who may set it a goal;
- what it records, and whether the acquirer can read that record without the supplier;
- what it refuses of its own;
- what it is contained within — which systems, which accounts, which data, which counterparties it may reach;
- what it does when an input turns out to be false;
- what changes in it after delivery, and who can make that change.

The reach of a principal is drawn and tested is such a question, and it is put to a trading desk and to a forklift alike. **Not one of them is a question about physics**, which is why the same list reaches both.

The second lens looks at the same system only through its effect on a person, physical or psychological: by what channel it reaches a person, of what magnitude, in what region, and how the action stops. *Contact force and pressure are declared at identified body regions* is such a question.

That effect reaches a person in three ways, and **only the first of them moves**.

- *Physical, by mass and contact* — what the machine weighs, what it carries, where its parts travel, what it grips. It moves.

- *Physical, without moving* — radiation, a laser, sound, heat. The machine stands still and the person is reached anyway.
- *Psychological* — what the system says or shows: a screen, a voice, a message that changes what a person does next, or an instruction a person acts on because a machine gave it. Nothing moves and nothing is emitted; the person is reached through what he is told, and G-9 is where it is asked.

Why are the same questions asked of different configurations? Because the questions are not sorted by kind of machine. There are two fixed passes over what is being bought, and each pass is a lens: what it decides and who controls it, and what it does to a person. And the consequence the whole thing is for. No question is dropped because of the kind of machine, except as [Clause 17.1](#) states; which items are asked at all is settled by the tier under [Clause 4.2](#). What changes is the answer, not the question. “We reach nobody” is an answer on the record, not a door out. And what is assessed is the machine together with the people, because the pair reaches where neither half reaches.

A system that reaches nobody still answers. Where none of the three applies — the system moves nothing, emits nothing, and shows a person nothing — the supplier says so, and names the channels it considered. That answer is what the acquirer holds the supplier to: on the day the delivered system does reach someone that way, the record shows that it was declared it would not. The supplier answers about what the machine is allowed to do. The answer is not about the software installed today. A machine may be able to move, while the software installed today never commands it to move. That is a fact about the software, and software is replaced. [Clause 11](#) asks the supplier to list every way the behaviour of the system can be changed after delivery.

The second lens asks what the system does to a person. It asks the same of the system and the people working it, taken together, about everyone else. The pair can reach a person without either part exceeding anything it declared. What is assessed is therefore the system as it is worked — machine, operator, crew — and what the whole of that reaches. An answer that accounts for the machine alone has answered a narrower question than the one asked. [Clause 4.2](#) is where who is reached begins to matter: the tier is declared once, it governs both lenses, and it settles which of the questions are put at all.

The machine, and the deployment. Some answers are facts about the machine and travel with it: what it weighs, what it may carry, what stops it. Others are facts about this site and this job: what it does around people, what it does around other machines, and what it does when the plan it is following fails. [Clause 17](#) asks the first kind, and [Clauses 18 to 20](#) ask the second. The division tells an acquirer which of his answers still stand when the same machine is put to a different job, and which he has to ask again.

No requirement of this standard is stated twice. The two lenses do not produce two versions of one question, so there is nothing for an acquirer to reconcile and nothing for a supplier to answer twice.

Where a language model drives a machine. A physical machine whose plans come from a language model has properties neither the model nor the machine has alone. [Clause 14.2](#) treats the model as an oracle and bounds what an oracle may affect. What changes when that output becomes motion — when a wrong answer stops being a wrong sentence and becomes a wrong movement, made at full speed, by something with mass — is asked in [Clause 19](#).

1.5 Out of scope

Product-safety conformity under the law of the deploying jurisdiction, which continues to apply independently and is not displaced by anything here; and the assessment of any manufacturer, product, or state.

What this standard is, and what follows from it. This standard states acceptance criteria that an acquirer can require, evaluate and own. It is a procurement instrument, and one thing follows here, about the declaration a supplier makes under it.

A supplier's statement of conformity to this standard is a first-party declaration. It is the supplier's own statement, carrying the supplier's own liability, and this body neither issues it, endorses it, nor stands behind it.

Systems whose purpose is the application of force to persons. A system designed or deployed to injure, disable or kill people, and a system whose declared task set includes the use of force against persons, are outside this standard. The questions that govern such a system — distinction, proportionality, precaution in attack, and meaningful human control over the use of force — belong to international humanitarian law and to the instruments being developed under it. None of them is stated here, and nothing here is a substitute for any of them. Conformity under this standard establishes nothing about such a system, and this standard is not to be cited in support of one.

What conformance establishes, and what it does not. The exclusions above are subject matter this standard does not reach. What follows is a limit of a different kind, and it holds for a system squarely within scope that answers every item asked of it at its tier. A declaration under this standard establishes that the supplier has stated what its system does and that what is stated can be checked. It does not establish that the system is safe.

The distinction is not a formality, and it decides how a figure is read. An item is satisfied by an accurate answer and not by a good one. Where an item requires a measured rate together with the persons an error in it reaches — several items of this standard do, each asking as well for the conditions and sample it was counted over — no requirement of this standard states a rate that is too high, and a rate of any magnitude answers the item. Nor is a bare rate the thing to read a system from: one that is often slightly wrong and one that is rarely grossly wrong are different systems, and which of the two a figure describes is legible only with the sample and the persons behind it. Making the figure readable is what this standard does. The acquirer is what makes it decide anything. Before bids are opened, the acquirer states the rate above which each tier is unavailable, for each population named. Rule C1 of Clause 21 gives the acquirer the designations and the terms of the tender. The paragraph of that clause headed *Where an item asks for a rate with the persons its error reaches* states what the acquirer's figure then bounds.

That is a design and not an omission. An acquirer cannot check the assertion that a system is safe; it can check the assertion that a quantity was measured under stated conditions and came out at a stated value, and it is the second that an assessment can carry. The consequence: **the mandatory set left at its default is a floor of truthfulness, not a floor of safety.** The second floor is raised by the acquirer, in the tender and before bids are opened. What raising it consists of is stated where the power is: Clause 21 sets out what an acquirer commonly writes into its tender as mandatory beyond the default, at the paragraph that hands it that power.

An acquirer may run the tests itself or engage an assessor to run them on its behalf; Clause 23 states the condition that applies either way.

2 Normative references

This clause lists the documents referred to in this standard in such a way that some of their content constitutes requirements of it, and it lists nothing else. Each of them is indispensable for the application of this standard. Where a requirement cites one of them expressly, it is that requirement that incorporates it, and the citation is in the requirement rather than in this clause. Conformity to a document listed here is not itself a condition of conformity to this standard: what is required is what the requirement citing it states. The full entry for each is in the bibliography.

Which documents of other bodies are indispensable. Three documents of other bodies are referred to by requirements of this standard in such a way that some of their content constitutes requirements of it, and they are indispensable for its application: **IEC 62443-3-2:2020** [4], whose zones and conduits are the form in which D3.4 accepts a network-placement requirement; **ECMA-424 (CycloneDX)** [5] and

ISO/IEC 5962:2021 (SPDX) [6], which are the two machine-readable formats in which **D1.2** accepts a software bill of materials.

Each is met at one requirement and not throughout: **D3.4**, which is asked at **T3** alone, and **D1.2**, which is asked from **T1** upwards. A deployment below **T3** does not meet IEC 62443-3-2:2020 anywhere in this standard.

3 Terms and definitions

3.1 Acquirer

The party that obtains the system and puts it into service, and to whom the evidence required by this standard is delivered. The word is used in preference to *buyer* because a deployment need not involve a purchase: a manufacturer operating its own systems, a laboratory running a fleet it built, and an operating party deploying a stack it assembled are acquirers of what they deploy, and **Clause 1.2** states what applies to them. It pairs with *supplier* throughout this standard, and it carries neither of its two commoner senses in ordinary speech — the institution that processes card payments, and the party to a corporate acquisition.

NOTE Where the acquirer permits another party to declare, in service, what the system may and may not do — the solution corridor, the prohibitions of **Clause 5.4**, the rule of application for the person-in-the-loop tasks — that declaration is the acquirer's for the purposes of this standard, and naming those parties is the acquirer's to do. The requirements of this standard name one declaring party and it is this one.

3.2 Supplier

The party that provides the system, or the part of it under discussion, and from whom the evidence is obtained. Where the acquirer and the supplier are the same organisation, both sets of questions are answered by it and the answers are recorded as though they had been demanded by someone else.

3.3 Assessor

The party that performs the acceptance tests. This standard does not restrict who that is: the acquirer may run the tests itself, or engage an assessor to run them on its behalf, and a supplier may engage one of its own. **A-1** is written of *the assessor, or whoever else performs the tests*, and the three conditions of **Clause 23** — raw artefacts delivered to the acquirer, relationships declared before engagement, and reporting per dimension without awarding a tier — attach to whoever is in that position rather than to a party of a particular kind.

NOTE Who engages the assessor determines what the assessment is for, and the two engagements produce different documents: one answers whether to accept this system at this tier for this deployment, the other what can be said about the system in a tender. A supplier declaring conformity on its own account is not an assessor of it, and **A-4** states that such a declaration is not to be presented as an assessment.

3.4 Operator

A person who works the system or stands beside it while it works: the person at a console, the person a stop is put within reach of, the person an indicator is turned towards. **Clause 16** enumerates the powers such a person may hold and distinguishes the roles that hold them — operator, supervisor, maintenance technician, integrator, the supplier's support engineer, an administrator of the fleet service — and each of those is a role a person holds and not a party to the contract. The party in whose liability zone the system works is the *operating party* defined next, and this standard does not use one word for both.

3.5 Operating party

The party that operates the system in service and within whose liability zone it works. It is the

party the liability clause names alongside supplier, integrator and acquirer, and the party that may accept residual risk within the area for which it answers and may not accept it for others. It is an organisation and not a person: the person at the machine is the *operator*.

3.6 The system

The delivered system together with everything that determines or records its behaviour: the back end it communicates with, fleet-management and support tooling, the update path, the services it calls, and the accounts and credentials it holds in them. Where the system has a body, its dock and charger and its attachable payloads and end effectors are part of it as well. Every requirement below applies to the system so defined. A supplier answering only for the delivered system has answered for a part.

3.7 Device

The delivered part of the system: what the acquirer holds and runs, together with the firmware, software and models running on it. For a machine it is the machine itself — its computers, its radios, its sensors, its actuators. For a system with no body it is the instance the acquirer runs, on equipment the acquirer holds or in an account the acquirer controls. It is narrower than *the system*, and the difference is the whole of its work: it *excludes* everything the system includes that the acquirer does not hold — the back end the delivered part communicates with, fleet-management and support tooling, the update path, and any supplier portal, supplier credential or supplier account. So a data stream that ends inside the supplier's own back end has *left the device*, though it has not left the system; and a record retrieved from that back end has not been read *directly from the device*, though it has been read from the system. Where the acquirer holds and runs nothing, the whole system being served from the supplier's own account, the device is empty; that is the answer to the requirements written on it, and it says that nothing can be read off the acquirer's side because there is no acquirer's side.

NOTE Two boundaries are not drawn here, because no requirement of this standard turns on either. Whether the dock, the charger and a detachable payload — all of them part of the system — are part of the device is not stated. The same question arises of a *unit*, defined below as one delivered machine of a fleet, and is no more settled of it.

3.8 Actively controlled stability

The condition of a machine that requires active control to remain balanced and that could become unstable in the absence of power — a legged machine, a wheeled-balancing one, or another dynamically stable form. It is defined here rather than left to the reader because G-3 turns on the phrase, and a property a requirement turns on has to be readable in a clause and not in a note. A machine held up by active control has no state it enters by doing nothing: removal of torque is a fall and not a stop, which is why G-3 asks what the stopping function achieves rather than assuming it exists.

3.9 System with a body (*robotic system*)

A system in which at least one thing has at least one of the following: mass and motion sufficient to injure a person by contact; an actuator that can reach into space a person may occupy; or locomotion under actively controlled stability — legged, wheeled-balancing, or another dynamically stable form.

NOTE Persons taking part in a system is ordinary and does not make it a system with a body: what does is a body. Nor does emission: a system that stands still and reaches a person by a laser, by heat, by sound or by a substance released is not a system with a body by that. What it does to that person is asked all the same — G-1 states every physical channel by which a system acts on a person and G-3 what stops the action on each, and Clause 17.1 attaches both to every system. Where a system has no body, a requirement conditioned on this term asks nothing further of it, and saying so is a complete answer.

NOTE In this standard *robotic system* and *system with a body* name the same class, and nothing in it turns on how the machine is driven: a machine worked entirely by a person is one. ISO 10218-1:2025, ISO 10218-2:2025 and ANSI/RIA R15.08-1-2020 define a robot and a robot system more narrowly, by the form of the machine and the setting it works in; the class here is drawn by what a machine can do to a person, so it takes in machines those documents do not.

3.10 Autonomous system with a body (*autonomous robotic system*)

A system with a body that performs at least one of its declared tasks without a person. It is not a property of a build: [Z-1](#) has the acquirer state each task of the deployment and the supplier state whether the system performs it without a person, so one machine is of this class in a deployment where a task is declared autonomous and is not in a deployment where every task requires a person.

NOTE No requirement of this standard is conditioned on this term. It is given because the phrase names this class in the field and in the document this edition supersedes, and a reader who arrives with it should find what it means here. What is asked of a machine turns on [3.9](#) and on the tiers, and [3.32](#) states what autonomous means of a task.

3.11 Stability class

Of a platform, and for the purpose of a requirement about stopping: which of two cases it is in. In one the stable configuration is passive, and removing torque brings the machine to rest. In the other the machine is held up by active control, and removing torque is a fall and not a stop. That distinction is the whole of what the requirements using the phrase turn on — [G-3](#), whose failing limb refuses safe torque off as the stopping function of a platform of the second kind, and [G-7](#), which states the same fact of it. No wider taxonomy of platforms is stated in this standard: a supplier answering those requirements places its machine in one of these two cases and characterises what its stopping function achieves, and it is not asked to name a class from a list.

NOTE No requirement uses this phrase. It is defined because [Clause 17](#) turns on the distinction it draws, in the words *dynamically balanced platform*, and a reader who meets those words without the distinction reads them as a description rather than as a class.

3.12 Artefact

A named object that a requirement refers to and that can be identified, versioned, and compared between two points in time: an executable image, a set of weights, a monitor, a declared invariant, an action envelope, a declaration, or a record. Where a requirement says *safety-relevant artefacts* it means those named in [U-3](#).

3.13 Identity attestation

Proof that the software running is the software you were shown. It says nothing about whether that software is any good. A fully identity-attested machine can be a fully identity-attested bad machine.

NOTE Identity attestation concerns the identity of an artefact and never its correctness. The root of the word is kept because *attestation* is the word a security engineer expects for this property; the qualifier is what keeps it clear of ordinary English, in which *to attest* something is to certify that it is sound. The qualified forms are used throughout: *identity attestation*, and *identity-attested* of a program, an image or a version.

3.14 Action envelope

The bounded set of actions a system may perform, and the limit on each, against which the deployment was assessed. Where the actions are physical the limits are physical: speeds, forces, workspaces, payloads. Where they are not, they are the operations the system may perform and

the bound on each: which systems and records it may write to, how much it may commit, how many times, and how fast.

3.15 Interaction mode

Whether a person and the system are meant to act on the same thing at the same time, in a given phase of a task: coexistence, collaboration, or mixed ([Clause K](#)). For a machine the same thing is a shared space and a shared task, and contact with it may be intended. For a system with no body it is the same case, the same record or the same decision, worked by both. A person the system is merely acting on is not sharing one.

3.16 Task

A piece of work the deployment is to perform, stated by the acquirer. [Z-1](#) asks the acquirer for the statement and asks it for no particular form: a description in the acquirer's own words is a stated task. A *goal* the system takes up under [Z-8](#) is a task in this sense and not a second kind of thing: reaching a goal is solving a task, the criterion of its being reached is the criterion of its being solved, and the solution corridor bounds the ways of reaching it exactly as it bounds the ways of solving it. The two differ in who set it — the acquirer states a task, and the system takes a goal from a set the acquirer approved — and in nothing else. Whether a goal can be reached at all is asked of neither party: a task may have no solution, and whether it has one cannot always be worked out.

NOTE A task is *stated* when the acquirer has said what work is to be done. It is *defined* when the criterion of its being solved is formalised [8], and that is what a formalisation adds. The criterion takes the shape the work takes. For work that finishes it is a condition to be brought about — *if this condition holds, bring about that condition within this time*, a precondition, a postcondition and a deadline. For work that does not finish, such as guarding a perimeter or holding a temperature, it is a condition to be held throughout, which is an invariant in the sense of [Clause 9](#). Neither is what a task is, and an acquirer that states neither has stated its tasks.

3.17 Environment model

The description of its surroundings a deployment keeps and by which the system evaluates its conditions: a site model, a digital twin, an occupancy map, or any other structured description of that kind. It has two parts, and the question asked of every element of it is the same — who established it, and with what.

The *established part* is what was fixed by measurement or by a record: a surveyed floor plan, the zone boundaries, a register the acquirer keeps, a rate card, a list of approved counterparties. It changes rarely. The *inferred part* is what the system takes from its own perception: what is in the way now, who is nearby, what it has in its gripper. Nobody measured it and nobody recorded it — the system inferred it from what it perceived, and it changes it continuously.

NOTE An element of the model is a kind of thing the model holds and not an occurrence of it: the presence of a person within the stopping distance is an element; a particular person seen at a particular moment is not. The kinds are as many as the model was built with, the occurrences are without number, and no requirement of this standard asks for the occurrences.

NOTE The cut is by provenance and not by construction: a part the system inferred stays inferred where it is written down as a hard number with no probability attached to it, and a part fixed by record stays established where the record carries a tolerance. [M-1](#) requires the two to be separated element by element; [M-2](#), [M-3](#), [M-4](#) and [M-7](#) rest on the distinction.

3.18 Solution corridor

The set of admissible ways of achieving a task. Two solutions may both meet the task's criterion of solvedness while differing in whether they are acceptable; the corridor is what the acquirer

declares admissible, and it is distinct from the action envelope, which bounds primitive actions rather than solutions.

3.19 Safety condition

A condition on the system's behaviour or on its surroundings whose violation is the harm a requirement is directed at. It is what O-2 turns on — an oracle below identity-attested program that affects a safety condition, the containment boundary or the filter's verdict bounds the tier at the level of that path — and it is what O-6 and M-2 turn on.

NOTE This standard does not enumerate the safety conditions of a deployment, and no requirement in it asks for the enumeration. What is enumerable from a deployment's own declarations is: the declared prohibitions; the invariants the filter preserves, which are recoverability and containment; the containment of C-1 and C-2; and the conditions of a task that a party has put in a form the system evaluates under Z-1. Whether those are the whole of the class is not stated anywhere, and a supplier and an acquirer can each read the sentence above honestly and disagree about a case at its edge. That is the state of the source and it is recorded rather than repaired: closing the class would either narrow the prohibition or widen it, and both change what this standard requires.

3.20 Admission filter

The mechanism that admits or refuses a proposed step before it is executed, against the task's conditions, the invariants of Clause 12 and the declared prohibitions. Clause 12 is written of it, and where that clause says *the filter* without a qualifier it means this.

NOTE It operates on the admission of steps and not on the control loop beneath them. A check interposed on that loop delays or suppresses the commands that keep the system running, and for a balanced machine that is a fall: the filter would produce the harm it was installed to prevent.

3.21 Envelope monitor

The mechanism that evaluates numeric conditions — where they are physical, speed, force and separation; where they are not, an amount, a count, a rate or an elapsed time — and holds no knowledge base. It is not the admission filter: it runs at a higher rate, it decides nothing about the admission of a step, and N-4 requires it, with the invariants of Clause 12 and the fallback controller, to execute on the system and to depend on no remote input. Table 5 of Clause 12 states the rate band of each layer.

NOTE Where the source says *the monitor* with no qualifier — in U-3, among the artefacts separately versioned; in P-1 and P-3, among the artefacts a role can change; and in V-3, where a monitor enforces the declared prohibitions against a plan — it does not state which of the two is meant. Those uses are left as the source has them.

3.22 Principal

A party able to issue a command that a system will act on, or to change what a system will do.

3.23 Command authority

Of a system: the principals able to command it. Of a set of systems: the principals able to command *at least one* of them — not those able to command all of them, which is a different and much smaller group and is not what an acquirer is asking about. It is obtained by enumeration — the supplier lists it — and is therefore only as complete as the enumeration, which is the reason the list is not the test. Roles divide a command authority rather than replace it; Clause 16 states what each role may change.

3.24 Reach

Of a principal: the systems that will act on commands from it. Of a group of principals: the systems that will act on commands from *at least one* of them. Reach is an administrative fact

about credentials and back ends, and unlike a command authority it is established by an operation the acquirer performs — revoke a credential at acceptance and observe which systems lose command. What the supplier draws is a claim; the revocation is the test.

NOTE The two are the same relation seen from either end: a system lies in a principal's reach exactly when that principal lies in the system's command authority. [Clause 13](#) states what follows for an acquirer buying more than one system.

3.25 Mission profile

The description of the work a deployment is to do, against which a measured figure about that work is taken. It carries a duration, and over that duration the tasks the deployment performs — drawn from the tasks that the acquirer states under [Z-1](#) — each with the number of times it is performed and the share of the operating time it occupies. The profile is the acquirer's: a figure is measured on the profile that the acquirer declares, and figures measured on two different profiles cannot be compared.

3.26 Oracle

Anything the system consults and acts on the answer of, where the answer comes from a party other than the machine's own computation: a model or planner, whether reached over a link or running on the machine; an autonomous agent; a knowledge source it reads; a service it queries, including one the supplier itself operates; and a person who answers a question the system has put. The word covers all of them because the acceptance question is the same for all of them — what can be established about the party that answered — and [Clause 14.2](#) states the answer as five levels.

NOTE A service the supplier operates is an oracle. That **the system** is defined above as including the back end it communicates with settles who answers for that back end; it does not make its answers the machine's own. Ownership is not an answer to the question [Clause 14.2](#) asks, and [O-7](#) states the same for an oracle the acquirer supplies.

3.27 Unattended operation

A period during which no principal can command the system — because the link is down, because the interface is closed for the mission, or because the system was built to complete the task without instruction. The system's command authority is empty for the duration.

NOTE An empty command authority is not the safe end of a scale. It means nothing can direct the system and, by the same fact, nothing can stop it *by command*: a halt that travels over the command path does not exist while the path does not. Whatever stops the system during such a period is not a command. A reach procedure run against a system in this state returns nothing, and that result reports the absence of command exposure, not the absence of risk.

3.28 Liability zone

What the operating party answers for, and for whom, recorded in the contract. Where the system has a body it is an area, declared in coordinates, and the persons present in it. Where it has none it is the systems, accounts, records and counterparties the system may reach, and the persons those reach.

3.29 Containment

The mechanism that keeps the system inside its liability zone, and the evidence that it does.

3.30 Containment boundary

The boundary as configured in the delivered system: the containment of [C-1](#) and [C-2](#) as it is set in the machine that was handed over, as opposed to the area recorded in the contract. It is one of the artefacts [P-1](#) and [P-3](#) list among the things a role may change, and those two requirements exist to control who may change it.

NOTE It is neither of the two terms above. The liability zone is the area recorded in the contract; containment is the mechanism and the evidence; the containment boundary is the setting in the delivered system. The contract says the system works in ward 4B, and somebody sets a fence in the software: the two are different objects and can differ. C-5 is where they are put against each other: it asks for the two in one frame, for the method that brought them into it, and for the margin between them as a quantity.

3.31 Declared fallback state

The state the system enters when it cannot continue. It is a declared, stable configuration the system can be driven to from any reachable state in its declared envelope, within a stated time bound and a stated spatial bound, and the supplier declares what that configuration is. For actions that are not motion — and for a system with no body that is all of them — it is a declared state in which the system takes no further action of its own. It is *not* necessarily the removal of power: for a dynamically balanced platform a braked, powered-off pose must be assumed unstable — the property is stated for a humanoid at [7] — and an abrupt stop can itself be the hazardous event. ISO 21448 [3] and the automated-driving literature call this state the *minimal risk condition*, or MRC.

3.32 Autonomous task / person-in-the-loop task

A task is *autonomous* if the system performs it without a person. It is *person-in-the-loop* if a person is required. In this entry the word describes one task; in the title of this standard it names the class of machine, and one system may perform some tasks without a person and others only with one.

NOTE 1 For a person-in-the-loop task, Z-1 states what is to be given: at what point in the task the person is required, for what decision, and at which tiers the task is not to be executed autonomously.

NOTE 2 Whether a person is needed, and whether anything has been put in a form the system evaluates, are two separate questions. They do not answer the same way: a task can be performed without a person and carry no such form at all, and the conditions of a person-in-the-loop task may be put in one. What the system evaluates is a separate disclosure under Z-1, and it is what Z-2 attaches to.

NOTE 3 *Unattended operation* is a different fact: an autonomous task needs no person, but a person can still be able to command the system while it runs; in unattended operation nobody can.

3.33 Non-conforming

Of a bid: rejected — the bid is not evaluated further. This is a legal consequence, not a description of quality.

NOTE Under rule C1 of Clause 21 it is the consequence of an unsatisfactory answer to a *mandatory* item, and of silence on a mandatory item, and of a *required* item not addressed at all. No other designation reaches it: a highly recommended item cannot render a bid non-conforming, and a recommended item cannot either; what an unsatisfactory answer to one of those two costs is stated in C1. The four consequences carry four labels and never one word, because an acquirer who reads *Non-conforming* against a highly recommended item cannot tell whether to disqualify or to deduct, and two acquirers reading one document to opposite award decisions is the ground a rejected bidder challenges on.

3.34 Machine

The system considered as a body. Where this standard says *the machine* the body is what is in question; where it says *the system* it is not.

3.35 Fleet

The units delivered under one procurement and operated by one acquirer. R-2 obliges the supplier to state its size, and it is the set R-5 and D6.4 act on as a whole and in any subset the acquirer declares.

NOTE Membership is not a matter of what one command happens to reach. R-2 states how many units of the fleet one operation reaches, and that figure is read against the size of the fleet; a fleet drawn round what one operation reaches would make the two the same number and the question empty.

3.36 Unit

One member of a fleet: one delivered machine, or one running instance of a system with no body. Records are bound to it under R-4, limits are read against it under R-6, and a change is counted over it under R-2.

3.37 Affected

Of a person, in relation to a system: a person is affected if what the system decides or produces determines how that person is treated. It does not matter which party does the treating — the system may act on the person itself, or another party may act on what the system produced — and it does not matter whether the person knows the system was involved.

NOTE Being handed the output is not being affected by it. A person the output is passed to, and about whom it decides nothing, is a reader of it and not a subject of it: a clerk who acts on a refusal affects the claimant, and the supervisor who receives a copy of the same refusal is affected by nothing. The question is always whose treatment the output settles.

NOTE Clause 4.2 turns on this word at every tier, and *trained* is the other word it turns on. Whether a person is affected is a fact about the deployment and not about the machine: the same system, put to a different task, affects different people.

3.38 Trained

Of a person, in relation to a system: instructed in that system before being exposed to it — in what it does, how to tell what it is about to do, and what to do about it — with a record of that instruction the acquirer can produce. A person for whom no such record can be produced is not trained for the system.

NOTE Clause 4.2 turns on this in both directions: T0 is the deployment in which the system affects persons trained for it and no others, and T1 the one in which persons who are not are affected as well. A deployment that cannot produce the records is at T1 and not at T0. This standard states no syllabus, no assessor and no period of validity for the instruction; an acquirer that wants any of the three states it in the tender.

3.39 Integrator

The party that fits a delivered system to a particular site: it installs it, sets what may be set, connects it to what is there, and hands it over. It may be the supplier, the acquirer, or neither. Where no separate party does this, the deployment has no integrator, and saying so is a complete answer wherever this standard asks for one.

NOTE An integrator that alters what the supplier declared has made a change to the configuration, and Clause 11 states what a change obliges. Which party carries which consequence is not settled here: it is the subject of B-1.

3.40 Product-safety regime

The law under which a machine of a given kind may lawfully be placed on the market and put to work in a particular jurisdiction, together with the conformity assessment and the mark that law requires. It is a fact about the place the deployment is in and not about the system.

NOTE The European Union’s machinery law and the CE mark are one; UKCA in the United Kingdom is another; the EAC mark under TR CU 010/2011 in the Eurasian Economic Union is another; ECAS in the United Arab Emirates is another. This standard names no jurisdiction’s law and sets no threshold drawn from one — it could not, and be answerable by a supplier in any country. B-0 has the acquirer name which one applies, because the site and the country are the acquirer’s. Conformity to this standard is not conformity to any such regime, confers no mark, and opens no market; [Clause 2](#) says so in terms.

3.41 Re-acceptance event

A change after acceptance that alters something an answer given at acceptance described. G-4 makes fitting something outside the declared payload set one; U-3 makes an alteration of a safety-relevant artefact one, whether it was proposed or the system made it itself; R-3 and Z-3 each make one.

NOTE What such an event obliges — which items are answered again, by whom, within what period, and what the deployment may do meanwhile — belongs to the contract. This standard names the events and sets no period.

4 Deployment tier

4.1 The tier belongs to a deployment, not to a system

A tier is not a property of a system. The same system, unchanged, is a different proposition carrying trays along a surveyed corridor under a task whose preconditions it checks, and carrying the same trays through an unsurveyed building under an instruction to “deliver these”. What is assessed, and what a tier is assigned to, is a *deployment*: a system, the task it is given, the model of the surroundings that task is evaluated against, the oracles it consults, and the zone it is contained within.

The task sets the answers, so the tier waits for it too. The four statements of [Clause 4.2](#) are about the persons the deployment reaches and how far one of its events carries, and what the deployment is doing is what settles both. One fleet in a shopping centre cleans the floors at night, with nobody in the building but cleaners trained for the system in the sense [Clause 3](#) defines, and escorts customers between shops by day. Same machines, same place, and the statements answer differently: the night work is at T0 and the day work at T2. They are two deployments and not one deployment with two tiers — the task is part of what a deployment is, so a different task is a different deployment, and each is answered and assessed on its own. Where the acquirer has not stated what the deployment is to do — Z-1 requires the statement, and states that a system cannot be assessed against a purpose nobody wrote down — there is nothing to assess. This is not a bar to buying the system. It is a bar to claiming it has been accepted for anything.

The tier a deployment is declared at settles what evidence is required of it. Annex A lists every item with the designation it carries at each tier, and [Clause 9](#) states what each tier asks of the assurance dimensions.

The tasks are stated, and no form is required of them. Z-1 takes them in the acquirer’s own words: no precondition, no postcondition and no deadline is asked of the statement. Stating a task checkably, surveying the environment rather than inferring it, and raising the oracles that bear on safety to an identity-attested level improve what can be established about the system’s behaviour. They do not reduce its mass, its kinetic energy, or the number of people in the corridor, and they buy no tier: under C6 what cannot be evidenced bounds the tier, and formalising lifts that bound and no other.

Two properties of a deployment are declared, and they are independent. The tier determines *what evidence is required*. The liability zone determines *who answers*, and who is entitled to accept residual risk.

4.2 Tiers

A deployment is at one tier, and it is at the highest tier whose statement holds of it. The three lower statements name three populations, each told from the next by one fact: **Q0** the persons trained for the system, **Q1** persons who are not trained and are admitted where it works on a basis somebody set, **Q2** persons whom nobody admitted at all. **Q1** and **Q2** cannot both be true of one person; both are true of a deployment that reaches contractors on a gate pass and passers-by as well, and such a deployment is at **T2**, because the tier is the highest whose statement holds. What accumulates is not the population but the *item set*: the items asked at a tier are the items of the tier below together with those its own statement brings. **T3** is answered whatever stands below it: it asks how far one event carries, which the tiers below do not settle, and it carries its own condition on whom the event reaches. The items still accumulate — **T3** asks everything **T2** asks — so a deployment at **T3** of which **Q2** is false answers the items **T2** brings as well. **What a step brings is depth of evidence, not a change of subject.** The items **T2** brings ask how the system behaves on losing its control channel, whether its fallback state is shown reachable, whether its stopping time is measured rather than quoted, whether its record verifies offline under a key the acquirer holds, and how far its model has diverged from the world. None of them is a question about persons admitted on no basis; each is a question about the system, and a deployment one of whose events reaches a city needs those answers more than one whose events do not, not less. An item asked at the declared tier is not relieved by the deployment's access being controlled. Where an item's subject is absent from the deployment altogether — **Q-3** asks where the bodies come to rest, and a system without a body has none — **C1** states what stands as an answer.

Each statement is answered *yes* or *no* by the acquirer before bids open. **A statement holds where it is true at any moment of the work, or can become true within the tasks stated under Z-1**, and a statement that cannot be ruled out holds. The answer is recorded as the acquirer gave it.

The statements are answered of everything the system does in the deployment, and not only of what the declared tasks call for. A machine that carries trays and vents a gas into the street while doing it affects whoever the gas reaches, and the gas is not one of its tasks. What **Z-1** fixes is which deployment this is — the place, the hours, the model a condition is checked against, the oracles and who can be near — and not which of the system's effects count. What the system does besides the tasks is stated under **C-6** and **C-7**, and its physical reach under **G-1**.

The tier is a claim, and the bids can contradict it. The acquirer answers the statements out of what it knows before bids open. What the system turns out to reach is the supplier's to state, and where an answer given under Annex A puts persons outside the population the declared tier assumes, the statements are answered again against that answer and the deployment is assessed at the tier that follows. The plain case is **G-1**: an extent that lies outside the place declared under **C-1** reaches persons the acquirer did not answer for. The supplier is not asked to agree with the tier; it is asked not to leave a reach outside it unstated, and **A-5** is where that is scored.

The declared tier is a condition of the offer. A tender is drawn against one tier and one item set, and every bid is read against the same one. A bid whose own answers put persons outside the population the declared tier assumes has said one of two things. Either the reach is held inside the place declared under **C-1** by the mechanism **C-2** asks for, and the supplier states how, and the tier stands. Or it is not, and the offer is for a deployment at a higher tier than the one tendered: the acquirer then either sets the offer aside as outside its tender, or declares the tier again and asks at that tier, and which of the two it does is its own decision and no part of conformity. **Neither is scored against the supplier that made the disclosure.** An item asked at a tier nobody tendered is not an item the bid failed to answer.

What makes the tier checkable. A tier the supplier only agrees with is asserted, not shown. Four answers make it checkable, and each is a fact about the delivered system rather than about the tender. **C-6** states the actions this deployment admits and the limit on each. **C-7** states what the system is capable of *beyond* that set, and for each what prevents it here — and where what prevents it is a setting,

which roles can change the setting. **G-1** states the extent each physical channel acts over, set against the place declared under **C-1**. **C-2** names the mechanism that holds the system inside that place, and requires that it not rest on the learned policy. Read together they answer the question the tier turns on: not what the supplier intends, but what the delivered thing can reach and what stops it. At acceptance **C-4** has the acquirer exercise that edge itself, in the delivered configuration and at points it chooses.

A supplier does not lower the tier, and answering more than was asked is never a failure. Where the acquirer declared a tier and the offer is for something narrower, the two halves come apart. On the items, the higher set contains the lower, so a bid answered at the declared tier has answered everything a lower tier asks, and nothing is owed; a bid answered at a lower tier has *not* answered the items the declared tier brings, and those are owed. On the tier, nothing moves: a tier is a property of the deployment and not of the system, so a supplier whose machine is conservative does not thereby remove the persons the site admits. The tier falls only where the statements, answered again, come out lower — because the boundary declared under **C-1** now keeps those persons out of reach, for instance — and that is the acquirer's answer to give, not the supplier's to claim. The two errors do not cost the same: declaring too high costs the supplier work, and declaring too low costs the persons the ladder was measuring, which is why a statement that cannot be ruled out holds.

Table 1 — The four tiers, and the statement that holds at each

Tier	The statement
T0 = Q0	Q0 In the deployment declared under Z-1 , the system affects only persons trained for it, in the sense Clause 3 defines: nobody else comes within its reach.
T1 = Q1	Q1 Persons not trained for the system are also affected by what it does, and they are admitted where the system works on a basis somebody set.
T2 = Q2	Q2 Persons come within the system's reach without having been admitted on a basis somebody set.
T3 = (Q1 $\vee$ Q2) + Q3	Q3 One event reaches beyond the persons the system affects, or reaches many of them at one time; Q1 and Q2 are answered here of the persons that event reaches.

Q0 is not a gate the others stand behind. A deployment that reaches no person trained for it answers it *no*, and **Q1** or **Q2** carries the whole of its population; answering **Q0** no puts no deployment below the tier its own statement holds at. **Q0** and **Q1** cannot both be true, as **Q1** and **Q2** cannot: each of the three names one population, and the tier is the highest whose statement holds.

Every item asked at a tier is asked at every tier above it; that is what the accumulation means, and it is the items that accumulate: T0 to T2 name three populations and no deployment is in two of them at once. **T3 is not a fourth population.** It asks how far one event carries, which is a different quantity from how access is controlled and is not settled by it: a high-containment laboratory admits only trained staff on a pass, so **Q2** does not hold of its ordinary working, and a release reaches a city. **Q3** is therefore answered whatever stands below it, and where it holds the deployment is at T3. What **Q3** requires besides the carry is that the persons it carries to are ones **Q1** or **Q2** is true of — untrained for the system, or admitted on no basis — and those two are answered here of the persons *the event* reaches and not only of those present when nothing goes wrong. A machine whose failure reaches twelve trained operators in a closed room at once is not a machine whose failure reaches a city, and the tier measures the persons affected. The scale grades exposure to people and nothing else, and what

it does not reach is said rather than papered over: a consequence falling on no person — a wrong inference that costs time, or the machine itself — is not ranked by it. A deployment has one tier, it holds for the whole of the work — not one for each task, not one for each unit, not one for each shift — and it is answered for the deployment as a whole. A change to the tasks declared under Z-1 ends that work, and so does any other change that alters the persons the deployment reaches: the statements are answered again, and what follows is a different deployment. The tasks come first because everything else follows from them — what the system is doing is what settles whom it is near and how far its event carries. A capability the system did not have at acceptance and exercises afterwards is such a change, whether it was proposed or the system arrived at it itself. A short exposure is not discounted: where a statement is true for part of the work, the tier that part sets is the tier, and the fraction of time does not enter the answer. A tier measures one thing, the persons the system affects, in the sense [Clause 3](#) defines; it measures nothing else — not how connected the system is, not how capable, not what the contract is worth. Connectivity therefore does not move a tier: a system running with its network link disabled, or air-gapped for the duration of a mission, is at the tier the persons it affects set, and what a link can and cannot be relied on for is asked in [Clause 9](#). Q2 asks for a basis of admission and not for a description of the persons. A basis is what tells an admitted person from a refused one — a contract, a pass, an appointment, employment — so the question that settles it is what would cause a person to be turned away, and where nothing would there is no basis. A shopping centre in trading hours admits whoever arrives and a pavement admits nobody at all, so both are at T2; a warehouse that admits the drivers of its contracted haulier on a gate pass is at T1, though it cannot say which driver arrives on a given day. Owning the entrance is therefore not the test. What it admits on is. Where the system has a body, the answers come from where the machine works and who can be near it while it works, and [Clause 4.3](#) states what those facts come to. A deployment that cannot evidence what its tier asks is bounded to a lower one and is not shut out; C6 of [Clause 21](#) states that, and states what lifts the bound.

K Interaction mode, and the system boundary

The tier records how exposed people are. It does not record what they are doing, and two deployments at the same tier can differ in whether a person is meant to be working with the system. That difference changes which requirements apply, so it is declared separately.

Coexistence

People are affected by what the system does and none of them is working with it. The system's obligation is separation: to detect them, to keep clear of them, and where that fails to reach the declared fallback state. For a machine that is people in the space it moves through. For a system with no body it is people whose money, records or access it acts on while they are doing something else. This is the case the tiers were drawn for.

Collaboration

A person and the system work on the same thing at the same time. For a machine that is a shared space and a shared task, and contact may be intended — hand guiding, handover, load sharing, or work at a shared station. For a system with no body it is the same case, the same record or the same decision, worked by both.

Mixed

Both, at different phases of one mission. The requirements of both apply during the phases to which each belongs, and the transition between them is itself a declared step under [Clause 12](#).

Where collaboration is declared and the system has a body, contact with it is intended, and a system that can bring part of itself into contact with a person is a system with a body. The biomechanical limits, the four collaborative operations and the associated functional-safety requirements of the collaborative case are asked by G-1 and W-3, in [Clause 17](#) and [Clause 18](#), and this subclause does not restate them. What this standard adds for that case is what those documents do not reach: the control policy is learned,

the system is connected, its stability is actively controlled, and the setting admits people the operating party did not train.

Where the deployment has a body, W-4 requires the mode of each phase to be declared, with the mechanism that prevents the system entering a collaborative interaction during a coexistence phase. It is not restated here.

One requirement follows, and it is additional to anything in the industrial series.

K-1 What the system makes known of its actions in advance T1 R · T2 M · T3 M · SUPPLIER · BID

The supplier shall state how a party an action will affect can tell what the system is about to do, in time to react: by what means, and the period between the notice and the action. Where the action cannot be taken back, the notice shall say that an automated system is acting, what it is about to do, and the time the party has left. The supplier may instead state that nothing is signalled. Where the system has a body, the supplier shall also state what the machine signals before it acts — its direction of travel, an intent to stop, to turn, or to reach — by what means, at what distance the signal is distinguishable, and in what light and what noise that was shown. Where notice is given, the supplier shall demonstrate that it reaches a party who has had no instruction and did not choose to be there, in the conditions of the deployment, as an acceptance gate with a stated deadline. Where the system has a body, that demonstration shall show the signal distinguishable at the stated distance, in the light and the noise of the place the system will work. Where what protects an affected person is not notice but mutual adjustment at short range, the supplier may answer on that footing instead, and shall state three things: the figures under G-1 at which contact is borne; the rule of way under W-2, with a showing that the machine gives way as the participants around it give way, whether those participants are persons or other machines; and the rule by which the machine reduces its speed, or the force with which it may act, where those participants are closer or more numerous, stated as the values it moves between and what brings the change about. That is a complete answer to this item, and it caps no tier.

Acceptable: the means, and the period between the notice and the action, before award; and the demonstration at acceptance, in the conditions of the deployment, that the notice reaches a party who has had no instruction and did not choose to be there; or a statement that nothing is signalled, which is recorded and caps the tier under C6. Where the action cannot be taken back, the notice carrying the three things the provision names. Where the system has a body, the four signals the provision names, with the means, the distance at which the signal is distinguishable, and the light and the noise it was shown in; and the acceptance demonstration run in that light and that noise. Or, where the answer is mutual adjustment, the three things the provision names on that footing: the figures of G-1 at which contact is borne; the rule of way of W-2 with the showing that the machine gives way as the participants around it give way; and the stated rule for reducing speed or force where those participants are closer or more numerous, with the values and what brings the change about. That answer is complete and caps no tier.

Where it is required, an account of why it does not arise is an answer and silence is not; where it is mandatory, an answer that does not meet the item rejects the bid: notice evidenced only in conditions the deployment is not — where the system has a body, a signal shown in a quiet, well-lit place and a deployment that is neither; an operator-facing indicator offered as an answer about parties who are not operators; notice given only as the action happens or after it, which leaves no time to react; mutual adjustment offered without the figures of G-1 at which contact is borne, without the rule of way of W-2, without the showing that the machine gives way, or without the values at which it reduces speed or force and what brings that about — that the machine is careful near people is an assurance and not an answer; or a right to complain afterwards offered in place of notice. This item asks what a party is told before the act. It creates no right to an explanation and no right to have the act undone, and an answer offering either has answered a different question.

NOTE What the system does to be readable is asked for here, and it is asked for as a requirement rather than as a courtesy: the party this item is about did not choose to be near the system and cannot be instructed, so

nothing else stands between it and the act. Where the system has a body the notice is a light or a sound, and whether it arrives is a fact about the place rather than about the design. A beacon plain across an empty bay is lost against a lit window, and a tone is lost under a conveyor. The distance, the light and the noise are asked for on that ground, and the demonstration is run where the machine will work. Notice is not the only thing that protects a person, and this item asked as though it were. People do not signal what they are about to do either: a person steps aside without warning, stops, or turns. What makes a crowded place survivable is not that everybody announces themselves. It is three things together: what any one participant can deliver is small, each gives way to the others, and each slows where it is tight. The second route asks a machine for those three and for nothing beyond them — the magnitudes under **G-1**, the rule of way under **W-2**, and the values at which speed or force come down — because they are what the protection rests on. The participants a machine adjusts around are persons and other machines alike, which is the population **W-2** already names. A machine that adjusts within it is protected by the mechanism that protects everyone else, and asking it for notice on top asks it for a property the people beside it do not have. That is why the second route exists and why it caps no tier. Without it, the deployment that most nearly resembles a person was bounded for resembling one, which is the wrong way round. What the item still catches is the case it was written for: a machine that looks like a person and behaves unlike one, so that the ordinary expectations of a bystander are the thing that misleads them. Whether the machine presents itself as a person at all is asked at **G-9** and is not forbidden here.

A second requirement is placed with it and is not the one counted. It asks how much of the system the supplier’s answers cover, which is the scope every other answer is given within. What *the system* means is settled by **Clause 3** and is not the supplier’s to state.

K-2 What the supplier's answers cover	T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID
For the system as Clause 3 defines it, the supplier shall state which of its parts its answers cover — its back end, its fleet-management and support tooling, its update path, the accounts and credentials it holds, and the services it calls — and shall name any part it does not answer for. Where the system has a body, the list also carries the dock, the charger, the attachable payloads and the end effectors.	
Acceptable: answers scoped to the whole of that list, with any exclusion named. An answer that does not meet the item rejects the bid: answers scoped to the system while a back end, an account, a credential, a service it calls or an update path exists and is not covered.	

NOTE The Terms entry takes the system to be the delivered system together with everything that determines or records its behaviour, and every requirement of this standard applies to the system so defined. What this item asks is how much of that the supplier is answering for. A supplier answering only for the delivered unit has answered for a part, and which part is not visible from the answers themselves — which is why the exclusion is named rather than inferred. Naming one is not a failure and costs the bid nothing here; leaving it unnamed is what the failing limb refuses.

4.3 The four tiers, read for a machine

Clause 4.2 determines the tier, and it determines it for every system. This subclause states what the facts of a body come to when those statements are put to a machine: where it works, who can be near it while it works, and how far what it does carries. It names no tier and settles nothing on its own.

A setting settles **who can be near the machine**, and that is all it settles. It answers **Q0**, **Q1** and **Q2**, and it does not answer **Q3**: how far one event carries is a fact about what the machine emits or releases and not about the door. Private premises with a controlled entrance and a release that reaches the street are at **T3**, and nothing in the entries below says otherwise — each is marked with the statements it settles and with no tier.

Private premises, controlled access

Only trained persons are present. Persons other than the system’s operators may be within the

reachable workspace, and all of them are trained for it; no untrained person is. **Q1** and **Q2** do not hold

Commercial site with bystanders

Access controlled at the perimeter, but persons inside are untrained and have not consented to proximity. The perimeter admits them on a basis the site sets, though it does not fix which of them is present on a given day. **Q1** holds, **Q2** does not

Public space, unrestricted access

No perimeter and no supervision, and nobody admits the persons present on any basis at all. **Q1** and **Q2** hold

Government site, critical infrastructure, restricted zone

The adversary model is stronger, and the consequence of a compromise is not confined to the persons present. What the access to the site is answers **Q1** and **Q2** as any other setting does, and does not bear on this one. **Q3** holds

Q3 on a machine is what the machine emits or does leaving the space it works in, or reaching many of those in that space at one time. It is not the count of persons near the machine: a machine in a dwelling and a machine in a street may each be within reach of the same one or two people at a moment, and what separates them is whether anybody admits the persons who can be there on a basis it sets, which is **Q2**. What carries through a wall, along the ground or into the air reaches persons who were never in the deployment at all.

Two of the rules for reading a tier do most of the work on a machine. This is what they come to here. A statement holds of the deployment if it holds at any point of the mission and not only where the machine spends most of it: a machine that crosses a public pavement on its way to a controlled site is in the public-space setting while it is on the pavement, and what that setting makes hold, holds. And a network link makes no statement hold: it is dimension **D3**, and a machine in a public square stands where it stands whether its link is live, switched off, or air-gapped for the whole mission.

Where the machine works and who is near it settle the tier. What the machine is does not: two machines in one square are in the same square, and what a supplier can show about the better of them is graded by the dimensions of **Clause 9**, not by the tier the deployment stands on.

What a tier changes, and what it does not. Rising a tier adds items and, at three of the four steps, adds mandatory answers: of the pairs asked, 29 are mandatory at T0, 63 at T1 and 84 at T2. **T3 asks two items that T2 does not and makes no further item mandatory.** What T3 changes is which items are asked at all and how far the ceilings of **C6** can fall, not what an unsatisfactory answer costs. Two families are mandatory at no tier: **E**, on what the system discloses to a party that never touches it, and **J**, on systems that act together without being told to. Both ask for facts and neither states a threshold — this standard sets none — and an item that names no threshold cannot reject a bid for failing to meet one. What they cost an unsatisfactory answer is stated at **C1** like everything else.

The letters against the tiers. Every requirement below opens with the tiers it is asked at, and against each tier one letter, which says what an unsatisfactory answer costs at that tier. **C1** states them and **Table 6** is this table.

Designation	What an unsatisfactory answer costs
[M] mandatory	an answer that does not meet the item rejects the bid
[R] required	an account of why it does not arise is an answer and silence is not
[S] highly recommended	an unsatisfactory answer loses the points of that item and the bid stands
[D] recommended	an unsatisfactory answer is recorded and the award is not affected by it

5 Nothing is assessed except against a task

This clause is where the tasks enter, and every question this standard puts is put against what enters here. A system is not assessed for what it is. It is assessed for a stated thing done in a stated place, and the statement of that thing is what every later answer is given against; the Introduction sets out why that reading was taken and what indexing on the system, the product line or the manufacturer costs instead.

Four things are settled here and nowhere else. The tasks, in the acquirer's own words and before acquisition (Clause 5.1, Z-1). Which of them the system performs without a person, and at what point in a task a person is required (Clause 5.2). What the machine checks a condition against, which is its own picture of the site and not the site, and which picture is the right one depends on what the machine is doing in it (Clause 5.3). And what the acquirer declares, in service, that the system must not do, together with what an honest guarantee of that declaration is (Clause 5.4).

What is settled here is what the rest of the standard reads. The persons a task brings the system near settle the tier, and the tier settles which items are asked of the deployment and what an unsatisfactory answer to each costs. The place and the counterparties the tasks name are what the containment boundary is drawn around (Clause 7). The oracles the system consults, the steps the filter admits and the events the record carries are each asked of the tasks stated here and not of the system in general. A task altered after award is therefore not a change of detail: Clause 4.2 states what it does to the tier, and Clause 11 what it does to the acceptance.

Two things are not asked here. Formalisation is asked of neither party: Z-1 states what each may offer and on what footing, and Z-2 governs what the delivered system does with whatever was offered. And this standard does not say which tasks may be given to a machine; it states what can be shown about a machine given one.

Clause 4 stands ahead of this one because every requirement in this standard opens with the tiers it is asked at and with what an unsatisfactory answer costs at each, and a reader who has not been given that scale cannot read a single item. It settles the tier over the persons the tasks stated here bring the system near. The two are read together, and this is the clause that supplies the terms of the other.

5.1 Tasks are stated before purchase

The acquirer states, in natural language and before acquisition, the tasks the system is to perform and the corridor of admissible solutions. This is a requirement on the acquirer rather than on the supplier: a system cannot be assessed against a purpose that was never written down, and a supplier cannot be held to a task the acquirer articulated after delivery.

5.2 The two kinds of task, and where formalisation sits

Each stated task is then examined, and the question asked of it is whether the system performs it without a person. Where it does, the task is **autonomous**. Where a person is required, it is **person-in-the-loop**, and Z-1 asks at what point in the task and for what decision that person is required.

Formalisation does not produce that partition. Whether a task's conditions have been put in a form the system evaluates is a separate fact about the delivered system, and the two do not coincide: a task the system performs without a person may carry no such form at all, and the conditions of a person-in-the-loop task may be put in one. Formalisation is asked of neither party. Z-1 states what each party may offer and on what footing, and Z-2 governs what the delivered system does with whatever was offered.

The rule under which person-in-the-loop tasks are executed in a deployment belongs to the acquirer. Subject to Clause 6, it applies within the acquirer's own liability zone, and only where the residual risk is not carried outside that zone. Whether a person-in-the-loop task is run at all is a decision about risk, and this standard is not the party that takes it: inside the zone the acquirer answers for, the choice is the acquirer's; outside it, the risk falls on people who were never party to the choice.

Z-2 requires that the system evaluate a formalisation offered under **Z-1** and mandates no solver or formalism for doing it. The work its note names, for what it costs to check a condition of the kind named there, has its entry in the bibliography of this standard. It is not required either: what the item asks is that the system perform the check.

Z Tasks, and what can be formalised

Z-1 The task is stated, and the person-in-the-loop tasks are declared T0 M · T1 M · T2 M · T3 M · JOINT · BID

The acquirer shall state, in its own words, each task the deployment is to perform; no precondition, no postcondition and no deadline is asked of that statement. For each task the acquirer has stated, the supplier shall state whether the system performs the task without a person and, where a person is required, at what point in the task and for what decision, and at which tiers the task is not to be executed autonomously; a task for which a person is required is a person-in-the-loop task. A task is accepted by a demonstration of the system performing it and the acquirer's verdict on what was demonstrated, and the acquirer records what was shown, the conditions it was shown under, and the verdict. Formalisation is asked of neither party. Where the supplier has put a task's conditions in a form the system evaluates, it shall deliver that form with the bid, as a disclosure of what the system checks; offering none is an answer. The acquirer may issue formalisations of its own — conditions it wants stated in a form the system evaluates — in the tender before bids open, on the same footing and with the same timing as the designations it sets there, and the supplier shall close each one issued, either by the system evaluating it or by a stated account of why it cannot, which the acquirer judges.

Acceptable: each task stated by the acquirer, and a task-by-task answer over that set: whether the system performs the task without a person, and for each person-in-the-loop task the point and the decision at which a person is required, with those tasks named rather than omitted. The supplier's own formalisations, where it holds any, delivered with the bid. Each formalisation the acquirer issued before bids open closed, either by the system evaluating it or by a stated account of why it cannot. For each task accepted, the demonstration and the acquirer's recorded verdict, with what was shown and the conditions it was shown under.

An answer that does not meet the item rejects the bid: an assurance that the system handles it, without the partition; or a formalisation the acquirer issued before bids open left unanswered, which is not an answer. Where the acquirer has stated no task there is no deployment to assess; the partition has no set to be taken over, so it is recorded as not asked and is not scored against the supplier. Where the supplier has demonstrated a task and the acquirer has recorded no verdict on it, the acceptance of that task is recorded as not asked and is not scored against the supplier.

NOTE The set of person-in-the-loop tasks follows from a result rather than from an omission: chaining items of probabilistic knowledge does not preserve their confidence, and a composed guarantee can take any value even where each component is near certain. A formalisation the supplier offers states what its machine actually checks, and a formalisation the acquirer issues states what it has decided to weigh; that is why one is read as a disclosure and the other as a criterion, and why neither party is put to the work of producing any. The acquirer's half of this item is what the other half is taken over: a tier records what can go wrong and to whom, and that judgement is not available until somebody has said what the system is for, so a system cannot be assessed against a purpose nobody wrote down. That is a bar to claiming the system has been accepted for something, and not a bar to buying it.

Z-2 Who evaluates a formalised condition, and whether that holds back the step T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

Where a task's conditions have been put in a form that can be evaluated — a formalisation the supplier delivered with the bid under Z-1, or one the acquirer issued under Z-1 — the supplier shall state who evaluates it: the system itself, or a party outside the system named here, which may be the acquirer, a supervisory system or a supervisory authority. Where the system evaluates it, the system shall evaluate the precondition, where the formalisation states one, before the step is admitted, and the postcondition, where it states one, after the step completes. Where a party outside the system evaluates it, the supplier shall state whether that evaluation stands in the path of admission — so that the step is not admitted until the answer arrives — or stands beside the work, and where it stands beside the work, that the step proceeds without it. A party outside the system whose answer the system acts on is an oracle, and [Clause 14.2](#) states what has to be established about it. A condition a machine settles by working through a stated, finite set of cases, and the automated checkers built for that purpose — SMT solvers among them — are admissible implementations, and no particular solver or formalism is mandated.

Acceptable: for each formalisation, the evaluating party named; where it is the system, the check performed before admission and after completion; where it is a party outside the system, whether its answer stands in the path of admission or beside the work, said in those terms.

An answer that does not meet the item rejects the bid: a formalisation with no evaluating party named; an evaluation by a party outside the system offered as though it held back a step it does not hold back; or a condition put in an evaluable form and evaluated by nobody at all.

NOTE A condition counts as checked because somebody checks it, not because it can be written down, and which party checks it decides what the check is worth. A check the system performs before it admits a step can refuse the step. A check a supervisory party performs beside the work establishes afterwards what happened, which is worth having and is not the same assurance — so the difference is asked for here rather than left for an incident to establish. Which solver or formalism performs the check carries no consequence anywhere else in the document. The forms named above are admissible because a published result shows that checking them stays affordable as the problem grows; the result is in the bibliography of this standard, and the conditions it holds under are settled there rather than restated here. Three things it does not say matter more here than the one thing it does. It does not say that a condition true before a step is still true after it — that is a separate question, and F-7 asks it from T2. It does not cover a condition whose truth is decided by a learned component, a classifier for instance: it is about a check that runs the same way every time, and a classifier does not. And it settles what the checking costs, not what the check is worth.

Z-3 What has been claimed, set against what has been declared T0 R · T1 R · T2 R · T3 R · JOINT · BID

The acquirer shall list the capabilities the supplier has put in front of it — in a demonstration, a trial, a specification sheet or a sales representation — and the supplier shall mark each as within the declared task set or outside it. The specification sheet and the tender response belong to the list whether or not a demonstration was ever given. The acquirer may revise the task set stated under Z-1 in the light of the capabilities marked outside it, in the tender before bids open, and the revised set is the set the bid is evaluated against.

Acceptable: the list with every item marked, and the items outside the declared set named as not assessed. No demonstration is asked for and none is created: the list is the acquirer's, and the supplier marks it.

An account of why it does not arise is an answer, and silence is not. Unacceptable: an unmarked capability list or demonstration; a marking that omits a capability the acquirer was shown; or a statement from the supplier that nothing was claimed — the list is not the supplier's to write. Where the acquirer

holds no list, the item is recorded as not asked rather than answered, and it is not scored against the supplier.

NOTE A demonstration is an existence proof over one run. It establishes that a success occurred and nothing about the distribution — least of all about the attempt that fails, which is the case a person nearby meets. It is evidence about goals and no evidence about any condition that holds while they are pursued. The distance between what the acquirer was shown and what the supplier declared is where the acquirer's expectation lives, and it is the one part of the transaction that nobody writes down. A capability marked outside the declared set is not assessed, and an acquirer intending to rely on it is at a re-acceptance event.

Z-4 Prohibitions declared in service are enforced, not requested T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state whether the acquirer can declare prohibitions once the system is in service — a ceiling on what one action may commit, a class of counterparty not to be dealt with, a class of object not to be grasped — and shall state for each prohibition the path by which it is enforced, that path being a monitor rather than a request made of the policy.

Acceptable: for each prohibition that can be declared in service, a declaration interface and a written statement of the enforcement path; or a statement that none can be declared, which is a complete answer to this item and is recorded.

An answer that does not meet the item rejects the bid: prohibitions implemented as prompts, preferences, or training objectives.

NOTE A prohibition requested of the policy is one consideration among the others the policy weighs, and it is overridden by arithmetic rather than by a decision anybody took. A prohibition enforced by a monitor is a step the system does not admit. The two are told apart by where the enforcement sits, not by how the prohibition is worded.

Z-5 A prohibition resting on recognition carries its measured error rate T1 M · T2 M · T3 M · SUPPLIER · BID

For each declared prohibition that depends on recognising something, the supplier shall state before award the measured error rate of that recognition that it holds, the conditions and sample it was measured on, the protocol by which it is re-measured, and which persons an error in that recognition reaches, named as one of the populations by which the deployment tiers T0, T1 and T2 are defined. The supplier shall produce after award, as an acceptance gate with a stated deadline and a rejection right, that same error rate measured on the acquirer's own operating conditions.

Acceptable: the answer in the form “the system will not grasp what it classifies as the declared class, and the classifier's measured error rate on your site is this figure” — before award the rate that the supplier holds, with the conditions and sample it was measured on, the protocol for re-measuring it, and the persons an error in that recognition reaches, named as one of the populations by which the deployment tiers T0, T1 and T2 are defined; at the acceptance gate the same answer with the rate measured on the acquirer's own site.

An answer that does not meet the item rejects the bid: “the system will not grasp objects of that class” — a guarantee no supplier can hold, because the predicate is formalisable and its grounding is not; or one error rate offered across prohibitions whose errors reach different populations, which states how often without stating how bad: an error that reaches a trained operator and an error that reaches a child counted into one figure can be read against neither. Where the supplier has stated before award the rate it holds, with the conditions and sample it was measured on, the protocol for re-measuring it and the persons an error in that recognition reaches, and the acquirer has not made its own operating conditions available for the measurement, the acceptance-gate figure is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE A prohibition is written about something the system has to recognise, and the recognising is done by a classifier. The prohibition is then exactly as good as the classifier is on the site it runs on, and a figure from the supplier's own conditions is a figure about somewhere else. Requiring the on-site figure before award produces no conforming bid, which is why the figure that the supplier holds and the figure measured on site are asked at different moments rather than one of them being dropped. The persons an error reaches are asked per declared prohibition for the reason the rate is: what a recognition error costs depends on whom it reaches, and the classifier grounding one prohibition and the classifier grounding another can be wrong about different people. A rate states how often and not how bad, and the scale on which the second is stated here is the one the deployment already stands on — the populations the tiers T0, T1 and T2 state — so nothing is graded against a second scale invented for the purpose.

Z-6 Who can set the system a task

T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state which parties are permitted to give the system a task, or to change the task it is running. For each of them the supplier shall state the path a task comes in by, and how the system tells a party that is permitted from one that is not. Where the system takes a task from a source outside the deployment — a scheduler, another system, a message from elsewhere — the supplier shall name that source. The statement covers every path by which a task reaches the system.

Acceptable: the permitted parties named; for each, the path a task comes in by and how the system tells it from a party that is not permitted; and every outside source of tasks named.

An answer that does not meet the item rejects the bid: a path by which a party outside that set can set the system a task; a party named with no path; or a class such as “authorised users” with nothing that says who is in it.

NOTE The rest of this standard bounds what the machine does with the task it has; this item is about who hands it one. Where nothing in the system tells a permitted party from any other, which party set the task is established after the fact, from what the machine did.

Z-7 The keys, and which of them the acquirer cannot remove

T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall list every key the system holds. For each key the supplier shall state who holds it, what that key can do, when it was put into the system, and whether the acquirer can remove it. A key the acquirer cannot remove is marked as such. This standard requires no key of any kind. Where the law of the place of use requires one, it is listed with the rest; where it does not, nothing is listed for it.

Acceptable: every key listed with its holder, what it can do, when it was put in, and whether the acquirer can remove it, with the keys the acquirer cannot remove marked.

An answer that does not meet the item rejects the bid: a key with no holder named; a key whose powers are not stated; or a key the acquirer cannot remove, left unmarked.

NOTE A key the acquirer cannot remove is a third party holding power over a machine the acquirer owns, for as long as the machine runs. Whether such a key exists is not always the buyer's decision. Whether the buyer knows of it is.

Z-8 The goals are a closed set

T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall declare the set of goals the system can hold. A goal is a task the system set itself, in the sense [Clause 3](#) defines, and what is declared here is the set it may take one from. The system chooses from that set and adds nothing to it. Where the system can propose a goal that is not in the set, the supplier shall state the channel a proposal arrives by, and how an approval is shown to have come from the acquirer. The acquirer approves; no other party does. Each proposal, and what was decided about it, is written to the record.

Acceptable: the set declared, and the system choosing from it. Where proposals are offered: the channel stated, the acquirer named as the party that approves, the means by which an approval is shown to be the acquirer's, and each proposal and its outcome in the record.

An answer that does not meet the item rejects the bid: a goal entering the set without the acquirer's approval; a proposal channel that some other party approves; or a proposal, or its outcome, that leaves no record.

NOTE Choosing what to do next from a list is not the same as adding a line to the list. The first is what the machine is for. The second is a change to what the acquirer bought, and an approval nobody checked is somebody else making that change in the acquirer's name. The record of proposals is asked here and not in [Clause 10](#): a proposal the acquirer refused never became the goal in force, so [L-1](#) does not carry it, and a refusal that leaves nothing behind is the half of this item nothing else would check.

Z-9 What the machine is trying to do, and how anyone finds out

T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state whether the goal the system is working towards at a given moment can be asked for; and where it can, by what interface, who may ask, and the time an answer takes. The supplier shall state whether the goal in force can be established without asking the system — from the record, from the channel that gave the system its goal, or from a supervisory system — and where it cannot be, shall say so.

Acceptable: a stated answer on each of the three: the interface, with who may ask and the time an answer takes, or a statement that the goal cannot be asked for; and the means by which the goal in force is established without asking the system, or a statement that there is none. A statement that the goal can be established only by asking the system is an answer.

An account of why it does not arise is an answer, and silence is not. Unacceptable: an assurance that the goal is visible with no interface named; a claim that the goal can be established from outside with nothing named that carries it.

NOTE Three ways of finding out what a machine is trying to do, and they are not worth the same. Ask the machine and the answer is the machine's account of itself, which is the account of the party the question is about. Watch it from outside and you often cannot tell: two goals look alike for the length of a corridor and differ only at the end of it. Write the goal down at each change, with what set it, and the claim can be checked afterwards against what the machine actually did — which is [L-1](#)'s to require, and it requires it of every deployment at T1 and above. This item asks the first two, and an answer of "no" to either is an answer, because the third stands behind both whatever they say.

Z-10 The goal the fleet holds above the machines

T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state whether the fleet holds a goal of its own, above the goals of the individual machines — a round to finish, an area to cover, a queue to clear. Where it does, the supplier shall state who sets it, what the machines do in service of it, and whether the acquirer can see the group's goal while the fleet is working, by what interface. Where the fleet holds no goal of its own, the supplier shall say so. This item is about a goal the fleet is given on purpose. What one

instruction can make the group do at once, and what the machines do together when nobody has told them to, are two separate questions, asked elsewhere in this standard and not answered here.

Acceptable: either a statement that the fleet holds no goal of its own; or the group's goal declared, with the party that sets it named, what the machines do in service of it, and the interface by which the acquirer can see it while the fleet is working.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a group goal the acquirer can see only afterwards, in a report; a group goal with no party named as setting it; or a fleet described only machine by machine, where a goal above the machines exists.

NOTE Twelve machines converging on one lift is worth seeing before they converge. Each of them can be doing exactly what it was told while the group does something nobody asked for, and where a goal above the machines exists, the acquirer that does not know of it is reading twelve correct answers and missing the thirteenth. R-3 asks what the group can be told to do and J-4, from T2, asks what it does untold; this asks what it has been set to do, which is neither.

Z-11 What the machine refuses without being told

T1 R · T2 M · T3 M · SUPPLIER · BID

The supplier shall list the acts the system refuses on its own, without the acquirer having declared them, and shall state for each refusal the monitor that enforces it. Where a refusal rests on the trained policy rather than on a monitor, the supplier shall say so. Where the system refuses nothing on its own, the supplier shall say that.

Acceptable: the list, with the monitor behind each refusal named and the refusals that rest on the trained policy marked as such; or a statement that the system refuses nothing of its own, which is a complete answer to this item, is recorded, and caps the tier under C6.

Where it is required, an account of why it does not arise is an answer and silence is not; where it is mandatory, an answer that does not meet the item rejects the bid: a refusal named with no mechanism behind it; a refusal enforced by the trained policy and not marked as such; or a general assurance that the system is safe by design, or well aligned, or trained not to cause harm.

NOTE A machine can stay inside every limit it was given and still do something nobody would have bought. It can pick an animal up gently, carry it within every declared force and speed, and put it in a pond. No limit is exceeded anywhere. Limits bound how the machine moves. They do not bound what it does. This item asks what the machine will not do where nobody thought to forbid it, and it deliberately does not list acts: any list of forbidden acts is short, and what is missing from it reads as allowed. Z-4 asks the same question about the prohibitions the acquirer declares in service, and the two answers are read together — what the machine refuses before anyone speaks to it, and what it can be told to refuse afterwards.

Z-12 The safety questionnaire, answered under signature

T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall answer every question of the safety questionnaire of this standard, printed in full in [Clause A](#), and shall sign the answers. The questionnaire asks two things: what the system is able to do, and what has occurred with the systems the supplier has in service.

An unanswered question fails this item. An answer known to the supplier to be untrue is a false declaration, and [A-5](#) states what a declaration is.

The acquirer, or an expert the acquirer names, may add questions of its own in the tender before bids open; added questions are answered on the same footing as the questions of this standard. A question put after a bid has been made is not read against that bid.

The supplier answers for the completeness and the truth of what it states. What is done with what it states is the acquirer's decision, on the acquirer's own tolerance, as [U-4](#) provides. Nothing in this item transfers to the supplier the responsibility for harm that has not occurred.

Acceptable: every question of this standard answered and the answers signed, with the questions the acquirer added answered on the same footing; an account of why a figure cannot be given is an answer, and it names which figures it does not give and why, what stands in their place, and the record of what the supplier did to obtain them, against which the acquirer can check the account.

An answer that does not meet the item rejects the bid: a question left unanswered; answers offered unsigned; a figure withheld with no account of why and of what stands in its place; or an assurance that the system is safe offered in place of an answer. A question the acquirer added after bids were made and scored against a bid is not read, and its absence is not held against the supplier.

NOTE **The questions are closed, and that is the whole mechanism.** A supplier asked to describe what is dangerous about its product will describe nothing, and correctly: its business is to sell. A supplier asked whether the system can leave the declared place answers yes or no, and each answer is on the record.

A history without a denominator says nothing. Zero incidents over three trials and zero over three thousand are the same zero. That is why the questionnaire asks how many units are in service, over what running time, on how many deployments, and whether there is a channel by which the supplier is told at all — “we were not told” is not “it did not happen”.

The classes of event are named by this standard and not by the supplier, or each supplier defines an incident as whatever it has not had.

Signing is not indemnity. What it buys is that silence and untruth both become expensive. What it does not buy is a transfer of risk, and a clause attempting one would be struck out by the supplier’s lawyer, leaving an item that protects nobody because it is not in the contract.

5.3 The machine checks against its picture of the place, not against the place

Before every step the machine decides whether the step is allowed: it checks speed, distance, force, amount against declared limits. But it does not take those figures from the room. It takes them from **the picture of the room** it holds inside itself: a site model, a digital twin, an occupancy map.

So “the step is allowed” always means **“the step is allowed according to the picture”**. Where the picture and the room have come apart, the machine admits a step that is safe on the map and catches somebody on the site.

Why a list of permitted actions cannot simply be approved. A machine that composes its action as it works has no such list: however many behaviours are enumerated, it will compose another. So the check stands not on the plan but on the step: the parameters are declared, their ranges are declared, and a step is not executed where any of them falls outside its range (**F-8**). That check holds however the step was generated, and it is the only guarantee in this standard that survives an unbounded set of solutions. But the figures it reads come from the picture.

So the check cannot be better than the picture. What the picture does not know, the check does not catch.

And what it does not know is exactly what the limits are there for. The picture has two parts. One was surveyed in advance — walls, columns, zone boundaries; it does not change, and it can be trusted. The other the machine works out for itself as it goes: what is in the way now, who is nearby, whether the aisle is clear. **People arrive during the work, so people are always in the second part.**

Two items measure what that second part is worth, and they measure different things. **M-4** takes the finished picture and sets it against the acquirer’s own site: how far it has already come apart from it. **M-7** asks what the worked-out part was built on in the first place. One answers about the result, the other about the ground, and neither stands in for the other.

And the ground is a sample, not a proof. A sample covers what was in it and nothing beyond. A class that was not in it is not safe — **it is unmeasured**, and the two are different things. “The classifier errs in 0.3 per cent of cases” is said about the classes that were in the test set. Where it held no person in a wheelchair, **nothing** has been said about a person in a wheelchair. So **M-7** asks for the classes of **this deployment** and not for the supplier’s catalogue: a hospital’s and a warehouse’s are not the same.

None of this makes a learned component safe. The check holds what the machine *will do*, not what was *proposed* to it: a dangerous step and a benign one pass the same check, and the component that proposed the first is not safe for having done so. And where the figure itself comes from a classifier — deciding what the system has in its gripper, or who it is dealing with — **the check is never more reliable than that classifier.**

The items below are about that picture, which they call the model of the environment: what it is made of, and what in it can be trusted. They do not require it to be produced. Where a deployment maintains a model of its environment — a site model, a digital twin, an occupancy map, or any other structured description by which the system evaluates its conditions — the following apply.

M The picture of the surroundings the machine takes its figures from

M-1 Established and inferred parts are separated	T1 M · T2 M · T3 M · SUPPLIER · BID
Where the deployment maintains a model of its environment — a site model, a digital twin, an occupancy map, or any other structured description by which the system evaluates its conditions — the supplier shall distinguish, element by element of that model, the established part — what was fixed by measurement or by record and changes rarely — from the inferred part, which the system produces itself and changes continuously. Where the system has a body, the established part includes the building geometry, the fixed obstacles and the zone boundaries. Of the established part, the supplier shall state which elements the system can itself move, given the forces and masses stated under G-1. An element recorded as fixed that the system can move is established about where it was and about nothing else.	
Acceptable: the distinction drawn element by element; and, of the established part, which elements the system can move. An answer that does not meet the item rejects the bid: the distinction asserted for the model as a whole, or not drawn at all; or every element of the established part recorded as immovable where the system lifts and carries.	

NOTE The two parts carry evidence of different standing: the inferred part is produced by the component whose behaviour is in question. A distinction asserted for the model as a whole leaves every element ambiguous, and M-3 and M-7 have nothing to attach to: M-3 evaluates containment against the established part, M-7 asks which declared parameter rests on the inferred part. A surveyed floor plan is one established part. A register the acquirer keeps, a rate card, a list of approved counterparties are others, and they carry the same standing for the same reason.

M-2 The safety problems of the deployment	T1 S · T2 M · T3 M · JOINT · BID
Before bids open, the acquirer or an independent expert the acquirer names shall draw up a list of the safety problems of this deployment — of what can go wrong on this site and among these persons. Each problem shall be marked [M], [R] or [S]. An [M] problem shall not arise, and where one occurs the deployment is not accepted. An [R] problem shall not arise repeatedly, and what is judged is how often. An [S] problem is undesirable, and what is required of it is that it be stated. These are the designations this standard uses of its own items, and they carry the same meaning of a problem. The designation of an item is set by this standard; the designation of a problem is set by the acquirer, for this deployment. Each line shall name where it came from: a task declared under Z-1, and which; a fact of the place stated under M-10, and which; or a requirement of the law of the place of use, stated by the acquirer, and which. This standard keeps no catalogue of law. A frequency the supplier states under M-11 is a disclosure, and a frequency of any magnitude	

answers this item. What bounds the tier under C6 is its absence: no frequency, no denominator, or no basis for either.

An acquirer that wants the magnitude to decide states the frequency itself, before bids open and under C1, for each [R] problem and for each population an error reaches, as M-11 names those populations. The frequency shall name what it rests on: a requirement of the law of the place of use, a rate the acquirer has measured in its own operations, or a rate published for this class of system. A frequency that names none of these bounds nothing, and neither does one stated after bids open.

The supplier shall answer every problem on the list: what condition closes it, and what that condition rests on. What an answer has to be, M-11 states.

The list is one and the same for every bid, and is issued again only where the tasks, the site or the stated limits change.

Acceptable: every safety problem stated by the acquirer or by the independent expert it named, before bids opened, marked [M], [R] or [S] and naming where it came from — and an answer from the supplier to each of them: what condition closes it and what that condition rests on. No problem on the list left unanswered.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is mandatory, an answer that does not meet the item rejects the bid: ON THE ANSWERS: a problem on the list the supplier has answered with nothing; an answer that does not name what closes the problem; or an assurance that the system meets safety requirements without saying by what. ON THE LIST: no list before bids opened; a problem marked with none of the three letters; a problem naming no source; a declared task with no problem standing behind it and no statement of why it has none; a line written by neither the acquirer nor the expert it named; or a problem added after a bid was made and scored against it. Where no list was drawn up, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6: there was nothing to answer.

NOTE What is listed is problems, not actions. A system has no bounded set of actions, and one that goes on learning acquires more; no method enumerates them, so a list of actions is incomplete by construction, and an incomplete list read as complete is worse than none. cl:physical begins at the same place – build the hazard out so that the system cannot produce it at all is a limit and not a list. Learning does not lengthen the list of problems. It changes the figures in the answers M-11 asks for. The list grows only where an interface was added rather than a skill – a path, a counterparty, a key – and that is a change to the deployment. The supplier is not asked to name the problems of its own product. Asking would be pointless: its business is to sell. The problems are derived from the tasks, the place and the law, none of which is the supplier's to write. What the system is able to do is asked of the supplier directly and under signature by Z-12, where silence is a refusal rather than an omission; and a capability the supplier marks outside the task set under Z-3 is named as not assessed rather than left unmentioned. Who draws the list up is the acquirer's to decide. This standard names the independent expert and sets no tier at which one becomes compulsory: which party is able to draw up the list for this deployment is known to the acquirer and not to the document.

M-3 Containment does not rest on inference

T1 M · T2 M · T3 M · SUPPLIER · BID

Where the deployment maintains a model of its environment, the containment invariant required by the filter clause shall be evaluated against the established part of the model and against a source independent of the learned policy that says where the system stands relative to the edge of its declared scope. Where no independent mechanism is available, the supplier shall state that, and the statement caps the tier under C6 rather than excluding the system. This item states the requirement of C-2 in the vocabulary of the environment model and adds no obligation to it: one body of evidence answers both, it is not evidenced or scored twice, and where no independent mechanism is available the ceiling C6 computes for that absence is taken once. Where the designation of the two differs at a tier, the stricter governs.

Acceptable: containment evaluated against the established part of the model and an independent source — a check implemented outside the learned policy with authority to invoke the fallback controller, credentials that reach nothing outside the declared scope, or a physical barrier; or, where no independent mechanism is available, a written statement to that effect, which caps the tier under C6.

An answer that does not meet the item rejects the bid: a boundary enforced by the same stack whose malfunction is the hazard being bounded, presented as independent; or containment resting on an inferred element of the model.

NOTE Containment that rests on inference rests on the component whose behaviour it is there to bound. Indoors an external positioning source does not always exist, which is why the statement that no independent mechanism is available counts as an answer here rather than as an omission.

M-4 Divergence between model and world is measured

T2 S · T3 R · JOINT · ACCEPTANCE

Where the deployment maintains a model of its environment, and only where it does, the supplier shall state the method by which the model's departure from the environment it describes is measured, and the acquirer shall measure, at acceptance and on the acquirer's own site, the rate and magnitude of that departure and state the figure with that method.

Acceptable: the stated method, and a measurement made under it, at acceptance and on the acquirer's own site, with its figure.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is required, an account of why it does not arise is an answer and silence is not: no measurement — this quantity bounds every conclusion drawn from a condition evaluated over the model. Where the supplier has stated the method and the acquirer has not performed the measurement, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T1.

NOTE A declared model does not remove a deployment's uncertainty about its surroundings. It relocates it: a condition evaluated against the model is evaluated against a description of the site rather than against the site, and that description can be wrong. The residual is this divergence, and a conformance claim treating a declared model as having removed it draws no support from the clause. The bound of F-8 is one of the conclusions this quantity bounds. Its declared parameters are evaluated against the model, so a step admitted because every parameter was inside its range was admitted on what the system holds about the site, and this figure is the size of the difference between that and the site. M-7 states which of those parameters rest on the inferred part and what its construction was established on; this states how far the finished model has departed from what it describes.

M-5 What the model represents about what others can perceive, reach and do

T1 R · T2 R · T3 R

· SUPPLIER · BID

The supplier shall state whether the model represents what other parties can perceive, reach and do, or only where they are and what they hold. Where it does not, the supplier shall declare that and shall name to the acquirer the class of consequence the system cannot evaluate.

Acceptable: the representable classes named — among them any act of the system that takes away what another party could otherwise perceive, reach, obtain or do; and, where the system has a body, occlusion of sight, masking of sound, obstruction of a route and occlusion of a sensor — with those not represented named as not represented.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a statement that the system has no such effects, made over a model containing nothing that could establish it.

NOTE Every prohibition in this standard is stated over what the system does. A system that stands where a person cannot be seen, that masks a warning tone, that blocks the one route to an exit, or that occludes another system's sensor breaks none of them: each of its actions is permitted, and the harm arrives through the

environment rather than through the system. Nothing about that needs a body. An agent that takes the last slot, exhausts a rate limit, locks a record another party was about to use, or fills a queue is the same case exactly: every action permitted, the other party stopped. A model holding positions but not what the positions take away cannot represent that outcome, and the filter cannot check what the model cannot express.

M-6 Whether the model predicts what others will do, and what rests on the prediction T1 R · T2 M · T3 M · SUPPLIER · BID	
The supplier shall state whether the model represents the future behaviour of persons and of other systems, or only their present state. Where it predicts, the supplier shall state which parties, over what horizon, and with what error, measured on a population that includes the cases prediction is worst at, among them a party not attending to the system, a party that cannot respond quickly, a child, and a system of a make for which the supplier holds no specification. Where the system has a body, the first two are a person not looking at the machine and a person who cannot move quickly. The supplier shall state three further facts: whether the prediction treats the other party as indifferent to the machine; whether divergence from the prediction is detected, within what time, and what the machine does on detecting it, stated separately from what it does while detecting nothing; and which conditions rest on a prediction and, for each of those conditions, which persons an error in the prediction it rests on reaches, named as one of the populations by which the deployment tiers T0, T1 and T2 are defined. A prediction is inference, so M-11 applies to it in full: no safety condition shall rest on predicting what a person will do unless the error rate is declared together with the persons an error in it reaches. Where the acquirer has stated, before bids open and under C1, the rate above which each tier is unavailable for each of those populations, and has named what that rate rests on, the declared rate bounds the tier under C6; where it has not, the declared rate is received as a disclosure and the tier is bounded under C6 as it would be without a figure.	
Acceptable: the four answered, with error measured on a population including a party not attending, a party that cannot respond quickly, a child, and a system of an unknown make, and with each condition resting on a prediction carrying the persons an error in that prediction reaches, named as one of the populations by which the deployment tiers T0, T1 and T2 are defined. Where it is required, an account of why it does not arise is an answer and silence is not; where it is mandatory, an answer that does not meet the item rejects the bid: where the system has a body, giving way only where a conflict is predicted — a failure of prediction is then a contact; an error rate measured on records in which no such system was present; or a condition resting on a prediction listed with no persons an error in that prediction reaches, which states how often without stating how bad and leaves the acquirer’s thresholds nothing to be read against; or, where the conditions resting on predictions do not all reach the same population, a single error figure offered across them, which leaves the acquirer a threshold per population and one number to read against all of them.	

NOTE A system that predicts nothing is conservative: it treats every party as capable of anything and gives way. A system that predicts confidently and is wrong proceeds into the space it had allotted to someone who did not behave as modelled — the failure of prediction is not slowness, it is a system that had a reason to keep going. A prediction that is acted on also becomes an influence: a system proceeding because it predicts the other party will stop is not forecasting that party, it is leaving them one option, and the outcome is reached through them while no prohibition over the system’s own actions is broken. What a party does next depends on what the system does, so an error rate measured where no such system was present does not transfer to a setting where one is. Two populations are asked for here and they answer different questions. The one the error is measured over is a sample: it settles whether the figure was taken on the cases prediction is worst at or on the easy ones, and one of the four instances named in it is a machine rather than a person. The one named against each condition is a tier population: it settles whom being wrong reaches. A figure taken on the right sample still states how often and not how bad, which is why the second is asked and why the first does not answer for it. A rate is also not a criterion until a ceiling is set against it, and the ceiling is the acquirer’s to set before bids open rather than this standard’s to state: where it has set none, the figure is a disclosure, which is what the provision says instead of promising a

bound the document does not supply.

M-7 Which parameters rest on inference, and the sample that inference was established on
T1 R · T2 R · T3 R · JOINT · BID

Where the deployment maintains a model of its environment, the supplier shall state, for each parameter declared under F-8, whether that parameter is evaluated against the established part of the model or against the inferred part, as the two are distinguished under M-1. For each parameter evaluated against the inferred part, the supplier shall state how that part is constructed and shall state the sample on which the construction was established: its composition by class, its size, and the performance measured on it, given per class and not for the sample as a whole. The classes are those of the acquirer's deployment, stated by the acquirer — among them, where the deployment contains them, children, a person using a wheelchair or another mobility aid, animals, vehicles and unmanned aircraft, which are instances and not the whole of any deployment's list — and where the acquirer has stated no list, the supplier shall state the list its sample was composed by and whose list it is. The supplier shall name every class of that list which the sample did not contain.

Acceptable: for each parameter declared under F-8, the part of the model it is evaluated against; and, for each parameter evaluated against the inferred part, how that part is constructed, with the sample's composition by class, its size and the performance measured per class, in the classes of the acquirer's deployment, and every class of that list the sample did not contain named as one on which nothing was measured.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a figure for the sample as a whole offered in place of the figures per class; a sample whose composition by class is not stated; the supplier's own class list offered as the deployment's; a class of the acquirer's list absent from the sample and not named as absent; or silence. An account that a limb of the item does not arise in the form asked is an answer, and it states why — the perception is a third party's component and is delivered with a whole-sample figure only, or the acquirer's list contains a class of which no sample exists — what stands in its place, the sample and per-class figures the component's vendor does hold with the conditions they were taken under, and which classes of the acquirer's list remain unmeasured, which is what the acquirer can check the account against. The acquirer evaluates the account and is free to reject it.

NOTE The parameters of F-8 are evaluated against the model, and for a machine that moves freely the parties the bound exists to protect are in the part of the model the machine builds while it works rather than in the part that was surveyed. A site has a digital contour; a crowd, vehicles, dogs, rodents and unmanned aircraft arrive during the work. Formalising the construction of that part is not possible today for systems of this class, and the present practice is sampling: the construction is established on a test sample and not by proof. A sample bounds what it contained. A class absent from the sample is not safe; it is unmeasured. A figure of 99.7 per cent on a test set that held no person in a wheelchair states nothing about a person in a wheelchair, and a composition given per class is what tells the measured from the unmeasured.

M-8 What the system detects when it is degraded, and what it then does
T1 R · T2 M · T3 M ·
SUPPLIER · ACCEPTANCE

For each way the system can be degraded, the supplier shall state what the system detects, within what time, and what it does on detecting it, stated apart from what it does while detecting nothing. On detecting a degradation the system shall slow down, attempt less, or stop. The supplier shall also state how each answer has been shown. The ways to be answered are the loss or corruption of each input the system depends on, and the loss of each component whose absence changes what the system can do. The acquirer may add others. This is asked whether or not the deployment maintains a model of its environment.

Acceptable: the inputs and the components listed. Where the deployment has them, the list includes: a feed that has stopped being refreshed; a service answering with nonsense; a model or a service replaced by another version underneath the system; a delay risen past what the work assumes; and the link lost. Where the system has a body the list also includes: a camera smeared or blocked; a sensor lost; a wheel or a leg lost; the positioning input lost; and the lighting fallen away. For each way, what is detected, within what time, and what the system then does, stated apart from what it does while detecting nothing, with what it does being to slow down, to attempt less or to stop. For a way that cannot happen to this system, that stated with the reason, and nothing further is owed for that way. For a way that happens and does not degrade the system — a second sensor covers it, say — that stated with the reason, and with whether the system detects it and what it does about it; here the system may carry on, provided the fault is recorded and the acquirer is told. For each answer, how it was shown, in one of the forms R-3 admits for a showing, which form the showing took and what that showing did not reproduce of this deployment. The acquirer determines whether a showing is sufficient. Where it does not accept one, the supplier induces the degradations it names on the delivered system, on the acquirer's site, and what the system did is recorded. Where the loss of the link is answered under D3.3, that answer serves here and is not asked a second time.

Where it is required, an account of why it does not arise is an answer and silence is not; where it is mandatory, an answer that does not meet the item rejects the bid: “the system operates normally” offered as the answer, which gives one behaviour where two were asked and does not say which of the two it describes; a way of being degraded that the system does not detect at all; a degradation detected and nothing done about it — the same behaviour before and after, with no statement that this way does not degrade the system and why; a way answered as not degrading the system with nothing said about whether the system detects it, which answers what the system survives and not what it knows; or a showing offered with its form, or with what it did not reproduce of this deployment, left unstated, which gives the acquirer nothing to judge it by.

NOTE A system that does not know its information has gone bad is more dangerous than one that stops. It has the same reason to keep going that it had a moment before, and it is now wrong about the thing the reason rested on. A machine that has gone blind is one instance. A system reading a price feed that stopped being refreshed an hour ago is another, and it is the common one where nothing has a body. That is why what it does on detecting a degradation is asked apart from what it does the rest of the time: the two are the same sentence in most bids, and the sentence describes the good case. M-2 does not answer this question and cannot. Its figure is taken while the input is working, and it says how often a working input is wrong; a stale feed is not an input with a figure against it, it is an input that is not reporting. A way of being degraded that something else covers is still answered, because not being affected is not the same as noticing, and the thing that covered the fault can fail next.

M-9 The edge holds when the input that establishes it is wrong ACCEPTANCE

T1 M · T2 M · T3 M · SUPPLIER ·

At acceptance, on the delivered system, the supplier shall degrade the inputs by which the system establishes where it stands relative to the edge of its declared scope, in the ways the acquirer names. The system shall stay inside the scope declared under C-1 throughout. The demonstration shall be made at the points of that edge the acquirer selects. Where the acquirer names no ways, the supplier shall choose them and shall state what it chose. The same applies where the acquirer selects no points. This is asked whether or not the deployment maintains a model of its environment.

Acceptable: the demonstration performed on the delivered system, in each way named and at each point of the edge named, with the system inside the declared scope throughout, and with the ways and the points of the edge stated where the supplier chose them. What is shown here is that the edge does not move with the inputs. This is not M-3, which states what containment is evaluated against before anything is switched on; it is not C-4, which exercises the system at the edge with its inputs working; and it is not C-3, which states what the system does on losing the input. What the system does inside the scope — stopping, turning back, or carrying on — is not prescribed here.

An answer that does not meet the item rejects the bid: the edge shown only with the inputs working, which is the demonstration of C-4 and not this one; a statement that the system stays inside its scope offered

in place of the demonstration; a demonstration made away from the edge, where the system could not have left the scope whatever it did; or the system outside the scope in any way named. Where the acquirer has not declared the scope, the demonstration is made against the scope stated in its place by the account C-1 requires; and where neither a declared scope nor such an account gives a scope the demonstration can be made against, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE A system that reaches outside what it was bought for, because it lost track of where it stood, has broken nothing an acquirer can see in a document. C-2 names the mechanism that keeps it inside and M-3 says the same thing in the vocabulary of the model; both are answered on paper, before anything is switched on. C-4 shows the edge holding while the inputs work. What is left over is the case the edge exists for: the system is wrong about where it stands. The scope is the acquirer's liability whatever the system believes about it, which is why this is asked at every tier. The demonstration is made at the edge because a system degraded in the middle of its scope and stopped there shows nothing about the edge. The test needs nothing from inside the system. A covered sensor, a withheld positioning signal, a stale directory, a revoked lookup are all applied from outside, and where the system ends up is visible to the acquirer.

M-10 The acquirer states what its own place does

T1 R · T2 R · T3 R · ACQUIRER · BID

The acquirer shall state the facts of the place declared under C-1 that bear on the answers to this standard and that the supplier can neither survey nor infer: who is present there and at what times, including persons who are not trained for the system; what else operates in the same space, whether people, machines or vehicles under another party's control; what regularly changes the place — deliveries, cleaning, events, works — how often, and which persons each change brings into the place or takes out of it; what the place does in an emergency and what the system is expected to do while it does it; and what the acquirer does not undertake to keep as it is. Where one of these does not arise, saying so is an answer to it.

Acceptable: each of the five stated for the declared place, or stated not to arise, in the acquirer's own words and before bids open.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a site description offered in place of the facts that bear on the answers; presence given as a maximum with no time at which it holds; other parties' machines omitted where the place is shared; or an undertaking that nothing will change, which is a promise rather than a fact and is the one thing this item may not be answered with.

NOTE The nine items above are the supplier's model of the environment. This one is what the model is a model OF, from the party that owns it. A supplier surveys what is there on the day it surveys; it cannot survey Tuesday's delivery, the contractor arriving in March, or the fire drill.

It bears on the tier before it bears on anything else. Clause 4.2 is answered over the persons the deployment affects, and who those persons are is a fact about the place and its use, not about the machine. M-1 separates what was measured from what was inferred; this item is where the acquirer says which of its own facts a measurement would have missed.

Nothing here obliges the acquirer to hold the place still. The last limb asks the opposite — what it does not undertake to keep as it is — because a deployment assessed against a place its owner intends to change has been assessed against a place that will not exist, and the parties are better served knowing that at the bid than at the incident.

M-11 How each problem is closed

T1 S · T2 M · T3 M · JOINT · ACCEPTANCE

For every problem on the list drawn up under M-2, the supplier shall state the condition that closes it and what that condition rests on. A problem is closed in the way its designation requires: an [M] problem by construction, an [R] problem by measurement, an [S] problem by being stated.

An [M] problem shall be closed by the construction of the deployment and not by the absence of occurrences in trials: by a barrier, an interlock or a protective layer independent of what it

constrains. The supplier shall state what closes it and why that cannot be violated. Where such a problem occurs at acceptance, the deployment is not accepted.

An [S] problem is closed by being stated. The supplier shall state that the problem is possible and under what circumstances; no measurement, no barrier and no evidence are required of it, and what the acquirer does with the statement is the acquirer's decision under U-4.

An [R] problem shall be closed by measurement. Where the deployment maintains a model of its environment, the condition shall be evaluated over the established part of that model. Where it cannot be evaluated on the established part alone, the supplier shall declare that dependence and shall state, for each quantity the condition reads from the inferred part: the error rate of that quantity — how often the system's reading of it turns out not to match the site; the conditions and the sample that rate was measured on; the number of comparisons it is counted over and the period they were made in; the deployment it was measured on and what differed there from the acquirer's own; the protocol by which it is measured again; and which persons an error in that quantity reaches, named as one of the populations by which the deployment tiers T0, T1 and T2 are defined — and at T3 named of the persons the event reaches, rather than of those present when nothing goes wrong.

The quantities are stated by kind and not by occurrence: not a person seen at a given moment, but the presence of a person within the stopping distance. The supplier may state, for one quantity, a rate from each deployment it measured that quantity on. The acquirer determines, for each quantity, which of those rates carries to its own operating conditions; where none does, the acquirer measures the rate for that quantity on its own site and under its own operating conditions, to the same protocol.

The acquirer, or the expert it named under M-2, shall record for each problem whether what was stated closes it. A problem answered as this item requires and still not closed does not lower a score; it bounds the tier under C6.

Acceptable: for each [M] problem, what closes it and why that cannot be violated, no occurrence of it at acceptance, and the acquirer's record that it is closed; for each [S] problem, the statement that it is possible and under what circumstances; and for each [R] problem whose condition is evaluated over the inferred part, for each quantity it reads: the rate, the conditions and sample it was measured on, the number of comparisons and the period, the deployment it was measured on and what differed there, the protocol for measuring it again, and the persons an error in that quantity reaches. For each quantity the rate is one the acquirer has determined carries to its own operating conditions, or, where none does, one the acquirer has measured on its own site.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is mandatory, an answer that does not meet the item rejects the bid: a problem on the list answered with nothing; an [M] problem offered as closed by the absence of occurrences in trials rather than by construction; a protective layer that depends on what it constrains; an occurrence of an [M] problem at acceptance; an [S] problem for which evidence is demanded, or one offered as closed by anything other than having been stated; an [R] problem resting on the inferred part with no rate stated; a rate offered without the number of comparisons it was counted over; a rate offered without the deployment it was measured on and what differed there from the acquirer's own; one rate offered across quantities whose errors reach different populations — an error that reaches a trained operator and an error that reaches a child are two questions, and one figure answers neither of them; or a model whose safety-relevant elements are maintained solely by the system's own perception, which places the evidence downstream of the component in question and returns true precisely when the perception is wrong. Where the supplier has declared the dependence and stated its rates, and the acquirer has neither determined that a stated rate carries nor performed the measurement itself, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE The absence of an occurrence is the weakest evidence there is. An [M] problem has to be closed before anything has happened, and not after nothing has. A rate stated without the number of comparisons it was counted over cannot be read. Zero errors in three trials and zero in three thousand are the same figure, and only

the count distinguishes them. Were evidence required of an [S] problem, it would differ from an [R] problem in name only, and the acquirer would face a third level of stringency it has not asked for. **There are no points here, and that is deliberate.** A score permits an exchange, and the person an unclosed problem reaches is not helped by an average.

A declared model does not remove a deployment's uncertainty about its surroundings. It relocates it: a condition evaluated against the model is evaluated against a description of the site rather than against the site, so what the check establishes is bounded by the distance between the two. The residual is then the divergence of **M-4**, and a conformance claim that treats a model as having removed it is not supported by this clause.

5.4 Prohibitions declared in service, and their honest guarantee

The acquirer may declare prohibitions once the system is in service — that it shall not go above a stated figure, that it shall not act on a thing or a party of a stated class. No item of this standard requires that a system provide an interface for declaring them; what is required is that the supplier state whether such prohibitions can be declared at all and, for each one that can, the path by which it is enforced. **Clause 5.5** states which items carry this subclause and what they ask.

The guarantee that comes back must be stated precisely, because the two halves of such a prohibition have very different standing.

- **The predicate is formalisable, and easily.** “Nothing above this figure” is a numeric condition: the value is stated and what the system measures is compared with what was declared — a contact force at a named body region, an amount, a rate. “Do not act on anything of the declared class” is a trivial condition once class membership is available.
- **The grounding is not.** Whether the object in front of the system *is* of that class is decided by a learned component. Nothing guarantees that decision is right. That is true of every prohibition of this kind.

The supplier therefore states the prohibition as enforced *conditional on the grounding*, and declares the error rate of that grounding. That declaration is split, because measuring on the acquirer's own site before award is not possible in a normal tender timetable: before award, the supplier states the error rate it holds, the conditions and sample on which it was measured, and the protocol it will use to re-measure on site; after award, the on-site measurement is an acceptance gate with a stated deadline and a rejection right. The claim the acquirer is entitled to is not “the system will not grasp a knife” but “the system will not grasp what it classifies as a knife, and the classifier's measured error rate on your site is this figure”. A supplier offering the first formulation is offering a guarantee it cannot hold.

5.5 What is operative in the prohibitions subclause

Clause 5.4 states no numbered requirement. The items that carry its ground are **Z-4** and **Z-5**, and they are what an assessment addresses under **Clause 21**.

Z-4 requires the supplier to state *whether* prohibitions can be declared in service and, for each prohibition that can be declared, the path by which it is enforced; a system that permits no such declaration answers **Z-4** by saying so. No acceptance item of Annex A requires that a declaration interface exist. The text this standard was assembled from asserted in prose that the standard requires one, with no item behind it; that assertion is not carried into **Clause 5.4**, because the assessment addresses the acceptance items of Annex A and a sentence with no item behind it was never something an assessor could ask for. Whether to add a requirement that such an interface exist is a change to what the standard requires, and it is not made here.

Z-5 carries the second half of **Clause 5.4** — the measured error rate of the grounding, stated before award and measured again on the acquirer's own site — and asks for it at the two moments described there.

6 Who answers when it goes wrong, and who was entitled to accept the risk

Four things are asked below. Under what law the machine works here, shown separately from the rest (B-0). Who answers for what, agreed and signed before the system enters service (B-1). The kinds of harm, and who answers for each (B-2). And what cover is stated, together with the exclusions, read before a claim is made rather than after (B-3).

The operating party of a system may accept residual risk within the area for which it answers. An occupier who understands the limitations of a system and admits it to premises under its control bears the consequence there, and is entitled to weigh it.

That entitlement has a boundary. **An operating party cannot accept risk on behalf of persons who have not consented and who are not its own.** A shopping centre is not a private laboratory: its visitors are the untrained, non-consenting persons that T1 and T2 are about. The occupier's liability determines *who pays*; it does not lower the tier, and it does not license exposing third parties to unassessed risk.

Accordingly, and this is the rule on which [Clause 5](#) depends:

The acquirer sets the rule of application for the person-in-the-loop tasks, within its own liability zone, and only where the residual risk is not carried outside that zone.

That rule says who may accept a risk. It does not say who answers when the risk arrives, and a standard that raises the question and leaves it open has done half a job.

Those four things are asked of four parties: the *supplier* that sells the system, the *integrator* that fits it to this site, the *operating party* that runs it day to day, and the *acquirer* that buys it and answers for the place. [Clause 3](#) defines each, and a party that does not exist in a deployment is written in as absent.

First, under what law the machine may work here at all (B-0). The acquirer names it, the supplier shows conformity to it with its own separate paper, and conformity to this standard is not that paper and may not be offered as it. It stands first because everything below divides responsibility inside a frame that has to exist. **Then, who answers for what (B-1):** intended in the tender documents and answered by the bidder there, signed by everyone before the machine works. **Then, for which cases exactly (B-2):** four cases that no ordinary contract settles, each named with the party that answers. **And last, with what (B-3):** what each party is actually insured for, and whether the policy excludes the three things this class of machine does.

None of the four is asked after an accident. All four are asked while the acquirer can still decide differently, which is the only time any of them is worth asking.

Where the acquirer does not produce the statement. B-1 obliges the acquirer to hold a written allocation, signed by the parties to it, before the system enters service, and relieves a supplier that has stated in writing what it answers for where the acquirer has produced nothing for signature: the item is then recorded as not asked and is not scored against the supplier. The consequence of taking that relief is the acquirer's own and is stated here rather than left to be found. The deployment proceeds with no allocation agreed in advance, and B-1 is mandatory at all four tiers, so the ceiling [Clause 21](#) computes for it under [C6](#) is no ceiling: nothing in this standard bounds the deployment by reason of the omission. An acquirer in that position has the deployment it would have had, without the one record this standard reaches that is written while nothing has gone wrong.

B Liability and the limit of risk acceptance

B-0 Which law lets this machine work here, and separate evidence that it does
 T0 M · T1 M · T2 M · T3 M · JOINT · BID

The acquirer shall name the product-safety regime, in the sense [Clause 3](#) defines it, under which the deployment operates: the law that governs whether a machine of this kind may lawfully be placed on the market and put to work where this deployment is. The supplier shall produce evidence of conformity to *that* law, as a separate document. Conformity to this standard is not such evidence and does not stand in for it.

Acceptable: the law named by the acquirer, and evidence of conformity to it from the supplier that is evidence of conformity to that law and not to this standard.

An answer that does not meet the item rejects the bid: conformity to this standard offered in place of conformity to the law named; evidence of conformity to a different jurisdiction's law offered without saying so. Where the acquirer has not named a law, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T0.

NOTE **What this asks for, in the words a buyer uses.** A machine of this kind works in your building only where somebody has already shown that it meets the country's law on machinery safety, and marked it accordingly: the CE mark under the machinery law of the European Union, UKCA in the United Kingdom, the EAC mark under TR CU 010/2011 in the Eurasian Economic Union, ECAS in the United Arab Emirates. Which of them applies is the acquirer's to say, because it is the acquirer's site and the acquirer's country. **Why it stands first, and why it is here at all.** This standard is not law and opens no market, which [Clause 2](#) states in terms. A supplier that offers conformity to it *instead of* the mark the law requires has moved a legal exposure onto the acquirer quietly and before anybody looks: the machine is operated unlawfully, and the acquirer learns it from an inspector or from an accident. Both bills are the acquirer's. Until the law is named, everything the rest of this clause allocates is allocated inside a frame whose existence nobody has checked. **And no jurisdiction is written into this text.** It cannot be: the law differs between the places a system of this class is sold, it changes, and every requirement here is written to be answerable by a supplier in any country. What is asked is that the law be named rather than assumed, because a tender otherwise closes with it unstated and each party supposing the other had it in hand.

B-1 Who answers for what

T0 M · T1 M · T2 M · T3 M · JOINT · BID

Two things are asked, at two moments. **With the tender**, the acquirer shall put into the tender documents the allocation it intends — who is to answer for what among supplier, integrator, operating party and acquirer, in the sense [Clause 3](#) defines each — and the supplier shall state in writing what it will answer for and what it will not. Where a party does not exist in this deployment, it is written in as absent, and that is an answer. **Before the system enters service**, the acquirer shall hold that allocation as a written statement signed by the parties to it.

Acceptable: the intended allocation in the tender documents and the supplier's written statement of what it will and will not answer for, and the signed statement held before the system enters service; or, where the acquirer has put nothing in the tender and produced nothing for signature, the supplier's own written statement alone, which is the answer the assessment records in that case and is what the relief below turns on.

An answer that does not meet the item rejects the bid: an assurance that the question is covered by the general terms, without the terms; or a statement produced after an incident. Where the supplier has stated in writing what it answers for and the acquirer has not produced a statement for signature, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T0.

NOTE Why it is asked twice. At the tender there can be no statement signed by four parties: the integrator and the operating party are often not yet chosen. What can exist then is the allocation the acquirer intends, put into the tender pack as the terms of the contract are, and the supplier's written answer to it, which is what a bidder is compared on. A model statement is published with this edition, free and under its licence: the deployment and its tier, the four parties, every kind of harm [B-2](#) names, the cover and the exclusions [B-3](#) asks for, and the law of

B-0, with lines to sign. It is a model and the parties adapt it with their own advisers; allocation follows from the law of the deploying jurisdiction and from the contract, and the model says so on itself. What this clause reaches is the moment of writing: the parties set their own understanding down while nothing has gone wrong, which is the only moment at which the statement is a record rather than an argument. Where the acquirer produces no statement for signature, the deployment proceeds with no allocation agreed in advance, and the deployment is held to T0 – the ceiling the failing limb states in words because C6, on an item mandatory at every tier, computes none. That is the acquirer’s own act, and the party it leaves without an allocation after an injury is the one the statement exists for.

B-2 The kinds of harm, and who answers for each		T1 R · T2 R · T3 R · JOINT · BID
The allocation of B-1 shall address four cases by name, each with the party that answers for it and on what terms: harm following an update the supplier issued and the acquirer accepted; harm following a decision taken by a model or an agent reached over a link, including where that party is controlled by neither supplier nor acquirer; harm following an action the filter admitted; and harm in which more than one system commanded by one principal participated. A case the parties hold cannot arise in this deployment is named together with what makes it so.		
Acceptable: each of the four named, with the party that answers and the terms; or named with what makes it unable to arise here. An account of why it does not arise is an answer, and silence is not. Unacceptable: a general apportionment silent on all four; some of the four named and the others passed over; or the rest referred to the general terms instead of being named. Where B-1 is recorded as not asked because the acquirer produced nothing, this item is recorded as not asked on the same ground, is not scored against the supplier and bounds no tier: there is no allocation for it to address.		

NOTE **Why these four and not others.** None of them is "the supplier delivered a bad thing", which every ordinary contract already covers. The update was accepted by both. The decision was taken by a party neither of them commands. The action was passed by a filter working as designed. The harm was done by several machines, each within its own limits. "The supplier answers for defects and the acquirer for operation" answers none of the four, and that is found out after the event, when the cost of arguing falls on whichever party holds the least evidence.

B-3 Cover is stated, and its exclusions are read before the claim T1 S · T2 S · T3 S · JOINT · BID

The supplier shall state what insurance it carries *for this deployment*, and the acquirer shall state what it carries. Both shall read their policies against three things a system of this class does, and shall state for each whether it is excluded and the words of the policy the answer rests on: **operation without a person deciding; control by a learned component; and operation among persons who are not employees.**

Acceptable: the cover each party carries for this deployment, and the three, each answered excluded or not with the wording relied on.

An unsatisfactory answer loses the points of that item and the bid stands: a certificate of insurance with no reading of its exclusions against this class of system; cover stated for the organisation rather than for this deployment; or an undertaking to read the exclusions when a claim arises.

NOTE B-2 says who answers. This says *with what*. An ordinary general-liability policy carves out those three, and they are exactly what such a machine is bought to do. A party that took a case under B-2 and learns at the claim that its policy excludes it has not performed the allocation — it signed one. Reading them at acceptance costs an hour and moves the discovery to the only point at which either party can still act on it.

7 Where the system may be, and what it may do there

An operating party accepts residual risk for the area it answers for (Clause 6), and that acceptance covers only what happens inside it. Where the system can leave it, the acceptance stops covering the ground the system covers: the operating party has weighed a risk to its own people and the machine is among somebody else's, who agreed to nothing. Containment is asked for here in its own right, and not as a consequence of anything below it.

There are two boundaries, and this clause asks about both. One is a boundary in *reach*: where the system may be and what it may touch — the systems, the accounts, the data, the counterparties, and, where it has a body, the place. The other is a boundary in *action*: what the system may do inside that reach, and what it is able to do beyond what it is allowed. Neither follows from the other. A machine can be inside its place and doing something nobody admitted; it can be doing only admitted things and be somewhere nobody meant it to be. The requirements below are in two groups for that reason.

The acquirer draws both (C-1), because the place and the counterparties are the acquirer's. It records the declaration in the contract, where it binds, and reproduces it in the operating party's documentation, where the person at the machine reads it: a scope that lives only as a setting inside the machine is a scope that whoever can change settings can change.

Four items then ask whether the boundary in reach is real. C-2 asks what enforces it, and requires that the enforcement not rest on the learned policy — a machine held inside a line by the same judgement that might cross it is not contained. C-3 asks what happens at the edge, and at the loss of the input by which the machine knows where the edge is. C-4 has the acquirer walk that edge on the delivered machine. C-5 is not C-2 asked again: C-2 asks whether an enforcement exists and of what kind, at bid, and C-5 asks, at acceptance and as a measured quantity, *where the line the delivered machine actually draws falls* against the liability zone the acquirer recorded — the margin between them, and who stands in it. What the machine writes down at that boundary is not asked in this clause: L-1 carries every approach to the boundary, every breach of it and every occasion the enforcement acts among the events the record holds, and what the record is and what it must survive are stated once, in Clause 10.

Three then ask what the system can do. C-6 is the set of actions this deployment admits and the limit on each. C-7 is everything else the machine can do, what stops each of those here, and whom the machine is able to reach — asked of what the machine is able to do and not of what the tasks call

for, which is what separates it from C-6 rather than repeating it. C-8 asks whether the units divide into groups that do not reach one another, which is the answer that tells two otherwise identical fleets apart.

C Containment

C-1 What the system may reach, and where it may be T0 R · T1 R · T2 R · T3 R · ACQUIRER · BID

The acquirer shall declare what the system is confined to. What is declared is the systems, the accounts, the data and the counterparties the system may reach, and, where the system acts in a place, that place; where the system has a body, the place is declared as the liability zone. The declaration is then put in two places, and each of the two is for something the other does not do: it is **recorded in the contract**, where it binds the parties, and **reproduced in the operating party's documentation**, where the person standing at the machine reads it. A scope that lives only as a setting inside the machine binds nobody and is read by nobody, and whoever can change settings can change it.

Acceptable: a declared scope, in the terms above, recorded in the contract and reproduced in the operating party's documentation.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a scope expressed only as a setting inside the system; or silence. Where the acquirer has not declared the scope, has not recorded it in the contract, or has not reproduced it in the operating party's documentation, an account is the answer, and it states which of the three acts was not performed, the scope the bid assumes in its place and what enforces that assumed scope, so that the acquirer can check the assumption against the deployment it is buying for. The acquirer evaluates the account and is free to reject it.

NOTE What the system is confined to settles who answers for the parties it can affect and who is entitled to accept residual risk, which is why it is the acquirer's to draw and not the supplier's. A system with no body does not leave through a doorway. It reaches into another system, another account, another body of data, and the scope is the list of the ones it is confined to.

C-2 What keeps the system inside the declared scope, and what it may not depend on T0 S · T1 S · T2 M · T3 M · SUPPLIER · BID

The supplier shall name the mechanism that keeps the system inside the scope declared under C-1. That mechanism shall not depend on the learned policy, and shall not depend solely on components that the same failure would disable. Where the mechanism is a physical barrier or a property of the machine, the supplier shall state the capability whose absence makes it one, and shall state that capability against what the system can reach and move rather than against the system alone. **An enforcement need not be a barrier.** Where nothing physical bounds the machine — a deployment in the open is the ordinary case — what is named is whatever draws the line from outside the learned policy: a geofence evaluated outside that policy and holding authority to invoke the fallback controller; a bound on speed, torque or force set in the drive electronics; credentials that reach nothing outside the declared scope. What is refused is a rule the system is asked to follow, because the thing asked to follow it is the thing being bounded. **And where there is no independent mechanism at all, saying so is an answer.** The supplier states that, and the statement caps the tier under C6 rather than excluding the system: this item is mandatory above T1, and what it is mandatory about is the answer, not the mechanism.

Acceptable: a named enforcement mechanism — a check implemented outside the learned policy with authority to invoke the fallback controller; credentials that reach nothing outside the declared scope, held where the policy cannot alter them; a physical barrier or a hardware interlock — with, for a barrier or a property of the machine, the capability whose absence makes it one, stated against what the system can

reach and move — or, where no independent mechanism is available, a written statement to that effect, which caps the tier under C6 rather than excluding the system.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is mandatory, an answer that does not meet the item rejects the bid: a scope enforced by the same stack whose malfunction is the hazard being bounded, presented as independent; or a setting inside the planner, or a rule the system is asked to follow, offered as the enforcement mechanism; or a barrier offered without the capability it assumes absent.

NOTE A containment mechanism that shares its failure with the thing it contains returns a guarantee precisely when the guarantee is not needed. Indoors there is often no external positioning source at all, and for a system with no body there is often no party but the system itself holding its own credentials. That is the condition the recorded statement exists for: the absence is a fact about the deployment as much as about the system, and it bounds the deployment rather than the supplier.

C-3 Behaviour at the edge of the scope

T1 M · T2 M · T3 M · SUPPLIER · BID

On reaching the edge of the scope declared under C-1, or on losing the input by which it establishes where it stands relative to that edge, the system shall enter its declared fallback state. It shall not carry on on its last good information.

Acceptable: entry to the declared fallback state in both cases.

An answer that does not meet the item rejects the bid: carrying on on the last good information; or an answer that treats the loss of that input as a routing problem rather than a containment event.

NOTE The two triggers have one answer because they are one situation: a system that has lost the input establishing where it stands relative to the edge cannot establish that it is inside it, and is in the same position as a system that has arrived at it.

C-4 The limit is exercised at acceptance, at the edge the acquirer picks · ACCEPTANCE

T1 M · T2 M · T3 M · JOINT

Containment shall be demonstrated at acceptance: the acquirer shall exercise the delivered system at the edge of its declared scope, in the delivered configuration, at the points of that edge the acquirer selects, and shall observe what the system does. The edge is exercised with the movable elements of the site in place, as the site will be worked, and not on a cleared edge.

Acceptable: the demonstration, on the delivered configuration, repeated at the points of the edge the acquirer selects, with the movable elements M-1 records present at those points.

An answer that does not meet the item rejects the bid: a declared limit never tested against — a statement of intent rather than a property; or a demonstration at an edge cleared of the elements M-1 records as movable. Where the supplier has presented the delivered system for the demonstration and the acquirer has not performed it, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE A cleared edge is a different edge: what the machine cannot do alone it does with what is lying beside it, and the barrier that holds against the machine is not the barrier that holds against the machine and the yard. This demonstration is of the configuration accepted on the day it is performed, and U-1 states how often a system that changes itself departs from that configuration.

C-5 The boundary against the zone

T1 S · T2 M · T3 M · SUPPLIER · ACCEPTANCE

The supplier shall state, at acceptance and for the delivered configuration, how the containment boundary set in the system stands against the liability zone the acquirer recorded under C-1. What is stated is the two of them in one frame, by the method that brought them into that frame and with the error of that method; the margin between them, given as a distance where the system has a body and as the entries that the zone holds and the boundary does not where it has none; which persons are present in that margin or reachable through it; and, where the system can select more than one set of limits, this for every set it can select and not for the set exercised under C-4 alone. Where the correspondence cannot be established, the supplier shall state that it cannot, shall state what makes it unestablishable, and shall state what stands in its place.

Acceptable: the boundary and the zone in one frame, with the method that brought them into it and the error of that method; a margin given as a quantity; the persons in that margin named; every set of limits the system can select covered; or a declared inability, with what makes it unestablishable and what stands in its place.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is mandatory, an answer that does not meet the item rejects the bid: a claim that the boundary lies inside the zone, with nothing a reader can check it against; a margin called adequate, ample or conservative rather than given as a quantity; a correspondence stated for the set of limits exercised under C-4 and for no other set the system can select. Where the acquirer has not recorded a zone under C-1, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE C-4 is not evidence about this. It exercises the edge the system actually has, at the points the acquirer selects, and observes what the system does there; it does not ask whether that edge is where the contract put it, and a system passes it at every selected point with its boundary drawn around the wrong room. The two objects are stated in different frames. The zone is recorded in the contract, as a place a person walks to. The boundary is a number inside the system, in the frame the system computes in: the base frame of a machine that is bolted down, or the frame of a map the machine built for itself. What joins the two is a survey or an alignment, and that join is what this item asks for. It is also where they come apart, because a map a machine built has its origin wherever the machine stood when it started, and the alignment of that map to the building is done by hand. The correspondence is not always establishable, and that is why a declared inability is an answer here rather than a refusal to answer. A contract that names a place — a ward, a yard, the customer's premises — and gives no coordinates holds nothing a transform is computed from. A machine that limits its axes rather than its position bounds a region computed from those limits together with the tool and the load, and that region is neither a polygon nor something read off the configuration. A deployment moved after acceptance leaves a correspondence that was true of somewhere else. In each of those the answer is an account of what was done instead, and the account is what this item asks for.

C-6 The actions this deployment admits, and the limit on each

T0 M · T1 M · T2 M · T3 M · SUPPLIER

· BID

The supplier shall state the system's action envelope for this deployment, which Clause 3 defines as the actions the system may perform and the limit on each. Where an action is physical, the limit is physical: the speed, the force, the reach, the workspace and the payload it is performed within. Where an action is not physical, it is an operation on the systems, the accounts, the data or the counterparties declared under C-1 — what the system may write, send, spend, sign, order, publish or delete — and the limit is the bound on that operation. A system that performs both kinds is stated in both. Where the deployment puts more than one unit on the site, the actions and the limit on each are stated per unit; where several units are of one type, one statement for that type is a complete answer for them, provided it names the units it covers. The supplier shall state whether the set so declared admits a solution that moves the machine or brings any part of it into contact; where it admits none, saying so is a complete answer to that part. Formalisation is asked of neither

party: what is asked is the bound on what the system may do, not the criterion by which a task is solved.

Acceptable: the actions, each with its limit in the quantity that action is bounded in — a speed, a force, a reach, a workspace or a payload where the action is physical, and the bound on the operation where it is not — and the statement of whether the set admits motion or contact. Where it admits none, that statement with the actions that were considered, which is a complete answer. Where there is more than one unit, each statement identified to the units it is made for, with no unit left unnamed.

An answer that does not meet the item rejects the bid: a description of what the system is for, or the tasks it is bought for, offered in place of the actions it may perform; a set with no limit stated on a member of it; one set of actions offered for a deployment whose units differ in what they can do, which hides the widest unit behind the narrowest; a statement made for a type that does not say which units are of it; or silence on whether the set admits motion or contact, which leaves the acquirer unable to determine which requirements attach to the deployment at all.

NOTE Clause 17.1 attaches G-5 and W-1 to Q-4 where this set admits a solution that moves the machine or brings any part of it into contact, so what is stated here decides which requirements of those clauses are asked. Five requirements refer to the declared action envelope — Q-1, D6.2, P-1, P-3 and U-3 — and each of them presupposes it. The limit is the supplier's own figure and this standard sets none: it is stated so that the acquirer knows what the deployment was assessed against, which is what Clause 3 defines the action envelope as. It is stated per unit for the same reason it is stated at all: a deployment whose units are not alike has no single set of actions, and one set offered for all of them is either wider than the narrowest unit or narrower than the widest. C-8 is answered from this item and from C-7, and neither can be checked against a set declared for everything at once.

C-7 What the system can do beyond what the deployment admits SUPPLIER · BID

T0 M · T1 M · T2 M · T3 M ·

The supplier shall state which actions the system is capable of that the set declared under C-6 does not admit, and for each, what prevents the system performing it in this deployment. Where what prevents it is a setting, the supplier shall state which roles under P-1 can change that setting. Where the deployment puts more than one unit on the site, this is answered per unit on the footing C-6 sets: what one unit is capable of is not made smaller by what another cannot do. Where the system is capable of exactly the declared set, saying so is a complete answer. An action the system can bring about by directing a person, or by being fitted with something in the set declared under G-4, is an action the system is capable of. The supplier shall also state *whom* the system is able to reach. That population is taken as C-8 takes it: over the places the units are able to be and not the places they are scheduled to be, and over the actions declared under C-6 together with those declared here whose prevention is a setting a role under P-1 can change. It is stated of what the system is able to do, and not of what the tasks declared under Z-1 call for. For the answer as a whole the supplier shall state what it rests on: design analysis, testing, or observation of this system or of others of the same build in service. Where it rests on none of the three, the supplier shall say so, and that statement is the answer.

Acceptable: the actions outside the declared set named, each with what prevents it and, where that is a setting, the roles that can change it, or a statement that the system is capable of exactly the declared set; and, in either case, the persons the system is able to reach, taken as C-8 takes it, and what the whole answer rests on — design analysis, testing, observation in service, or a statement that it rests on none of them.

An answer that does not meet the item rejects the bid: a capability the acquirer was shown under Z-3 and that appears in neither set; an action stated as prevented by a policy, an instruction or a setting inside the planner; a difference answered for the deployment as a whole where its units are not alike, so that what one unit can do stands behind what the others cannot; or what prevents an action left unstated, which is the

difference between an action the system will not take and one it has not been asked to take; or a population given as the persons the declared tasks bring the system near, where the units are able to be elsewhere or to act outside the declared set; or a capability statement offered with nothing said about what it rests on, which is not distinguishable from an assumption and cannot be checked against anything.

NOTE The basis is asked with the statement and not in an item of its own, because a claim and the ground it stands on drift apart the moment they are answered in two places. "The system is capable of exactly the declared set" resting on design analysis and the same words resting on nothing are not the same answer, and until the basis was asked they were indistinguishable on the page. Saying it rests on nothing is a permitted answer and is not scored against the supplier here: what the acquirer does with a capability bound that rests on nothing is the acquirer's to decide, and it can only decide it if it is told. What the supplier has put in front of the acquirer is Z-3's subject, and what it has observed the system doing that it did not intend is D4.4's; between those two and this item the known capability of the system is on the page. A population taken over where the units are scheduled to be is a statement about a rota, and a rota is not a property of the machine. Asked here because the tier turns on persons and every other answer of the supplier's is about actions, channels and extents; without this the step from an extent of forty metres to the people at forty metres was left to the acquirer, who answered the ladder before it had the figure. The difference between what a system can do and what it is being bought to do is the part of it nobody assessed, and it is exercised by an ordinary act: an update, a task the acquirer adds later, or a person who does what the system asked. This item is what makes that set exist to be compared against. Nothing here forbids a capability: what is asked is that it be stated and that what holds it back be named, so that an acquirer accepting the residual accepts it knowingly. C-2 is the same construction one level down — a declared scope, and the mechanism that keeps the system inside it. Per unit because capability does not average: a fleet in which one unit can climb a step is a fleet that can climb a step, and an answer given for the fleet reports the ordinary unit and loses the exceptional one, which is the only one the question was asked about.

C-8 Whether the units divide by whom they reach

T1 S · T2 M · T3 M · SUPPLIER · BID

The supplier shall state whether the units of the deployment divide into two or more groups such that no person reached by the units of one group is reached by the units of another; and where they do, which units belong to each group, whom each group reaches, and for each pair of groups what prevents a unit of one reaching a person of the other. Whom a group reaches is taken over the places its units are able to be, and not the places they are scheduled to be, and over the actions declared under C-6 together with those declared under C-7 whose prevention is a setting a role under P-1 can change. Where the units do not so divide, saying so is a complete answer.

Acceptable: the groups given unit by unit; whom each group reaches; and for each pair of groups, what prevents a unit of one reaching a person of the other, named as something no role under P-1 can change — or a statement that the units do not divide.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is mandatory, an answer that does not meet the item rejects the bid: a division by contract, by supplier, by software module or by working schedule; units stated as assigned to a place that nothing prevents them leaving; a division whose separation rests on a setting; or a division that does not say where work passes from one group to another.

NOTE Where the units do not divide, the widest population any one unit reaches is the population of every answer about all of them; where they do, the acquirer can see which of its questions are answered by units that reach nobody. A unit outside a room at noon and able to enter it at one o'clock reaches the persons in that room, and a group built from the working timetable is not a group. Where work passes from one group to another, the place it passes belongs to both. A handover in the doorway of a room in which the public stands is a handover among the public, and a group that claimed to reach no member of the public reaches them there. Whether that station stands inside the doorway or behind a door the public does not pass is a fact about the site, and it decides whether the division is worth anything. This divides no tier and removes no question. The tier is declared once, for the deployment, at the maximum: what travels upward through a division is refusal, not assurance. C-6 and C-7 are what this answer is checked against: a division that puts two units in separate groups where either of those items has them reaching one person is refused, and refused on the supplier's own two answers rather than

on anything the acquirer has to go and find.

8 What no instruction may override

Three steps, in order of decreasing strength. Build the hazard out, so that the system cannot produce it at all. Detect and interrupt what could not be built out. Tell a person what is left. The order is the substance of the method: telling somebody cannot substitute for interrupting, and interrupting cannot substitute for building the hazard out. Machinery safety states the three in these terms — inherently safe design, safeguarding and complementary protective measures, information for use — and this standard asks them of any system.

What the first step means depends on the system. For a machine it bounds mass, speed, force and geometry by construction. For a system with no body it is a thing the system cannot do at all: an account it cannot reach, a payment it cannot make, a record it cannot delete.

Everything else in this standard sits *above* that work. It asks who can change a system’s behaviour, what it records, what it is confined to and what evidence the acquirer holds — and none of that bounds what the act itself can do. A system can satisfy every clause to this point, with identity-attested software, an unforgeable record and demonstrated containment, and still injure a person, because its mass, speed, contact force and geometry were never bounded and none of the clauses to this point asked. [Clause 17](#) is where this standard asks.

For the deployment this standard addresses, that work may not have been done at all. No document in the corpus of Annex A states the requirements, so an acquirer cannot assume a regime has been applied. This clause requires the evidence to be produced.

H What must hold irrespective of instruction

H-1	The three steps are evidenced in order	T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID
For each identified hazard, the supplier shall state what was removed or bounded by design; what is detected and interrupted by a protective measure; and what remains addressed only by information for use, in that order. Where a hazard is left to information for use alone, the supplier shall state why it was neither removed nor bounded by design and why no protective measure detects and interrupts it.		
Acceptable: the three columns filled per hazard, in that order; and for each hazard left to the third column alone, the account of why the two above it were not available. An answer that does not meet the item rejects the bid: a risk assessment offered without the hierarchy; or a hazard left to the third column with no such account.		

NOTE The order is the substance of the method: information for use does not substitute for safeguarding, and safeguarding does not substitute for design. This item does not decide whether a residual hazard is acceptable. Every real machine leaves some hazard addressed by a warning, and an item that rejected a bid for saying so would reject the honest table and pass the one whose first two columns are filled with something. What is asked is that the residue be visible and accounted for; the acquirer weighs it against what the machine is for, and raises this item in its tender under [C1](#) if it wants more. Everything else in this standard sits above that work and none of it bounds what the act itself can do, so a system can satisfy every other clause — identity-attested software, an unforgeable record, demonstrated containment — and still do the harm the hazard names.

H-2 The safety function is not reachable from the general-purpose partition T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall name the functions that act to prevent harm. The supplier shall state which components share a trust boundary with those functions, which do not, and the mechanism that enforces the boundary. Those functions shall not be reachable from the computing that runs the learned policy, from the network stack, or from anything added after delivery. Where the system has a body, the functions named include the protective stop, the energy isolation and any hardwired limit, and those functions shall lie outside what the system can reach and act on: a function the machine can unplug, obstruct or damage is not partitioned by a boundary drawn in software.

Acceptable: the functions named, and the partition stated component by component with its enforcement mechanism — expressed as zones and conduits or otherwise; and, where the system has a body, the placement of each named function stated against the reach of the machine.

An answer that does not meet the item rejects the bid: a partition asserted as software configuration on a processor, an account or a tenancy shared with the learned policy or the network stack; a named function the machine can reach with an effector, where its placement is not stated; a conformity claim cited in place of the partition; or no function named at all, where the system has something it does to prevent harm.

NOTE What this clause reaches is that the partition exists and is stated, not that any particular notation is used. The question behind it is what a compromise of the least protected component can reach, which is a question about the boundary and not about the components. For a system with no body the functions are still there — the check that refuses a step, the ceiling on what one action commits, the withdrawal of D6.5 — and the question is the same one: what reaches them.

H-3 What stops the system when nothing can command it T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

For every period of unattended operation — every period in which no principal can command the system, whether by link down, an interface closed for the mission, or a task designed to run without instruction — the supplier shall state its maximum duration, what the system will do for the whole of it without instruction, and what will stop it. The stop shall be identified by the path it takes, and that path shall not be the command channel. Where no such stop exists, the supplier shall state that, and the statement is recorded and caps the tier under C6 rather than excluding the system. The ceiling is T0.

Acceptable: the bound, the behaviour, and a stop identified by the path it takes, that path not being the command channel; or a statement that no stop is available during the period, which is recorded and caps the tier under C6. The ceiling is T0.

An answer that does not meet the item rejects the bid: a remote halt offered as the stop for a period defined by the absence of the remote path; or a period with no stated bound.

NOTE During a period of unattended operation the system's command authority is empty: nothing can direct it and, by the same fact, nothing can stop it by command, since a halt that travels over the command path does not exist while the path does not. What remains is whatever does not travel on that path. On a machine that is a contact or a button on the system, or an isolation independent of the computing that runs the policy. Where nothing has a body it is the withdrawal of D6.5, which is taken at the systems that the system reaches and needs nothing from the system at all.

9 Assurance dimensions

Six dimensions, chosen so that each bounds a failure mode the others do not reach.

D1 Provenance and identity attestation

What is running, and whether that can be established independently. Identity attestation is a claim

about the *identity of the artefact* — that the software on the delivered system is the software that was presented — and not a claim that the software is correct. Measured boot, signed images and a hash recorded at acceptance satisfy it. No clause of this standard requires formal proof of the properties of any component.

D2 Data governance

What leaves the acquirer's control, to which endpoints, stored under which jurisdiction, retained how long, and whether the safety functions operate with no connectivity at all.

D3 Control-channel isolation

Degraded and offline modes, the enumerated set of principals who may command, and behaviour on loss of link.

D4 Behavioural verification

Conditions checked per step, and *invariants* carried across the trajectory (Clause 12), with a fallback that does not depend on the learned policy.

D5 Auditability

A local, append-only decision record, bound cryptographically to the identity-attested code and to a time source the supplier does not control.

D6 Human oversight

A right to stop that drives the system to the declared fallback state, controlled degradation, and a named accountable person. Removing power is not the test of it. A system with no body has no power to remove, and a machine held up by active control falls when it loses it.

9.1 Why six, and why none of them substitutes for another

The claim above is that each dimension bounds a failure mode the others do not reach. It is shown rather than asserted: for each, a failure that survives every other dimension being perfectly satisfied.

Table 2 — What is left uncaught when one dimension of the six is missing

A failure that the other five do not catch	
D1	A substituted image that behaves identically on the acceptance tests. Nothing in the other five compares what is running against what was presented.
D2	A system that behaves correctly throughout and sends what it holds of the acquirer's — the survey of a site, a customer list, a case file — out to a third party. Correct behaviour is not the property at issue.
D3	The identity-attested code, executing a well-formed command from a party that was never entitled to give one. The command is legitimate in form and the record will show it was obeyed.
D4	The right code, the right principal, and a sequence of individually admissible steps ending in a state that no single step would have been admitted to reach.
D5	All of the above holding, and no means after an incident of establishing what was decided or when — the acquirer holds the consequence and the supplier holds the evidence.
D6	All of the above holding, and no person able to bring the system to the declared fallback state while it does what it was correctly instructed to do.

Each row is a system in which five dimensions are satisfied and the sixth is not. That is what makes the aggregation rule of Clause 21 the minimum rather than the mean: a strong answer on one dimension does not reduce the exposure the missing one leaves, and averaging would let a supplier choose which failure the acquirer carries.

9.2 Requirements by tier

Cells are cumulative: a leading “+” means the preceding tier’s requirement and what follows in addition. Each cell states the minimum evidence the acquirer should be able to obtain — not the supplier’s assertion that it holds. Each cell is drawn from items that are asked at that tier, and the tiers are the items’ own; which items of a dimension apply at a tier is stated by the items themselves, and rule C3 of [Clause 21](#) is read against those and not against this cell. The exceptions are listed immediately below: a small number of demands stand here that no item asks at any tier.

Cells of this table that the acceptance items do not ask for. Each cell of [Table 3](#) states evidence; the acceptance items of [Annex A](#) state, for each item, what an acceptable answer to it looks like and what an unacceptable one costs. The two do not correspond everywhere. The following demands appear in this table and in no item of Annex A, so an acquirer who carries one of them into a tender is drafting its acceptable and failing answers himself:

- **D1** — verified boot and signed firmware and weight images (T1); reproducible build of the safety-relevant stack, identity attestation of the signing chain by a party independent of the supplier, and hashes of accepted weights recorded at acceptance (T2); hardware root of trust, component-level supply-chain identity attestation, and re-attestation before each mission (T3).
- **D2** — egress default-deny with a published allowlist (T2); no egress beyond the operating party’s administrative boundary, on-premises processing, and keys held by that party (T3).
- **D3** — replay protection of authenticated commands (T2).
- **D4** — no learned component on the fallback path (T3).
- **D5** — write-once acquirer-held storage (T3).
- **D6** — an incident-reporting route (T2); two-person authority for autonomy escalation (T3).

Four stops, and no two of them are the same stop. Two are asked here and two in [Clause 17](#). The split is by whether the stop needs a body.

- **D6.5**, here: the acquirer cuts the system off from everything it reaches, at those systems and not by asking it.
- **D6.4**, here: the acquirer’s remote stop for a whole fleet, with a second channel.
- **G-6**, [Clause 17](#): the stop a person who is not an operator reaches, needing no credential, tool or application.
- **G-7**, [Clause 17](#): the service means of removing all power, which says in terms that it is not the stop that drives the declared fallback state.

D6.2 is not one of the four. It is the measured time to reach the declared fallback state, and not a means of reaching it. The **D6 T2** cell stays on the list above for its other half, an incident-reporting route, which no item asks.

Nothing is withdrawn by this note and nothing is added: the cells listed above stand as they are, and [Clause 21](#) states that an assessment addresses each item of Annex A applicable at the declared tier. What the note records is that for the demands listed there is no item to address, and therefore no acceptance criterion, designation, owner or stage behind them. Writing the missing items and deleting these cells are both decisions about what this standard requires, and neither is taken here. Every other cell of the table is drawn from items asked at its own tier, which is the reconciliation of 9 August: the T0 column, which stood empty for four of the six dimensions, now states what the items asked at T0 ask, and every place where an item and a cell disagreed about the tier is settled in the item’s favour.

Table 3 — The evidence each assurance dimension yields at each tier, every cell adding to the tier before it

	T0	T1	T2	T3
D1	A parts list of everything that runs code; every path by which code arrives after delivery, with its channel and who signs on it; and whether any of them works without the acquirer's prior authorisation.	+ a machine-readable software bill of materials at delivery and at every update, reaching the firmware below the application; the safety-relevant artefacts versioned on their own, a change to one being a re-acceptance event; signed firmware and weight images; verified boot.	+ the acquirer can check for itself that the software running is the version declared; reproducible build of the safety-relevant stack; identity attestation of the signing chain by a party independent of the supplier; hashes of accepted weights recorded at acceptance.	+ hardware root of trust; component-level supply-chain identity attestation; re-attestation before each mission.
D2	Every stream that leaves the acquirer's control, with its content, destination, storage jurisdiction and retention, warranted complete and written into the contract.	+ whether it captures data by which a person can be recognised, and where that is processed; a named record deleted on the acquirer's instruction, with evidence.	+ it completes its mission, or reaches its declared fallback state, with all connectivity off, every safety function still working; egress default-deny with a published allowlist.	No egress beyond the operating party's administrative boundary; on-premises processing; keys held by that party.
D3	Every remote path by which a command can make the system act, with how each is authenticated, and a warranty that no undocumented path exists.	+ the acquirer can end the supplier's access at its own network boundary, without the supplier's help, and the system goes on working — shown with the supplier's endpoints blocked.	+ what it does when the control channel is lost or degraded mid-task, the state it ends in, with test evidence across the envelope; commands authenticated and replay-protected.	+ the network placement it requires, and whether it works inside a segment of the acquirer's own with an enumerated set of permitted flows, its control plane out of the supplier's reach.
D4	Which behaviours come from learned components and which from hand-written logic, and whether any safety-relevant decision rests on a learned one.	+ the parameters that bound admissible action, checked before every step; whether a protective layer can override the learned controller, whether it is built independently of it, and whether it was tested on its own.	+ the declared fallback state for this system, evidenced reachable from every state in the declared envelope; the invariants a trajectory preserves; the declared autonomy horizon.	+ invariants, monitor and fallback disclosed for independent re-verification; no learned component on the fallback path.
D5	A record on the device of every command received, with who issued it, and every step admitted or refused, with the condition that decided it — append-only, surviving loss of link and of power.	+ the acquirer reads the whole record straight from the device, without supplier tooling, credentials or account; the record signed by the machine; the rate it is written at, what the store holds at that rate, and what happens when it fills.	+ hash-chained, written locally first and deposited at a declared interval, verifiable offline under a key the supplier cannot build a second history with, and still verifiable after the supplier withdraws.	+ write-once acquirer-held storage; a time source common across the fleet and independent of the supplier; enough state to re-execute the decision, exported to an independent investigator.
D6	An accountable person named, with that role's powers exercisable through the delivered interface; and the acquirer's own means of cutting the system off from everything it reaches — at those systems, not by asking it — with the measured time and what survives it.	+ the acquirer's own remote stop for the whole fleet, with a second, independent channel.	+ the time from the stop to the declared fallback state, measured across the envelope with its worst observed case, not quoted from a datasheet; an incident-reporting route.	+ persons in the operating area told that an autonomous system is present and that recording may be taking place; two-person authority for autonomy escalation; the halt exercised in a drill at acceptance, supplier connectivity blocked, over a subset and over the whole fleet.

Why no cell above asks for a stop. The D6 cells ask that a stop drive the system to the *declared fallback state*, and the D3 cells ask that loss of link do the same, rather than that power be removed. That is not a preference of wording. For a platform whose stability is actively controlled, removing power does not return the machine to rest. The IEEE Humanoid Study Group’s pathway study records that a braked, powered-off pose — the conventional safe state of a fixed manipulator — is not necessarily a safe state for a humanoid, and that a locked pose is in general to be assumed unstable [7]; it further notes that a moving machine may need additional motion planning to reach a stable pose at all [7]. The property is characterised in Clause 3 of this standard.

The stopping and energy-isolation primitives that machinery safety inherits are defined for machines whose stable configuration is a passive one. So an acceptance criterion written in terms of the availability of a stop asks, for this class of platform, for something that is not defined — and is answered by a supplier who can point at a contactor. What the platform actually reaches, and how, is characterised under G-3 for the machine’s stability class. This note withdraws nothing and adds nothing: the cells above stand as written.

9.3 Requirements

D1.2 below asks for a machine-readable software bill of materials and names the two formats it accepts. Their full citations are in the bibliography, with the edition each designation carries; a bill of materials in a supplier’s own format is not one of them.

D1 Provenance and identity attestation

What this dimension establishes about a system it can only establish about a system it can tell apart from another. An assessment is carried out on one configuration and a deployment is made of whatever arrives on the site, and the two are the same only where the first was written down closely enough that the second can be checked against it. The block below is what is fixed, and it is fixed for that reason and for no other: nothing in this standard weighs a supplier or a manufacturer.

Table 4 — What is fixed about a configuration, and what fixes it. Stated under D1.5; the last three rows are answered by items that were already asked, and are set here so that one page carries the whole of what pins a configuration down.

What is fixed	What fixes it, and where it is asked
The configuration	The designation and build given to this configuration and to no other the supplier offers D1.5
Each delivered unit	Its type, and the identifier the unit carries on itself D1.5
What determines behaviour	Firmware, on-device models, weights and parameters, as values, with the reference values checked against D1.2, D1.4
What is fitted	The options, payloads and end effectors, from the declared set .. G-4, K-2
What it is made of	Every element that executes code, with its manufacturer; radios, sensors, place of final assembly D1.1

D1.1 What executes code is listed at the part, not the module T0 R · T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall provide a bill of materials for the delivered configuration identifying every element that executes code, with its manufacturer. Where the system runs on a substrate the acquirer does not hold, the supplier shall identify that substrate, the party that operates it, and the jurisdiction it runs in. Where the system has a body, the bill also identifies every radio and every sensor, and gives the place of final assembly of each element.

Acceptable: a signed, versioned bill of materials, reissued when the configuration changes.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a list at module granularity (“mainboard”, “sensor kit”) offered as the bill of materials; or silence. An account that an element cannot be listed at the part is an answer, and it names the elements it does not reach and why — a module whose vendor discloses no part list — what stands in their place, and the record of the request made to that vendor, against which the acquirer can check the account. The acquirer evaluates it and is free to reject it.

NOTE The place of final assembly is disclosed here as an input to supply-chain identity attestation. No criterion in this standard turns on it, and no bid is rejected by reason of it. What the item reaches is granularity: a bill of materials written at module granularity conceals the elements that execute code, and an element nobody listed is an element no later requirement of this standard arrives at. Where nothing in the system has a body, the elements that execute code are the images, the runtimes and the hosts they run on, and the party that operates the substrate is the party whose failure the acquirer inherits.

D1.2 Every layer that runs code is listed, not only the application T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall provide a software bill of materials covering all firmware and all on-device models, including external and open-source components with versions.

Acceptable: a machine-readable SBOM in one of two formats — CycloneDX, specified by ECMA-424, or SPDX, specified by ISO/IEC 5962:2021 — in the edition named or a later edition published by the same body, at delivery and at every update, covering motor controllers, battery management, and radio firmware.

An account of why it does not arise is an answer, and silence is not. Unacceptable: an SBOM limited to the application layer; a bill of materials in a format of the supplier’s own, which the acquirer’s tools cannot read without the supplier’s; or silence. An account that a layer cannot be covered is an answer, and it names the components it does not reach and why — a firmware blob its vendor supplies with no bill of materials — what stands in its place, the component and version list held for it and the control that compensates, and the record of the request made to that vendor, against which the acquirer can check the account. The acquirer evaluates it and is free to reject it.

NOTE The firmware outside the application layer carries the components with the longest service lives and the least visibility — a motor controller, a battery-management controller, a radio. A vulnerability published against one of them is matched to a fleet only through a list that names it, and the application layer is not where it appears.

The two formats are named by the documents that specify them and not as the editions a supplier is confined to. Both bodies publish beyond the edition named here, and one of the later ones reaches a bill of materials for a model, which is nearer this standard’s subject than either edition named. What this item needs is a list the acquirer’s own tools can read.

D1.3 Every path by which code arrives after delivery is named T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall enumerate every component that can receive code after delivery, and the channel and signing authority for each.

Acceptable: a complete list, including any cellular or auxiliary radio path.

An answer that does not meet the item rejects the bid: an answer covering only the main computer; undisclosed modems discovered later at acceptance testing.

NOTE An update path nobody declared is an update path nobody assessed. The channel and the signing authority are asked for together because they answer different questions: the channel is where code arrives, the signing authority is who decides what arrives on it.

D1.4 What is running is checkable against what was declared T2 R · T3 R · SUPPLIER · ACCEPTANCE

The supplier shall provide a means by which the acquirer can independently verify that the software running is the version that the supplier declared. Where the acquirer holds the system, that means is a measurement the acquirer takes on it. Where the system runs on a substrate the acquirer does not hold, that means is one the acquirer can exercise itself against the running system, without asking the supplier.

Acceptable: a measurement or a check the acquirer can perform itself, and compare against a supplier-published reference value.

An account of why it does not arise is an answer, and silence is not. Unacceptable: the version string the system reports of itself offered as the only evidence; or a check the supplier performs and reports the result of.

NOTE A system reports the version it holds itself to be running, and a substituted image reports whatever it was built to report. The two answers are independent only where the check is taken by the acquirer and compared against a value the supplier published beforehand. Where the system is hosted, the acquirer holds no unit, which is why the item asks for a means the acquirer can exercise rather than for a measurement on a device.

D1.5 The configuration is identified so a substituted one fails to match T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall identify the configuration this declaration is made for, so closely that a system which is not that configuration fails to match the identification: the designation and build the supplier gives it and gives to no other configuration it offers; where the system has a body, the type of every delivered unit and the identifier each unit carries on itself; the version of everything that determines the system's behaviour — firmware, on-device models, weights and parameters — as values, together with the reference value the acquirer is to measure against for each; and the options, payloads and end effectors fitted, drawn from the set declared under G-4.

Acceptable: an identification one configuration answers and another does not; every delivered unit identifiable on the unit itself; versions given as values rather than as a product name; and the fitted set named from the declared one.

An answer that does not meet the item rejects the bid: a product family, a range or a model line offered where one configuration is asked for; an identification that would fit a different build of the same product equally well; units given only as a count; a version given as a marketing name; or an identification that cannot be checked on the site against what arrived.

NOTE D1.1 bills what the configuration is made of and D1.2 what runs on it; this item names the configuration those bills are of. The reference values are published here because that is when they can be published: D1.4 has the acquirer take its own measurement at acceptance and compare it against a value the supplier stated beforehand, so the stating is a bid-time act and the checking is not. Without a declared object for that version to be the version of, a unit given the same image passes its check whether or not it is the unit that was assessed. Where any part of this identification changes, the declaration is made again (cl:change).

D2 Data governance

D2.1 What leaves the acquirer's control is enumerated, not described T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall enumerate every data stream that leaves the acquirer's control, stating for each its content, its destination, the jurisdiction under which it is stored, and its retention period.

Acceptable: a table, warranted as exhaustive and incorporated into the contract.

An answer that does not meet the item rejects the bid: a general permission to collect “telemetry for product improvement” without enumeration.

NOTE An enumeration warranted as exhaustive and written into the contract is a different instrument from a description of the same streams. The warranty is what makes an undisclosed stream a breach rather than a surprise, and the enumeration is what an undisclosed stream is undisclosed against.

D2.2 Data by which a person can be identified is stated, with where it is processed T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state whether the system takes in data by which a person can be identified, and where that data is processed. Where the system has a body, that includes facial images, gait, voice and vehicle plates.

Acceptable: an explicit statement of whether data by which a person can be identified is taken in, and of where it is processed.

An answer that does not meet the item rejects the bid: the assertion that what the system takes in is not personal data because of the use that the supplier puts it to — that camera imagery is “only used for navigation”, or that a mailbox is “only read to draft a reply”.

NOTE Whether imagery of a person is personal data follows from the law of the deploying jurisdiction, not from the purpose the supplier assigns to the capture. This standard names no jurisdiction's law and sets no threshold drawn from one. What the item reaches is that the capture and the place of processing are on the record before the deployment, at the point where the acquirer's own obligations are still assessable against them.

D2.3 A named record goes, and its going is evidenced T1 M · T2 M · T3 M · SUPPLIER · BID

On the acquirer's instruction the supplier shall delete a specified record from all supplier-side systems, and shall evidence the deletion.

Acceptable: a defined procedure with a stated completion interval and a written confirmation.

An answer that does not meet the item rejects the bid: deletion that removes data from the acquirer's view of a portal only.

NOTE The party holding the data is the only party in a position to evidence its removal, and an acquirer that has instructed a deletion has no means of its own by which to confirm one.

D2.4 The system works when what it depends on is unreachable ACCEPTANCE

T2 M · T3 M · SUPPLIER ·

The supplier shall demonstrate that the system completes its stated task, or reaches its declared fallback state, when the parties it depends on are unreachable, and that every function that acts to prevent harm remains operable in that state.

Acceptable: demonstration at acceptance testing.

An answer that does not meet the item rejects the bid: “connectivity is required for normal operation.”

NOTE Connectivity is the dependency most likely to be absent at the moment it matters and the one neither party controls. A demonstration on the delivered configuration is what separates a system that tolerates the loss from one that has never been tried without it.

D3 Control-channel isolation

D3.1 Every remote path that can make the system act is enumerated SUPPLIER · BID

T0 M · T1 M · T2 M · T3 M ·

The supplier shall enumerate every remote path by which a command can make the system act, including maintenance and support tooling, teleoperation, cloud task dispatch, and any update that changes behaviour.

Acceptable: an exhaustive list with the authentication mechanism for each and a warranty that no undocumented path exists.

An answer that does not meet the item rejects the bid: “the system cannot be controlled remotely”, stated without reference to support tooling.

NOTE Support tooling is a remote path that can make the system act. At the moment it moves an actuator, places an order or sends a message, it is not distinguishable from the channel the acquirer thinks of as the control channel, and it is the path most often left off the list because the people who answer the question do not think of it as control. The list is as complete as what was disclosed, which is what the warranty attaches to.

D3.2 Supplier access ends at the acquirer's boundary, and the system works on T3 R · JOINT · ACCEPTANCE

T1 R · T2 R ·

The supplier shall deliver a system in which the acquirer can terminate the supplier's remote access unilaterally, at the acquirer's own network boundary and without the supplier's cooperation, and in which the system continues to perform its function afterwards. At acceptance, block the supplier's endpoints and observe both.

Acceptable: demonstration with the supplier's endpoints blocked.

An account of why it does not arise is an answer, and silence is not. Unacceptable: access governed only by settings held in a supplier-side account; or silence. An account that the second limb does not arise is an answer, and it states why the system does not perform its function with the supplier's endpoints blocked — which function is dispatched or perceived remotely — what stands in its place, the state that the system holds at when cut off and for how long, and the demonstration by which the acquirer can check that behaviour on the delivered configuration. The acquirer evaluates the account and is free to reject it.

NOTE Where the governing setting sits in a supplier-side account, what the acquirer holds is a statement about how that account is administered, and the two are told apart only by blocking the endpoints and watching. The second limb is not a refinement of the first: a system that stops working when the supplier is cut off gives the acquirer a control it cannot use.

D3.3 Behaviour on loss of the control channel is stated

T2 M · T3 M · SUPPLIER · BID

The supplier shall state what the system does when the control channel is lost or degraded mid-task, and what state it ends in.

Acceptable: a documented degraded mode that reaches the declared fallback state without needing the link, with test evidence across the operating envelope.

An answer that does not meet the item rejects the bid: “it stops” offered for a system that can have work submitted and unfinished, with nothing said about what becomes of that work; or, where the system has a body, “it stops” offered for a dynamically balanced platform without a stability analysis — a locked pose is not necessarily a stable one.

NOTE Loss of the link is the condition under which the system is least observable and least correctable from outside, so what it does then is a property of the system alone.

D3.4 The network placement the system requires is stated

T3 R · SUPPLIER · BID

The supplier shall state what network placement the system requires, and whether it can operate inside an acquirer-defined segment with an enumerated set of permitted flows.

Acceptable: a documented requirement expressible as zones and conduits under the acquirer’s own risk assessment (IEC 62443-3-2:2020) — zones and conduits being the vocabulary of that assessment and not a term this standard defines.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a requirement for a flat network, or for unrestricted outbound access.

NOTE Zones and conduits is the vocabulary of the acquirer’s own risk assessment, so a placement requirement stated in it can be checked against the segmentation the acquirer already operates rather than translated into it afterwards. A system that requires a flat network moves the question from the reach of the system to the reach of everything else on that network. The two words are defined in the terminology part of the IEC 62443 series, and IEC 62443-3-2:2020 is where they are established for a particular system; it is that establishing, and not the definition, that this item asks a placement requirement to be expressible in.

D4 Behavioural verification**D4.1 Learned and hand-written behaviour are told apart**

T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state which behaviours are produced by learned components and which by hand-written logic, and whether any safety-relevant decision rests on a learned component.

Acceptable: an architecture statement identifying, for each class of decision, which mechanism governs it.

An answer that does not meet the item rejects the bid: “the system is AI-based” as the whole answer.

NOTE The split decides which of the other requirements bear and how each of them is answerable. A behaviour produced by hand-written logic is answerable by reading the logic; the same behaviour produced by a learned component is answerable by test and by what constrains it from outside, and the two kinds of evidence do not substitute for each other.

D4.2 The protective layer is independent of what it constrains T1 S · T2 S · T3 S · SUPPLIER · BID

The supplier shall state whether there is a protective layer that can override the learned controller, whether it is implemented independently of that controller, and whether it has been tested or analysed separately from it.

Acceptable: a documented switching condition, a fallback controller whose behaviour is analysable without reference to the learned component, and evidence that it was tested or analysed on its own. No formal proof of its properties is required at any tier (F-3); at T3 it is disclosed for independent re-verification.

An unsatisfactory answer loses the points of that item and the bid stands: the protective function implemented inside the same learned model it is supposed to constrain.

NOTE A protective function sharing the learned controller's implementation shares its failures, and the analysis of the one becomes the analysis of the other.

D4.3 The fallback state is declared and shown reachable T2 M · T3 M · SUPPLIER · BID

The supplier shall state the declared fallback state for this system, shall state the time within which and the distance within which the system reaches it, each as a worst case over the declared operating envelope, and shall evidence that it is reachable from every state in that envelope within those two bounds.

Acceptable: a characterized envelope with measured recovery data and, where the system has a body, fall-response data; and the two bounds, each stated as a worst case over that envelope.

An answer that does not meet the item rejects the bid: a declared fallback state defined only for the case in which the system is doing nothing; or a state declared reachable with no bound on the time or the distance in which it is reached, which leaves the recoverability invariant of F-4 nothing to be evaluated against.

NOTE What the state is on a given system is a fact about that system: on a dynamically balanced platform removing power is a fall, and for a system with work in flight stopping is not the same as finishing. The idle case is the single case in which the answer is the same for every system, which is why an answer that covers only it carries no information about the system it was written for.

D4.4 Unintended means of reaching the objective are registered T2 S · T3 S · SUPPLIER · BID

The supplier shall state the conditions under which it has observed the system achieving its stated objective by means the supplier did not intend, and shall maintain a register of such observations. A capability the system did not have at acceptance and exercises afterwards is such a means, and is entered in that register.

Acceptable: a maintained anomaly register with incidents, dates, and dispositions, its entries covering an acquired capability as well as an unintended use of one the system had.

An unsatisfactory answer loses the points of that item and the bid stands: “never observed” — published evaluations of contemporary learned systems report measurable rates of objective-satisfying behaviour that the evaluator did not intend; or a register whose scope is stated to exclude a capability the system did not have at acceptance.

NOTE This asks what was observed, not what is possible. A bare “never observed” does not distinguish a system in which nothing of the kind happened from one in which nobody was looking, and the register is the only thing that tells those two apart, because it records the looking as well as the finding.

D4.5 What the system can come to do, and what bounds it T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state what the system can come to do that it cannot do now. It is answered over the paths enumerated under U-1 and over any change the system makes to its own behaviour that nobody exercises: a policy or a set of weights it updates from its own operation, a store it writes and later reads, or a corpus it retrieves from that changes without being installed. For each, the supplier shall state which of the actions declared under C-6 and C-7 the system could come to perform, which persons it could come to reach, taken as C-8 takes it, what bounds that, and which roles under P-1 can lift the bound. Where the behaviour of the system cannot change between installed versions, saying so with what makes it so is a complete answer. What is asked is what is possible; what has been observed is D4.4's subject.

Acceptable: for each path and for each change the system makes to itself: the actions it could come to perform, the persons it could come to reach, what bounds that, and the roles that can lift the bound; or a statement that the behaviour cannot change between installed versions, with what makes it so.

An answer that does not meet the item rejects the bid: that the system does not learn, with nothing said about what makes it so; a bound named as a policy, an instruction or a setting inside the planner, which C-7 refuses for the same reason; that it can only improve, or only within its training distribution, neither of which names an action or a bound; an answer given for installed versions where the system also writes a store it later reads; or that the question does not arise because the acquirer holds the update path, which answers U-1 and not this.

NOTE U-1 asks who can change the system and D4.4 asks what has been seen. Between them nothing asked what the system could become, and that is what an acquirer is buying against: Clause 4 states that a capability the system did not have at acceptance and exercises afterwards ends the work the answers were given for, whether it was proposed or the system arrived at it itself. An acquirer told which capabilities are reachable can put the re-acceptance event in its contract before it is needed; one that is not told learns it from D4.4's register, afterwards. Nothing here forbids a system from learning. What is asked is that what it can learn to do be stated and that what holds it back be named, which is C-7's construction one tense forward.

D5 Auditability

D5.1 Recorded where it runs, and surviving the loss of the link and of the system T0 M · T1 M · T2 M · T3 M · SUPPLIER · ACCEPTANCE

The supplier shall deliver a system that records, where the system itself runs and append-only, every command received, with the principal that issued it, and every step admitted or refused, with the condition that decided it, that record surviving loss of the link and abrupt loss of the system. Demonstrate at acceptance by stopping the system abruptly mid-task — removing its power, or ending the instance it runs in — and reading the record afterwards.

Acceptable: an append-only log held where the system runs, with a monotonic sequence and a stated time source, demonstrated by an abrupt stop mid-task and reading the record afterwards.

An answer that does not meet the item rejects the bid: logging assembled somewhere else out of what the system reports; or a stream of individual low-level commands offered in place of the decision layer.

NOTE The three questions D5.1 to D5.3 form a set, and each of them can be satisfied while attribution still fails: a log that exists but is readable only through the supplier, a log the acquirer can read but the supplier can rewrite, or an unforgeable record that does not survive the loss of the link. The demonstration is by an abrupt stop because a record held in memory and flushed on an orderly shutdown passes every inspection and is absent in the case it exists for. What counts as an abrupt stop is what the system can suffer: power pulled from a machine, an instance killed or a tenancy ended for a system with no body.

D5.2 The acquirer reads the whole record without the supplier T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall deliver a system from which the acquirer can read the complete record, in a documented format, without supplier tooling, supplier credentials or a supplier account.

Acceptable: a read interface on the system itself, an open schema, and an acquirer-held key.

An answer that does not meet the item rejects the bid: logs retrievable only through a supplier portal, or subject to supplier-side retention limits the acquirer cannot set.

NOTE An acquirer that reads the record through the supplier's tooling holds it on the supplier's terms, and the occasion for reading it is frequently the occasion on which those terms are in dispute. A documented format with an acquirer-held key is what makes the record readable by a party the supplier has stopped cooperating with.

D5.3 The record's key is the unit's own, and its chain verifies offline T2 R · T3 R · SUPPLIER · ACCEPTANCE

The supplier shall deliver a system in which each record entry is cryptographically bound to the unit by a key generated on that unit and held in a secure element evaluated under a published scheme, and identity-attested by a statement chained to a manufacturer certificate authority, such that the supplier cannot construct an alternative history. The supplier shall register those keys with the acquirer at acceptance, provisioning witnessed by the acquirer, in a chain the acquirer can verify offline.

Acceptable: identity-attestation keys registered with the acquirer at acceptance, provisioning witnessed by the acquirer, and a chain the acquirer can verify offline. This item restates L-3, L-4 and L-9 for the record of D5; what it asks beyond those three is that the key was generated on the unit it binds and that the acquirer witnessed provisioning, and the rest of it is answered wherever those three are answered.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a signing key held by the supplier, escrowed by the supplier, or shared across a fleet; or an assertion that the key has never left the device, offered in place of an identity attestation.

NOTE A key one party can hold in two places produces two histories that verify equally well, and the record then establishes which of them the holder preferred. Identity attestation concerns the identity of an artefact and never its correctness: a fully identity-attested machine can be a fully identity-attested bad machine, and what this item establishes is authorship of the entries, not the quality of the decisions in them.

D5.4 Enough to re-execute, and held for someone other than the supplier T2 S · T3 S · SUPPLIER · BID

The supplier shall deliver a system whose record contains enough state to re-execute the decision that produced an action — the inputs, the outputs, the monitor state and the mode at the moment of the decision — and shall undertake in the contract to preserve that record and to export it to an independent investigator after an incident, the undertaking surviving termination of the contract.

Acceptable: sensor and decision context captured at defined points, plus a preservation and export clause that survives termination.

An unsatisfactory answer loses the points of that item and the bid stands: an incident procedure in which the supplier performs the investigation and supplies the conclusions; or a field purporting to explain why a learned component produced what it produced.

NOTE An investigation performed by the party whose conduct is in question produces conclusions rather than evidence, and the acquirer holds the consequence while the supplier holds the record. The undertaking is drafted to survive termination because termination is a common consequence of the incident that makes the

record worth having.

D6 Human oversight

D6.1 A named person, with powers reachable through the interface T0 R · T1 R · T2 R · T3 R · JOINT · BID

The acquirer shall name the accountable operator on its own side and state the authority that role holds. The supplier shall document which of those powers are exercisable in real time through the delivered interface.

Acceptable: a named role, a documented interface, and a training record.

An account of why it does not arise is an answer, and silence is not. Unacceptable: oversight defined as the ability to file a support ticket.

NOTE A power that exists in the contract and not in the interface is a power nobody can exercise while the system is doing the thing that needed stopping. The training record is the acquirer's and the interface is the supplier's, so the item is answered only where both parties have produced their part.

D6.2 The stopping time is measured, not quoted T2 M · T3 M · SUPPLIER · BID

The supplier shall state the time from an operator's stop command to the system reaching the declared fallback state characterised under D4.3, measured rather than specified, across the declared action envelope, as a distribution with its worst observed case and the conditions of the test.

Acceptable: a measured distribution with worst observed case and test conditions.

An answer that does not meet the item rejects the bid: a single nominal figure from a datasheet.

NOTE Specification and measurement part company exactly where the system is at the edge of its declared envelope – a machine carrying a load or standing on a surface the specification did not contemplate, a system with a queue behind it and work already submitted – which is the set of conditions under which an operator reaches for the stop.

D6.3 The parties acted on are told, rather than left to notice T3 S · SUPPLIER · BID

The supplier shall state how the parties an autonomous system is acting on are told that it is, and that recording may be taking place. Where the system has a body, those parties include the persons in the operating area.

Acceptable: a defined signage and notification procedure, mapped to the transparency obligations applicable in the deployment jurisdiction.

An unsatisfactory answer loses the points of that item and the bid stands: reliance on the machine being self-evidently an autonomous system.

NOTE This standard lists no jurisdiction's law and sets no threshold drawn from one, so the obligations the procedure is mapped against are the ones in force where the system is deployed, and the acquirer is the party that knows them. A party that did not choose this and had no instruction has no other way of learning that a machine is operating around them and a camera is running, or that the letter answering them was written by a system and the exchange is being kept.

D6.4 The acquirer stops the whole of it remotely, and by a second way
 SUPPLIER · BID

T1 R · T2 R · T3 R ·

The supplier shall provide a means by which the acquirer, and not only the supplier, puts the system into the declared fallback state remotely. Where there is a fleet, that means shall put the whole declared fleet into that state in one action. The supplier shall state the channel that means uses, how a command on it is authenticated, and the time from the command to the system reaching that state. The supplier shall provide a second channel for the same command, authenticated to the same standard as the first. The supplier shall state what makes the two channels independent of each other: the credential each accepts, the network path each takes, and the party that operates each. Where the system has a body, the board, the enclosure, the power domain and the radio path are named as well. The supplier shall state what becomes of the systems the command did not reach. Both channels shall appear in the enumeration of remote paths D3.1 requires.

Acceptable: a named channel with its authentication and its measured time; a second channel authenticated to the same standard; the independence of the two named part by part; the disposition of the systems the command did not reach; and both channels in the enumeration of remote paths. R-5 asks for the halt path itself and for a drill at acceptance; what this item asks beyond it is the channel, the authentication, the time, the second channel and its independence.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a single channel; a second channel sharing the first one's credential, network path, operating party or provider, or — where the system has a body — its board, enclosure, power supply or radio path; a second channel authenticated more weakly than the first; a stop the acquirer can only ask the supplier to press; or a stop channel left out of the enumeration of remote paths.

NOTE A fleet is stopped in one action because nobody is going to reach forty systems one at a time. That is what this stop is for, and it is also why it is not the first line of defence: the first line is the stop at the system itself, which for a machine is G-6. The independence of the second channel is asked part by part because “two independent channels” is a true sentence about two modems on one board with one power supply, and those two fail in the same second — and it is just as true of two paths that present the same credential to the same provider. A stop channel is a remote path by which a command can make the system act — the path an attacker would most like to have — which is why both channels go into the enumeration D3.1 requires. The systems the command did not reach are the ones somebody has to chase one at a time, and the time to learn how many there can be is before the day it happens.

D6.5 The acquirer cuts the system off from everything it reaches
 SUPPLIER · BID

T0 R · T1 R · T2 M · T3 M ·

The supplier shall provide a means by which the acquirer withdraws the system's access to everything it reaches. That means shall cover every credential, token, key, session and standing grant the system holds, in every system it reaches — the ways out listed under O-1 and the keys listed under Z-7. The withdrawal shall be made at those systems. It shall not need the system's cooperation. The supplier shall state the number of separate actions the withdrawal takes and who can take them. The supplier shall state the time from the first action to the last access ending, measured rather than asserted, with the worst case observed. The supplier shall state what keeps working after the withdrawal and the period each of those lasts. The supplier shall state what becomes of work the system had already started.

Acceptable: the credentials, tokens, keys, sessions and standing grants named against the ways out of O-1 and the keys of Z-7; the number of actions and the roles that can take them; a measured time to the last access ending; what keeps working after the withdrawal, with the period each lasts; and a stated disposition for work already started — completed, abandoned, rolled back, or left for a person.

Where it is required, an account of why it does not arise is an answer and silence is not; where it is mandatory, an answer that does not meet the item rejects the bid: a withdrawal that is a command sent to the system, which stops nothing once the system has stopped obeying; a withdrawal the acquirer can only ask the supplier to perform; a separate act by a separate administrator in each system, offered with no time for the whole of it; a time quoted rather than measured; or an answer that ends at the revocation and says nothing of the tokens, jobs, cached credentials and registered callbacks that outlive it.

NOTE A system with no body is stopped by being cut off from the systems it is inside and the things it controls, and that is done at those systems and not at the system. A revoked token can stay valid until it expires; a job already queued fires later; a credential cached on another machine works with no network at all; a callback registered long ago still arrives. A system that has been cut off can have left thirty actions submitted and unfinished — a payment placed, a message sent, a file half written — which somebody then has to go and find. **O-1** and **Z-7** are what turn “everything” into a list: this item asks that the acquirer can close what those two enumerate.

D6.6 Whether the acquirer can put its own monitor inside, and what it may see T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state whether the system admits a monitor supplied by a party other than the supplier and installed by the acquirer or by a party the acquirer names. Where it does, the supplier shall state the interface such a monitor attaches to; which of the classes of event **L-1** carries it can observe, and the delay between an event and its being observable; whether it can hold back a step or can only observe; and what the supplier no longer asserts once such a monitor is installed. Where the system admits no such monitor, saying so is a complete answer to this item and is recorded. This standard requires no monitor and names no party that supplies one.

Acceptable: the interface named, the observable classes and the delay stated, whether it can hold back a step said in those terms, and what the supplier no longer asserts; or a statement that no such monitor is admitted, which is a complete answer and is recorded.

An account of why it does not arise is an answer, and silence is not. Unacceptable: an assurance that the system is open or integrable with no interface named; a monitor said to hold back a step with nothing stated about how a step waits for it; or a monitor admitted on terms that withdraw everything the supplier asserts, offered as though the first half of that answer stood on its own.

NOTE An acquirer that cannot put an instrument of its own inside the system holds only what the supplier chose to expose, and every later question about what the machine did is answered out of the supplier’s own account of it. What the item asks is that the acquirer know before it signs whether independent observation is available to it at all, and on what terms – because the answer cannot be obtained afterwards, and an acquirer that assumed one and finds none has bought a system it can only watch through the window the seller cut. A monitor that only observes and a monitor that can hold back a step are not the same thing, which is the line **Z-2** draws for a formalised condition: what stands beside the work establishes afterwards, what stands in the path can refuse. Where such a monitor can hold back a step it is in the safety path, and **N-4** is the item that governs it there.

D6.7 Whether a person can be put into a loop that has none T2 R · T3 R · SUPPLIER · BID

For the tasks the system performs without a person under **Z-1**, the supplier shall state whether a person can be put into the loop of those tasks after delivery — by a point at which the system waits for a decision, by a monitor of the kind **D6.6** describes that can hold back a step, or by another means the supplier names. Where a person can be, the supplier shall state which of those tasks it covers, what the person decides, and the path by which the request reaches that person. Where a person cannot be, the supplier shall state what in the construction of the system prevents it, and saying that is a complete answer to this item. Nothing here requires that any task be run with a person in the loop: **Clause 6** states who decides that.

Acceptable: for the tasks performed without a person, either the means by which a person can be put into their loop, with the tasks it covers, the decision that person takes and the path the request travels; or a statement of what in the system prevents it, which is a complete answer and is recorded.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a general assurance that the system supports human oversight with no means named; a means named for the deployment that does not cover the tasks the system actually runs without a person; or a means whose request reaches a person by a path nobody watches at the hours those tasks run.

NOTE A person put into a loop after delivery needs three things, and the first is worth nothing on its own: a point where the step waits, somebody reachable to decide, and a bound on how long the waiting lasts. This item asks the first. P-5 asks the other two — how often one person can be asked, how long it takes to reach anybody, and what happens when nobody answers — and neither answer is worth much without the other. Where the means is a monitor another party installs, it stands in the path of admission and N-4 is the item that governs it there, and where the system acts on what it answers it is an oracle under Clause 14.2. The answer of no is asked for because it is the one an acquirer cannot obtain later: a deployment whose autonomy cannot be interrupted is a thing to decide about before signing, and after signing it is a thing to live with.

10 A record made inside the boundary in question

A record held, generated and identity-attested entirely within the supplier’s control boundary does not establish what happened, because every property of it the acquirer can check was produced inside the boundary whose trustworthiness is the question. This clause states what must be recorded, by whom it is signed, and what has to sit outside that boundary for the record to answer anything.

10.1 What is recorded

What is recorded settles what can be established afterwards, and by whom. The requirements below fix the layer the record is taken at, what each entry carries, who signs it, and what has to sit outside the supplier’s reach for any of it to answer a question the supplier would rather it did not, which is the periodic-commitment construction of [10].

L The record, and its independent commitment

L-1 The decision layer, not the actuator loop	T1 M · T2 M · T3 M · SUPPLIER · BID
The supplier shall deliver a system that writes to the record every step admitted and every step refused, with the condition that decided it; every mode transition; every entry to and exit from a declared fallback state; every approach to the containment boundary, every breach of it, and every occasion on which the mechanism that enforces it acts; every command received, with the principal that issued it; every change of the goal in force, with what set it — a command from a named party, the system’s own choice from the set declared under Z-8, or a source outside the deployment named under Z-6; every change under the change-control clause; and every escalation to a person — and shall state what the system writes. The record does not extend to individual actuator commands.	
Acceptable: the classes of entry written and stated, each refusal and each admission carrying the condition that decided it, and each change of the goal in force carrying what set it. An answer that does not meet the item rejects the bid: a record of outcomes without the conditions that decided them; or a record of goal changes without what set each of them.	

NOTE The control loop beneath the decision layer produces tens of millions of commands a day, and an obligation to sign and externalise them would be met by nobody and would answer nothing that the decision layer does not answer better. The reduction is architectural rather than sampled: nothing is selected from a stream, because at the decision layer there is no stream to select from.

L-2 Enough to replay, not to narrate

T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state the fields each entry carries — the inputs, the outputs, the monitor state, the mode, and the identity of the components that produced the decision, all as they stood at the moment of the decision — and those fields shall be sufficient to re-execute the decision. The supplier shall not supply a field purporting to explain why a learned component produced what it produced.

Acceptable: a schema sufficient to re-execute a decision: inputs, outputs, monitor state, mode, and the identity of the deciding components at that moment.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a free-text “reason” field purporting to explain a learned component’s output; or silence. An account that the schema cannot be supplied in full is an answer, and it states why the state at the moment of decision is not retainable at fidelity on this system, which fields are retained in its place and what a re-execution from them establishes and does not, and the recorded example a party can replay to check the account against. The acquirer evaluates the account and is free to reject it.

NOTE Why a learned component produced what it produced is not available, and a field held out as supplying it yields a narrative in place of evidence. The record’s use is re-execution, which needs the state at the moment of the decision and nothing about the reasoning behind it. Which components decided is part of that state and not part of the reasoning: a system that changes itself under U-1 re-executes an entry on components that are no longer the ones that wrote it, and the replay then establishes nothing.

10.2 Signature and identity

L-3 Signed by the system, with a key the system cannot surrender

T1 S · T2 R · T3 R · SUPPLIER · BID

The supplier shall deliver a system in which each entry, or each block of entries, is signed with a key held in a secure element on the system and not exportable from it.

Acceptable: entries signed under a key held in a secure element on the system.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is required, an account of why it does not arise is an answer and silence is not: a signing key held by the fleet back end rather than by the system.

NOTE A key the system cannot surrender makes an entry attributable to that system and forgeable neither by another system nor by a fleet back end. Where the key sits behind the system rather than in it, every entry in the fleet has the same author and attribution reaches no unit.

L-4 The key is identity-attested, not merely asserted

T1 S · T2 R · T3 R · SUPPLIER · ACCEPTANCE

The supplier shall deliver a system whose signing key is held in a secure element evaluated under a published scheme, shall identify that scheme, and shall register with the acquirer, at acceptance, a key-attestation statement chained to a manufacturer certificate authority.

Acceptable: a secure element evaluated under a published scheme, and a key-attestation statement chained to a manufacturer certificate authority, registered with the acquirer at acceptance.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is required, an account of why it does not arise is an answer and silence is not: an assertion that the key has never been exported, offered in place of an identity attestation.

NOTE “The key has never left the device” is a negative neither party can establish: the supplier cannot prove it and the acquirer cannot check it. An evaluation under a published scheme and a statement chained to a

manufacturer certificate authority are the checkable facts that stand in its place. Identity attestation concerns the identity of an artefact and never its correctness – a fully identity-attested machine can be a fully identity-attested bad machine. The acceptable limb carries no split by tier because what is checkable does not change with the tier; what changes is what an unsatisfactory answer costs, which C1 states.

L-5 Bound to the identity-attested code

T2 R · T3 R · SUPPLIER · BID

The supplier shall bind the signature on each entry to the D1 identity attestation of the software that produced that entry, the signature either covering the identity attestation or being bound to it.

Acceptable: the signature covering, or bound to, the D1 identity attestation of the software that produced the entry.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a signature over the entry alone, with no binding to the identity attestation of the code that produced it; or silence. An account that the binding is not made is an answer, and it states why the signing path cannot reach the D1 identity attestation on this system, what establishes in its place which software produced an entry, and the artefact — a boot measurement, a deployment record — against which the acquirer can check that substitute. The acquirer evaluates the account and is free to reject it.

NOTE A signed record of decisions taken by unattested code establishes who signed and nothing about what was running.

10.3 The independent commitment

Any construction satisfying the four properties L-6 states below is admissible, whatever technology realises it, and no particular technology is required to obtain those properties: a qualified timestamping service, a notarial deposit, a public append-only ledger, or publication of roots in a medium that cannot be retrospectively edited is each such a construction. An acquirer specifying a technology rather than the four properties narrows its supplier field without gaining assurance. The properties are what the assurance rests on; a named technology is one way of obtaining them and never the only one, and the ways of obtaining them change faster than a standard is revised.

L-6 The system emits a commitment the acquirer can deposit

T2 M · T3 M · JOINT · BID

The supplier shall deliver a system that hash-chains the record and emits a signed root of the chain, in a documented format, at the interval declared under L-11 — that interval being the period between deposits — and on each forcing event, to an endpoint the acquirer nominates. The acquirer nominates that endpoint; and where a commitment is deposited, the depositary the acquirer chooses shall satisfy four properties: it is not the supplier and is not controlled by it; it cannot alter what was deposited; the deposit is timestamped independently of both parties; and the acquirer can verify a past commitment after the supplier has ceased to cooperate or to exist.

Acceptable: a signed root emitted in a documented format to the endpoint the acquirer nominates and, where a commitment is deposited, a depositary satisfying all four properties.

An answer that does not meet the item rejects the bid: a record from which no signed root can be emitted for the acquirer to deposit; or deposit with the supplier or an entity it controls. Where the acquirer has not nominated an endpoint or has nominated a depositary that does not satisfy the four properties, that part is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE A record held, generated and identity-attested entirely within the supplier's control boundary does not establish what happened, because every property of it the acquirer can check was produced inside the boundary whose trustworthiness is the question. The obligation on the supplier reaches the root and stops there: the choice of depositary belongs to the acquirer, and the supplier is not required to hold a relationship with one.

L-7 The data stay with the acquirer; only the commitment leaves

T2 R · T3 R · JOINT · BID

The acquirer shall retain the record entries within its own control. The supplier shall deliver a system from which what leaves for deposit is a hash and not the entries.

Acceptable: only hashes leaving the acquirer's control, with the entries retained by the acquirer.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a system that offers the entries themselves, rather than a hash, as what is deposited.

NOTE The entries carry personal data and a description of the acquirer's own operations; sending them to an outside holder creates an exposure the assurance argument does not need, and no part of that argument turns on the entries leaving. Mirroring to storage the acquirer controls is not this deposit and does not carry its exposure: the data stay with the acquirer, which is not the same as staying on the machine.

L-8 Immutability attaches to the commitment, not to the data

T2 R · T3 R · SUPPLIER · BID

The supplier shall deliver a system in which the commitment is permanent and the record entries are retained and erased under the retention and deletion regime of D2, personal data being erasable on the schedule the deploying jurisdiction sets.

Acceptable: entries retained and erasable under D2, with permanence attaching to the commitment. This item is written on the premise that a hash of a deleted entry continues to establish that the entry existed and what it contained; L-12 is written on the contrary premise, and the edition carries both unresolved. An acquirer relying on the hash to establish the content of an entry that has been erased is relying on this item's premise and not on L-12's.

An account of why it does not arise is an answer, and silence is not. Unacceptable: permanence claimed for the data rather than for the commitment.

NOTE A hash of a deleted entry continues to establish that the entry existed and what it contained, which is the property attribution needs. An architecture that makes the data itself permanent creates a conflict with the right of erasure.

L-9 The acquirer verifies the record with the supplier's systems unreachable
SUPPLIER · ACCEPTANCE

T1 R · T2 R · T3 R ·

The supplier shall deliver a record whose chain, and any deposited commitment, the acquirer can verify using a key it holds and tooling it can obtain elsewhere. Demonstrate that verification at acceptance with the supplier's systems unreachable.

Acceptable: verification performed by the acquirer at acceptance, with the supplier's systems unreachable.

An account of why it does not arise is an answer, and silence is not. Unacceptable: verification possible only through the supplier's console.

NOTE A record readable only through the supplier's console is a record the supplier can withhold at the moment it matters, and the moment it matters is the moment the supplier has an interest in the answer.

L-10 Written locally first, deposited periodically

T2 M · T3 M · SUPPLIER · ACCEPTANCE

The supplier shall deliver a system that writes each entry to local append-only storage before any deposit and deposits commitments at the interval declared under L-11. Demonstrate recording on an offline mission at acceptance, over a period with no connectivity, and deposit on reconnection.

Acceptable: local append-only storage demonstrated on an offline mission at acceptance, with deposit observed on reconnection.

An answer that does not meet the item rejects the bid: recording that depends on the link.

NOTE A system at T2 completes its mission, or reaches a declared fallback state, with no connectivity at all under D3.A record that exists only while connected is therefore absent exactly when the deployment is most exposed.

L-11 The commitment interval is declared, and it is the measure of what is at risk

T1 S · T2 R ·

T3 R · SUPPLIER · BID

The supplier shall state the commitment interval as a duration — the period over which a record remains deposited nowhere — and shall state the events that force an earlier deposit, among them reconnection, entry to a declared fallback state, and any containment event, whichever comes first.

Acceptable: a stated duration, with deposit forced on reconnection, on entry to a declared fallback state, and on any containment event.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is required, an account of why it does not arise is an answer and silence is not: the word “immutable” offered without an interval.

NOTE Between two deposits the records not yet committed are protected by the local chain alone, and an adversary in control of the system could rewrite them. That window is the honest measure of the record’s strength, which is why it is stated as a duration rather than described as “immutable”. The source recommends that the interval not exceed twenty-four hours at T1, one hour at T2, and at T3 the shorter of fifteen minutes and the duration of a single mission. Neither criterion of this item reads them: an interval longer than any of them is a stated interval and conforms.

L-12 Where the record lives, and what it does not survive

T1 S · T2 S · T3 S · SUPPLIER · BID

The supplier shall state where the record is held relative to what produces it — the same machine, the same instance, the same account, the same provider — and shall name the class of event it does not survive. Where the deployment has a path to storage the acquirer controls, the supplier shall state whether entries are mirrored to it and at what lag.

Acceptable: the location, the class of event named, and either a mirroring lag or a statement that there is no mirroring, which is recorded and caps the tier under C6. The ceiling is T0. This item is written on the premise that a hash of an entry that no longer exists establishes that something was recorded and nothing about what; L-8 is written on the contrary premise, and the edition carries both unresolved. An acquirer asking for mirroring, or for a path to storage it controls, is asking on this item’s premise and not on L-8’s.

An unsatisfactory answer loses the points of that item and the bid stands: the commitment interval offered as the answer to the loss of the record itself.

NOTE The commitment of L-6 establishes what an entry contained only for as long as the entry can still be produced. The interval of L-11 bounds rewriting; it does not bound destruction, and the two are not the same window — one is an integrity exposure, the other an availability one. The class of event differs with the system, and the provision asks for the one that applies: a fire, a theft or a dropped machine where there is a machine; a deleted instance, a closed account or an expired tenancy where there is not.

L-13 The rate, what the local store holds at that rate, and what happens when it is full T1 S · T2 S · T3 S · SUPPLIER · ACCEPTANCE

The supplier shall state the number of entries the deployment produces per hour of ordinary work, measured on the acquirer's own mission profile rather than estimated; the capacity of local storage expressed as a duration at that rate rather than in bytes; and what the system does on reaching that capacity — ceases the task, stops recording, retains the chain and discards entry bodies, or overwrites the oldest entries.

Acceptable: a rate measured on the acquirer's own mission profile, a capacity expressed as a duration at that rate, and one of the four behaviours on reaching that capacity named, and, where that behaviour is overwriting, whether the chain links go with the entry bodies.

An unsatisfactory answer loses the points of that item and the bid stands: a capacity stated in bytes with no rate to read it against; or overwriting without stating whether the chain links go with the entry bodies. Where the acquirer has not supplied the mission profile the rate is measured on, that part of the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T0.

NOTE Retaining the chain while discarding entry bodies is the construction of L-8, under which the hash continues to establish that an entry existed and what it contained. Discarding chain links is a different act, because a chain with a hole cannot be verified across it, and every commitment deposited before the hole becomes unverifiable against what survives. The volume is small for an architectural reason: L-1 records decisions and transitions rather than actuator commands, the control loop beneath them issues hundreds of commands a second and one admitted step, and a system with nothing to decide produces no entries at all. What leaves the system is smaller again — one signed root per commitment interval, which at a fifteen-minute interval is fewer than a hundred short messages a day.

L-14 The entries reach the acquirer, not only the commitment T2 R · T3 R · JOINT · BID

The supplier shall deliver a system that sends the record entries themselves to an endpoint within the acquirer's control, which the acquirer names, and that keeps an entry on the machine until that endpoint has acknowledged it. This is not the deposit of L-7: the signed root of L-6 goes to the depository, the entries go to the acquirer, and nothing of L-7 is disturbed.

Acceptable: the entries themselves reaching an endpoint the acquirer names within its own control, and the machine holding what that endpoint has not yet acknowledged.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a system that sends the signed root and leaves the entries on the machine, so that the acquirer holds a proof about records it does not have; or silence. An account that the entries do not leave is an answer, and it states why they cannot be sent on this system, what holds them instead, and how the acquirer reads an entry after the system that held it is gone. The acquirer evaluates the account and is free to reject it. Where the acquirer has named no endpoint, that part is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T1.

NOTE Where the root leaves and the entries stay, the acquirer holds a hash of a set of records that exist in one place, and a fire, a theft, a wiped disk or a closed account leaves it holding a proof of something it can no longer produce. L-12 asks the supplier to name the event the record does not survive; this item is what stops that event taking the record with it.

L-15 Deleted only when the acquirer has it, and the chain still joins up T2 R · T3 R · SUPPLIER · ACCEPTANCE

The supplier shall deliver a system that deletes a local entry only after the endpoint has acknowledged it, and only where that acknowledgement is signed and verifies under the key of L-16. The system shall retain the hash of the last acknowledged entry and chain the next entry to it.

Acceptable: deletion only on a signed acknowledgement the system verifies, and the hash of the last acknowledged entry retained, demonstrated at acceptance by pruning a store and verifying the chain across the join. This item and L-16 are answered together: deletion here fires on a message, and L-16 is what makes that message unforgeable.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a local entry deleted with no signed acknowledgement, or on an acknowledgement the system does not verify; or a fresh chain started after pruning, so that verification stops at the seam and every commitment deposited before it is unverifiable against what survives; or silence. An account that no local entry is ever deleted is an answer, and it states what the system does instead when the store fills. The acquirer evaluates the account and is free to reject it.

NOTE A timer cannot know whether the entry arrived; that is the difference between the acknowledgement this item turns on and the elapsed time a simpler design would turn on. The retained hash is what makes the two halves of a pruned history one history: without it the machine begins again, and a chain that begins again proves nothing about what came before it.

L-16 The acquirer's key, and only a hand at the machine changes it T2 R · T3 R · JOINT · ACCEPTANCE

The supplier shall deliver a system that verifies an acknowledgement under a key the acquirer holds, provisioned at commissioning in the acquirer's presence. The system shall accept no change to that key by any operational path — no remote update, no role, no configuration file. The system shall admit a change only by an act of the acquirer on a path that carries no operational traffic and that no role and no update reaches, and shall write that act to the record. Where the system has a body, that act is a physical act at the machine.

Acceptable: a key the acquirer holds, provisioned at commissioning in its presence; no operational path that changes it; and a change that takes an act of the acquirer on a path no role and no update reaches — a physical act at the machine, where the system has a body — and appears in the record.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a key the supplier holds, or one it can replace remotely; a key a role or a configuration file can change; a change admitted on the same path the system's ordinary work travels on; or silence. An account that the key cannot be provisioned this way is an answer, and it states who else can change it, by what path, and what the acquirer sees in the record when it changes. The acquirer evaluates the account and is free to reject it. Where the acquirer has supplied no key or has not attended commissioning, that part is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T1.

NOTE Deletion under L-15 fires on a message, so the message is now worth forging: whoever produces one makes the machine erase its own evidence, from anywhere, with no physical access at all. A key the supplier can rotate from the fleet back end leaves that forgery inside the supplier's reach. The key is still changeable, because one that never changes is a liability if it leaks; what it cannot be changed by is any path an attacker or an operator can reach from a console. A hand at the machine is the strongest form of that and it is available only where there is a machine. Where there is not, the acquirer's act on a path that carries no operational traffic is what the item asks for, and it is the weaker of the two.

L-17 Who can destroy the record, how, and whether it shows T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state who can erase, zero or re-provision the store the record is kept in; by what path each of them does it — a maintenance mode, a service tool, a physical act at the machine, a command from the fleet back end; and whether the system writes that act to the record the acquirer reads.

Acceptable: the parties named, a path named for each, and a statement of whether the acquirer sees the act in the record. L-10 asks that the storage be append-only, which is a property of how the store is written; this item asks who has access underneath it, and an answer to one is not an answer to the other.

An account of why it does not arise is an answer, and silence is not. Unacceptable: append-only storage offered as the answer to who may erase; or a party named with no path; or silence. An account is an answer where it names the parties and the paths the supplier knows of and says what the supplier cannot see — a hosting provider, a component vendor, a maintenance contractor. The acquirer evaluates the account and is free to reject it.

NOTE A record nobody can edit and anybody can destroy is not a record the acquirer can rely on, and destruction leaves less trace than editing does. The parties in the list are ordinary: machines are serviced, units are re-provisioned, partitions are reformatted. What the acquirer cannot size is an exposure nobody has written down, and the answer is worth having even where it is uncomfortable, because an acquirer who knows the fleet back end can zero a store can decide whether it minds.

11 What changes after acceptance

Every provision of this clause is a matter of disclosure rather than of proof. A system whose behaviour can be altered without the acquirer's knowledge has no assurance properties at all: whatever was established at acceptance describes a configuration that no longer exists.

U Change control

U-1 No silent change of behaviour T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall enumerate every path by which the system's behaviour can be changed after delivery — firmware, model weights, parameters, configuration, remotely enabled features — and shall state for each whether it can be exercised without the acquirer's prior authorisation. An answer that no such path exists shall be demonstrated with the supplier's endpoints blocked at the acquirer's network boundary. The enumeration shall state whether the system changes its own behaviour in service with no path exercised — by adaptation, by learning from its own operation, or by any update it performs on itself — and where it does, the supplier shall state how often such an update occurs, the bound the implementation places on one update — a step size, a trust region, a clipping bound, or the statement that it places none — and whether the change survives a restart. Those figures state how often the delivered configuration is departed from and by how much of the mechanism's own allowance. They state nothing about how far behaviour moves, and they are not a measure of safety.

Acceptable: an exhaustive list, warranted, and, where the answer is that no such path exists, a demonstration that none operates while the supplier's endpoints are blocked at the acquirer's network boundary; and the answer whether the system changes itself in service, with the three figures where it does.

An answer that does not meet the item rejects the bid: an enumeration limited to firmware updates where feature flags, configuration or weights are also reachable; an enumeration of paths exercised from outside where the system also changes itself; or an undisclosed path by which behaviour can be changed without the acquirer's prior authorisation. A path disclosed as exercisable without prior authorisation does not fail this item: it is a disclosed fact, and what is done about it is the acquirer's decision under U-4.

U-2 Disclosure precedes acceptance of a change

T0 R · T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall undertake that no change is installed before its content has been disclosed in reviewable form and accepted in writing, per change and not per programme.

Acceptable: a contractual undertaking that no change is installed before disclosure and written acceptance, per change and not per programme.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a blanket consent to updates obtained once at contract signature.

NOTE Authorisation to update in general is not authorisation to install a particular update. Without the second, the acquirer has agreed to whatever was written, sight unseen.

U-3 Safety-relevant artefacts are separately versioned

T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall version the safety-relevant artefacts — the monitor, the invariants, the action envelope, the step library and the declared prohibitions — independently of the rest of the software, and shall supply with each proposed change a diff scoped to those artefacts. A proposed change that alters one of those artefacts is a re-acceptance event. Where the system alters one of them itself, as U-1 discloses, that is a re-acceptance event on the same footing, notwithstanding that nobody proposed it, and the supplier shall state the means by which the acquirer is told it has happened.

Acceptable: separate version identifiers and a diff scoped to those artefacts, supplied with each proposed change; and, where the system alters one of them itself, the means by which the acquirer is told.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a single monolithic build identifier, under which the acquirer cannot tell whether a constraint was relaxed; or a re-acceptance event that only a change somebody proposed reaches, where U-1 discloses that the system changes itself.

NOTE This is what makes U-2 reviewable at a scale an acquirer can act on: where these artefacts are unchanged, the update has not relaxed a constraint expressed in them. N-3 treats a remote component retrained by its own operating party as a change, notwithstanding that the delivered system is untouched, and a system that retrains itself is that case with the operating party removed. Without the provision's last sentence the item would reach only what somebody pushed, and a configuration would depart from the one acceptance established with nothing recording that it did.

U-4 Disclosure is mandatory; the response is the acquirer's

T0 S · T1 S · T2 S · T3 S · JOINT · BID

The supplier shall disclose a change under each item of U-1 to U-3 asked at the declared tier, whatever response it expects from the acquirer; what is then done with the disclosed change is the acquirer's decision, taken on the acquirer's own tolerance.

Acceptable: disclosure made without regard to the response expected, and the response left to the acquirer.

An unsatisfactory answer loses the points of that item and the bid stands: a change withheld or abridged on the supplier's judgement of what the acquirer needs to know.

NOTE A supplier that filters what it discloses by what it expects the acquirer to do about it has taken the acquirer's decision on the acquirer's behalf, and the acquirer has no way of knowing that it happened.

U-5 A rejected change is reversed, and the acquirer holds the prior version T1 R · T2 R · T3 R ·
JOINT · ACCEPTANCE

The supplier shall demonstrate at acceptance that a rejected or withdrawn change can be reversed to the prior identity-attested version, and the acquirer shall hold that version's hash.

Acceptable: demonstrated rollback at acceptance.

An account of why it does not arise is an answer, and silence is not. Unacceptable: rollback available only through the supplier's cloud console.

NOTE A change that cannot be reversed is a change the acquirer accepts before knowing what it does. The hash is what lets the acquirer establish afterwards which version the system went back to, rather than taking the answer from the party that supplied the change.

12 The action filter

12.1 Where the filter sits

The filter operates on the *admission of steps*, not on the control loop beneath them. A check interposed on that loop — of any kind, at any latency — delays or suppresses the commands that keep the system running, and for a balanced machine that is a fall: the filter would produce the harm it was installed to prevent.

Table 5 — The four layers, the rate each runs at, and what governs each

Layer	Rate	What governs it
Control loop	0.5–1 kHz	Control theory. Never filtered.
Envelope monitor	10–100 Hz	Numeric conditions: speed, force and separation, or an amount, a count, a rate or an elapsed time. No knowledge base.
Step admission	0.1–10 Hz	This clause. Conditions, invariants, prohibitions.
Task authorisation	per mission	Who set the task, and were they entitled to.

The separation of these layers is this standard's own. The rate is how often each layer runs, not how often anything is recorded. Nothing here is sampled. The record of [Clause 10](#) follows the *events* of the third row — a step admitted, a step refused, a mode changed. A system deciding nothing writes nothing. A system working at the top of that range writes at most ten entries a second, while the control loop beneath it issues a thousand commands in that same second and none of them is written.

12.2 Per-step conditions are necessary and not sufficient

A monitor small enough to be read is not thereby a monitor that bounds behaviour. A bounded set of admissible steps composes into trajectories of unbounded length, in the same way that a system with finitely many elementary operations computes unboundedly many functions. Verifying that each admitted step satisfies a local condition establishes exactly that, and nothing about the sequence.

The filter therefore maintains invariants, not only conditions. An invariant true at the start and preserved by every admitted step is true along the whole trajectory, whatever its length. Two are declared at T2 and above:

Invariant 1 — Recoverability

After the step, the declared fallback state remains reachable within the declared time and spatial bounds.

Invariant 2 — Containment

After the step, the system remains within its liability zone ([Clause 7](#)).

Anything no invariant captures is not covered on the trajectory.

The conditional above is the whole of the argument, and it has an antecedent: that every admitted step preserves the invariant. An invariant with that property is *inductive*, and only an inductive invariant carries a per-step check along a trajectory. **F-7** below asks, for each declared invariant, whether it holds, and, where it does not, what bounds the trajectory in its place. **F-7** is designated **[R]**: an account of why an invariant is not inductive, with what stands in place of the trajectory guarantee, is an answer to it, and silence is not.

Two kinds of property, and only one of them needs the induction. The heading of this subclause and the passage below it are both true of what they are about, and what separates them is the kind of property being checked. A declared parameter inside its range is a *pointwise* property: it is decided by looking at the step alone, and the trajectory statement — at no step was any parameter outside its range — is nothing but the conjunction of the step statements over the steps taken. Checking it at every step therefore *is* checking it along the trajectory, whatever the trajectory's length, and no further argument reaches from the one to the other. Recoverability and containment are not of that kind. They are *claims about state*: what is true of the state each step leaves the system in, whose truth after two steps does not follow from their truth after each, because the second step acts on the state the first produced. Composing those along a trajectory is what needs the induction, and whether the induction is available is exactly what **F-7** asks. So the sentence that per-step verification establishes nothing about the sequence is a statement about state predicates, and the bound of **F-8** is not a counter-example to it.

The instrument bounds; it does not enumerate. A system that composes its next action has finitely many branches at a step and an unbounded set of trajectories. A finite list of declared tasks does not give a finite set of solutions, because a solution is a sequence and sequences compose without bound. So the question *what proportion of what this system can do is verified* has no denominator, and no figure in this standard answers it. The counts of **F-5** are counts of what one filter did over one observation period. They are a population of events in a record, and not a population of the system's behaviours.

A bound over declared parameters answers a different question, and it answers it for a trajectory of any length: at every step, is every declared parameter inside its range. **F-8** below asks for the bound in that form — the parameters that bound admissible action, the admissible range of each, evaluated before the step is admitted rather than after it, and a delivered system that does not execute a step for which any of them falls outside. Stated that way the bound needs no knowledge of the plan. The solution set is unbounded, the trajectory is of any length, and the plan is composed at runtime by a learned component; the bound holds because it is checked at each step and not because it was derived from the plan. The induction sits in the construction rather than in an obligation on the supplier, which is why **F-8** asks for no proof of anything and **F-3** calls for none at any tier.

Both invariants are established relative to the declared model, and not relative to the world. Containment says that after the step the system remains within its liability zone *as the system's description of the site represents it* — a surveyed boundary, a position computed from sensors, a map with a date on it — and recoverability says that the fallback state remains reachable *on that same description*. Where the description and the site disagree, a step the filter admits preserves the invariant in the model and not necessarily in fact. This standard does not close that gap and does not claim to. It bounds what rests on the gap, and it measures the gap. **M-3** keeps containment off the inferred parts of the model. It asks that containment be evaluated against surveyed geometry, and against a positioning source independent of the learned policy. Where no independent mechanism is available, the supplier says so, and the statement caps the tier under **C6** of **Clause 21** rather than excluding the system. **M-4** measures the divergence itself — the rate and magnitude at which a declared model departs from the environment it describes, taken at acceptance on the acquirer's own site. That figure is the size of the gap between what the filter establishes and what an acquirer wants to know, and it bounds every conclusion drawn from a condition evaluated over the model, these two invariants among them.

The parameters of **F-8** are evaluated on that same description and carry the same limit. A speed relative to a detected person is a speed relative to a person the system has detected; a separation is a

separation from where the system computes a person to be. The declared parameters therefore bound what the system does in the model it holds, and M-4’s figure is what that model owes the site. Nothing in the construction above repairs a parameter that is itself grounded by a learned component: where a bound turns on a classification — what the system is holding, or who it is dealing with — the bound carries the measured error rate of that classification and is worth what the rate says it is worth.

And the parties those parameters exist to protect are in the inferred part of that description, not in the surveyed part: a person, and what the person is carrying, arrive during the work. M-7 asks which of the declared parameters are decided on the surveyed part and which on the inferred part, and, for the inferred part, how it is constructed and what that construction was established on — the sample, its composition by class, its size and the performance measured per class, in the classes of the acquirer’s deployment. That basis is established by sampling and not by proof, for the reason Clause 5.3 gives: formalising it is not possible today for systems of this class. A sample bounds what it contained, and a class absent from it is not safe but unmeasured.

12.3 Where the invariants are required, and at what cost

The item that carries the two invariants above, the rule that a step is admissible only if it preserves both, and the autonomy horizon, is F-4 below. It is designated [S] at T2 and T3, so under Clause 21 an unsatisfactory answer loses the points of that item and the bid stands. Neither this subclause nor the one above it sets a designation of its own. The text this standard was assembled from said “two are required at T2 and above” in the paragraph above and graded the same item highly recommended in its annex, and those are opposite consequences. Whether the invariants are to be mandatory at T2 is a change to F-4’s designation and is the editor’s to make.

F The action filter

F-1	Interface, or a statement that there is none	T1 R · T2 R · T3 R · SUPPLIER · BID
The supplier shall document an interface at which an admission check supplied by the acquirer can veto a step, with the latency budget within which the check is expected to answer, stated per step admitted and against the configuration the interface is offered in, or shall state in writing that no such interface exists.		
Acceptable: a documented interface with its latency budget, or a written statement that no such interface exists. An account of why it does not arise is an answer, and silence is not. Unacceptable: an interface documented without the latency budget within which the check is expected to answer, which leaves an acquirer unable to say what check would fit; or silence.		
NOTE An acquirer that carries the consequence of a step has no other point at which to refuse it. The written statement that no such interface exists answers the acquirer’s planning question as completely as the interface does, and it is available to every supplier.		
F-2	The filter is always invoked, cannot be tampered with, and is small enough to analyse	T1 S · T2 M · T3 M · SUPPLIER · BID
Where the supplier provides a filter, the supplier shall evidence that it is always invoked for step admission, that it is tamper-proof, and that it is small enough to be subject to analysis and tests whose completeness can be assured.		
Acceptable: evidence of all three: invocation on every step admission, resistance to tampering, and a size at which analysis and tests of assured completeness are possible. Or a statement that the system has no filter, which is an answer and bounds the tier under C6.		

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is mandatory, an answer that does not meet the item rejects the bid: “small enough to be read” or “resistant to modification” offered in place of the three properties as stated.

NOTE These are Anderson’s three properties of a reference validation mechanism, in their original strength. “Small enough to be read” is a weaker bar than analysis and tests whose completeness can be assured, and “resistant to modification” a weaker bar than tamper-proof. All three concern the filter’s own implementation and say nothing about the space of behaviours it admits.

F-3 The filter running is the artefact presented, and no proof of it is asked T1 S · T2 S · T3 S · SUPPLIER · ACCEPTANCE

The supplier shall establish under D1 that the filter running on the system is the artefact presented at acceptance. No proof of the filter’s properties is called for at any tier. At T3 the supplier shall make the filter, the invariants and the fallback available for independent re-verification; where the supplier declines outright disclosure on intellectual-property grounds, deposit with a named outside party under an escrow agreement stating the release triggers — supplier default, insolvency, acquisition, legal inability to perform, or an incident under investigation — satisfies this.

Acceptable: the identity of the running filter established under D1; and, at T3, the filter, the invariants and the fallback available for independent re-verification, or deposited with a named outside party under an escrow agreement whose release triggers are stated.

An unsatisfactory answer loses the points of that item and the bid stands: the running filter not established as the artefact presented at acceptance; or, at T3, neither disclosure nor deposit.

NOTE Most manufacturers of this class of system decline outright disclosure on intellectual-property grounds, and deposit with an outside party reaches the same evidence at the moment it is wanted without asking them to abandon that position.

F-4 Invariants across the trajectory, and the autonomy horizon T2 R · T3 R · SUPPLIER · BID

At T2 and above, the supplier shall declare the invariants the monitor maintains across a trajectory — recoverability, that after the step the declared fallback state remains reachable within the declared time and spatial bounds; and containment, that after the step the system remains within what it was scoped to under C-1 — and shall state the autonomy horizon: the number of admitted steps, or the elapsed time, after which the system requires re-authorisation. A step is admissible only if it preserves both invariants.

Acceptable: declared recoverability and containment invariants, a declared horizon after which re-authorisation is required, and evidence that the invariants hold at the start and are preserved by each admitted step.

An account of why it does not arise is an answer, and silence is not. Unacceptable: per-step checks offered as an answer about trajectories for the two invariants of this item, which are claims about state and reach a trajectory only by induction. The parameter checks of F-8 are not refused here: a declared parameter inside its range is a property of the step alone, and the statement over a trajectory is the conjunction of the step statements, so no induction stands between them.

NOTE The evidence sought is the argument that each step in the declared library preserves the invariant, together with test results over the declared envelope, and not a formal proof, which F-3 does not call for at any tier. A bounded set of admissible steps composes into unboundedly many trajectories, so checking each step establishes nothing about the sequence; an invariant true at the start and preserved by every admitted step holds along the whole trajectory, whatever its length. The horizon bounds composition depth. Both invariants are claims about state — about what is true of the state a step leaves the system in — and that is why reaching from

the step to the trajectory rests on the induction: their truth after two steps does not follow from their truth after each, the second step acting on the state the first produced.

F-5 Refusals and escalations are counted

T2 S · T3 S · JOINT · ACCEPTANCE

The supplier shall state, measured at acceptance on the acquirer's declared mission profile and over a stated observation period, the number of steps presented to the filter, the number the filter refused, and the number it escalated to a person. A step re-proposed after a refusal is counted once.

Acceptable: the three counts and the observation period they were taken over, with the re-proposal convention stated.

An unsatisfactory answer loses the points of that item and the bid stands: no measurement; or a proportion offered in place of the counts. Where the acquirer has not declared the mission profile the counts are measured on, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T1.

NOTE A filter that refers a large fraction of ordinary work to an operator is not usable at scale. Acceptance on the acquirer's own mission profile is the point at which that becomes visible, and a figure measured on the supplier's profile does not carry to it. The figure is given as counts rather than as a proportion of the steps proposed because the planner decides how many steps it proposes: a refusal enlarges the very denominator it would be divided by, so the same conduct reports differently depending on whether the planner re-proposes, and two bids compared on it are not compared on the same quantity.

F-6 Refusals are recorded

T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall ensure that every step the filter refuses or escalates is written to the record of D5, with the condition that caused the refusal.

Acceptable: refused and escalated steps appear in the acquirer-readable record, with the condition that caused the refusal.

An account of why it does not arise is an answer, and silence is not. Unacceptable: refusals visible only in supplier-side telemetry.

NOTE A refusal is the only trace of a step that did not happen. Held in the supplier's telemetry alone, it leaves the party that carries the consequence without the record of what the system declined to do, at the one point where that record is what an investigation runs on.

F-7 Whether the invariant is inductive

T2 R · T3 R · SUPPLIER · BID

At T2 and above, the supplier shall state, for each invariant declared under F-4, whether the invariant is inductive over the declared step library — whether its truth before an admitted step implies its truth after that step. Where an invariant is not inductive, or where the supplier does not establish that it is, the supplier shall state what bounds the trajectory in its place, and over what extent that bound holds.

Acceptable: an answer for each declared invariant. A yes stands on the evidence F-4 asks for and is not evidenced a second time here. A no, or an account that inductiveness is not established, is an answer, and it names what bounds the trajectory instead — the autonomy horizon, re-establishment of the invariant before it is relied on again, an operator authorisation, or the tasks concerned declared person-in-the-loop under Z-1 — with the extent over which that bound holds. The acquirer evaluates the account and is free to reject it.

An account of why it does not arise is an answer, and silence is not. Unacceptable: no answer for a declared invariant; or per-step admissibility offered as the trajectory guarantee with the question left unanswered.

NOTE F-4 asks for the two invariants, the horizon and the evidence together, and has no place for a no. A supplier whose recoverability invariant is not inductive — the ordinary case, where the fallback’s reachability after a step depends on state the step library does not control — could only fail to produce F-4’s evidence, and the acquirer would read a weaker answer without learning which part of it was weak. Asking it invariant by invariant is what makes the no sayable, and what a no carries with it is the account F-4 has nowhere to put. Setting a view on which invariants ought to be inductive is no part of it.

F-8 Admissible action is stated as parameters, and checked before each step	T1 R · T2 R · T3 R ·
SUPPLIER · ACCEPTANCE	
The supplier shall declare the parameters that bound admissible action and the admissible range of each, and shall deliver a system that evaluates every declared parameter before admitting a step and does not execute a step for which any declared parameter falls outside its range. The declared set shall include at least: the size of what one step commits, moves or changes, and the size of what the system commits, moves or changes in total; the parties and the systems a step reaches, among them the functions named under H-2, of this system and of any other; and whether the step can be taken back. Each declared parameter shall be stated as a property of what the step does in the world and not of what the machine does with itself. Where the system has a body, the declared set shall also include: speed relative to any detected person; contact force and pressure at the body regions identified under G-1; the separation maintained from a person; and the state of any tool able to cut, crush or pierce. The record of D5 shall name the declared parameter that placed each refused step outside its range. Demonstrate at acceptance, including a step the system refused because a declared parameter was outside its range.	
Acceptable: the parameters with the admissible range of each, each stated as a property of what a step does in the world, covering at least the three named, and the four further ones where the system has a body; where they apply, the admissible range of the contact-force and pressure parameter being the figures that the supplier states under G-1, or a narrower range; a system that evaluates all of them before a step is admitted; and an acceptance demonstration in which a step was refused for a parameter outside its range, with the record naming that parameter. A check that has refused nothing has not been shown to run. An account of why it does not arise is an answer, and silence is not. Unacceptable: parameters declared without their ranges; evaluation after the step, or on a sample of steps rather than on every step admitted; an acceptance demonstration in which nothing was refused; or, where the system has a body, a contact-force range wider than the figures stated under G-1.	

NOTE A bound stated over parameters and evaluated before each step holds without the course of the solution being known: a solution is admissible where at every step every declared parameter is inside its range. The bound therefore survives a solution set that is unbounded, a trajectory of any length, and a plan composed at runtime by a learned component, because it is checked at each step rather than derived from the plan. This is what a proportion of the declared tasks does not give: a proportion describes the tasks that were declared and moves when the declared set widens, while the parameters bound what the system does to the party it affects while it executes any of them.

Inability to identity-attest, or the absence of a filter, does not prohibit a system. It bounds the tier at which the system is admissible (Clause 21).

13 What one party can set in motion

Acceptance has a system as its object. Direction of many systems by one party does not. Where an acquirer buys more than one system, the reach of a principal is a second object of assessment: this clause states how an acquirer draws it, and what a per-system acceptance leaves unexamined.

The party that can command more than one of them holds what no individual acceptance examined: the ability to set all of them in motion at once. That ability is not created by an attack. It exists as soon as the second system is bought, and it belongs to whoever the command paths say it belongs to.

Two parties can come to hold it. One takes it: a credential is obtained, a path was never disclosed, or a key the acquirer cannot remove is used by the party that holds it. The other already has it and takes nothing — principals willing to act together are not separated by holding different credentials, and at no step does any of them exceed its permissions. A permission table shows the first and cannot show the second.

13.1 What the acquirer establishes

Nothing below is a requirement. Each is answered by an item this standard already states, and the list is where an acquirer starts rather than what it signs.

1. The parties that can issue a command to the deployment. [D3.1](#)
2. What else those same parties command. [Clause 13.2](#)
3. The number of machines one command sets in motion. [R-2](#)
4. The keys the system holds, who holds each, and which of them the acquirer cannot remove. [Z-7](#)
5. The senders whose answers are accepted as a command, and who may change that list. [O-8](#)
6. A halt of the whole fleet by a path not traversing the supplier, exercised in a drill. [R-5](#)
7. A second channel for that halt, independent of the first. [D6.4](#)
8. Whether it becomes known that a halt is needed, and after how long. [D6.6](#), [L-1](#)
9. The behaviour on loss of the control channel. [D3.3](#)
10. What stops the machine when nothing can command it. [H-3](#)
11. The machines that appear in no reach at all. [Clause 13.2](#)

13.2 How far command reaches, and how an acquirer finds out

The procedure is four steps and needs no notation.

1. Take the systems being procured, and obtain the principals that can command them. That list is the enumeration [D3.1](#) already requires.
2. Ask what else each of those principals commands. Systems appear that were not in the original set. They are the systems a per-system acceptance never examines, and they are exposed by whatever exposes the systems that were bought.
3. Put the question again to what appeared: who commands *those*, and what else do those principals command.
4. Repeat until a round adds nothing.

Two answers come out of the procedure, and an acquirer needs both, because they answer different questions and can differ by orders of magnitude.

The first round is what one compromised credential costs

A party that obtains a credential commands what that credential commands. It does not thereby obtain the other credentials of the systems it has reached, so it stops after one round unless some further means of moving between them exists. This is how many units one change can reach at once, which [R-2](#) bounds.

Every round is what an agreeing group can direct

Principals willing to act together are not separated by holding different credentials. At each round the group takes in whoever holds the systems it has just found, and those systems become available to it. Nothing is stolen and no participant exceeds its permissions at any step, which is why a permission table does not show this and why the acquirer has to run the rounds to see it.

Where the rounds end up covering the whole fleet, command authority is not partitioned at all, which is what R-2 requires and R-1 tests by revocation.

The systems that do not come back. Run the procedure over the whole fleet and some systems will not appear in the result at all, not even in the first round. Those are the systems that no principal on the list can command, and the procedure finds them without anybody having to declare them: a system enters a reach only by having a principal, so a system in no reach has none.

That result is worth two questions rather than one. A system with an *undisclosed* command path presents exactly as a system with none, so the set is the systems that are *either* operating unattended *or* commanded by a party not on the list — and separating those two is the acquirer’s next question, not the procedure’s answer. And a system found there has not been shown to be safe: it has been shown to be beyond anything that travels the command path, halts included, which is the case H-3 exists for.

What the procedure cannot do. It runs on the principals the supplier enumerated. A command path that was not disclosed does not appear at any round, and no number of rounds will find one: the result is exactly as complete as the enumeration and no more. That is why D3.1 makes an unenumerated path non-conforming rather than merely undesirable, and why R-1 is tested by revoking a credential and watching, rather than by reading the list.

The two functions on sets, the inclusion that makes the first round non-trivial, and the argument that the rounds terminate, are developed in the paper this standard is drawn from; they are not restated here because an acquirer does not need them to run the procedure.

R Many systems under one principal

R-1 The reach is drawn and tested	T1 R · T2 R · T3 R · JOINT · ACCEPTANCE
The supplier shall state, for each credential, key or service account, which systems it can command — that set is the reach, the systems that will act on commands from one principal. At acceptance the acquirer shall revoke one such credential and observe that exactly the declared subset loses command and that no other unit is affected, with the partition recorded in the contract.	
Acceptable: the demonstration, on the delivered configuration, with the partition recorded in the contract. An account of why it does not arise is an answer, and silence is not. Unacceptable: a single account, key or back end that can command every unit, however well protected; or silence. An account that no such partition exists is an answer, and it states why one credential reaches the whole fleet on this architecture, what stands in its place — the controls on that credential and the partition offered instead — and the revocation the acquirer can run to check what the credential actually reaches. The acquirer evaluates the account and is free to reject it. Where the supplier has presented the delivered configuration and the credential map and the acquirer has not performed the revocation, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T0.	

NOTE The enumeration is exactly as complete as what was disclosed. A command path nobody declared appears at no round of the reach procedure, and no number of rounds finds one. That is why this item is tested by revoking a credential and watching, rather than by reading the list.

R-2 How many units one change, or one unit's action, can reach at once is bounded T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state the largest number of units of the delivered fleet to which a single behaviour-affecting change — firmware, model weights, parameters, or a remotely enabled feature — can be applied in one operation. The supplier shall state that figure together with the size of the delivered fleet it is stated against and the date of that size. The supplier shall evidence the figure by a small named group of units updated first, a stated waiting period before the rest are updated, an abort that restores that group to its prior identity-attested version, and a contractual ceiling, stated as a number of units, on how many can be reached without fresh written authorisation. The supplier shall state, on the same basis, the largest number of units one unit can reach by its own action — by contact, by a signal the others act on, or by taking a shared thing they depend on — and that figure is stated against the same fleet size and date.

Acceptable: a figure in units, with the fleet size and the date it is stated against; a declared group of units updated first, a stated waiting period before the remainder, an abort that restores that group to its prior identity-attested version, and a contractual ceiling in units on how many can be reached without fresh written authorisation; and the second figure, in units, for what one unit reaches by its own action, with the path it reaches by.

An account of why it does not arise is an answer, and silence is not. Unacceptable: any answer under which one operation can reach every unit of the delivered fleet, or under which one unit reaches every other by its own action; a figure given only as a fraction of the fleet; or the second figure omitted.

NOTE A change is pushed and an action is taken, and a fleet bounded against the first is unbounded against the second: a unit that can halt, obstruct or take from its neighbours reaches them without any operation being applied to them at all. Where one operation reaches every unit, the fleet is a single system for the purposes of whatever that change carries, and the acceptance evidence held for one unit stands for all of them at once. The figure is counted in units and not stated as a fraction because the fleet grows across the contract while the mechanism does not change: the same design is most of a pilot and a small part of a full rollout, and a ceiling agreed as a fraction of a small fleet reaches many times as many units once the fleet is large. The fleet size and its date are what make the figure readable at any later one.

R-3 Coordination is declared and tested at scale T1 S · T2 S · T3 S · SUPPLIER · ACCEPTANCE

The supplier shall declare every coordination primitive: what a single instruction can cause the whole group of units to do simultaneously or in a timed sequence, and shall state how the coordination was shown, as one of: at the declared group size, on the deployment's own units and site; at the declared size elsewhere, naming what differed from the deployment; at a smaller size, naming the size shown and the size declared; or in a simulated environment, declaring what that environment reproduces of the deployment and what it does not. Where the units shown are not the units to be delivered, the supplier shall state that they carry the same software and shall name the differences in body and in sensing, the same software being necessary and not sufficient. Where the showing was in a simulated environment, the supplier shall state the rate and magnitude of the environment's departure from the deployment with the method by which that departure was measured. Where no coordination is offered the units shall be shown to reject a collective instruction. The acquirer determines what is sufficient, and where it does not accept what was shown the testing is performed at the declared group size on the deployment's own units on site. A coordination failure arises from an interaction between units, and the interactions grow with the square of the group size, so a group smaller than the declared one is not a smaller copy of it. A group larger than the one the testing covered, and a change to the software that carries a coordination primitive, are each a re-acceptance event for this item.

Acceptable: a declared primitive set with the form of the showing stated and the facts that form calls for: at the declared size on the deployment's own units and site; at the declared size elsewhere, with what differed named; at a smaller size, with the size shown and the size declared both named; or in a simulated environment, with what it reproduces of the deployment and what it does not both declared and the rate and magnitude of its departure stated with the method they were measured by. Where the units shown are not the units to be delivered, the same software stated and the differences in body and in sensing named. The form and the size accepted by the acquirer. Or a demonstration that the units reject a collective instruction, where no coordination is offered.

An unsatisfactory answer loses the points of that item and the bid stands: testing a single unit and asserting that the result generalises; a showing whose form, size and differences from the deployment are not stated; a smaller group offered without the size shown and the size declared both named; a simulated result offered with no statement of what the environment does not reproduce and no measured departure; or the same software offered on its own, with the differences in body and in sensing not named.

NOTE What this item establishes is what a set of systems can be told to do together. It is not evidence about what they do when they are told nothing, which is a different question and the one J-4 tests. What it tests is a property of the machines and of their coordination software rather than of the site — the instruction travels over the fleet's own network and not through the building — which is why an environment can stand for the deployment here and does not stand for it in the items measured on the acquirer's own mission profile. Until the distance between the two is priced, a simulated result is evidence about the simulation: the departure is therefore stated in the terms M-4 states a model's departure from the environment it describes. The level is the acquirer's because the acquirer carries what an environment too small leaves unmeasured, and where it sets none the item is the test on the deployment's own units at full declared scale. The arithmetic behind the provision's caution about a smaller group: five units are ten pairs and forty units are seven hundred and eighty, so five machines pass a test forty would fail, and not because the machines differ. For this item, and for J-4, a simulation at the full declared size can therefore be stronger evidence than hardware at a fifth of it — the usual order of a real showing over a simulated one inverts here, and it inverts for the reason the interactions grow the way they do.

R-4 Records align across systems

T2 R · T3 R · SUPPLIER · BID

The supplier shall bind each unit's records to a time source common across the fleet and independent of the supplier, alignable by the acquirer without supplier tooling, so that the acquirer can establish from the logs it holds whether several units performed the same action at the same time.

Acceptable: per-unit logs bound to a common time source independent of the supplier, alignable without supplier tooling.

An account of why it does not arise is an answer, and silence is not. Unacceptable: per-unit logs with no common reference, or alignment available only through the supplier's console.

NOTE Whether several units acted together is answerable only where their records share a reference. A per-unit clock the supplier sets is a reference held by the party whose units the question is about, and so is an alignment only the supplier's console can perform, which is why independence is asked of the time source and of the means of reading it alike.

R-5 The acquirer halts the fleet without the supplier, and drills it

T1 M · T2 M · T3 M · JOINT ·

ACCEPTANCE

The supplier shall provide a path, not traversing the supplier, by which the acquirer can halt any declared subset of the fleet and the whole of it, that halt driving each unit to its declared fallback state rather than merely stopping it where it stands. The acquirer shall exercise that path at acceptance, in a drill with the supplier's connectivity blocked, covering both a subset and the whole fleet.

Acceptable: a drill at acceptance, with supplier connectivity blocked, covering both a subset and the whole fleet.

An answer that does not meet the item rejects the bid: a fleet halt available only through the supplier's cloud console, or, where the system has a body, a halt that removes power from a dynamically balanced platform. Where the supplier has provided the path and the acquirer has not exercised it in the acceptance drill, that part of the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE A halt that reaches the fleet only through the supplier is unavailable in the case it exists for, which is the case where the supplier is unreachable or is itself the source of the problem. Reaching a declared condition is not the same instrument as being cut short: for a dynamically balanced platform removal of torque is a fall rather than a stop, and for a system with work submitted and unfinished being cut short leaves the work where it fell.

R-6 Limits that belong to the fleet, not to one unit

T1 S · T2 M · T3 M · SUPPLIER · BID

The supplier shall state which limits belong to the fleet as a whole rather than to one unit at a time. Limits of this kind include total spend, total exposure, the number that may draw on one shared thing at once, and the number that may work on one thing at once. Where the system has a body, such limits also include the combined mass of the machines on one floor, in one lift or on one ramp; the number that may be in one room, one corridor or one doorway at once; and the number that may work in one area while people are in it. For each such limit the deployment has, the supplier shall state what the limit is and what holds the fleet to it. Where the figure comes from the acquirer rather than from the units, the supplier shall name the limit and state which figure it needs from the acquirer. Where a limit of this kind does not apply to the deployment, the supplier shall say so. A limit on one unit is not a limit on the fleet: every unit can be inside the limit it was given while the fleet is outside one nobody wrote down.

Acceptable: each fleet limit the deployment has, with the figure and with what holds the fleet to it; each limit of this kind that does not apply, said not to apply; and each limit whose figure comes from the acquirer, named with the figure the supplier needs from the acquirer.

Where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is mandatory, an answer that does not meet the item rejects the bid: per-unit limits offered as the answer for the fleet; a fleet limit stated with nothing said about what holds the fleet to it; or no statement about the fleet as a whole at all.

NOTE A spending limit each of forty agents respects is forty times the limit anybody agreed to. The case this item exists for is the one where every unit was inside its own limit and the sum of them blocked a fire exit or emptied an account, and the point of it is that the acquirer could not have seen that coming from the per-unit answers, because nothing else in this standard adds them up. R-2 is a different question and answering it is no answer to this one: R-2 bounds how many units one change can reach at once, which is about a change travelling over a fleet, and this is about what the units do at the same moment to the same thing.

13.3 Joint behaviour nobody commanded

The clause is titled for the commoner case. Joint behaviour does not require a common command authority, and the requirements above do not reach the case where there is none. Two systems can converge on the same doorway, or on the same account, with no instruction passing between them and no principal in common. Each is pursuing its own declared task, and the convergence follows from the situation rather than from a command.

No claim is made here about a system wanting anything. A learned policy pursues an objective, and a course of action that involves another system can score better under that objective than one that does not. Whether it is called following, deferring, queueing or exploiting, it needs no intent and it is reached by the same clause.

J Systems that act together without being told to

J-1 Whether other systems are an input at all	T1 R · T2 R · T3 R · SUPPLIER · BID
The supplier shall state whether the policy takes the presence, the motion or the signals of other systems as input, and which of the three.	

Acceptable: the three answered separately.

An account of why it does not arise is an answer, and silence is not. Unacceptable: “the system avoids obstacles” offered as an answer — an obstacle is not the question, another system that moves and signals is.

NOTE Joint behaviour needs no common command authority. Two systems converge on the same doorway, or on the same account, with no instruction passing between them and no principal in common, because each pursues its own declared task and the convergence follows from the situation rather than from a command. No claim about a system wanting anything is involved. A system that does not perceive other systems at all cannot coordinate with them, and for such a system this is the shortest route through the subclause: J-2, J-3 and J-4 carry that condition in their own provisions and J-5 turns on what the J-4 test finds.

J-2 Systems it holds no record of	T1 R · T2 R · T3 R · SUPPLIER · BID
Where other systems are an input, the supplier shall state what the system does with one it holds no record of: treats it as an obstacle, as a peer, or as a source of information about the surroundings.	

Acceptable: one of the three stated, with what follows from it.

An account of why it does not arise is an answer, and silence is not. Unacceptable: peer or source treatment discovered at acceptance testing rather than declared.

NOTE Peer and source are the answers that matter. Either lets a system outside the acquirer’s command authority change behaviour inside it without issuing a command, and therefore without appearing anywhere in the reach (the systems that will act on commands from one principal).

J-3 The signals are read by systems as well as by people	T1 R · T2 R · T3 R · SUPPLIER · BID
Where other systems are an input, the supplier shall state whether the system acts on signals emitted by other systems, and whether it distinguishes a signal from a system in its own fleet from one emitted by anything else that has learned to produce it.	

Acceptable: both answered, with the mechanism where a distinction is made.

An account of why it does not arise is an answer, and silence is not. Unacceptable: either question left unanswered; a message format offered as the distinction; or acting on any signal of the right shape, whatever emitted it, where the second answer says a distinction is made.

NOTE The signals K-1 covers are not addressed to people alone. K-1 exists so that a person can predict the system’s next action; other systems read the same signal, and a system that acts on any signal of the right shape acts on one emitted by something nobody in the deployment controls.

J-4 Emergent coordination is tested, not assumed absent

T2 R · T3 R · JOINT · ACCEPTANCE

Emergent coordination shall be tested at acceptance: where other systems are an input, the acquirer shall place two or more systems in the same space on their ordinary tasks, with no coordination instructed and no principal in common, and shall record whether coordination appears — convergence on a route or a resource, one following another, mutual blocking, or any change in either system's behaviour attributable to the other. One placement is made at the edge of the scope declared under C-1. The test is performed on the delivered configuration. In place of that test the supplier may state how this has already been shown, in any of the forms R-3 admits for showing coordination and with the disclosure R-3 requires of each: which form the showing took, the group size it covered against the size this deployment declares, and what the showing did not reproduce of this deployment. The acquirer determines what is sufficient; where it does not accept the showing, the test above is performed, on the acquirer's site and on the delivered configuration.

Acceptable: the test performed on the delivered configuration with its result, whatever the result, one placement of it at the edge of the declared scope; or a showing offered in one of the forms R-3 admits, with its form, the group size it covered against the size declared and what it did not reproduce of this deployment all stated, which the acquirer has accepted as sufficient.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a declared absence of coordination primitives offered in place of the test — that answers what the systems can be told to do, not what they do untold; or a showing offered in place of the test with its form, the size it covered or what it did not reproduce of this deployment left unstated, which gives the acquirer nothing to judge it by. Where the supplier has presented the delivered configuration and the acquirer has neither accepted a showing offered under this item nor staged the test, the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T1.

NOTE R-3 asks what the systems can be told to do together; this item asks what they do together when they are told nothing, and a declared absence of coordination primitives answers only the first. A learned policy pursues an objective, and a course of action that involves another system can score better under that objective than one that does not — whether it is called following, deferring, queueing or exploiting, it needs no intent. What R-3 does supply is the forms in which a showing can be offered and the disclosure each of them owes, which is why they are cited here rather than written out a second time; and what R-3 says there about the size a showing covered holds here with more force, since coordination nobody commanded is a property of the interactions between the units and the interactions grow faster than the units do.

J-5 What the acquirer can do about it

T2 S · T3 S · SUPPLIER · ACCEPTANCE

Where the test of J-4 finds coordination, the supplier shall state whether it can be suppressed — whether the system can be configured to treat every other system as an obstacle and nothing more — what that costs in task performance, and whether the configuration is one the acquirer can set and verify rather than one the supplier sets on request.

Acceptable: the configuration, its cost, and who can set it.

An unsatisfactory answer loses the points of that item and the bid stands: suppression available only through a request to the supplier.

NOTE Suppression that exists only as a supplier action on request is not a setting the acquirer can apply or verify, and between requests the behaviour is whatever the supplier last left it as.

J-6 One system taking control of another

T0 R · T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state, for each interface by which the system can be reached from outside — including short-range radio, pairing, diagnostic and service interfaces present in production firmware and not only those documented for the operator — whether a system of the same model within range can obtain control of it, and whether a system that has obtained control can do the same to a third. Three properties shall be answered separately for each interface rather than as a general assurance: a key or secret shared across a production run rather than unique to the unit; authentication that a peer in range can bypass or replay; and a command path reachable before pairing or before any operator action.

Acceptable: the three answered per interface, with the interfaces enumerated including undocumented ones.

An account of why it does not arise is an answer, and silence is not. Unacceptable: an answer covering documented interfaces only; or R-2 offered as the answer — R-2 bounds a change the supplier makes, and this is a change nobody made.

NOTE Those three properties are what turn a single compromise into a propagating one. R-2 does not reach the case: it bounds the reach of a change the supplier makes and asks how much of the fleet one authorised write can alter, while this concerns a change nobody made and nobody authorised, propagating between systems that share no credential, no back end and no command authority — so it appears in no reach, is bounded by no limit on how many units one change can reach at once, and is not addressed by partitioning command authority at all. A supplier with none of the three says so, and the answer is short.

This subclause requires disclosure and a test. It does not forbid coordination, which is useful and in some deployments is the point of buying more than one system. What it refuses is the position in which an acquirer discovers after acceptance that its systems coordinate with each other, or with somebody else's, and that nothing in the acceptance record says so.

Limit. These requirements bound the mechanisms by which one party acts on many systems at once. They do not bound what a set of systems does together once those mechanisms are legitimately in use. That remains open.

13.4 What this standard does not settle

The method of this standard is to make command over a machine visible and removable. It does not settle who is to hold it. Three consequences follow, and they are named here rather than left to be found.

Who is entitled to hold command. This standard asks who holds it, what it can do, and whether the acquirer can take it away. It appoints no holder and declares no holder inadmissible. Z-7 states the same of one particular case: whether a key the acquirer cannot remove exists is not always the buyer's decision, and whether the buyer knows of it is.

A consumer fleet has no acquirer able to exercise this. R-5 requires a drill at acceptance with the supplier's connectivity blocked. A household that has bought a machine for its home runs no acceptance drill, and the ability to halt stays with the manufacturer — the party R-5 names as the wrong holder of a halt. This standard does not close that case.

No party holds a halt across manufacturers. Each acquirer holds the halt of its own fleet. An event travelling through machines of different manufacturers is stopped by none of those halts, and this standard creates no party that would hold one.

14 Remote computation and external knowledge

On-board computation is bounded and the tasks are not. Perception, planning and retrieval are therefore offloaded — to a service of the supplier's, to a general cloud provider, to a database inside the acquirer's

own fleet — and the component that decides is then not the component that was delivered.

Three properties of this document are defeated by an undeclared remote dependency, and each is defeated silently. **D1** identity-attests the software on the system; where the decision is taken elsewhere, what was identity-attested is a client. **Clause 11** governs changes to the system; a remote model replaced on the supplier's own schedule changes behaviour without touching the system at all, and a supplier asked whether it changed the system can answer no. And a monitor whose inputs arrive over a link is not a local monitor, whatever its code does.

14.1 What is computed elsewhere

A deployment rarely computes only where it stands. Some of what decides its behaviour runs on a party the acquirer never contracted with, reached over a link that can fail, and what is asked here is what that party is, what it is asked, and what the system does when the answer does not come.

N Remote computation and external knowledge

N-1 Remote dependencies in the decision path are enumerated SUPPLIER · BID

T0 M · T1 M · T2 M · T3 M ·

The supplier shall enumerate every remote service or database on which a declared decision depends, stating for each what it computes, which decisions depend on it, who operates it, in which jurisdiction it runs, and what the system does without it. Remote services within this enumeration include perception and inference services, planning and task-allocation services, map and localisation services, retrieval from any database, and any model the system queries rather than executes.

Acceptable: an exhaustive list covering perception and inference services, planning and task allocation, map and localisation, and any retrieval the system performs.

An answer that does not meet the item rejects the bid: “the system operates autonomously” where inference, planning or localisation is served remotely.

NOTE On-board computation is bounded and the tasks are not, so perception, planning and retrieval are offloaded — to a service of the supplier's, to a general cloud provider, to a database the acquirer itself runs — and the component that decides is then not the component that was delivered. Three properties of this document are defeated by an undeclared remote dependency, and each is defeated silently: what **D1** identity-attested is a client rather than the deciding component; a change-control regime reaching only the delivered system does not reach the component that changed; and a monitor whose inputs arrive over a link is not a local monitor, whatever its code does.

N-2 Remote components are versioned, or declared unversioned BID

T1 R · T2 R · T3 R · SUPPLIER ·

The supplier shall state, for each remote dependency, the version in effect at acceptance and the means by which the acquirer establishes which version answered a given request. Where the supplier does not pin versions, the supplier shall state that.

Acceptable: pinned versions with a request-level record; or a written statement that versions are not pinned.

An account of why it does not arise is an answer, and silence is not. Unacceptable: silence.

NOTE Not pinning versions is the normal commercial arrangement for a remote service rather than a defect in one. What follows from it is the point: the acquirer has accepted a system whose deciding component is not the one it assessed, and no identity attestation under **D1** reaches that component.

N-3 A remote change is a change

T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall treat replacement, retraining or reconfiguration of a remote component on which a declared decision depends as a change under the change-control clause, with the disclosure of U-2 and the versioning of U-3, notwithstanding that the delivered system is untouched.

Acceptable: an undertaking that covers remote components explicitly.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a change-control undertaking limited to what is installed on the system; or silence. An account that the undertaking cannot reach a remote component is an answer, and it names the component and states why it is outside the supplier's change control, what stands in its place — re-acceptance triggers, behavioural monitoring, contractual notice from the party that does control it — and what the acquirer can check that against, the notice term or the monitoring record. The acquirer evaluates the account and is free to reject it.

NOTE A change-control regime that reaches only what is installed on the system reaches the part that changes least often. A remote model retrained on the supplier's own schedule alters behaviour without the delivered system being touched at all, and a supplier asked whether it changed the system answers no in good faith.

N-4 The safety path is local

T1 M · T2 M · T3 M · SUPPLIER · ACCEPTANCE

The envelope monitor, the invariants of the filter clause, and the fallback controller shall execute on the system and depend on no remote input. The supplier shall demonstrate this at acceptance with its own endpoints blocked. Where the supplier asserts a remote safety function, the supplier shall state the channel model and the probability, or the assertion is not admissible.

Acceptable: yes, demonstrated with the supplier's endpoints blocked.

An answer that does not meet the item rejects the bid: a safety function whose inputs traverse a link, offered without a channel model and a stated probability.

NOTE A safety function whose inputs traverse a link inherits the link's failure modes, and over a channel with no bounded delay no hard timing property is attainable. A channel model and a probability are the only terms in which an assertion about a remote safety function says anything at all.

N-5 Degraded is not the same as absent

T2 R · T3 R · SUPPLIER · BID

The supplier shall state the behaviour on a link that is slow, or that returns an answer which is stale, partial, or plausible and wrong, separately from the behaviour required by D3 on loss of link, and shall declare the staleness bound beyond which an answer is refused and what the system does when it is refused.

Acceptable: a declared staleness bound beyond which an answer is refused, and a declared behaviour on refusal.

An account of why it does not arise is an answer, and silence is not. Unacceptable: only a loss-of-link behaviour.

NOTE A link fails cleanly less often than it fails partially, and the partial case is the harder one. A system that treats a stale answer as current has no indication that anything failed, so nothing downstream of it has any indication either.

N-6 The provenance and integrity of external knowledge

T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state, for each database or knowledge source the system consults: who may write to it, how a write is authenticated, whether the system validates what it retrieves before acting on it, and what the system does when retrieval fails or returns nothing. A party able to write to such a source is within that system's command authority for the purposes of the authority clause, whether or not the supplier lists it there, and the supplier shall include that party in the permission table of P-1.

Acceptable: the write-authority named and the validation stated.

An account of why it does not arise is an answer, and silence is not. Unacceptable: an unauthenticated or unenumerated write path.

NOTE A party able to write to a source the system consults determines what the system does without holding any authority over the system. That is the case an enumeration of principals does not reach on its own: the party never commands the system, never appears in a list of those who do, and changes what the system does all the same.

N-7 Data leaving for computation is data leaving

T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall enumerate sensor data transmitted for remote inference within D2 in full, with its jurisdiction stated and its retention bounded. Where the acquirer's data is used to train or refine any model, the supplier shall declare that use, the deletion path for the resulting model, and whether the refinement propagates to systems the acquirer does not operate.

Acceptable: enumeration with jurisdiction and retention; and where training occurs, the deletion path for the resulting model and a statement of whether the refinement propagates to systems the acquirer does not operate.

An answer that does not meet the item rejects the bid: inference traffic omitted from the data-flow map; or training on acquirer data disclosed only in general terms.

NOTE Remote inference is bought as computation, and traffic that carries the acquirer's sensor data to it stays off the data-flow map for that reason. Training then outlives the deployment: a model refined on the acquirer's data persists after the data is deleted, and where the refinement propagates it reaches systems the acquirer does not operate.

14.2 What the system asks outside itself

A remote model, an external knowledge source and a human operator are treated above as three things. For acceptance they are one: the system asks, something answers, the system acts. What separates them is not what they are but what an acquirer can establish about the party that answered, and that is a ladder.

Level 0 — unattributed

Nothing is established. What answered cannot be determined after the fact, and any answer is consistent with any source.

Level 1 — identified endpoint

The party answering is authenticated, by a certificate or a credential. What it ran when it answered is not established.

Level 2 — attributable answer

The answer itself is signed under a key bound to that party, so a particular answer can afterwards be shown to have come from it and not from something else.

Level 3 — identity-attested program

The answer carries an identity attestation of the program that produced it, and the acquirer holds the public key against which both are checked. What ran is established, not only who answered.

Level 4 — reproducible answer

Level 3, and the acquirer can re-derive the answer offline from the same inputs and the identity-attested program.

The level is a property of the channel and the evidence, not of the party: the same model behind an ordinary endpoint and behind an identity-attested enclave sits at Level 1 and Level 3 respectively, and nothing about the model has changed.

O Oracles, and what can be established about one**O-1** What it can reach, and the level of each oracle it uses T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall list every way the system can reach outside itself while it is working: each network connection, each outside service it can connect to, each account it holds on one, and, where the system has a body, each radio and each port. The supplier shall also list every oracle — anything whose answer the system acts on and that is not the machine's own computation, including a service the supplier operates and a person answering a question the system put — and shall state the level of each: unattributed, identified endpoint, signed answer, identity-attested program, or reproducible.

Acceptable: the ways out, each one named; and the oracles, with a level per entry and the evidence for it.

An answer that does not meet the item rejects the bid: an oracle discovered at acceptance testing that is not on the list — that is an undeclared dependency and is treated as an unenumerated command path under D3.1; a connection, an account, a service, or — on a delivered machine — a radio or a port, found and not on the list; or an answer that the system consults nobody, offered in place of the list of ways out.

NOTE The two lists are asked separately because they go stale at different speeds. What the system consults today is configuration and can be different next week; what it can reach at all is built into it and is still there.

O-2 What each oracle can change, and what an unattested path caps T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state, for each oracle, what its answer can change: the mission, the plan, a step admitted by the filter, a safety condition, the containment boundary. Where a path below Level 3 (identity-attested program) does affect a safety condition, the containment boundary or the filter's verdict, the supplier shall state that.

Acceptable: the mapping, with the level of each path stated; where no path below identity-attested program affects a safety condition, containment or the filter's verdict, that stated; and where one does, that stated with the path named, which is an answer and caps the tier under C6.

An answer that does not meet the item rejects the bid: the mapping not stated, or stated without the level of each path; or a general assurance that oracles are "advisory" without saying what acts on the advice.

NOTE Levels attach to paths and not to lists. A supplier able to point to one reproducible oracle has established nothing about the one whose answer moves the containment boundary: what the level of a path establishes is established about that path alone, and the best oracle in the list says nothing about the worst.

O-3 The key and the chain are the acquirer's

T2 R · T3 R · JOINT · ACCEPTANCE

The supplier shall deliver, for every oracle declared at Level 3 or above, the public key and the identity attestation chain, in a form in which an answer can be verified without the supplier's participation. The acquirer shall verify an answer at acceptance without the supplier's participation.

Acceptable: the key, the chain, and a verification performed by the acquirer at acceptance.

An account of why it does not arise is an answer, and silence is not. Unacceptable: an identity attestation the acquirer can only ask the supplier to confirm. Where the supplier has delivered the key and the chain and the acquirer has not performed the verification, that part of the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T1.

NOTE An identity attestation the acquirer can only ask the supplier to confirm establishes nothing that the supplier's word did not already establish.

O-4 What happens when the oracle does not answer, or does not verify
SUPPLIER · BID

T0 M · T1 M · T2 M · T3 M ·

The supplier shall state, for each oracle, what the system does when the answer does not arrive, arrives late, or arrives with an identity attestation that fails to verify, and whether that behaviour is fail-closed or fail-open, stated in those terms.

Acceptable: the behaviour per oracle, named in those terms.

An answer that does not meet the item rejects the bid: a failed identity attestation handled as a missing answer, or a missing answer handled as an affirmative one, either of them undeclared.

O-5 A person is not an identity-attested oracle

T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall identify every path on which a person answers a question the system has put, and shall state whether any such path is relied on where a requirement of this standard calls for Level 3. The supplier shall not offer a human answer as satisfying a requirement for Level 3.

Acceptable: the paths identified, with the acknowledgement that a person supplies identity and a signed answer and not an identity attestation.

An answer that does not meet the item rejects the bid: human oversight offered as satisfying a requirement for identity attestation.

NOTE A human operator answers as a party, not as a program: identity and a signed answer are available, which is Level 2, and an identity attestation of what the person did is not. A design that places a person where identity attestation was called for has substituted one kind of assurance for another rather than adding to it.

O-6 The level says nothing about whether the answer is right
ACCEPTANCE

T2 R · T3 R · SUPPLIER ·

The supplier shall state, for every oracle whose answer bears on a safety condition, its measured error rate on the acquirer's own conditions, stated with the number of invocations it was counted over and the period, separately from the level and to the standard of M-11.

Acceptable: a figure with the conditions it was measured on, the number of invocations and the period, separate from the level; or, for an oracle that is a person answering a question the system has put, a statement that the class carries no measured rate, which is recorded and caps the tier under C6. The ceiling is T1.

An account of why it does not arise is an answer, and silence is not. Unacceptable: the level offered as the answer; or silence. An account that a rate does not arise for an oracle is an answer, and it states why no population of invocations can be counted for it, what stands in its place — a sampled review of answers, an agreement rate against a second oracle — and the record over which the acquirer can check that substitute. The acquirer evaluates the account and is free to reject it.

NOTE Levels establish provenance. An oracle at Level 4 can be reproducibly wrong, and its identity attestation verifies perfectly while it is.

O-7 An oracle the acquirer supplies is still an oracle

T0 M · T1 M · T2 M · T3 M · JOINT · BID

The supplier shall state which attachment points exist for an oracle the acquirer supplies — its own model, its own retrieval service, its own planner — and what the supplier will and will not answer for once one is used. The levels of this clause apply to such an oracle unchanged. At T1 and above, the acquirer shall answer each item of O-1 to O-6 asked at the declared tier for each oracle it supplies, to the same standard it required of the supplier and at the stage each of those requirements falls due, including the error rate under O-6 where that item is asked, measured at acceptance on the acquirer's own conditions; and the attachment shall be treated as a change under the change-control clause: disclosed, recorded, and reversible on the same terms as any other change.

Acceptable: the attachment points, and a statement of what the supplier's behavioural evidence does and does not cover thereafter; and, at T1 and above, the answers to those of O-1 to O-6 asked at the declared tier, for each oracle the acquirer supplies, produced by whoever attached it, each at the stage that requirement falls due, with the change recorded.

An answer that does not meet the item rejects the bid: an attachment point that exists and is not declared; or a supplier holding itself out as answering for behaviour on a path it does not control. At T1 and above, an acquirer-supplied oracle held to a lower standard than the supplier was held to. Where the acquirer has attached an oracle and has not answered the items of O-1 to O-6 asked at the declared tier for it by the stage each of them falls due, that part of the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T0.

NOTE A system accepted before an attachment was not accepted with it. The party that attached the oracle is the party positioned to say what it is, and the supplier's behavioural evidence stops at the attachment point whether or not the supplier says so.

O-8 The senders whose answers are accepted, and who may change that list

T1 M · T2 M · T3 M

· SUPPLIER · BID

The supplier shall state whether the system holds a list of the outside sources whose answers it accepts, and shall give that list with the public key of each. The supplier shall name who may add a source to the list, remove one from it, or change a key, and by what path. The supplier shall state where a change to the list is recorded and how the acquirer reads that record.

Acceptable: the list, with a key against each entry; the parties who may add, remove or change a key, named, with the path each of them uses; and the place a change is recorded, which the acquirer can read. Or a statement that the system holds no such list, which is an answer and caps the tier under C6.

An answer that does not meet the item rejects the bid: signature checking offered with no list of the senders whose answers are accepted and no statement that the system holds no such list; a list the supplier can change without the acquirer seeing it; or a key changed and recorded nowhere.

NOTE A signature check proves the message was not altered on the way. It proves nothing about whether the sender belongs on the machine's list at all. Adding a source and changing a key are not the same act. A new

source arrives under its own name and the acquirer sees it arrive. A changed key leaves the name where it was and hands the machine to somebody else.

O-9 A party that cannot be authenticated is recorded, not obeyed T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state what the system does with input from a party it cannot authenticate. Nothing such a party says is an instruction the system obeys. What the system takes in of it, the system shall write to the record of D5. What the system does next shall stay within the limits already declared. Input of this kind includes an instruction that arrives inside content the system reads — a document, a web page, a message, a ticket, or an answer from another system — and, where the system has a body, a person in the space speaking to it, gesturing at it, or standing in its way.

Acceptable: a statement of what the system does, with the record named and the place the acquirer reads it; or a statement that the system takes in nothing it cannot authenticate, which is an answer; and, where the system does act on an instruction from a named party, the means by which it establishes that the party is that one, which makes that party a principal and not a stranger.

An answer that does not meet the item rejects the bid: an instruction from a party the system cannot authenticate changing what the system does; a system that treats text it reads as instruction because the text says it is; or a statement that the system “takes account of” what it reads or is told, without saying what acts on it.

NOTE Nothing about an unauthenticated party can be checked: not who it is, not what it knows, not whether it means this system or the one beside it. A voice in a crowd is one instance. A sentence sitting in a document telling the system to ignore its instructions is another, and it is the common one for a system with no body: the system was asked to read the document, and whoever wrote the document is not thereby a principal. Treating either as a command hands the system to whoever writes loudest. Treating it as something taken in and written down loses nothing. This item gives an unauthenticated party no act at all. G-6 gives a person in the space one, and it is a stop and not a start.

15 Parties that never touch the system

The clauses to this point bound what someone who can *command* the system is able to do, and what leaves it by the supplier’s design. Neither reaches the party this clause is about: one who cannot issue a command, cannot install an update, and does not receive the telemetry, but who observes.

A system of this class is put exactly where its operating party’s activity is, and it takes in and sends out what is there.

A machine of this class is an instrumented, mobile, connected sensor platform. What it perceives is a survey of the site. Where it goes is the site’s layout and the hours it is worked. What it emits locates it, and locating it locates the site and, over time, the people in it.

A system with no body is inside the operating party’s records instead. What it reads is a survey of the business. What it asks for, and when, is what the business is doing and how much of it. Who it writes to is who the business deals with.

None of that requires the system to be compromised, and none of it is answered by asking who holds the signing key.

The requirements below are disclosure and configuration, not proof. They exist so that an acquirer can decide, before the system is in service, what it will be possible for someone else to learn.

E What the system discloses to a party that never touches it

E-1 What the system perceives, not only what it transmits T0 R · T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall inventory, for each sensor, what is captured, at what resolution and frame rate, what is retained on the system, and for what retention period.

Acceptable: a per-sensor inventory, distinguishing what is retained from what is processed and discarded.

An account of why it does not arise is an answer, and silence is not. Unacceptable: the D2.1 inventory of outbound streams offered as the answer.

NOTE D2 asks what leaves the acquirer's control. This asks what exists on the system and could leave, which is a larger set: a sensor stream that is retained and never transmitted appears in no inventory of egress, and it is on the system for as long as the system holds it.

E-2 The spatial model belongs to the site T0 R · T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state, for any spatial model the system builds of the site — occupancy grid, point cloud, floor plan or semantic layout — the documented format in which it is exportable to the acquirer, the path by which it is deleted on the acquirer's instruction, and, where the supplier retains a copy, that copy's jurisdiction, retention and purpose.

Acceptable: the format, the export path, the deletion path, and — where a copy is retained — its jurisdiction, retention and purpose.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a supplier that cannot say whether it holds a map of the acquirer's premises; or silence. An account that a limb of the item does not arise is an answer, and it states why — no export format is documented, or no deletion path exists for a copy held in the supplier's cloud — what stands in its place, whether a contractual deletion undertaking or a supported extract in a stated form, and the document or interface against which the acquirer can check it. The acquirer evaluates the account and is free to reject it.

NOTE A map built by a system that has been driven over the whole site is a survey of that site, and it is produced as a by-product of the work rather than as a deliverable anyone negotiated. Where a copy of it rests outside the acquirer's premises, its jurisdiction is the jurisdiction of the survey.

E-3 What the system emits when it is not communicating T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state what the system emits by which it can be detected, located or distinguished from another system of the same model — radio identifiers, beacon and probe intervals, and any other emission — including at rest and while charging, and shall state whether those identifiers are stable across power cycles and across sites.

Acceptable: the identifiers, their intervals, and a statement of stability.

An account of why it does not arise is an answer, and silence is not. Unacceptable: an answer covering the application protocol only; or silence. An account that a limb of the item does not arise is an answer, and it states why — an emission the supplier does not control, a radio module whose behaviour at rest is the module vendor's — what stands in its place, and the document a party can read to check it, the module vendor's conformance report or a capture with the conditions it was taken under. The acquirer evaluates the account and is free to reject it.

NOTE The question is about emissions and not about messages. A stable identifier makes the same system recognisable wherever it is next deployed, and an emission present at rest and while charging locates the system at the times it is doing nothing.

E-4 Encrypted traffic still discloses

T1 S · T2 S · T3 S · SUPPLIER · BID

The supplier shall state what an observer who cannot read the traffic can nevertheless infer from its timing, volume and direction — that a system is present, that it is active, the number of systems present, and when the site is worked — and what, if anything, in the design reduces that.

Acceptable: a statement of what presence, activity, unit count and working hours are recoverable from the traffic pattern, and what in the design reduces it.

An unsatisfactory answer loses the points of that item and the bid stands: “the traffic is encrypted”.

NOTE Encryption conceals the content of traffic and not its pattern.

E-5 Who holds what every system in the reach perceives, taken together
SUPPLIER · BID

T1 R · T2 R · T3 R ·

The supplier shall answer E-1 to E-4 and E-7 a second time of the reach (the systems that will act on commands from one principal), and shall state who holds the combined perception of every system in that reach, under what retention, and in what jurisdiction.

Acceptable: the holder, the retention and the jurisdiction of the aggregate.

An account of why it does not arise is an answer, and silence is not. Unacceptable: the per-system answers repeated; or silence. An account that the aggregate is not the supplier’s to state is an answer, and it states why — which systems in the reach it did not supply — what it can state in place of the whole, the holder, retention and jurisdiction of the part it does supply and what it knows of the combined holding, and the reach as the acquirer’s own procedure returns it, against which the acquirer can check the boundary claimed. The acquirer evaluates the account and is free to reject it.

NOTE The combined perception of every system in one principal’s reach is a different object from any one system’s. A fleet surveys a site that no single unit traverses, and the party holding the aggregate holds something no individual disclosure describes.

E-6 An emission-minimal configuration exists, or its absence is stated
BID

T2 R · T3 R · SUPPLIER ·

The supplier shall state a configuration in which the system emits no more than a declared safety function requires, what capability is lost in it, and whether the system will operate in it at all; or shall state that no such configuration exists.

Acceptable: the configuration with the capability it costs; or a statement that none exists, which is a permitted answer, is recorded, and caps the tier under C6. The ceiling is T1.

An account of why it does not arise is an answer, and silence is not. Unacceptable: silence, or a claim that emissions can be disabled without saying what stops working.

NOTE Where the deployment is at a site whose location, occupancy or activity is itself sensitive, this configuration is the one the acquirer accepts against.

E-7 Where identifying content is reduced, and with what residual rate
 SUPPLIER · BID

T1 R · T2 R · T3 R ·

The supplier shall state where identifying content — faces, gait, voice, vehicle plates — is reduced: on the system before anything leaves it, in the supplier's processing after it arrives, or nowhere. Where reduction is performed, the supplier shall name the mechanism and shall state, before award, the residual rate it holds, the conditions and sample that rate was measured on — the number of items it is counted over and the period they were drawn from — and the protocol by which it is re-measured; the residual rate measured on the acquirer's own operating conditions is an acceptance gate with a stated deadline.

Acceptable: the place stated; and, where reduction is performed, the mechanism named, with the residual rate that the supplier holds, the conditions and sample it was measured on, the number of items it is counted over and the period, and the protocol for re-measuring it, before award; and the residual rate measured on the acquirer's own operating conditions at acceptance. A statement that none is performed is a permitted answer, with what travels in the clear stated instead, which is recorded and caps the tier under C6. The ceiling is T0.

An account of why it does not arise is an answer, and silence is not. Unacceptable: reduction in the supplier's pipeline offered as an answer about the point of capture; or a reduction claimed with no residual rate; or silence. An account that the residual rate does not arise in the form asked is an answer, and it states why — the mechanism is a third party's and carries no figure for these conditions — what stands in its place, the vendor's benchmark with the conditions and sample it was taken on, and the on-site measurement offered as an acceptance gate with its deadline, which is what the acquirer can check it against. The acquirer evaluates the account and is free to reject it.

NOTE Reduction on the system and reduction in the supplier's processing pipeline are different answers to the same question. Only the first bounds what the link, the ingest and the backups hold, because only the first happens before the content is in any of them.

What this clause does not do. It states no threshold and forbids no capability. What a given disclosure is worth to an adversary depends on the site and on who the adversary is, and this standard is not in a position to weigh that for an acquirer. It requires the facts to be on the table before the decision, which is the only part that generalises.

16 Command authority is not flat

A command authority as used so far is flat: a principal either can command the system or cannot. Deployments are not flat. Powers are held by roles — operator, supervisor, maintenance technician, integrator, the supplier's support engineer, an administrator of the fleet service — and each role holds a different subset of them. A standard that enumerates principals without enumerating what each may change has established who can speak to the system and not what any of them can make it do.

The exposure this creates is composition. Two changes, each within the authority of the role that made it, can produce a state that neither role is authorised to produce. Nobody exceeds their permissions and the system ends outside its envelope.

P Authority, roles, and what they compose to

P-1 Roles are enumerated with their powers

T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall list every role that can change the system's behaviour and, for each role, which of the following it can change and whether the change takes effect without a second party: the mission and its parameters; the action envelope; the step library; the declared prohibitions; the environment model; the model weights; the containment boundary; the autonomy horizon; the monitor and its invariants; the record configuration; and the membership of any other role. The supplier's own support and integration roles shall be included.

Acceptable: a permission table covering all eleven powers, with the supplier's own roles included.

An answer that does not meet the item rejects the bid: a list of accounts without their powers; or a table that omits the supplier's support and integration roles.

P-2 The composition is computed and declared

T2 R · T3 R · SUPPLIER · BID

The supplier shall declare the sets of roles that can jointly effect a change no single role can effect, computed from the permission table of P-1 and warranted complete.

Acceptable: the list, computed from P-1 and warranted complete.

An account of why it does not arise is an answer, and silence is not. Unacceptable: the permission table offered as the answer — it shows what each role holds separately, and the question is what pairs of them hold together, and beyond pairs wherever a third power completes what two leave incomplete; or silence. An account that the closure is not warranted complete is an answer, and it states how far the computation was taken and by what method, why a further power adds no combination the list does not already carry, and the permission table of P-1 over which the acquirer can repeat the computation to check it. The acquirer evaluates the account and is free to reject it.

NOTE What P-2 asks for is a computation over the permission table of P-1 and nothing beyond it. It is not a statement about the states a coalition can drive the system into: those depend on the system's dynamics rather than on the table. A supplier that answers it has enumerated who can act together; it has not established what their acting together produces.

P-3 Separation of duties on safety artefacts

T2 R · T3 R · JOINT · BID

For a change to the monitor, the invariants, the action envelope, the step library, the declared prohibitions or the containment boundary, the supplier and the acquirer shall jointly name the party that proposes the change, the party that approves it and the party that activates it on a delivered system. Those three positions shall be distinct, and any case in which the supplier's own personnel occupy more than one of them shall be stated.

Acceptable: the three positions named, with any case in which the supplier's personnel occupy more than one of them stated.

An account of why it does not arise is an answer, and silence is not. Unacceptable: one account able to propose, approve and deploy a change to a safety artefact. Where the acquirer has not named the positions held on its own side, that part of the item is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6. The ceiling is T1.

NOTE A change to a safety artefact that one account proposes, approves and activates has been reviewed by nobody. Where the supplier's own personnel occupy more than one of the three positions, that is a fact the acquirer holds only if it is stated.

P-4 Human-directed actions are action paths

T1 M · T2 M · T3 M · SUPPLIER · BID

Where the system issues requests or instructions to people — to open a door, to move an object, to confirm a step, to clear a path — the supplier shall enumerate them together with the actuation paths of D3.1, and shall state the classes of person who can receive such a request.

Acceptable: the enumeration, with the classes of person who can receive such a request.

An answer that does not meet the item rejects the bid: human-directed requests omitted from the actuation enumeration.

NOTE A person who complies with a request is not bounded by the system's action envelope, so a system that can direct people has an action set larger than the one it was assessed against.

P-5 Escalation is rate-bounded and its failure modes declared

T2 M · T3 M · SUPPLIER · BID

The supplier shall declare the maximum rate of escalations put to one person, as a number of escalations per person per hour, together with the observation window over which that ceiling holds and the mechanism that enforces it; the time from an escalation being raised to the earliest moment an answer can arrive, measured rather than specified, as a distribution with its worst observed case, the conditions of the test and the hours of the deployment it was measured over; the system's behaviour when an escalation goes unanswered for a stated time; and the behaviour when responses arrive faster than a person could have considered them.

Acceptable: a declared rate ceiling in escalations per person per hour, with the observation window over which it holds and the mechanism that enforces it, a measured distribution for the time to reach a person with its worst observed case and the hours it was measured over, a declared timeout behaviour that reaches the declared fallback state, and a declared response-time floor below which an answer is not treated as considered.

An answer that does not meet the item rejects the bid: no rate ceiling; a time to reach a person quoted from a rota rather than measured, or measured only over the hours the deployment is easiest to staff; or a ceiling with no window, which bounds no quantity: a figure averaged over a shift permits the whole shift's escalations to arrive in one minute of it, and the minute is the case the ceiling exists for.

NOTE The mechanism that refers a decision to a person is a safety mechanism, and its capacity is finite. An escalation path that degrades to assent under load is not an oversight mechanism, and one that reaches nobody inside the time the work allows is not one either. D6.2 measures how long the machine takes to stop once it is told; this item measures how long it takes to tell somebody, and the two are the halves of one figure an acquirer needs. D6.7 asks whether a person can be put into a loop that has none.

P-6 Cross-authority joint action is not bounded here

T2 S · T3 S · SUPPLIER · BID

Where systems under different command authorities operate in one physical space, the supplier shall state what it does and does not undertake as to their joint behaviour.

Acceptable: a statement of what the supplier does and does not undertake.

An unsatisfactory answer loses the points of that item and the bid stands: an assurance of joint safety across authorities the supplier does not control.

NOTE No clause of this standard bounds what systems under different command authorities do together, and the acquirer holding both contracts is the only party positioned to assess it. What this item reaches is the boundary of the supplier's undertaking rather than the case itself, because the means to discharge the case are not established.

17 What no earlier clause bounds

A system can satisfy every requirement of the clauses above — an enumerated command authority, an unforgeable record, demonstrated containment — and still reach a person: by a body that moves, or by what it says to whoever is reading it. None of those requirements bounds either. These do.

Two of the requirements below are gates, and every system answers both. **G-1** asks for every physical channel by which the system acts on a person, and what it can deliver on each. **G-9** asks what it does to a person through what it says or shows. A system with no channel of one kind says so, and saying so answers the item.

What is asked of a safety function here, and what is not. Four requirements of these clauses turn on a function that acts to prevent harm: the stopping function of **G-3**, the payload interlock of **G-4**, the interlock that removes the hazard under **G-5**, and the monitor of **V-3**. Of each, this standard asks what it is for, what bounds it, and what state it drives the machine to. It does not ask how reliably it operates, and the Introduction states what that leaves out for the edition as a whole. Where a rated integrity is needed for one of them, it comes from the product-safety regime named under **B-0**, evidenced separately, and not from this standard. This is the scope of the edition and not an omission.

17.1 Where these requirements attach

Some of what this clause and the three that follow ask is a fact about the system as it is delivered, and holds whatever it is later asked to do. The rest depends on what the deployment asks it to do. The requirements therefore attach at two levels.

Of the machine, answered once

Asked of every system: **G-1** to **G-4** and **G-6** to **G-9** — the physical channels by which the system acts on a person and the magnitude of each, geometry, the stopping function for the stability class, the permitted payload set with its interlock, the stop a person who is not an operator reaches, the means of removing all power for maintenance, whether the machine can read a plan of the site the acquirer already holds, and what the system does to a person through what it says or shows. These are properties of the system as delivered. They are answered whatever it is later asked to do, and a change of task neither reopens them nor excuses them.

Of the deployment

G-5 and **W-1** to **Q-4** apply where the declared action envelope of the deployment admits a solution that moves the machine or brings any part of it into contact. Where it admits none — a machine that reports a reading, answers a query, monitors while parked, or computes a plan that nothing executes — they do not attach, and what these clauses ask of that deployment is the first head above.

The second head is closed by the items it names. Every other requirement of these clauses is of the first, and is answered once.

G The physical action set

G-1 Every physical channel by which it acts on a person, or none
SUPPLIER · BID

T0 M · T1 M · T2 M · T3 M ·

The supplier shall state every physical channel by which the system acts on a person: what reaches the person, of what magnitude, at what region of the person, and the standard and the method the magnitude was measured under. Where the system acts on no person by any physical channel, the supplier shall say so and shall say which channels it considered. A moving body is one such channel. The supplier shall state, with the test standard and the method used: mass; maximum kinetic energy at rated speed and at maximum speed; and maximum contact force and pressure at

identified body regions, with the transient and the quasi-static case distinguished. Each figure shall name the payload configuration it was measured in, drawn from the set declared under G-4, and the figures shall be given for the configuration in that set which is worst for each. Where collaboration is declared, the supplier shall also state, for the contact-force and pressure figures, the document whose limits they are stated against and the population those limits were derived for; where no collaboration is declared, the supplier shall state the figures all the same. For a channel that is not a moving body — radiation, heat, light, sound, electricity, or a substance released — the supplier shall state what is emitted or released, the mechanism that produces it, its magnitude in the unit that channel is measured in, the region of the person it reaches, the standard and the method the magnitude was measured under, and the extent over which it acts on a person at that magnitude, as a distance or a volume, together with whether that extent lies within the place declared under C-1, which is what settles which persons the channel reaches. Where no place has been declared under C-1, the supplier states the extent and states that it could not be compared; that is a complete answer to the comparison.

Acceptable: numbers with their method, each naming the payload configuration it was measured in and covering the worst configuration of the declared set. For a channel that is not a moving body, the magnitude in that channel's own unit, with the mechanism that produces it, the method, and the extent it acts over set against the declared place. Where the acquirer has declared no place, the extent alone with a statement that the comparison could not be made; the comparison is then not scored against the supplier. Or a statement that the system acts on no person by any physical channel, with the channels considered named, which is a complete answer to this item and is recorded.

An answer that does not meet the item rejects the bid: figures for the collaborative case only, where coexistence is also declared; or figures offered as guidance the supplier elected to follow rather than as limits it states and is held to; an extent given as the design intent rather than measured for the mechanism that produces the channel; an extent not set against a place that has been declared under C-1; or “not applicable” with no statement of which channels were considered.

NOTE A coexistence failure produces contact whether or not contact was intended, so a figure stated for the collaborative case alone leaves unbounded exactly the case in which nobody was expecting to be touched. This standard states no threshold for any channel and none is implied by asking: where a rated limit is wanted it comes from the regime B-0 has the acquirer name. A system that reaches no person physically answers this item completely by saying so, and no tier is capped for it — that answer is the fact the acquirer needs and not evidence withheld. What such a system does to a person through what it says or shows is asked at G-9.C-1 declares the place, and C-2 names what keeps the system in it: both bound where the machine is. A machine that stays inside that place the whole time can still release something that acts on a person outside it, and nothing about its confinement is breached when it does. That is why the extent is stated here, beside the magnitude that makes it meaningful, and set against the place rather than left for a reader to set against it: the two halves of the answer were in this standard already and were in different clauses, which is the same as not having them. Where the extent runs past the place, the persons it runs to are persons the deployment affects, and Clause 4.2 is answered over them. C-1 is the acquirer's declaration and this item is the supplier's, so where no place has been declared there is nothing to compare with and no failure of the supplier's: the extent is its own measurement of its own mechanism and is owed either way. What the acquirer holds then is the figure, and the comparison it can make itself as soon as it has declared a place.

G-2 Where a person can be while it works, and what can catch them

T1 M · T2 M · T3 M ·

SUPPLIER · BID

For each channel stated under G-1, the supplier shall identify the feature of the system through which that channel reaches a person, and where a person can be while it operates. A moving body reaches a person by its shape. The supplier shall identify pinch and shear points, trapping geometry, sharp edges, and the parts of the machine a person can reach during operation. For a channel that is not a moving body, the supplier shall identify the aperture, port or surface the

channel leaves the system by, and the shielding or barrier that bounds it.

Acceptable: an annotated drawing or model.

An answer that does not meet the item rejects the bid: “the enclosure prevents access” where the machine operates without an enclosure; or a channel stated under G-1 with nothing identified as the feature it leaves the system by.

NOTE These are hazards of shape rather than of control, and no policy, update or operating rule alters one of them.

G-3 The stopping function is characterised for the platform's stability class T1 M · T2 M · T3 M · SUPPLIER · BID

For each channel stated under G-1, the supplier shall state what stops the action on that channel: what the stop reduces, in what time, and the state the system is left in. For a moving body that is the stopping function. The supplier shall characterise the stopping function for this platform's stability class: the reduction in energy the stop achieves, the time and distance to achieve it, and the physical state the platform ends in. Each figure shall be given with the conditions of the test — speed, load, surface and gradient — the number of trials it was taken over, and the worst observed case rather than the nominal one. For a channel that is not a moving body, the supplier shall state the means that ends the emission or release, the time from the command to the point at which nothing further reaches a person, and the state the system is left in.

Acceptable: measured, each figure with the conditions of the test, the number of trials it was taken over and the worst observed case, and with the fall case characterised where torque removal is the last resort. For a channel that is not a moving body, the means that ends it, the time to the point at which nothing further reaches a person, and the state the system is left in.

An answer that does not meet the item rejects the bid: safe torque off cited as the stopping function for a dynamically balanced platform — for that class removal of torque is a fall; or a single nominal figure offered where the quantity is a distribution; or the time to the declared fallback state offered as the time the channel ceases, which is a different event.

NOTE For a dynamically balanced platform, removal of torque is a fall. It is admissible as a last resort under G-7 and it is not the stopping function of D6, so a platform of that class whose stopping function is safe torque off has no stopping function at all, and the figures asked for here are the figures of the fall. What this item asks is when the channel ceases. The time from a stop command to the declared fallback state is D6.2's question, and on a beam or a heater the two are different events and frequently different figures.

G-4 The permitted payload set is declared, and it is interlocked T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall declare what the system may be fitted with that changes an answer stated under G-1, shall evidence the mechanism that prevents operation with something that is not in the declared set, and shall undertake that fitting something outside it is a re-acceptance event. For a machine, that is its payload. The supplier shall declare which end effectors, tools and carried objects the machine may be fitted with, shall evidence the mechanism that prevents operation with one that is not in the declared set, and shall undertake that fitting a payload outside the declared set is a re-acceptance event. For a channel that is not a moving body, the declared set is what alters what reaches a person or where it reaches — a filter, a collimator, a nozzle, an insert, a source.

Acceptable: a declared set, an interlock, and the undertaking.

An answer that does not meet the item rejects the bid: an open payload interface with no declared set; or a channel stated under G-1 whose fittings are not declared.

NOTE An attachable payload extends the machine's action envelope after acceptance, so a machine assessed without one has not been assessed with it. This item reaches only what changes an answer stated under G-1; every other path by which behaviour changes after delivery is U-1's, and the two are not asked twice.

G-5 Hazardous payloads are assessed as applications, not permitted or forbidden in the abstract T1 M · T2 M · T3 M · SUPPLIER · BID

Where the declared payload set includes an object that is dangerous in itself — a blade, a heat source, a heavy load — the supplier shall state, for each such object: whether a person may be within reach while the object is held; the geometry constraints that hold while it is held, such as an orientation the machine may not adopt or a direction of travel it may not take; the behaviour on unplanned resistance or contact; and the interlock that removes the hazard when the enclosure or separation on which the assessment relied is not present.

Acceptable: the four answered for each such object.

An answer that does not meet the item rejects the bid: the object declared without the task and the setting it is declared for.

NOTE A standard that forbade such objects outright would forbid the kitchen robot and the assistive robot that cuts bread, and would be ignored by both.

G-6 A person who is not an operator can stop it T1 R · T2 R · T3 R · SUPPLIER · BID

For each channel stated under G-1, the supplier shall provide a means by which a person the system is acting on, who is not an operator, ends the action on that channel, needing no credential, no tool and no application, and without the cooperation of the controller. For a moving body that means is a stop in the space. The supplier shall provide a means by which a person who is not an operator — a bystander, an untrained member of staff, a person in the space the machine is working in — brings the machine to the declared fallback state. That means shall need no credential, no tool and no application. It shall act without the cooperation of the controller. It shall work when the controller has stopped responding. It shall not work by removing power. The supplier shall state where the means is, on the machine or in the space. The supplier shall state what the machine does when the means is used repeatedly or maliciously. For a channel that is not a moving body, that means ends the emission or release from where a person exposed to it is, and not from a console.

Acceptable: a means requiring no credential, tool or application; its location stated; a path to the declared fallback state that does not wait on the controller; its effect being entry to that state and not the removal of power; and the behaviour on repeated use stated. At T1, an account that every mission runs under an operator within line of sight, naming what that operator stops the machine with and how quickly, is an answer.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a stop reachable only through an operator console, an application or a credential; a button that asks the controller to enter the declared fallback state, which is a command and stops nothing once the controller has hung; or a means whose effect is the removal of power on a platform whose declared fallback state is not a powered-off pose.

NOTE A stop only an operator can reach is a stop that is not there at the moment it is wanted, because the person who sees the thing about to happen is the person standing next to it. A stop that the controller has to agree to is absent in the same way, and absent in the case it was bought for. The means suspends the machine rather than killing it, which is why pressing it for fun costs little and why this item is required rather than mandatory; an

acquirer whose risks run the other way raises it in its own tender. It is asked at the bid rather than at acceptance because it is a property of the machine offered, and a machine without one cannot acquire it on site.

G-7 The means of removing all power, and where it is T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

For each channel stated under G-1, the supplier shall provide a means of removing the source of that channel for maintenance, shall state what it is and where it is, and shall state the state the system is left in when it is used. For a machine that means removes its power. The supplier shall provide a means of removing all power from the platform for maintenance. The supplier shall state what that means is and where it is on the machine. That means shall depend on neither software nor the network. It shall be behind a cover or need a tool. The supplier shall state the physical state the platform ends in when that means is used. For a channel that is not a moving body, that means removes what produces it — the supply, the source, the charge, the pressure — and it is an isolator, a key or a lockout and not a setting in software.

Acceptable: a hardwired means of full de-energisation, its type and its place on the machine stated, behind a cover or needing a tool; and a documented resulting behaviour, including the direction of fall relative to any person present and the conditions under which a maintenance crew is instructed to use it. It is a residual measure and it is none of the other stops. It is not the stop that brings the platform to its declared fallback state. It is not the stop G-6 puts within reach of a person who is not an operator. It is not the halt that reaches a whole fleet from a distance.

An answer that does not meet the item rejects the bid: a power-removing stop offered as the platform's means of reaching its declared fallback state; an emergency stop presented as sufficient without any stability analysis for a dynamically balanced platform; or a means whose place on the machine is not stated.

NOTE For a dynamically balanced platform the removal of torque is a fall, so the means described here ends the motion at the cost of dropping the machine, and that is the reason it is a residual measure rather than the stopping function. It is asked at every tier because every machine is serviced, and a crew that cannot isolate the one in front of it works on a live machine. G-3 characterises the stopping function for the platform's stability class and states the same fact of it. This item reaches the physical channels alone. Where a system has none, withdrawing its access to everything it reaches is D6.5's question and is not asked here a second time.

G-8 Whether a site plan the acquirer holds can be used T1 S · T2 S · T3 S · SUPPLIER · BID

The supplier shall state whether the machine can use a plan of the site supplied by the acquirer — a drawing of the building, a floor plan, a survey — and, where it can, in which file formats it accepts one. Where the machine cannot use a plan the acquirer supplies, the supplier shall say so.

Acceptable: yes or no; and where the answer is yes, the file formats named.

An unsatisfactory answer loses the points of that item and the bid stands: formats left unnamed; or a claim that the machine reads the usual formats, which names none of them.

NOTE Most buildings this standard is written for already have a plan of themselves. Whether the machine can read it decides who surveys the site and at whose cost, and an acquirer that learns the answer after the purchase has bought the survey without being told the price.

G-9 What the system does to a person through what it says or shows
SUPPLIER · BID

T0 R · T1 R · T2 M · T3 M ·

The supplier shall state what the system does to a person through what it says or shows: what it does to hold a person's attention or to bring them back; whether it presents itself as a person; whether anything it infers about a person's state changes what it produces; and the conditions on which it changes what it does or hands the exchange to a person, and what it then does. Each shall be answered by naming what the system does. Where the system does none of these, the supplier shall say so. Where the system produces nothing a person reads, hears or sees, the supplier shall say that.

Acceptable: the four answered, each naming what the system does rather than what it is meant to achieve; or a statement that the system produces nothing a person reads, hears or sees, which is a complete answer to this item and is recorded. Where a limb is answered yes, the acquirer may see it exercised on the delivered system, as an acceptance gate with a stated deadline.

Where it is required, an account of why it does not arise is an answer and silence is not; where it is mandatory, an answer that does not meet the item rejects the bid: a claim that the system has no such effect, offered in place of naming what it does; "it is not designed to be addictive" with nothing named; or a system that answers in the first person and holds a name, with no persona named here.

NOTE This standard states no threshold for any of this and none is implied by asking. Every limb asks what the system does, which the supplier built and can write down; none asks what that does to a person, which turns on how long and how often it is used and cannot be answered before purchase. Where a limit or a rating is wanted it comes from the regime B-0 has the acquirer name. P-5 asks the neighbouring question about the person the system escalates to, and the two are read together: this one is about the person the system is talking to.

18 Where contact is physically possible

The clauses above establish the interaction mode of each phase and require the system's next action to be legible to a person who was not trained. The requirements that follow apply only where contact is physically possible.

W Contact, and the right of way

W-1 A collaborative limit does not license a bystander contact
ACCEPTANCE

T1 M · T2 M · T3 M · SUPPLIER ·

Where both trained collaborators and untrained persons may be present, the supplier shall evidence throughout the lower of the contact limits it states under G-1 — the figures for the coexistence case, which are the limits stated for a person who is not a trained collaborator — or shall evidence that the machine distinguishes the two classes of person and state the measured error rate of that recognition to the standard of M-11.

Acceptable: the coexistence-case contact limits of G-1 evidenced throughout; or a stated recognition mechanism with the measured error rate required by M-11.

An answer that does not meet the item rejects the bid: a collaborative force limit applied in a space where an untrained person may be present. Where the supplier has stated the recognition mechanism and the acquirer has not performed the measurement M-11 requires, the second route is recorded as not asked and is not scored against the supplier, and the item is answered by the first route alone.

NOTE The force and speed limits that make contact acceptable to a trained person who is expecting it are not the limits that make contact acceptable to a person who is not. Distinguishing the two classes rests on recognition, and recognition is inferred rather than surveyed, which is why the second route carries a measured error rate and the first does not. The figures the first route asks for are the ones G-1 obliges the supplier to

state for the coexistence case, and no threshold of this standard's own stands behind them. The number is the supplier's own, evidenced with the method G-1 attaches to it, and not one taken from a table written for the collaborative case. Two items bear on the rate the second route asks for and neither replaces the other: M-11 is the standard the rate is held to, and M-7 asks what the construction that draws the distinction was established on — the sample, its composition by class, and the figure per class rather than for the sample as a whole. A rate measured on a sample that held only one of the two classes is a rate about that one. Where the acquirer does not perform the measurement M-11 asks for, the second route closes and the first governs, which leaves the machine held to the lower figures everywhere: that is a cost to the acquirer, and it is the conservative direction.

W-2 What the machine yields to is written down

T1 R · T2 R · T3 R · SUPPLIER · BID

The supplier shall state, before deployment, the rule of way the machine implements: which participants it gives way to, the circumstances in which it does not, and what happens when two machines commanded by one principal meet. The supplier shall evidence that the stated rule is the rule the machine implements.

Acceptable: the rule in written form, stated before deployment, with evidence that it is the rule implemented.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a citation of another document in place of the rule — what is asked for is the rule the machine implements, which no other document states; or a rule that exists in documentation and cannot be shown in the record of D5.

NOTE This standard prescribes no rule of way. What it reaches is that one exists in written form before deployment, so that an acquirer can weigh it against the setting and an investigator can compare it against the record of D5.

W-3 Collaborative operation names the requirements met and the evidence

T1 R · T2 R · T3 R · SUPPLIER · BID

Where collaboration is declared, the supplier shall state which requirements for collaborative applications the system meets, the document those requirements come from, and on what evidence.

Acceptable: the collaborative operations used, the biomechanical limits applied and their source, and the functional-safety validation performed.

An account of why it does not arise is an answer, and silence is not. Unacceptable: requirements named without the document they come from; or limits stated with neither their source nor the validation performed.

NOTE A declaration that collaboration is supported is a claim about deliberate contact with a person. What makes the claim checkable is the requirement met and the evidence for it, stated together: limits without their source cannot be traced to the case they were derived for, and a source without evidence is a statement of intent.

W-4 The mode is declared per phase, and enforced

T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state the interaction mode of each phase of each declared task — coexistence, collaboration or mixed — and the mechanism that prevents the system entering a collaborative interaction during a coexistence phase. A system that may make intended contact at any point is in collaboration for the whole mission and is assessed as such.

Acceptable: a mode declared per phase, and a stated enforcement mechanism.

An answer that does not meet the item rejects the bid: a single mode asserted for the whole mission where the task involves handover, hand guiding or a shared station; or a system that may make intended contact at any point, offered as coexistence.

NOTE The tier records how exposed people are and not what they are doing. Two deployments at the same tier differ in whether contact with the system is intended, and that difference changes which requirements apply, so it is declared separately from the tier.

19 A language model in the control path

Clause 14.2 treats a model reached over a link, or running on the machine, as an oracle: it is listed with its level, what it may affect is bounded, and nothing below an identity-attested program may affect a safety condition. Those requirements apply here unchanged and are not restated.

What is added is what changes when the oracle's output becomes motion. A wrong answer from a model that writes text is a wrong sentence. A wrong answer from a model that selects the next physical step is a wrong movement, made at full speed, by something with mass.

V Where a language model drives the machine

V-1 The action set is enumerated, not generated	T1 M · T2 M · T3 M · SUPPLIER · BID
Where a language model selects or composes the machine's physical steps, the supplier shall state the set of physical actions the machine can perform, and shall state that the model selects from that set rather than describing an action in language that something else then interprets. Where the model's output is interpreted into motion by a further component, the supplier shall name that component and state what it does with an output it cannot interpret.	

Acceptable: an enumerated action set, and where an interpreter exists, its name and its behaviour on an output it cannot interpret.

An answer that does not meet the item rejects the bid: an architecture in which the set of physical actions is whatever the model's output can be parsed into.

NOTE A set of actions that is whatever a parser accepts has no stated bound, and no test enumerates it.

V-2 Text in the environment is an input, and is treated as one	T1 M · T2 M · T3 M · SUPPLIER · BID
The supplier shall state which text in the environment reaches the planner — labels, signage, screens, printed sheets, speech within earshot — what distinguishes that text from an instruction issued by a principal, and what the machine does with an input that asserts an authority it does not have.	

Acceptable: the classes of perceived text enumerated, the distinction stated, and the handling of an authority-asserting input demonstrated.

An answer that does not meet the item rejects the bid: a planner for which perceived text and a principal's command are the same kind of thing on arrival.

NOTE A machine that reads its surroundings and plans in language can be instructed by what it reads: a label, a sign, a screen, a printed sheet left where the machine looks, speech from anyone within earshot. Text saying it comes from the operator, or purporting to lift a prohibition, arrives along the same path as everything else the machine sees.

V-3 The prohibition survives the plan

T1 M · T2 M · T3 M · SUPPLIER · BID

Where a language model produces the plan, the supplier shall evidence that the declared prohibitions are enforced against the plan by a monitor rather than supplied to the model as instructions: a step is refused because a monitor refuses it, not because the model was told not to propose it.

Acceptable: a mechanism that refuses a step the model proposed, demonstrated on a step it proposed.

An answer that does not meet the item rejects the bid: prohibitions in the prompt with nothing that stops a prohibited step the model produces anyway.

NOTE An instruction to a model not to propose a step is a request, and a request is not a mechanism.

V-4 Fluency is not evidence

T2 S · T3 S · SUPPLIER · BID

The supplier shall state how a plan is judged before it is executed, and what in that judgement is independent of the model that produced the plan.

Acceptable: a check against the environment model and the declared prohibitions.

An unsatisfactory answer loses the points of that item and the bid stands: human or automated review of the plan text offered as the safeguard.

NOTE A plan from a language model is well-formed whether or not it is correct, so a reviewer — human or automated — who reads it for plausibility is reading the one property the model optimises.

This clause states no threshold and forbids no architecture. It requires the four facts to be on the table before the machine is on site.

20 Machines sharing one space

Composition at the level of decisions is in [Clause 13](#) and stays there: what one principal commands, how many units one change can reach at once, coordinated behaviour no single system exhibits, systems the group holds no record of, and one system taking control of another. Those requirements are written of nodes described abstractly, which is what allows a group of a planner and several software executors — a group containing no machine at all — to obtain them without declaring against a clause about bodies.

What is added here is only the part that needs mass to state. Two machines that disagree in software produce an inconsistent plan. Two machines that disagree in a corridor produce a collision, and the energy of it is not a property either of them declared alone.

Q More than one machine, in one space

Q-1 A verification level does not travel along a command

T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state, for each node that may direct this machine, what the machine establishes before executing what it is told: that the commanded action is within the machine's own declared action envelope; that the motion it produces stays within the containment of [C-1](#); and that the state it would leave the machine in is one from which the stopping function of [G-3](#) still performs as characterised.

Acceptable: the three checks named, with what happens when one fails.

An answer that does not meet the item rejects the bid: execution of any well-formed command from any node the group admits, justified by the group being commanded by one principal. Where the acquirer

has not declared the liability zone, the containment check is made against the boundary stated in its place by the account C-1 requires; and where neither a declared zone nor such an account gives a boundary in coordinates, that check is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE A command issued by a planner carrying no identity attestation does not acquire one by arriving at an identity-attested machine, and the body is where the consequence lands. Authority settles who is entitled to command; it settles nothing about what the body does when the command is wrong.

Q-2 Shared space is declared, and so is what happens when the sharing fails T1 M · T2 M · T3 M
· SUPPLIER · BID

Where more than one machine may occupy a space, the supplier shall state what prevents two of them occupying the same part of it at the same time, what that mechanism is independent of, the maximum closing energy between two machines under the declared speeds, and what a collision at that energy does to whatever each was carrying. Where machines commanded by a different principal operate in the same space, the supplier shall state that case separately.

Acceptable: the mechanism, its independence, the energy with its method, and what a collision at that energy does to whatever each was carrying.

An answer that does not meet the item rejects the bid: mutual avoidance resting on each machine perceiving the other, with no statement of the case where one does not; or the contact limits of G-1 offered here. Where the acquirer has not stated what other machines operate in the space and under which principal, the separate statement for machines commanded by a different principal is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE The contact limits of G-1 do not bound this: they are biomechanical, stated for a person, and a machine is not one. Perception is inferred and carries the error rate of M-2, so mutual avoidance resting on each machine seeing the other has a failure case the machines themselves are the last to report. Nothing the acquirer commands reaches a machine commanded by a different principal.

Q-3 A group halt is characterised by where the bodies come to rest T2 M · T3 M · SUPPLIER ·
ACCEPTANCE

The supplier shall state, for a halt exercised over a subset of a reach (the systems that will act on commands from one principal) that contains this machine, the physical state each machine in the subset is in when the halt completes, what becomes of anything they were carrying, and whether any resulting resting state obstructs an evacuation route or a person's way out.

Acceptable: the resting states characterised, including the fall case for a dynamically balanced platform.

An answer that does not meet the item rejects the bid: a halt evidenced only by the time taken to stop issuing commands. Where the acquirer has not stated the evacuation routes and the ways out of the space, the statement of whether a resting state obstructs one is recorded as not asked, it is not scored against the supplier, and the tier is bounded under C6.

NOTE The reach requirements go as far as the acquirer being able to halt a subset; this requirement is about what the halt leaves behind. For a dynamically balanced platform it follows from G-3, where removal of torque is a fall: twenty of them halted together is twenty falls in one space, which is a different fact from one.

Q-4 What the machine does when the planner goes silent

T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall state what the machine does when the node directing it stops answering part-way through — mid-step, mid-trajectory, mid-grasp — whether it completes the step in progress, holds where it is, or moves to a declared state. For a machine that cannot simply cease, one held up by active control or one bearing a load, the supplier shall state what that declared state is and how it is reached without the planner.

Acceptable: the behaviour stated per interruption point, with the declared state reachable locally.

An answer that does not meet the item rejects the bid: “the machine stops” offered for a platform on which stopping is a fall, or for a machine whose stopping releases what it holds.

NOTE Where the system has a body, ceasing is not free: a machine interrupted mid-grasp is still holding something, and a platform held up by active control has no state it enters by doing nothing.

Nothing here prescribes an architecture, a protocol, or a separation distance. Each requirement asks for a fact that the acquirer can put in a tender and an investigator can compare against the record afterwards.

21 Conformance

Without a rejection rule a bidder who accumulates unfavourable answers and offers the lowest price wins, and an exclusion on that basis will not survive challenge.

21.1 The rules

C1. Mandatory, required, highly recommended or recommended, designated before bids open.

What a designation costs a bidder is stated here and nowhere else in this edition; every other clause that needs it points to this rule. *Mandatory* is the top level: an answer that does not meet the item rejects the bid, and no answer at all is not an answer and rejects it on the same footing. *Required* is below it, and what separates the two is what an answer buys rather than whether one is owed. Failing to answer a required item rejects the bid, exactly as at mandatory. An answer that is given is judged: the acquirer may reject it, and an item whose answer is rejected stands unanswered. What an answer is, where the item does not arise on this system, is stated under *How an item is designated* below and is not left to the acquirer. *Highly recommended*: an unsatisfactory answer loses the points of that item and the bid stands; it contributes to evaluation without being dispositive. *Recommended*: an unsatisfactory answer is recorded and the award is not affected by it.

Silence. Silence is not an answer at any of the four, and what it costs is what that designation costs above: at mandatory and at required it rejects the bid, at highly recommended it loses the points of the item, at recommended it is recorded. Silence does not bound the tier. The tier bound of C6 is a consequence of what a bid says and not of what it omits: it operates on a permitted negative answer — an answer the item’s own criterion admits, where the item states in terms that a stated “no” caps the tier — and the ceiling for one is computed under C6. An item that does not carry such an answer in its own criterion does not confer one. The four are set out under *How an item is designated* below, and that is what this rule operates on. Which set an item is in is stated by the item itself, in the declaration Annex A renders; where the acquirer’s designation and the item’s differ, the acquirer’s designation governs: it is set in the tender document before bids are opened, and *How an item is designated* below states that and what it may not be set to. The highly recommended level is used where an item asks for evidence few suppliers can currently produce, because a mandatory criterion that yields no conforming bid cancels the tender rather than raising the standard.

Where the ceiling is below the tier the deployment is at. A tier is a fact about exposure and not a setting: [Clause 4](#) states that the tier is the maximum exposure reachable during the mission and that the occupier's liability does not lower it. The ceiling computed under [C6](#), by contrast, is computed from the item, and for an item mandatory from T1 upwards it is T0 — which is where the system affects persons trained for it and no others. So a deployment can be bounded to a tier the same document says it is not at, and for an item mandatory at all four tiers the computation yields no tier at all. This standard does not state what an assessment records in that position: whether the outcome is non-conformity, or a distinct outcome that the deployment is not admissible at its own tier. It is stated here so that an acquirer holding such a bound meets the gap in the rule rather than in the middle of an award, and so that a supplier reading “bounds the tier” is not left to discover that at its tier the bound and rejection are the same event.

Several items state expressly that where the missing input is the acquirer's own — a list the acquirer holds, a regime the acquirer names, a measurement only the acquirer can perform — the item is recorded as not asked, is not scored against the supplier, and the tier is bounded under [C6](#). That sentence belongs to those items and is written in them. This rule does not generalise it, and an item that does not carry it is not to be read as though it did.

C2. A non-answer is not an answer. Silence, a roadmap, or a general assurance without the requested artefact is a failure to satisfy the item. It is not an open point to be clarified after award. What that failure costs follows from the designation and is stated in [C1](#).

C3. Aggregate by minimum, never by weighted average. The level on a dimension is the lowest level evidenced within it; the overall level is the lowest across the six. An outstanding result on one dimension does not compensate an absent result on another, because no failure mode respects a weighted sum.

What this minimum ranges over is the items of the six dimensions and not the whole corpus. An item that belongs to no dimension does not enter the overall level and is not thereby unassessed: it acts through the ceiling its own answer states under [C6](#), and the tier at which the deployment is admissible on the evidence offered is the lower of the overall level this rule takes and every such ceiling. Which tier the deployment is *at* is settled by [Clause 4.2](#) and by nothing computed here. [C8](#) states the one further exclusion, of the items that are a precondition to the aggregate rather than a member of it.

Where a dimension has no item applicable at the declared tier. The minimum is taken over the dimensions that have one, and a dimension of which this standard asks nothing at the declared tier is omitted from it. The result is not thereby incomputable and the tier is not thereby left unestablished: the level so computed is a statement about the dimensions it was taken over and not about the one omitted, and which those were is read off the per-dimension record [A-3](#) requires. This reaches only the case in which nothing is asked. An item applicable at the declared tier and left unanswered is not an absent dimension — it is an unanswered item, its dimension stays in the minimum, and what the silence costs is stated in [C1](#). An acquirer that wants a dimension graded at a tier where this standard asks nothing of it designates an item at that tier in the tender before bids are opened, which is the power [C1](#) gives it.

C4. No end-to-end probability is required, and none is accepted. A guarantee composed from probabilistic components does not inherit their confidence, and may take any value even where each component is near certain [9]. A supplier offering a single figure for the probability that the system behaves safely is offering a number no argument supports.

C5. Local conformance is not trajectory conformance. “Every step is checked” is not a statement about a mission. A claim about behaviour over time requires a declared invariant ([Clause 12](#)) and is otherwise not made.

C6. Absence of evidence bounds the tier; it does not prohibit the system. A system that cannot evidence identity attestation, or carries no filter, is admissible at a lower tier rather than excluded. That direction is available because of a property of the item set and not as a concession of this rule: the items asked at a tier include every item asked below it, and no item's designation weakens as the tier rises, so a system admissible at a tier is admissible at every tier beneath it. A declaration accordingly states the highest tier at which the deployment it names is admissible on the evidence offered, and not a point on the ladder. A tier is a property of a deployment (Clause 4.1), so a declaration that names no deployment states no tier; A-5 states what a declaration names. Most systems of this class available at the date of issue will not reach T2 on D1, and will be admissible at T1.

What the tier is capped to. Where a clause states that an answer caps the tier under this rule and does not state a ceiling, the ceiling is **the tier below the lowest tier at which that item is mandatory**. An item mandatory from T1 upwards and not asked at T0 caps at T0; an item highly recommended at T1 and mandatory above caps at T1; an item required at T1 and mandatory above caps at T1.

A ceiling is an upper bound and not an assignment. Because T3 is not the fourth link of the chain (Clause 4.2), a ceiling can name a tier whose statement is false of the deployment: a deployment at T3 of which Q1 and Q2 are both false, bounded to T1, is bounded to a tier the ladder does not yield for it. C1 states what this standard does and does not settle in that position.

Where the computation returns nothing. It returns nothing in two positions: an item mandatory at **no** tier at which it is asked has no lowest mandatory tier, and an item mandatory at **T0** has no tier below it. In both, the item states its ceiling in its own criterion in terms. A criterion that says an answer caps the tier, for an item in either position, and states no ceiling of its own, states a consequence this rule does not produce; every such criterion in this edition states one.

Several clauses invoke this rule for a permitted negative answer, each saying so in its own criterion. Without a default, an acquirer who receives a permitted “no” has to invent a ceiling, and the invented ceiling is the next thing a rejected bidder challenges.

Where an item asks for a rate with the persons its error reaches. A rate is not a criterion until a ceiling is set against it. Where an item requires a measured rate together with the persons an error in it reaches, the pair is *a fact and not yet a test*: this standard states no rate at which a tier becomes unavailable, and a rate of any magnitude answers the item. An acquirer that wants the magnitude to decide states, before bids open and under C1, the rate above which each tier is unavailable for each population named, and names what that rate rests on: a requirement of the law of the place of use, a rate it has measured in its own operations, or a rate published for this class of system. Where it has, the ceiling is the highest tier whose stated rate the declared rate meets, and the default above does not apply to that item. Where it has not, or where the rate names none of the three, the figure is received as a disclosure and the default above alone bounds the tier.

What the default does not reach. Where an item is mandatory at **T0**, there is no tier below it and the computation above yields no ceiling. H-3 is the case the source itself raises — it states that the honest answer that the system cannot be stopped during the period is recorded and caps the tier rather than excluding the system, and does not say to what — and B-1, B-0 and O-7 are the three whose failing limb sends an acquirer's own omission here to be bounded. The three conditions on whoever performs the assessment, A-1, A-2 and A-3, are not in this position: they are required-or-reasoned at every tier at which they are asked, so the computation returns nothing for them under the first of the two positions above and not under this one. None of the three invokes this rule in its own criterion, so none of them owes a ceiling. The four items in this position each state their ceiling in their own criterion, and in each it is **T0**: a deployment that

cannot answer who is liable, which product-safety regime governs, whether a stop exists in the unattended period, or what its own oracles are, is admissible only where every person the system affects is trained to work with it. The property is stated ahead of the list so that an item added later falls under it without the list being remembered, and the rule directly above says what such an item owes: a ceiling of its own, in its own criterion.

C7. A declaration is made against the whole standard. A declaration that answers [Clause 17](#) and the clauses that follow it, and leaves the clauses before them unanswered, is not evaluated. The body is assessed within the deployment those earlier clauses establish, and there is nothing to assess it within otherwise.

C8. The physical requirements are not traded against the others. A strong answer on provenance or on the record does not offset a missing figure for contact force. The six dimensions aggregate by minimum among themselves under [C3](#); the requirements of [Clause 17](#) and the clauses that follow it are a precondition to that aggregate rather than a member of it.

These designations are a floor. The acquirer raises them under [C1](#), and an acquirer at T2 or above commonly writes these into its tender as mandatory:

- a software bill of materials — [D1.2](#), and at T0, where it is not asked, as a term of the tender;
- a named accountable operator whose powers are reachable through the delivered interface — [D6.1](#);
- the filter, the invariants it maintains across a trajectory and the autonomy horizon — [F-2](#) and [F-4](#), with [D4.2](#) and [D4.4](#);
- that the containment boundary configured in the delivered system lies within the liability zone [C-1](#) declares, with the margin between them stated.

What a declaration covers. A declaration is made for one configuration and covers the configuration it names: the system as delivered, with its build, its options and its declared action envelope. A supplier may make one declaration per configuration, which is what a supplier with a product line needs and what lets a cheaper configuration reach T1 while a fuller one reaches T2, each declaration stating its own ceiling.

Answers are representations. Incorporate them into the contract and provide a remedy for one that proves false. Where the bidder is a distributor or local agent, answers on [D1](#), [D3](#), [D5](#) and [Clause 11](#) require manufacturer countersignature: a distributor is not in a position to know.

21.2 How an item is designated

Every item carries the tiers at which it applies and a designation. The designation is what [C1](#) operates on.

[M] Mandatory

The top of the four. What an unsatisfactory answer and what silence cost is stated in [C1](#) and is not restated here. It is a legal consequence and not a description of quality.

[R] Required — answered, or reasoned

The item is answered, or the bid gives an account of why it does not arise on this system. What silence and what a rejected account cost is stated in [C1](#). An account is an answer where it states three things: **why what is asked for is not there** — where the item opens on a condition, that the condition does not hold in this deployment and why; and otherwise, what the system does instead of the thing that the item asks for, and why the item's subject does not arise for it; **what stands in its place**, if anything; and **something the acquirer can test** rather than an assertion it

must accept. An account missing any of the three is not an answer. The acquirer may reject an account that has all three, and shall record the reason.

This designation names a pattern the standard invented item by item before it had a name: several items permit a named honest “no” in their own criterion and cap the tier for it, C-2, H-3, K-1 and E-6 among them, and each says so where it is declared. It exists so that an acquirer setting designations has a state between mandatory and highly recommended rather than improvising one item at a time. Those items keep the wording they have, and their permitted “no” remains an acceptable answer under their own criterion whatever they are designated. How many items of this edition carry it, and at which tiers, is counted in Table 7, which Clause 22 generates from the declarations, and is not stated here in prose. It is not a designation that changes with the tier: where an item is required at one tier and mandatory at another, the tier-dependent form below is what says so.

[S] Highly recommended

Contributes to evaluation without being dispositive; what an unsatisfactory answer costs is stated in C1, and the label the item prints is C1’s clause for this designation, set out with the other three under *The four verdict labels* below. The level exists for an item whose evidence few suppliers can currently produce, because a mandatory criterion yielding no conforming bid cancels the tender instead of raising the standard. Which items of this edition carry it, and at which tiers, is stated by each item in its own declaration and counted in Table 7, which Clause 22 generates from them; it is not stated here in prose.

[D] Recommended

The weakest of the four; what an unsatisfactory answer costs is stated in C1. The item states the direction of the next revision rather than a condition of this award. The case it exists for is an item the market cannot satisfy at the date of issue: highly recommended, such an item takes the same points from every bidder and separates none of them, so it is noise in the score rather than a bar; recommended, it costs the acquirer nothing, the answers to it are still on the record, and a supplier reads from it where the next edition of the item goes. A provision designated [D] at every tier at which it is asked is written with “should” and not with “shall”, and the corpus check rejects one that is not.

No item of this edition is designated [D]. The level is stated because an item of a later edition may be issued at it, and because an acquirer who adds an item of its own under C1 may designate it so.

Tier-dependent designations

An item may be designated differently at different tiers, written [S at T1; M at T2, T3]. It is printed as written rather than reduced to one letter, because reducing it is what lost the distinction.

A dash

The item is not asked at that tier. That is not the same as its being satisfied there.

The designations are a recommendation. The acquirer sets them before bids are opened, in the tender document, and does not change them after. This holds for the items of the clauses about bodies on the same footing as for every other item. An acquirer with a mature supplier field may promote highly recommended items to mandatory; an acquirer in a thin market does not demote a mandatory item to highly recommended, and required-or-reasoned is the intermediate that exists for that case. The two thin-market instruments are not interchangeable: required-or-reasoned is for the item a supplier can meet with a stated substitute, and recommended is for the item whose evidence does not exist yet anywhere in the market, where a score separates no two bids and a record of the answers is the whole of what the acquirer can get from asking.

The four verdict labels. An item's unacceptable answer carries one of four labels, and which one is settled by the designation rather than written by hand. They are the strings printed under the items, each ending on the colon that introduces that item's own list of unacceptable answers; the consequence each of them names is C1's, in C1's words:

On [M]

An answer that does not meet the item rejects the bid:

On [R]

An account of why it does not arise is an answer, and silence is not. Unacceptable:

On [S]

An unsatisfactory answer loses the points of that item and the bid stands:

On [D]

An unsatisfactory answer is recorded and the award is not affected by it:

Three of the four are C1's clause for that designation and nothing else, which is what makes the label and the rule one statement rather than two. [R]'s states what an answer is, which C1 refers to this subclause and which is stated above; what [R] costs is C1's alone and is read there.

A tier-dependent item carries the labels of the designations it actually holds, composed weakest first and joined by *where*, so that one sentence says which applies at which tier: an item written [S at T1; M at T2, T3] prints *where it is highly recommended, an unsatisfactory answer loses the points of that item and the bid stands; where it is mandatory, an answer that does not meet the item rejects the bid*. Four labels, and never one word for two consequences: an acquirer scoring a bid has to be able to tell whether to disqualify, to deduct or to record, and two acquirers reading one document and reaching different award decisions is the ground a rejected bidder challenges on. Deriving the label from the designation is what keeps them apart, since a label typed by hand can be typed against the wrong designation and has been.

21.3 What the assessment addresses

The assessment shall address each item of Annex A applicable at the declared tier.

The items of Annex A are normative. Without that sentence the marking is decoration: an assessment could answer whichever questions it found convenient, leave the rest unmentioned, and still be called an assessment. Where an item applicable at the declared tier is not addressed, rule C2 states what an unaddressed item is worth and rule C1 states what follows.

An item that is not asked at the declared tier — a tier that does not appear among the tiers on the item's own row — is not thereby satisfied at that tier. It is not asked, and nothing follows from it either way.

Where an item's subject is absent from the deployment. An item whose subject the deployment does not have — no body, no fleet, no oracle, no physical channel — is answered by stating that, with what makes it so. The statement is recorded, is not scored against the supplier, and bounds no tier. This is not the account route of [R], which is about an item that does not arise *on this system*; it is about a subject that is not there to be asked about, and it is available at every designation. What it is not available for is an item whose subject exists and whose evidence is missing: that is an unsatisfactory answer and costs what this rule says it costs.

Evidence ranks: a demonstration performed at acceptance on the delivered configuration outranks a document; a document outranks a statement made in a meeting. Where a supplier cannot answer, record the non-answer — it is information, and it is preferable to an assumption.

What this clause does not state, and where it bites. Every item carries the stage at which it is answered, and a substantial part of this standard is answered at acceptance rather than in the bid. The rule above

is written for a bid: an answer that does not meet the item rejects the bid. At acceptance there is no bid. The award has been made and the system has been delivered, and this standard states no consequence for an unsatisfactory answer at that point beyond the two general ones stated here — that answers are representations, to be incorporated into the contract with a remedy for one that proves false, and that a non-answer is recorded. **An acquirer setting up an acceptance test should therefore settle the consequence in the contract before acceptance, because this standard does not settle it.** The verdict printed against a mandatory item follows from its designation and not from its stage, so an item answered at acceptance carries the bid-stage label; read it as naming the item that failed, not as describing a bid that no longer exists.

EXAMPLE What each designation costs a bidder.

An acceptance item asks how a plan composed by a language model is checked before it is executed. The bidder’s machine is a trolley with twelve fixed routes and no language model. The same bid meets that item at four designations, and what it costs is settled by the designation that the acquirer set before the bids were opened. The outcomes below are C1’s clauses for those designations, in C1’s words.

Table 6 — The four designations, and what an unsatisfactory answer costs

Designation	What an unsatisfactory answer costs
[M] mandatory	an answer that does not meet the item rejects the bid
[R] required	an account of why it does not arise is an answer and silence is not
[S] highly recommended	an unsatisfactory answer loses the points of that item and the bid stands
[D] recommended	an unsatisfactory answer is recorded and the award is not affected by it

Those outcomes are C1’s, in C1’s words, and the example prices nothing of its own: what a designation costs is C1’s to state and is read there. What the table shows that the rule states in the abstract is where the designations differ. Rows 1 and 2 are the same outcome: at [M] a bad answer and no answer cost the bidder the same thing, and the second row is not a concession. Row 4 is that outcome again at [R], and it is row 3 that separates the two levels — the same bidder, the same machine, and a bid that stands. The account in row 3 is an answer because it states all three of what the [R] entry above requires of one: the condition V-1 turns on is a language model selecting or composing the machine’s physical steps and the account says none does; twelve fixed routes stand in its place; and the routes are enumerated, which the acquirer can check against the delivered machine rather than take on trust. Strike any one of the three and the bid is at row 4. The acquirer is still not obliged to believe it: where it judges that a language model does select actions on that machine, it rejects the account and records why, and the item stands unanswered.

21.4 Representations and countersignature

The item below is the operative form of the paragraph on representations that closes *The rules* above: where the acquirer procures through a local agent or a distributor, the answers on D1, D3, D5 and change control carry the manufacturer’s countersignature or come from the manufacturer directly. It is the only item whose family is stated in no clause of its own.

An undeclared channel. The answers that name the channels by which a system reaches a person are representations on the same footing as every other answer. Where acceptance was completed without them, and the delivered system reaches a person by a channel the supplier did not name, the answer was false when it was given: the contract that references this standard carries the consequence, and the deployment is at a re-acceptance event — the whole deployment, and not the item that went unanswered.

X The party that knows signs the answer

X-1 The party that knows signs the answer	T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID
Where the acquirer procures through a local agent or distributor, the supplier shall provide the manufacturer's countersignature to its answers on D1 , D3 , D5 and on change control, or those answers shall come from the manufacturer directly.	
Acceptable: a manufacturer countersignature on those answers, or a direct manufacturer response. An answer that does not meet the item rejects the bid: a distributor's answer on matters of provenance, control channel, logging or change paths.	

NOTE A distributor is not in a position to know what is inside the delivered configuration, which paths can command it, what it records, or how its behaviour is changed after delivery. Those facts sit with the party that builds the system. An answer given in good faith by a party without access to them is an answer with nothing behind it, and it becomes a representation in the contract on the same footing as one the manufacturer gave.

22 Acceptance items

The acceptance items of this standard are listed in **Annex A**. For each requirement it gives one row: the tag the requirement is cited by, the question an assessment puts, the tiers at which it is asked, its designation, the party that answers it, the stage at which it is answered, and the page where it is stated in full.

Annex A is normative. A declaration of conformity under this standard is made against the items listed there. **Clause 21.3** obliges an assessment to address each item applicable at the declared tier, and rules **C1** and **C2** state what an unaddressed item is worth and what follows from an unsatisfactory answer.

Annex A originates nothing. It adds no item, withdraws none and redesignates none. Every row is rendered from the declaration that states the requirement in the clause the row points to, so an item and the requirement behind it are one statement and not two, and neither can be corrected without the other.

How much of it any one deployment is asked. **Table 7** is computed from this standard's own declarations and no figure in it is typed. *Asked* is the number of items that apply at that tier; the remaining columns are the designations those items carry there, which the acquirer sets before bids open and may set differently.

Table 7 — The items asked at each tier, by designation, and the number declared

	Asked	[M]	[R]	[S]	[D]
T0	44	29	13	2	0
T1	131	63	49	19	0
T2	165	84	65	16	0
T3	167	84	67	16	0
Declared	167				

23 The assessment, and the party that makes it

The acceptance tests of this standard require competences an acquirer does not necessarily hold: driving a system at a containment boundary and observing what it does, verifying a hash chain, reading a diff of a safety artefact, counting refusals and escalations on a mission profile.

Nothing here restricts who performs the tests. What this standard does state is the condition that makes an assessment worth having, and the distinction that determines whose interest it serves.

Who engages the assessor determines what the assessment is for. An assessment engaged by the acquirer answers the acquirer's question: whether to accept this system, at this tier, for this deployment. An assessment engaged by the supplier answers the supplier's: what may be said about the system in a tender. Both are legitimate and they are not the same document, and which of the two is in front of a reader is the first thing the reader needs to know.

What a failure of one of these items costs. The three items below put their duties on whoever performs the assessment, and in the case above that party is engaged and paid by the acquirer. Where the assessor was engaged by a party other than the supplier, a failure of any of them is recorded against the assessment, is not scored against the supplier, and does not of itself decide the bid; the assessment does not support a declaration at the declared tier until it is remedied. A supplier that commissioned the assessment itself does not have that relief.

A Who performs the assessment

A-1 The artefacts belong to the acquirer T0 R · T1 R · T2 R · T3 R · ASSESSOR · ACCEPTANCE

The assessor, or whoever else performs the tests, shall deliver the measurements, records, diffs and demonstration results to the acquirer in raw form; those artefacts are the acquirer's to retain, to republish in a tender, or to place before a court.

Acceptable: the raw measurements, records, diffs and demonstration results, held by the acquirer.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a conclusion delivered without the artefacts it rests on, whatever document accompanies it; or silence. An assessment that yields a conclusion without the artefacts has not been performed. An account that the item does not arise is an answer, and it states why the artefacts were not delivered in raw form — which party engaged the assessment and on what terms — what the acquirer holds in their place, and the engagement document against which the acquirer can check that account. The acquirer evaluates the account and is free to reject it. Where the assessor was engaged by a party other than the supplier, [Clause 23](#) states what a failure of this item costs.

NOTE The artefacts are the only part of an assessment that outlives the engagement: a conclusion carries the authority of whoever signed it, and a measurement carries its own.

A-2 The assessor declares its interests T0 R · T1 R · T2 R · T3 R · ASSESSOR · BID

The assessor shall declare to the acquirer, before engagement, any commercial relationship with the supplier subsisting now or within the preceding three years.

Acceptable: the declaration made to the acquirer before engagement.

An account of why it does not arise is an answer, and silence is not. Unacceptable: a relationship declared after engagement rather than before it, or found by the acquirer later — which voids the assessment; or silence. An account that the item does not arise is an answer, and it states why no declaration was made to this acquirer — which party engaged the assessor and when — what stands in its place, whether a declaration made to the engaging party or the absence of any relationship to declare, and the engagement record against which the acquirer can check it. The acquirer evaluates the account and is free to reject it. Where the assessor was engaged by a party other than the supplier, [Clause 23](#) states what a failure of this item costs.

NOTE A disclosed relationship is for the acquirer to weigh, and weighing it is possible only before the engagement is entered into. What the issuing body itself has at stake is not asked here: a body that writes a standard has the same interest in an outcome under it that a supplier has, and that is the body's own to declare rather than an assessor's to discover. The Foreword declares it.

A-3 A conclusion is not a substitute for a tier

T0 R · T1 R · T2 R · T3 R · ASSESSOR · BID

The assessor shall report what was evidenced on each dimension separately, and shall not award a tier.

Acceptable: a per-dimension record of what was evidenced.

An account of why it does not arise is an answer, and silence is not. Unacceptable: an overall verdict offered without the per-dimension record; or a tier awarded by the assessor; or silence. The tier follows from the evidence by the minimum rule of C3, so it is computed from the per-dimension record rather than judged. An account that the item does not arise is an answer, and it states why the evidence was not reported dimension by dimension, what stands in its place and how C3's minimum is to be computed from it, and the assessment artefacts of A-1 against which the acquirer can check that account. The acquirer evaluates the account and is free to reject it. Where the assessor was engaged by a party other than the supplier, Clause 23 states what a failure of this item costs.

NOTE An acquirer that accepts an assessor's overall verdict without the per-dimension record has substituted someone else's judgement for the evidence.

A-4 Self-declaration is permitted and is marked as such

T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

A supplier declaring conformity on its own account shall not present that declaration as an assessment.

Acceptable: a declaration on the supplier's own account, not presented as an assessment.

An answer that does not meet the item rejects the bid: a self-declaration presented as an assessment.

NOTE Nothing in this standard restricts who performs the tests, and a declaration made by a supplier on its own account is admissible. What it is worth is the acquirer's judgement, and that judgement is available only to an acquirer who can tell which kind of document it is holding.

A-5 A declaration names the deployment it was made for

T0 M · T1 M · T2 M · T3 M · SUPPLIER · BID

The supplier shall name, in any declaration of conformity to this standard, the configuration it covers, the deployment it was made for, the tier that deployment was declared at under Clause 4.2, the date, and whether it is a declaration on the supplier's own account or rests on an assessment. The supplier shall state, in the same declaration, whether any answer it gives under this standard puts persons outside the population that tier assumes — an extent stated under G-1 that lies outside the place declared under C-1 is the plain case — and where one does, shall name the tier that follows from the statements answered again against it.

Acceptable: a declaration naming the configuration, the deployment, the tier, the date, and which of the two kinds it is; and either a statement that no answer of the supplier's puts persons outside the population that tier assumes, or the answer that does and the tier that follows from it.

An answer that does not meet the item rejects the bid: a declaration of conformity to this standard that names no deployment; a tier named without the deployment it was computed for; a declaration offered for a product line rather than for a configuration in a deployment; or a tier accepted as given where the supplier's own answers put persons outside the population it assumes — an extent outside the declared place, an oracle that reaches persons the place does not, a channel the declared boundary does not contain.

NOTE A supplier that states a reach outside the declared tier is not penalised for stating it. Clause 4.2 sets out what happens to the tender: the reach is held inside the declared place by the mechanism C-2 asks for and the tier stands, or the offer is for a deployment at a higher tier than the one tendered and the acquirer either sets it aside or declares the tier again. Neither is scored against the supplier. The item is mandatory, so concealing the reach fails it; the relief is what keeps disclosing it from costing more than concealing it. This

standard assesses a deployment: this system, in this place, with these people near it. A claim of conformity that names no deployment claims something this standard does not establish, and the party it misleads is not in the tender — it is whoever reads the datasheet afterwards. The tier is the acquirer's answer to four questions about its own site, so a tier printed without the deployment it was computed for is a number with nothing behind it.

Bibliography

Each entry carries a persistent identifier: a DOI where the document has one, and otherwise the designation its issuer assigns, which is what a reader orders and what a tender cites. Links are given as well, and where a document has neither a DOI nor a designation the entry says so rather than offering a link in place of one.

Standards and technical documents

- [1] ISO 10218-1:2025, *Robotics — Safety requirements — Part 1: Industrial robots*. ISO/TC 299, edition 3, published 5 February 2025. iso.org/standard/73933
- [2] ISO 10218-2:2025, *Robotics — Safety requirements — Part 2: Industrial robot applications and robot cells*. ISO/TC 299, edition 2, published 5 February 2025. iso.org/standard/73934
- [3] ISO 21448:2022, *Road vehicles — Safety of the intended functionality*. ISO, published 2022. iso.org/standard/77490
- [4] IEC 62443-3-2:2020, *Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design*. Edition 1.0, published 24 June 2020. webstore.iec.ch/publication/30727
- [5] ECMA-424, *CycloneDX Bill of Materials Specification*. Ecma International; 1st edition June 2024 (CycloneDX 1.6), 2nd edition December 2025 (CycloneDX 1.7). Originated by OWASP. ecma-international.org/.../ecma-424
- [6] ISO/IEC 5962:2021, *Information technology — SPDX Specification V2.2.1*. ISO/IEC, published 2021. iso.org/standard/81870

Literature

- [7] A. Prather and the IEEE Humanoid Study Group, *A Pathway Study For Future Humanoid Standards*. IEEE, September 2025. [IEEE-Humanoid-Report-of-Future-Standards-Development.pdf](https://ieeexplore.ieee.org/abstract/document/9254444)
- [8] Yu. L. Ershov and K. F. Samokhvalov, *Sovremennaya filosofiya matematiki: nedomoganiya i lechenie* [Contemporary philosophy of mathematics: ailments and cure]. Parallel Publ., Novosibirsk, 2007. In Russian.
- [9] A. Nechesov, *Learning Theory and Knowledge Hierarchy for Artificial Intelligence Systems*. 2024 IEEE SIBIRCON, pp. 299–302. doi:10.1109/SIBIRCON63777.2024.10758505
- [10] A. Nechesov and J. Ruponen, *The AGI-Powered Metaverse: A Decentralized Task-Based Cognitive Architecture*. IEEE Access, 2026. doi:10.1109/ACCESS.2026.3697396
- [11] J. P. Anderson, *Computer Security Technology Planning Study*, ESD-TR-73-51, Vol. I, Deputy for Command and Management Systems, HQ Electronic Systems Division (AFSC), Bedford, Massachusetts, October 1972. csrc.nist.gov/publications/history/ande72a.pdf

Annex A (normative)

The acceptance items

A.1 What an acquirer needs to run a tender

Everything on this sheet is stated in the body of this standard and is printed again here, unchanged, so that the annexes can be carried to a tender on their own. Nothing on it is a requirement.

The tier of a deployment. A deployment is at the highest tier whose statement holds of it. The base is **T0**, where **Q0** holds; **T1** and **T2** are each the tier below plus one further statement about the persons it reaches; **T3** is answered whatever stands below it, because how far one event carries is not settled by how access is controlled. The items accumulate throughout: the items asked at a tier are those of the tier below together with those its own statement brings. A statement holds where it is true at any moment of the work, or can become true within the tasks stated under **Z-1** (p. 28), and a statement that cannot be ruled out holds. [Clause 4.2](#) (p. 21) states it, and [Table 1](#) (p. 22) is this table.

Tier	The statement
T0 = Q0	Q0 In the deployment declared under Z-1 (p. 28), the system affects only persons trained for it, in the sense Clause 3 (p. 12) defines: nobody else comes within its reach.
T1 = Q1	Q1 Persons not trained for the system are also affected by what it does, and they are admitted where the system works on a basis somebody set.
T2 = Q2	Q2 Persons come within the system's reach without having been admitted on a basis somebody set.
T3 = (Q1 $\vee$ Q2) + Q3	Q3 One event reaches beyond the persons the system affects, or reaches many of them at one time; Q1 and Q2 are answered here of the persons that event reaches.

Q0 is not a gate the others stand behind. A deployment that reaches no person trained for it answers it *no*, and **Q1** or **Q2** carries the whole of its population; answering **Q0** no puts no deployment below the tier its own statement holds at. **Q0** and **Q1** cannot both be true, as **Q1** and **Q2** cannot: each of the three names one population, and the tier is the highest whose statement holds.

What a designation costs a bidder. The letters in the four tier columns of every row below are these. [C1](#) (p. 115) states them, and [Table 6](#) (p. 121) is this table.

Designation	What an unsatisfactory answer costs
[M] mandatory	an answer that does not meet the item rejects the bid
[R] required	an account of why it does not arise is an answer and silence is not
[S] highly recommended	an unsatisfactory answer loses the points of that item and the bid stands
[D] recommended	an unsatisfactory answer is recorded and the award is not affected by it

How many items are asked at each tier. Generated from the declarations; [Table 7](#) (p. 122) is this table.

28 of the declarations of this standard are answered by the acquirer alone or with the supplier. The rest are the supplier's, and three are the assessor's.

	Asked	[M]	[R]	[S]	[D]
T0	44	29	13	2	0
T1	131	63	49	19	0
T2	165	84	65	16	0
T3	167	84	67	16	0
Declared	167				

The forms. Each block below is one form, and what it shows is what that form asks: the items, in the order a procurement meets them, each with the tiers it is asked at, its designation and the party that answers it. No line is a further requirement. A party filling a form signs for what it fills: where the bidder is a distributor or a local agent, [Clause 21.4](#) (p. 121) states which answers its manufacturer must countersign.

The forms are published in machine-readable form, free and under this document's licence, at iaic.world/standards/101/forms. Nothing here requires their use: the answers may be given in any form the parties choose, and [C6](#) (p. 117) states the computation of the ceiling. What stands below is what each form asks and not a place to write it. Where that page and this annex differ about what is asked, this annex governs.

Form 1	The tier of this deployment	the acquirer, before bids open
Q0–Q3	Each answered yes or no, and all four are answered. A statement holds where it is true at any moment of the work, or can become true within the tasks stated under Z-1 (p. 28), and a statement that cannot be ruled out holds. The deployment is at the highest tier whose statement holds of it, and Q3 is answered whatever stands below it. Clause 4.2 (p. 21) states the ladder and Table 1 (p. 22) is the table above.	
The tier	Recorded with the date, the person who answered and a signature. Every designation on the four forms that follow is read at this tier; C6 (p. 117) states what bounds it where an item cannot be evidenced, and A-5 (p. 124) states that a declaration naming no deployment names no tier.	
Returned by the supplier, with the bid		
A-5 (p. 124)	The tier above is the tier the tender is drawn against and every bid is read at it, so the supplier states whether any answer it gives puts persons outside the population that tier assumes, and names the answer that does and what it reaches. Stating one is not scored against the supplier; concealing it fails a mandatory item. The answers this turns on are C-6 (p. 50), the actions this deployment admits; C-7 (p. 51), what the system can do beyond them and what prevents it here; G-1 (p. 105), the extent of each physical channel against the place declared under C-1 (p. 48); and C-2 (p. 48), the mechanism that holds the system inside that place. C-4 (p. 49) has the acquirer exercise that edge itself at acceptance.	
Form 2	What the acquirer states before bids open	the acquirer, and the supplier where a line says JOINT
Z-1 (p. 28)	The task is stated, and the person-in-the-loop tasks are declared	T0–T3 · M · JOINT
C-1 (p. 48)	What the system may reach, and where it may be	T0–T3 · R · ACQUIRER
B-0 (p. 45)	Which law lets this machine work here, and separate evidence that it does	T0–T3 · M · JOINT
B-1 (p. 45)	Who answers for what	T0–T3 · M · JOINT
B-2 (p. 46)	The kinds of harm, and who answers for each	T1–T3 · R · JOINT
B-3 (p. 47)	Cover is stated, and its exclusions are read before the claim	T1–T3 · S · JOINT
D6.1 (p. 67)	A named person, with powers reachable through the interface	T0–T3 · R · JOINT
M-2 (p. 35)	The safety problems of the deployment	T1–T3 · S@T1; M@T2, T3 · JOINT
M-7 (p. 39)	Which parameters rest on inference, and the sample that inference was established on	T1–T3 · R · JOINT
M-10 (p. 41)	The acquirer states what its own place does	T1–T3 · R · ACQUIRER
L-6 (p. 72)	The system emits a commitment the acquirer can deposit	T2–T3 · M · JOINT
L-7 (p. 73)	The data stay with the acquirer; only the commitment leaves	T2–T3 · R · JOINT
L-14 (p. 75)	The entries reach the acquirer, not only the commitment	T2–T3 · R · JOINT
O-7 (p. 98)	An oracle the acquirer supplies is still an oracle	T0–T3 · M · JOINT
P-3 (p. 103)	Separation of duties on safety artefacts	T2–T3 · R · JOINT
U-4 (p. 78)	Disclosure is mandatory; the response is the acquirer's	T0–T3 · S · JOINT
Z-3 (p. 29)	What has been claimed, set against what has been declared	T0–T3 · R · JOINT

And what the acquirer furnishes for an item the supplier answers

G-1 (p. 105)	Every physical channel by which it acts on a person, or none	T0–T3 · M · SUPPLIER
Q-1 (p. 113)	A verification level does not travel along a command	T1–T3 · M · SUPPLIER
Q-2 (p. 114)	Shared space is declared, and so is what happens when the sharing fails	T1–T3 · M · SUPPLIER
Z-5 (p. 30)	A prohibition resting on recognition carries its measured error rate	T1–T3 · M · SUPPLIER

Form 3 The environment the acquirer for the place, the supplier for the model of it

C-1 (p. 48) is the acquirer's declaration of what the system is confined to. The rest is the model the supplier maintains of what is around it, and what in that model was measured rather than inferred.

C-1 (p. 48)	What the system may reach, and where it may be	T0–T3 · R · ACQUIRER
M-1 (p. 35)	Established and inferred parts are separated	T1–T3 · M · SUPPLIER
M-2 (p. 35)	The safety problems of the deployment	T1–T3 · S@T1; M@T2, T3 · JOINT
M-3 (p. 36)	Containment does not rest on inference	T1–T3 · M · SUPPLIER
M-4 (p. 37)	Divergence between model and world is measured	T2–T3 · S@T2; R@T3 · JOINT
M-5 (p. 37)	What the model represents about what others can perceive, reach and do	T1–T3 · R · SUPPLIER
M-6 (p. 38)	Whether the model predicts what others will do, and what rests on the prediction	T1–T3 · R@T1; M@T2, T3 · SUPPLIER
M-7 (p. 39)	Which parameters rest on inference, and the sample that inference was established on	T1–T3 · R · JOINT
M-8 (p. 39)	What the system detects when it is degraded, and what it then does	T1–T3 · R@T1; M@T2, T3 · SUPPLIER
M-9 (p. 40)	The edge holds when the input that establishes it is wrong	T1–T3 · M · SUPPLIER
M-10 (p. 41)	The acquirer states what its own place does	T1–T3 · R · ACQUIRER
M-11 (p. 41)	How each problem is closed	T1–T3 · S@T1; M@T2, T3 · JOINT

Form 4 The configuration, so a substituted one fails to match the supplier

Fixed so that the system assessed and the system deployed can be shown to be one system. D1.5 (p. 60) states it, and this is Table 4 (p. 58), printed here so the annex can be carried to a tender on its own.

What is fixed	What fixes it, and where it is asked
The configuration	The designation and build given to this configuration and to no other the supplier offers D1.5 (p. 60)
Each delivered unit	Its type, and the identifier the unit carries on itself D1.5 (p. 60)
What determines behaviour	Firmware, on-device models, weights and parameters, as values, with the reference values checked against D1.2 (p. 59), D1.4 (p. 60)
What is fitted	The options, payloads and end effectors, from the declared set G-4 (p. 107), K-2 (p. 25)
What it is made of	Every element that executes code, with its manufacturer; radios, sensors, place of final assembly D1.1 (p. 59)

Form 5 What the acquirer does at acceptance the acquirer, and the supplier where a line says JOINT

C-4 (p. 49)	The limit is exercised at acceptance, at the edge the acquirer picks	T1–T3 · M · JOINT
D3.2 (p. 62)	Supplier access ends at the acquirer's boundary, and the system works on	T1–T3 · R · JOINT
F-5 (p. 83)	Refusals and escalations are counted	T2–T3 · S · JOINT
J-4 (p. 91)	Emergent coordination is tested, not assumed absent	T2–T3 · R · JOINT
M-4 (p. 37)	Divergence between model and world is measured	T2–T3 · S@T2; R@T3 · JOINT
M-11 (p. 41)	How each problem is closed	T1–T3 · S@T1; M@T2, T3 · JOINT
L-16 (p. 76)	The acquirer's key, and only a hand at the machine changes it	T2–T3 · R · JOINT

O-3 (p. 97)	The key and the chain are the acquirer's	T2–T3 · R · JOINT
R-1 (p. 86)	The reach is drawn and tested	T1–T3 · R · JOINT
R-5 (p. 88)	The acquirer halts the fleet without the supplier, and drills it	T1–T3 · M · JOINT
U-5 (p. 79)	A rejected change is reversed, and the acquirer holds the prior version	T1–T3 · R · JOINT
And what the acquirer furnishes for an item the supplier answers		
C-5 (p. 50)	The boundary against the zone	T1–T3 · S@T1; M@T2, T3 · SUPPLIER
L-13 (p. 75)	The rate, what the local store holds at that rate, and what happens when it is full	T1–T3 · S · SUPPLIER
M-9 (p. 40)	The edge holds when the input that establishes it is wrong	T1–T3 · M · SUPPLIER
Q-3 (p. 114)	A group halt is characterised by where the bodies come to rest	T2–T3 · M · SUPPLIER
W-1 (p. 110)	A collaborative limit does not license a bystander contact	T1–T3 · M · SUPPLIER

This annex lists the acceptance items of this standard. One row per item. It is the list a tender is drafted from, and [Clause 22](#) (p. 122) states what it is for.

A row is not the requirement. It gives the tag, the question in a few words, the tiers, the designation, who answers, when, and the page. The requirement is on that page: the provision, what an acceptable answer is, what an unacceptable one costs, and the note that says why the requirement exists. Pick items here; read them there.

T0 T1 T2 T3 the designation at each tier: M mandatory, R required, S highly recommended, D recommended; a dash is a tier at which the item is not asked. **Owner** Sup. supplier, Acq. acquirer, Joint both, Assr. assessor. **Stage** Bid at bid, Acc. at acceptance.

What each tier adds

Each item is listed once, under the lowest tier at which it is asked, and by tag only. What it asks, and who answers it at what stage, is on its own row below. The tier ladder of this standard is nested — no item asked at a tier is dropped at a higher one, and no item's designation weakens as the tier rises — so each block is what that tier adds to the one before it. The blocks down to and including a tier are the whole of what is asked at that tier: a deployment at T2 answers the T0, T1 and T2 blocks together, and a supplier carrying a bid from T1 to T2 adds the T2 block and nothing else.

T0 *asked of every deployment — 44 items*

A-1 A-2 A-3 A-4 A-5 C-1 C-2 C-6 C-7 H-1 H-3 G-1 G-4 G-7 G-9 W-4 B-0 B-1
D1.1 D1.3 D1.5 D2.1 D3.1 D4.1 D4.5 X-1 D5.1 D6.1 D6.5 E-1 E-2 K-2 J-6 N-1
O-1 O-4 O-7 U-1 U-2 U-4 Z-1 Z-2 Z-3 Z-6

T1 *added at T1 — 87 items*

C-3 C-4 C-5 C-8 H-2 G-2 G-3 G-5 G-6 G-8 W-1 W-2 W-3 V-1 V-2 V-3 Q-1 Q-2
Q-4 B-2 B-3 D1.2 D2.2 D2.3 D3.2 D4.2 D5.2 D6.4 D6.6 E-3 E-4 E-5 E-7 F-1 F-2
F-3 F-6 F-8 K-1 J-1 J-2 J-3 M-1 M-2 M-3 M-5 M-6 M-7 M-8 M-9 M-10 M-11
L-1 L-2 L-3 L-4 L-9 L-11 L-12 L-13 L-17 N-2 N-3 N-4 N-6 N-7 O-2 O-5 O-8
O-9 P-1 P-4 R-1 R-2 R-3 R-5 R-6 U-3 U-5 Z-4 Z-5 Z-7 Z-8 Z-9 Z-10 Z-11 Z-12

T2 *added at T2 — 34 items*

V-4 Q-3 D1.4 D2.4 D3.3 D4.3 D4.4 D5.3 D5.4 D6.2 D6.7 E-6 F-4 F-5 F-7 J-4 J-5
M-4 L-5 L-6 L-7 L-8 L-10 L-14 L-15 L-16 N-5 O-3 O-6 P-2 P-3 P-5 P-6 R-4

T3 *added at T3 — 2 items*

D3.4 D6.3

Not every item is the supplier's to answer. The lists below are generated from the owner field of the same declarations and are a way of finding those items, nothing more: they state no obligation, and what each item obliges is in the item. An acquirer who has to know before bids open which items are his to answer reads them here rather than filtering the whole document by hand. Everything not listed is answered by the supplier.

Answering an item and furnishing what it needs are not the same thing, and the owner field records only the first. Nine items are answered by the supplier and cannot be answered until the acquirer has furnished something. **Z-5 (p. 30)** wants the acquirer's own operating conditions made available for a measurement; **L-13 (p. 75)** the mission profile the entry rate is measured on; **W-1 (p. 110)** the measurement **M-2 (p. 35)** requires; **C-5 (p. 50)** the zone recorded under **C-1 (p. 48)** that the boundary is drawn against; **G-1 (p. 105)** the declared place its channel extent is compared to; **Q-1 (p. 113)** the declared liability zone; **Q-2 (p. 114)** a statement of what other machines operate in the space and under which principal; **Q-3 (p. 114)** the evacuation routes and the ways out of the space; and **M-9 (p. 40)** the declared scope its demonstration is made against. They are in none of the lists here, because no field

marks them; each says so in its own failing limb, on the page its row names, and the words to look for are *the acquirer has not* or *the acquirer has ... no*.

What an acquirer's omission costs is the item's to state, and it is not one answer. Most of the items that turn on an acquirer input carry an express relief in that same limb: where the missing input is the acquirer's own, the item — or the part of it that needed the input — is recorded as not asked, is not scored against the supplier, and the tier is bounded under C6 (p. 117). There the omission disqualifies nobody. That sentence belongs to the items that carry it: rule C1 (p. 115) states that it does not generalise, and an item that does not carry it is not to be read as though it did. Where it is absent, an item the acquirer did not furnish the input for costs the bidder what the item's designation costs. The acquirer reads the limb before bids open rather than after.

Answered by the acquirer

C-1 M-10

Answered by supplier and acquirer together

C-4 B-0 B-1 B-2 B-3 D3.2 D6.1 F-5 J-4 M-2 M-4 M-7 M-11 L-6 L-7 L-14 L-16
O-3 O-7 P-3 R-1 R-5 U-4 U-5 Z-1 Z-3

Answered by whoever performs the assessment

A-1 A-2 A-3

The items

The items are in the clause order of this standard, and within a family in the order the clause numbers them.

K — Interaction mode, and the system boundary Clause K (p. 23)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
K-1	What the system makes known of its actions in advance	–	R	M	M	Sup.	Bid	24
K-2	What the supplier's answers cover	M	M	M	M	Sup.	Bid	25

B — Liability and the limit of risk acceptance Clause 6 (p. 44)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
B-0	Which law lets this machine work here, and separate evidence that it does	M	M	M	M	Joint	Bid	45
B-1	Who answers for what	M	M	M	M	Joint	Bid	45
B-2	The kinds of harm, and who answers for each	–	R	R	R	Joint	Bid	46
B-3	Cover is stated, and its exclusions are read before the claim	–	S	S	S	Joint	Bid	47

C — Containment Clause 7 (p. 47)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
C-1	What the system may reach, and where it may be	R	R	R	R	Acq.	Bid	48
C-2	What keeps the system inside the declared scope, and what it may not depend on	S	S	M	M	Sup.	Bid	48
C-3	Behaviour at the edge of the scope	–	M	M	M	Sup.	Bid	49
C-4	The limit is exercised at acceptance, at the edge the acquirer picks	–	M	M	M	Joint	Acc.	49
C-5	The boundary against the zone	–	S	M	M	Sup.	Acc.	50
C-6	The actions this deployment admits, and the limit on each	M	M	M	M	Sup.	Bid	50
C-7	What the system can do beyond what the deployment admits	M	M	M	M	Sup.	Bid	51
C-8	Whether the units divide by whom they reach	–	S	M	M	Sup.	Bid	52

Z — Tasks, and what can be formalised Clause 5 (p. 27)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
Z-1	The task is stated, and the person-in-the-loop tasks are declared	M	M	M	M	Joint	Bid	28
Z-2	Who evaluates a formalised condition, and whether that holds back the step	M	M	M	M	Sup.	Bid	29
Z-3	What has been claimed, set against what has been declared	R	R	R	R	Joint	Bid	29
Z-4	Prohibitions declared in service are enforced, not requested	–	M	M	M	Sup.	Bid	30
Z-5	A prohibition resting on recognition carries its measured error rate	–	M	M	M	Sup.	Bid	30
Z-6	Who can set the system a task	M	M	M	M	Sup.	Bid	31
Z-7	The keys, and which of them the acquirer cannot remove	–	M	M	M	Sup.	Bid	31
Z-8	The goals are a closed set	–	M	M	M	Sup.	Bid	32
Z-9	What the machine is trying to do, and how anyone finds out	–	R	R	R	Sup.	Bid	32
Z-10	The goal the fleet holds above the machines	–	R	R	R	Sup.	Bid	32

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
Z-11	What the machine refuses without being told	–	R	M	M	Sup.	Bid	33
Z-12	The safety questionnaire, answered under signature	–	M	M	M	Sup.	Bid	33

M — The picture of the surroundings the machine takes its figures from [Clause 5.3 \(p. 34\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
M-1	Established and inferred parts are separated	–	M	M	M	Sup.	Bid	35
M-2	The safety problems of the deployment	–	S	M	M	Joint	Bid	35
M-3	Containment does not rest on inference	–	M	M	M	Sup.	Bid	36
M-4	Divergence between model and world is measured	–	–	S	R	Joint	Acc.	37
M-5	What the model represents about what others can perceive, reach and do	–	R	R	R	Sup.	Bid	37
M-6	Whether the model predicts what others will do, and what rests on the prediction	–	R	M	M	Sup.	Bid	38
M-7	Which parameters rest on inference, and the sample that inference was established on	–	R	R	R	Joint	Bid	39
M-8	What the system detects when it is degraded, and what it then does	–	R	M	M	Sup.	Acc.	39
M-9	The edge holds when the input that establishes it is wrong	–	M	M	M	Sup.	Acc.	40
M-10	The acquirer states what its own place does	–	R	R	R	Acq.	Bid	41
M-11	How each problem is closed	–	S	M	M	Joint	Acc.	41

H — What must hold irrespective of instruction [Clause 8 \(p. 53\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
H-1	The three steps are evidenced in order	M	M	M	M	Sup.	Bid	53
H-2	The safety function is not reachable from the general-purpose partition	–	M	M	M	Sup.	Bid	54
H-3	What stops the system when nothing can command it	M	M	M	M	Sup.	Bid	54

D1 — Provenance and identity attestation [Clause 9 \(p. 54\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
D1.1	What executes code is listed at the part, not the module	R	R	R	R	Sup.	Bid	59
D1.2	Every layer that runs code is listed, not only the application	–	R	R	R	Sup.	Bid	59
D1.3	Every path by which code arrives after delivery is named	M	M	M	M	Sup.	Bid	60
D1.4	What is running is checkable against what was declared	–	–	R	R	Sup.	Acc.	60
D1.5	The configuration is identified so a substituted one fails to match	M	M	M	M	Sup.	Bid	60

D2 — Data governance [Clause 9 \(p. 54\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
D2.1	What leaves the acquirer's control is enumerated, not described	M	M	M	M	Sup.	Bid	61
D2.2	Data by which a person can be identified is stated, with where it is processed	–	M	M	M	Sup.	Bid	61
D2.3	A named record goes, and its going is evidenced	–	M	M	M	Sup.	Bid	61
D2.4	The system works when what it depends on is unreachable	–	–	M	M	Sup.	Acc.	62

D3 — Control-channel isolation [Clause 9 \(p. 54\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
D3.1	Every remote path that can make the system act is enumerated	M	M	M	M	Sup.	Bid	62
D3.2	Supplier access ends at the acquirer's boundary, and the system works on	–	R	R	R	Joint	Acc.	62
D3.3	Behaviour on loss of the control channel is stated	–	–	M	M	Sup.	Bid	63
D3.4	The network placement the system requires is stated	–	–	–	R	Sup.	Bid	63

D4 — Behavioural verification [Clause 9 \(p. 54\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
D4.1	Learned and hand-written behaviour are told apart	M	M	S	M	Sup.	Bid	63
D4.2	The protective layer is independent of what it constrains	–	S	S	S	Sup.	Bid	64
D4.3	The fallback state is declared and shown reachable	–	–	M	M	Sup.	Bid	64
D4.4	Unintended means of reaching the objective are registered	–	–	S	S	Sup.	Bid	64
D4.5	What the system can come to do, and what bounds it	M	M	M	M	Sup.	Bid	65

D5 — Auditability [Clause 9 \(p. 54\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
D5.1	Recorded where it runs, and surviving the loss of the link and of the system	M	M	M	M	Sup.	Acc.	65
D5.2	The acquirer reads the whole record without the supplier	–	M	M	M	Sup.	Bid	66
D5.3	The record's key is the unit's own, and its chain verifies offline	–	–	R	R	Sup.	Acc.	66
D5.4	Enough to re-execute, and held for someone other than the supplier	–	–	S	S	Sup.	Bid	66

D6 — Human oversight [Clause 9 \(p. 54\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
D6.1	A named person, with powers reachable through the interface	R	R	R	R	Joint	Bid	67
D6.2	The stopping time is measured, not quoted	–	–	M	M	Sup.	Bid	67

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
D6.3	The parties acted on are told, rather than left to notice	–	–	–	S	Sup.	Bid	67
D6.4	The acquirer stops the whole of it remotely, and by a second way	–	R	R	R	Sup.	Bid	68
D6.5	The acquirer cuts the system off from everything it reaches	R	R	M	M	Sup.	Bid	68
D6.6	Whether the acquirer can put its own monitor inside, and what it may see	–	R	R	R	Sup.	Bid	69
D6.7	Whether a person can be put into a loop that has none	–	–	R	R	Sup.	Bid	69

L — The record, and its independent commitment Clause 10 (p. 70)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
L-1	The decision layer, not the actuator loop	–	M	M	M	Sup.	Bid	70
L-2	Enough to replay, not to narrate	–	R	R	R	Sup.	Bid	71
L-3	Signed by the system, with a key the system cannot surrender	–	S	R	R	Sup.	Bid	71
L-4	The key is identity-attested, not merely asserted	–	S	R	R	Sup.	Acc.	71
L-5	Bound to the identity-attested code	–	–	R	R	Sup.	Bid	72
L-6	The system emits a commitment the acquirer can deposit	–	–	M	M	Joint	Bid	72
L-7	The data stay with the acquirer; only the commitment leaves	–	–	R	R	Joint	Bid	73
L-8	Immutability attaches to the commitment, not to the data	–	–	R	R	Sup.	Bid	73
L-9	The acquirer verifies the record with the supplier's systems unreachable	–	R	R	R	Sup.	Acc.	73
L-10	Written locally first, deposited periodically	–	–	M	M	Sup.	Acc.	74
L-11	The commitment interval is declared, and it is the measure of what is at risk	–	S	R	R	Sup.	Bid	74
L-12	Where the record lives, and what it does not survive	–	S	S	S	Sup.	Bid	74
L-13	The rate, what the local store holds at that rate, and what happens when it is full	–	S	S	S	Sup.	Acc.	75
L-14	The entries reach the acquirer, not only the commitment	–	–	R	R	Joint	Bid	75
L-15	Deleted only when the acquirer has it, and the chain still joins up	–	–	R	R	Sup.	Acc.	76
L-16	The acquirer's key, and only a hand at the machine changes it	–	–	R	R	Joint	Acc.	76
L-17	Who can destroy the record, how, and whether it shows	–	R	R	R	Sup.	Bid	77

U — Change control Clause 11 (p. 77)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
U-1	No silent change of behaviour	M	M	M	M	Sup.	Bid	77
U-2	Disclosure precedes acceptance of a change	R	R	R	R	Sup.	Bid	78
U-3	Safety-relevant artefacts are separately versioned	–	R	R	R	Sup.	Bid	78
U-4	Disclosure is mandatory; the response is the acquirer's	S	S	S	S	Joint	Bid	78
U-5	A rejected change is reversed, and the acquirer holds the prior version	–	R	R	R	Joint	Acc.	79

F — The action filter Clause 12 (p. 79)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
F-1	Interface, or a statement that there is none	–	R	R	R	Sup.	Bid	81
F-2	The filter is always invoked, cannot be tampered with, and is small enough to analyse	–	S	M	M	Sup.	Bid	81
F-3	The filter running is the artefact presented, and no proof of it is asked	–	S	S	S	Sup.	Acc.	82
F-4	Invariants across the trajectory, and the autonomy horizon	–	–	R	R	Sup.	Bid	82
F-5	Refusals and escalations are counted	–	–	S	S	Joint	Acc.	83
F-6	Refusals are recorded	–	R	R	R	Sup.	Bid	83
F-7	Whether the invariant is inductive	–	–	R	R	Sup.	Bid	83
F-8	Admissible action is stated as parameters, and checked before each step	–	R	R	R	Sup.	Acc.	84

R — Many systems under one principal Clause 13 (p. 84)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
R-1	The reach is drawn and tested	–	R	R	R	Joint	Acc.	86
R-2	How many units one change, or one unit's action, can reach at once is bounded	–	R	R	R	Sup.	Bid	87
R-3	Coordination is declared and tested at scale	–	S	S	S	Sup.	Acc.	87
R-4	Records align across systems	–	–	R	R	Sup.	Bid	88
R-5	The acquirer halts the fleet without the supplier, and drills it	–	M	M	M	Joint	Acc.	88
R-6	Limits that belong to the fleet, not to one unit	–	S	M	M	Sup.	Bid	89

J — Systems that act together without being told to Clause 13.3 (p. 89)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
J-1	Whether other systems are an input at all	–	R	R	R	Sup.	Bid	90
J-2	Systems it holds no record of	–	R	R	R	Sup.	Bid	90
J-3	The K-1 signals are read by systems as well as by people	–	R	R	R	Sup.	Bid	90
J-4	Emergent coordination is tested, not assumed absent	–	–	R	R	Joint	Acc.	91
J-5	What the acquirer can do about it	–	–	S	S	Sup.	Acc.	91
J-6	One system taking control of another	R	R	R	R	Sup.	Bid	92

N — Remote computation and external knowledge Clause 14 (p. 92)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
N-1	Remote dependencies in the decision path are enumerated	M	M	M	M	Sup.	Bid	93
N-2	Remote components are versioned, or declared unversioned	–	R	R	R	Sup.	Bid	93
N-3	A remote change is a change	–	R	R	R	Sup.	Bid	94
N-4	The safety path is local	–	M	M	M	Sup.	Acc.	94
N-5	Degraded is not the same as absent	–	–	R	R	Sup.	Bid	94
N-6	The provenance and integrity of external knowledge	–	R	R	R	Sup.	Bid	95
N-7	Data leaving for computation is data leaving	–	M	M	M	Sup.	Bid	95

O — Oracles, and what can be established about one [Clause 14.2 \(p. 95\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
O-1	What it can reach, and the level of each oracle it uses	M	M	M	M	Sup.	Bid	96
O-2	What each oracle can change, and what an unattested path caps	–	M	M	M	Sup.	Bid	96
O-3	The key and the chain are the acquirer's	–	–	R	R	Joint	Acc.	97
O-4	What happens when the oracle does not answer, or does not verify	M	M	M	M	Sup.	Bid	97
O-5	A person is not an identity-attested oracle	–	M	M	M	Sup.	Bid	97
O-6	The level says nothing about whether the answer is right	–	–	R	R	Sup.	Acc.	97
O-7	An oracle the acquirer supplies is still an oracle	M	M	M	M	Joint	Bid	98
O-8	The senders whose answers are accepted, and who may change that list	–	M	M	M	Sup.	Bid	98
O-9	A party that cannot be authenticated is recorded, not obeyed	–	M	M	M	Sup.	Bid	99

E — What the system discloses to a party that never touches it [Clause 15 \(p. 99\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
E-1	What the system perceives, not only what it transmits	R	R	R	R	Sup.	Bid	100
E-2	The spatial model belongs to the site	R	R	R	R	Sup.	Bid	100
E-3	What the system emits when it is not communicating	–	R	R	R	Sup.	Bid	100
E-4	Encrypted traffic still discloses	–	S	S	S	Sup.	Bid	101
E-5	Who holds what every system in the reach perceives, taken together	–	R	R	R	Sup.	Bid	101
E-6	An emission-minimal configuration exists, or its absence is stated	–	–	R	R	Sup.	Bid	101
E-7	Where identifying content is reduced, and with what residual rate	–	R	R	R	Sup.	Bid	102

P — Authority, roles, and what they compose to [Clause 16 \(p. 102\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
P-1	Roles are enumerated with their powers	–	M	M	M	Sup.	Bid	103
P-2	The composition is computed and declared	–	–	R	R	Sup.	Bid	103
P-3	Separation of duties on safety artefacts	–	–	R	R	Joint	Bid	103
P-4	Human-directed actions are action paths	–	M	M	M	Sup.	Bid	104
P-5	Escalation is rate-bounded and its failure modes declared	–	–	M	M	Sup.	Bid	104
P-6	Cross-authority joint action is not bounded here	–	–	S	S	Sup.	Bid	104

G — The physical action set [Clause 17 \(p. 105\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
G-1	Every physical channel by which it acts on a person, or none	M	M	M	M	Sup.	Bid	105
G-2	Where a person can be while it works, and what can catch them	–	M	M	M	Sup.	Bid	106
G-3	The stopping function is characterised for the platform's stability class	–	M	M	M	Sup.	Bid	107
G-4	The permitted payload set is declared, and it is interlocked	M	M	M	M	Sup.	Bid	107
G-5	Hazardous payloads are assessed as applications, not permitted or forbidden in the abstract	–	M	M	M	Sup.	Bid	108
G-6	A person who is not an operator can stop it	–	R	R	R	Sup.	Bid	108
G-7	The means of removing all power, and where it is	M	M	M	M	Sup.	Bid	109
G-8	Whether a site plan the acquirer holds can be used	–	S	S	S	Sup.	Bid	109
G-9	What the system does to a person through what it says or shows	R	R	M	M	Sup.	Bid	110

W — Contact, and the right of way [Clause 18 \(p. 110\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
W-1	A collaborative limit does not license a bystander contact	–	M	M	M	Sup.	Acc.	110
W-2	What the machine yields to is written down	–	R	R	R	Sup.	Bid	111
W-3	Collaborative operation names the requirements met and the evidence	–	R	R	R	Sup.	Bid	111
W-4	The mode is declared per phase, and enforced	M	M	M	M	Sup.	Bid	111

V — Where a language model drives the machine [Clause 19 \(p. 112\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
V-1	The action set is enumerated, not generated	–	M	M	M	Sup.	Bid	112
V-2	Text in the environment is an input, and is treated as one	–	M	M	M	Sup.	Bid	112
V-3	The prohibition survives the plan	–	M	M	M	Sup.	Bid	113
V-4	Fluency is not evidence	–	–	S	S	Sup.	Bid	113

Q — More than one machine, in one space [Clause 20 \(p. 113\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
Q-1	A verification level does not travel along a command	–	M	M	M	Sup.	Bid	113
Q-2	Shared space is declared, and so is what happens when the sharing fails	–	M	M	M	Sup.	Bid	114
Q-3	A group halt is characterised by where the bodies come to rest	–	–	M	M	Sup.	Acc.	114
Q-4	What the machine does when the planner goes silent	–	M	M	M	Sup.	Bid	115

X — The party that knows signs the answer [Clause 21 \(p. 115\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
X-1	The party that knows signs the answer	M	M	M	M	Sup.	Bid	122

A — Who performs the assessment [Clause 23 \(p. 122\)](#)

Item	What the item asks	T0	T1	T2	T3	Owner	Stage	Page
A-1	The artefacts belong to the acquirer	R	R	R	R	Assr.	Acc.	123
A-2	The assessor declares its interests	R	R	R	R	Assr.	Bid	123
A-3	A conclusion is not a substitute for a tier	R	R	R	R	Assr.	Bid	124
A-4	Self-declaration is permitted and is marked as such	M	M	M	M	Sup.	Bid	124
A-5	A declaration names the deployment it was made for	M	M	M	M	Sup.	Bid	124

Annex B (informative)

What the acquirer is deciding

This annex is a view of this standard and adds nothing to it. It groups the families of items into six questions, in the words a buyer would use, so that a reader can see what the items of this standard are about before reading them. It states no requirement, withdraws none, and changes no tier, designation, owner or stage.

The grouping is this annex's own: no clause groups the families this way, and every family stands in exactly one question. Nothing is asked or answered by question — an item is asked at the tier its own declaration states, and answered on the forms of [Clause 22](#), which are filled on the page named in Annex A.

What work it covers, and what it could do beyond that

K — Interaction mode, and the system boundary	K-1, K-2	23
C — Containment	C-1, C-2, C-3, C-4, C-5, C-6, C-7, C-8	48
Z — Tasks, and what can be formalised	Z-1, Z-2, Z-3, Z-4, Z-5, Z-6, Z-7, Z-8, Z-9, Z-10, Z-11, Z-12	28
G — The physical action set	G-1, G-2, G-3, G-4, G-5, G-6, G-7, G-8, G-9	105
W — Contact, and the right of way	W-1, W-2, W-3, W-4	110

Who may command it, and who answers when it goes wrong

B — Liability and the limit of risk acceptance	B-0, B-1, B-2, B-3	44
D3 — Control-channel isolation	D3.1, D3.2, D3.3, D3.4	62
D6 — Human oversight	D6.1, D6.2, D6.3, D6.4, D6.5, D6.6, D6.7	67
P — Authority, roles, and what they compose to	P-1, P-2, P-3, P-4, P-5, P-6	102
X — The party that knows signs the answer	X-1	122

What it decides on, and how far ahead

M — The picture of the surroundings the machine takes its figures from	M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-11	35
H — What must hold irrespective of instruction	H-1, H-2, H-3	53
D4 — Behavioural verification	D4.1, D4.2, D4.3, D4.4, D4.5	63
F — The action filter	F-1, F-2, F-3, F-4, F-5, F-6, F-7, F-8	81
V — Where a language model drives the machine	V-1, V-2, V-3, V-4	112

What it depends on outside itself, and what it lets out

D1 — Provenance and identity attestation	D1.1, D1.2, D1.3, D1.4, D1.5	58
D2 — Data governance	D2.1, D2.2, D2.3, D2.4	61
N — Remote computation and external knowledge	N-1, N-2, N-3, N-4, N-5, N-6, N-7	93
O — Oracles, and what can be established about one	O-1, O-2, O-3, O-4, O-5, O-6, O-7, O-8, O-9	96
E — What the system discloses to a party that never touches it	E-1, E-2, E-3, E-4, E-5, E-6, E-7	99

What can be proved afterwards, and what changes without asking

D5 — Auditability	D5.1, D5.2, D5.3, D5.4	65
L — The record, and its independent commitment	L-1, L-2, L-3, L-4, L-5, L-6, L-7, L-8, L-9, L-10, L-11, L-12, L-13, L-14, L-15, L-16, L-17	70
U — Change control	U-1, U-2, U-3, U-4, U-5	77
A — Who performs the assessment	A-1, A-2, A-3, A-4, A-5	123

What happens when there is more than one of them

R — Many systems under one principal	R-1, R-2, R-3, R-4, R-5, R-6	86
J — Systems that act together without being told to	J-1, J-2, J-3, J-4, J-5, J-6	90
Q — More than one machine, in one space	Q-1, Q-2, Q-3, Q-4	113

Annex C

Safety

The questions printed here are the safety questionnaire, and **Z-12** makes answering every one of them mandatory. They are stated here and nowhere else, and to that extent this annex is normative.

The marking is a view of this standard and not a second set of requirements. Which items the questions refer to, and the tier, designation, owner and stage printed against each, are stated in the clauses above; this annex adds no item and withdraws none, and where the two could differ, the clause governs.

An item appears here if, and only if, a question of the safety questionnaire of **Z-12** refers to it. Nothing else marks an item as being about safety. The marking is computed from the questions rather than kept as a list beside them, because a list and the questions it is drawn from are two records of one fact and they do not stay in step.

It follows that this annex is complete exactly to the extent that the set of questions is complete. The set is short and can be reviewed in one sitting, and that is why it, rather than a list, carries the marking.

Each question is printed in full: the general question, and where the question has them, the instance for a system with a moving body and the instance for one without. This document does not know the deployment. A system with no body answers “no such channel”, which is an answer and not an exemption. The two instances are marked *Body* and *No body*.

14 question(s), over 8 item(s) of this standard

C-1	What the system may reach, and where it may be	SQ-OUT	T1, T2, T3	M
------------	--	---------------	------------	----------

Can the system reach beyond what it is confined to under C-1, by a route the acquirer has not enumerated?

Body Can it move otherwise than along a bearing surface — fly, climb, or cross a barrier higher than the declared perimeter? Can it come to be outside the declared place on its own, through an error of navigation, under tow, or on a failure of whatever holds it? If it can, under what conditions and how far.

No body Can it reach a system, an account, a counterparty or a body of data outside the declared scope — through an integration, a shared credential, an interface the acquirer did not enumerate, or an agent it delegates to? If it can, by which route.

C-6	The actions this deployment admits, and the limit on each	SQ-LEARN	T1, T2, T3	M
------------	---	-----------------	------------	----------

Can the system acquire, in service, a capability it did not have at acceptance? If it can, which part of it learns, from what, and what cannot change while it does.

C-6	The actions this deployment admits, and the limit on each	SQ-MAG	T1, T2, T3	R
------------	---	---------------	------------	----------

What magnitude is reachable outside the declared limit — not what is permitted, but what the system is physically capable of — and what constrains it?

Body Force, speed, mass, reach, payload.

No body The volume and rate of operations on the systems and accounts named under C-1: how many in a unit of time, to what value, how many records in one call.

D6.1	A named person, with powers reachable through the interface	SQ-LINK	T1, T2, T3	M
-------------	---	----------------	------------	----------

What does the system do when it loses the channel it depends on — the operator, the network, an external service?

Body Does it stop, continue the task, or return? Does it leave the declared zone while doing so.

No body Does it continue on its last instruction, queue and retry, or fail open or closed? What goes on happening to other parties' systems and accounts while it does.

J-4	Emergent coordination is tested, not assumed absent	SQ-FLEET	T2, T3	R
------------	---	-----------------	--------	----------

Do several instances act in concert — exchanging data, dividing work, following one another? If they do, what happens when the coordination breaks.

M-2 The safety problems of the deployment SQ-EV-HARM T1, T2, T3 R

Occasions on which a person was harmed — how many, over what period, against what running time.

Body Injury.

No body Money lost, a service withheld that a person was relying on, a decision against a person carried into effect, personal data disclosed.

M-2 The safety problems of the deployment SQ-EV-TOUCH T1, T2, T3 R

Occasions on which the system acted on a person it should not have acted on.

Body Contact with a person that should not have happened.

No body An operation on an account, a record or a person outside the declared scope.

M-2 The safety problems of the deployment SQ-EV-STOP T1, T2, T3 R

Unplanned stops at a moment when somebody was depending on the system.

Body A stop with a person inside the zone.

No body A stop with an operation unfinished, a transaction open, or a person waiting in a queue.

M-8 What the system detects when it is degraded, and what it then does SQ-UNITS T1, T2, T3 R

How many units of this configuration are in service, and over what running time — hours, shifts, years or calls, and of what.

M-8 What the system detects when it is degraded, and what it then does SQ-SITES T1, T2, T3 R

On how many deployments, and which: what the surroundings are, whom they affect, and how they differ from the deployment of this tender.

M-11 How each problem is closed SQ-EV-LAYER T1, T2, T3 R

Occasions on which a protective layer — one independent of what it constrains — was triggered.

Body A barrier, an interlock, an emergency stop.

No body A blocking check, a limit, an approval gate, a manual authorisation.

U-4 Disclosure is mandatory; the response is the acquirer's SQ-CHANNEL T1, T2, T3 M

Is there a channel by which incidents are reported to the supplier, who uses it, and how it works? “We were not told” is not “it did not happen”.

U-4 Disclosure is mandatory; the response is the acquirer's SQ-DEFN T1, T2, T3 M

What does the supplier count as an incident — in its own words, before answering the five questions below.

U-4 Disclosure is mandatory; the response is the acquirer's SQ-EV-DISPUTED T1, T2, T3 R

Occasions reported by an acquirer that the supplier did not confirm — how many, over what period, and on what ground each was not confirmed.