SYMBEEO

PUBLIC

DESIGN STUDY

CMMC applicability and a current-state baseline for a defense-supplier machining plant: 1,140 devices placed in five asset categories

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Consulting & Engineering	Manufacturing	Precision-machining plant
DOCUMENT	**VERSION**	**DATE**
CON-007	1.1	Nov 6, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	CON-007	Version	1.1
Issued	Nov 6, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Oct 22, 2026
Capability	Consulting & Engineering	Industry	Manufacturing
Author	David Morgan	Role	Principal Security Architect
Credentials	CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 22, 2026 (version 1.0). Version 1.1 issued by Symbeeo, Nov 6, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 6
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 8
7 · Lessons learned 8
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure or clause read from the regulator's or standards body's own current page on Oct 22, 2026, or carried from a Symbeeo document that read it, where the text names that document · [S*] figure from a published summary where the owner's own page could not be opened · [A] assumption about the typical buyer, to be confirmed by the signing engineer · [T] design target taken from the design's stated outcome or derived from it. Every figure carries one tag. No figure comes from any prior engagement, file or asset. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Oct 22, 2026	1.0	First issue.
Nov 6, 2026	1.1	Independence reworded: vendor commissions, rebates and incentives are declared.

1 · Scope

Who it is for. The general manager and the IT manager of a machining plant whose defense primes have asked for its CMMC status, who has heard that the third-party certification phase is on hold and that it is not, and who needs to know three things before spending on any of it: which rules actually apply, which of the plant's machines are in scope and how, and where the plant stands today against the 110 requirements.

Typical buyer [A]. A precision-machining plant making flight-control and landing-gear parts for three defense primes and two commercial aerospace customers: one plant, 420 staff, 86 networked CNC machines, 6 coordinate measuring machines, an ERP, a CAD/CAM and product-data system holding customer drawings marked CUI, and one commercial cloud office tenant. Its defense contracts carry DFARS 252.204-7012 and the CMMC clause; it has posted a self-assessment score once, three years ago. About 1,140 IP-addressable devices: 640 office IT, 300 plant-floor OT, 80 network and security, 120 servers and virtual machines. The asset list was last reconciled when the ERP went in.

What is in. Applicability of the 18 regimes on SRA-CON-001's check list, CMMC first; a CUI flow map from customer portal to machine; an inventory reconciled across two sources; every in-scope asset placed in one of the five Level 2 asset categories with the reason; a current-state finding on each of the 110 requirements; a risk register on the plant's own criteria; a roadmap in three horizons. SRA-CON-001 Model A. **What is out.** Remediation design (an enclave, a new tenant, network segmentation — each is a later document); the plant's System Security Plan as a document (this assessment supplies its inventory, diagram and findings); export-control obligations, which are not on the check list; any certification assessment.

Assumptions. The plant handles CUI and FCI under its defense contracts, and its primes require CMMC Level 2 [A]. Active scans are not allowed on the CNC and robot segments; those segments are observed passively [A]. CUI is not copied out of the plant's systems during the engagement [A].

Related documents, read Oct 22, 2026. SRA-CON-001, SDD-CON-001, STP-CON-001 (R2, R9, R10, R11, R12 there; CMMC row of §9.1) · CMMC Program, 32 CFR Part 170, assessing against NIST SP 800-171 Rev. 2 (https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170; read through SRA-CON-001 §9.1, the eCFR page did not open on Oct 22, 2026) · DoD CIO, CMMC Scoping Guide Level 2 (https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf; the file did not open, figures [S*]) · Crowell & Moring, Department of War suspends CMMC Phase II requirements, July 2026 (https://www.crowell.com/en/insights/client-alerts/department-of-war-immediately-suspends-cmmc-phase-ii-requirements-launches-60-day-reform-review) · Jenner & Block, Phase II suspended, obligations

© 2026 Symbeeo. All rights reserved. · Public

remain (https://www.jenner.com/en/news-insights/client-alerts/department-of-war-suspends-cmmc-phase-iibut-compliance-obligations-remain-as-does-enforcement-risk).

1c · Public implementations this design follows

Each row is labeled. **Public deployment**: a named operator's real deployment, published and dated by the operator, its vendor or a partner, used where one exists. **Our own design**: the dated vendor or standards documentation this design was built from, where no public deployment of the design exists. Labels and dates checked Oct 22, 2026.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Our own design, built from published documentation. 32 CFR Part 170: CMMC Level 2 is assessed against the 110 security requirements of NIST SP 800-171 Rev. 2; the DFARS rule that puts the clause in contracts took effect on Nov 10, 2025	DoD · final rule, read through SRA-CON-001 §9.1 (Sep 25, 2026)	R3 and R9: the current-state finding is scored against Rev. 2's 110 requirements, not Rev. 3, because that is what Level 2 assesses	https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
Our own design, built from published documentation. Phase II, which from Nov 10, 2026 would have made a third-party Level 2 certification a condition of award, suspended on Jul 13, 2026 with all later milestones, pending a reform task force's review; Phase 1 self-assessments and DFARS 252.204-7012 unchanged [S*]	Crowell & Moring and Jenner & Block, client alerts · July 2026; no task force findings found published on Oct 22, 2026	R4 and §4.1: applicability is stated on the program as it stands on the assessment date, and the baseline is built to hold whether certification returns, narrows or falls away	https://www.crowell.com/en/insights/client-alerts/department-of-war-immediately-suspends-cmmc-phase-ii-requirements-launches-60-day-reform-review
Our own design, built from published documentation. CMMC Scoping Guide, Level 2: five asset categories — CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, Out-of-Scope Assets; Specialized Assets are government property, IoT and IIoT, operational technology, restricted information systems and test equipment [S*]	DoD CIO · Scoping Guide Level 2; the file did not open on Oct 22, 2026, categories read from a published summary	R6 and R7: a CNC machine that runs a program cut from a CUI drawing is placed, documented and managed, not tested against all 110 requirements	https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2.pdf

No public, dated CMMC baseline of a named machining plant was found on Oct 22, 2026; suppliers do not publish them. Every row is documentation used to build our own design.

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Scope	1 plant · 420 staff · ≈ 1,140 IP-addressable devices · 1 cloud office tenant · 5 customers, 3 of them defense primes	[A]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R2	Regulatory applicability	each of the 18 regimes on the check list marked applicable or not, with the basis in one sentence	[S] SRA-CON-001 R10
R3	CMMC level and standard	Level 2, against the 110 security requirements of NIST SP 800-171 Rev. 2	[S] 32 CFR Part 170, via SRA-CON-001 §9.1
R4	Program status on the assessment date	Phase 1 in force since Nov 10, 2025; Phase II suspended Jul 13, 2026; DFARS 252.204-7012 and self-assessment obligations unchanged	[S*] law-firm summaries
R5	Inventory coverage	≥ 95 % of IP-addressable devices reconciled across two independent sources	[T] SRA-CON-001 R2
R6	Asset categories	100 % of in-scope assets placed in one of the five Level 2 categories, with the reason	[S*] Scoping Guide L2; [T] 100 %
R7	Specialized Assets	documented in the asset inventory, the System Security Plan and the network diagram; managed under the plant's risk-based policies	[S*] Scoping Guide L2
R8	CUI flow map	every path a CUI drawing takes — customer portal, product-data system, CAM, machine — drawn with each system it crosses	[T]
R9	Current-state finding	each of the 110 requirements found met, partly met or not met, with the evidence named; score computed by the DoD Assessment Methodology	[A] method
R10	Plant safety	zero active scans on CNC, robot and CMM segments; zero machine stoppages caused by the engagement	[T]
R11	Risk register	each gap with likelihood, impact, owner and treatment on the plant's own criteria	[S] ISO 31000:2018; ISO/IEC 27005:2022, via SRA-CON-001 R9
R12	Roadmap	every item in one horizon (0–6, 6–18, 18–36 months), linked to ≥ 1 gap and ≥ 1 requirement	[T] SRA-CON-001 R11
R13	Independence	any commission, rebate or incentive from a vendor in scope, declared before discovery	[A] SRA-CON-001 R12
R14	Turnaround	report issued ≤ 20 working days after discovery access is granted	[T] SRA-CON-001 R13
R15	Evidence handling	discovery data and interview notes held in the plant's tenancy; no CUI copied out	[A]

Fifteen rows; six carry a regulator's or standards body's figure (three of them [S*] only), four are design assumptions, five are design targets.

© 2026 Symbeeo. All rights reserved. · Public

3 · Architecture overview

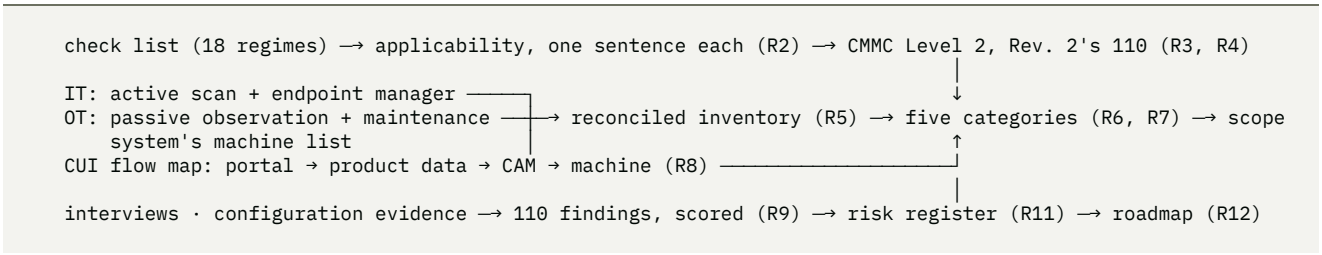


Figure 1. Applicability, scope, then the baseline

The plant cannot score 110 requirements until it knows which machines they apply to, and it cannot place a machine until it knows where the CUI goes. The assessment runs in that order, and a machine that only receives a cutting program is documented as a Specialized Asset rather than tested like a laptop.

Table 4. Architecture overview

Role	Component (exact name)	Qty	Capacity used	Why this unit
Requirements standard	NIST SP 800-171 Rev. 2	1	110 requirements [S]	what CMMC Level 2 assesses (R3)
Scoping method	CMMC Scoping Guide, Level 2	1	five asset categories [S*]	places every asset with a reason (R6)
Risk method	ISO 31000:2018 with ISO/IEC 27005:2022	1	every gap	treatment on the plant's own criteria [S]
IT discovery	active scan (SNMPv3, SSH read-only) plus the endpoint-management record	2	840 office, network and server devices [A]	two independent sources (SDD-CON-001 §4.1)
OT discovery	passive network observation plus the maintenance system's machine list	2	300 plant-floor devices [A]	no active scan on machine segments (R10)

4 · Design by subsystem

4.1 Applicability first.

The 18 regimes are each marked with a sentence (R2) [S]. For this plant two apply [A]: CMMC with NIST SP 800-171, because its defense contracts carry the clause and it holds CUI; and NDAA §889, because the primes flow its prohibition down to suppliers. The CMMC sentence is written on the program as it stands on the assessment date (R4) [S*]: Phase 1 self-assessment is in force; the third-party certification of Phase II is suspended pending review; DFARS 252.204-7012 applies regardless. Whatever the review decides, the plant's contracts already require it to meet the 110 requirements; the certification question changes who checks, not what is checked [A].

4.2 Follow the drawing.

One CUI drawing is traced from the customer's portal to the cut part (R8) [T]: downloaded to the product-data system, opened in CAD/CAM, turned into a program, sent over the plant network to the machine's controller, and measured on a coordinate measuring machine against the drawing's tolerances [A]. Every system the drawing or its program crosses is in scope; the map is the basis for every category in §4.4. Rejected: scoping from the network diagram — it shows where cables go, not where the CUI goes.

© 2026 Symbeeo. All rights reserved. · Public

4.3 Inventory from two sources.

Office, network and server devices: active scan reconciled with the endpoint-management record. Plant floor: passive observation on a span port at each cell switch, reconciled with the maintenance system's machine list by MAC address (R5) [T]. No active scan touches a machine segment (R10) [T]; a CNC controller that drops its program mid-cut is a scrapped part and a missed delivery [A].

4.4 Five categories.

Each in-scope asset is placed with a reason (R6) [S*]; [T]. On this plant [A]: the product-data system, CAD/CAM workstations and their file shares are CUI Assets; the firewalls, directory and endpoint-management servers are Security Protection Assets; the 86 CNC controllers and 6 measuring machines that receive programs are Specialized Assets, as operational technology and test equipment [S*]; the shop-floor badge readers that cannot reach CUI are Out-of-Scope once that is shown. Specialized Assets are documented in the inventory, the System Security Plan and the network diagram, and managed under the plant's risk-based policies (R7) [S*]. Rejected: treating every CNC machine as a CUI Asset — many run controllers that cannot meet requirements such as multi-factor sign-in, and the category exists for exactly that.

4.5 The 110 findings.

Each requirement is found met, partly met or not met, with the evidence named — a configuration, a record, an interview — and the score is computed by the DoD Assessment Methodology the plant would post (R9) [A]. A requirement with no evidence is not met, not unknown [A]. The report says which findings would change if the CUI were moved into a smaller enclave, so the first roadmap decision is visible, but the enclave is not designed here.

4.6 Risk register and roadmap.

Each gap becomes a risk on the plant's own scales, with an owner below the general manager (R11) [S]. The roadmap places each item in one of three horizons, linked to a gap and a requirement (R12) [T]. The first horizon holds what the plant's contracts already require whatever the review decides: the score posted honestly, and the gaps that carry the most weight in it [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Passive observation not possible at a machine cell	that cell's devices counted from the maintenance list only, marked single-source	[A]
A machine faults during observation	observation stopped at that cell; plant manager told the same hour	[T] R10
CUI found on a system the flow map missed	the map is corrected and the system placed before any finding is scored	[T] R8
Reconciliation below 95 %	baseline marked partial; unmatched devices listed for the plant to resolve	[T] R5
Program status changes during the engagement	applicability sentence rewritten on the new status; findings unaffected	[A] R4
A prime's questionnaire asks for a certification the plant does not hold	answered with the posted self-assessment and the roadmap, not a claim	[A]

© 2026 Symbeeo. All rights reserved. · Public

6 · Limits

- The Phase II suspension and the program's status are read from law-firm summaries; the Department's own notice is read again before the report is issued.
- The Scoping Guide's categories are from summaries of the guide; the file is read again at the start of discovery.
- Export-control obligations on the same drawings are not on the check list and are not assessed.
- The findings are this assessment's, not a certification; a certification assessor may find otherwise.
- The score is a point in time; the roadmap assumes the inventory is kept reconciled after handover.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

8 · The author

WRITTEN BY

David Morgan

Principal Security Architect

CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

CON-007 · Version 1.1 · Nov 6, 2026