



QUALITY MANUALS | FIRST EDITION

IAF CONNECTED FACTORY & OT CYBERSECURITY MANUAL

Secure automation and
vehicle software provisioning

STABLE RELEASE

Document No. IAF-MAN-OTC-001 | Revision 01

PLC, SCADA and robot networks
Engineering data and digital twins
Secure first flash and operational recovery

International Automotive Federation

English master text | 14 September 2026

iaf.com

Publication identity and use

IAF Connected Factory & OT Cybersecurity Manual

This manual provides the requirements, operating procedures and evidence framework for its defined automotive manufacturing activities. Apply it through a controlled site implementation plan and equipment-specific work instructions.

Control	Publication record
Document	IAF-MAN-OTC-001 IAF Connected Factory & OT Cybersecurity Manual
Edition / revision	First Edition Revision 01 Stable Release
Text issue	14 September 2026 English master text
Document owner	IAF Quality function with the relevant automotive technical committee
Custodian	IAF Secretariat / Document Controller
Institutional authority	Competent authority under IAF-CON-001; publication does not amend the Constitution.
Site adoption	Site Director and accountable technical leads record the actual approval reference, scope and operational effective date.
Classification	Public core manual. Completed plant records follow their assigned access and retention controls.

Reading and applying requirements

“Shall” identifies a requirement when adopted by a site, programme or agreement. “Should” identifies a recommendation. An example is illustrative; it is not a machine setting, test acceptance limit or completed operating record. Annex worksheets may be reproduced for controlled internal use.

Controlled implementation

Stable Release identifies the completed publication text. Site approval, process validation, competence authorization and equipment release are recorded when performed. A missing safety limit, test criterion or release authority prevents activation of the affected operation. Mandatory law, product requirements and validated equipment instructions remain applicable.

Relationship to IAF recognition

Use of this manual does not by itself confer membership, Corporate Recognised status, accreditation, certification or a licence to use IAF marks. Those decisions follow the applicable IAF guides, independent evaluation and recorded scope.

Contents

Every entry links to its section. Page numbers include the cover.

1 Purpose, scope and security objectives	5
2 Terms, trust boundaries and asset states	6
3 Governance, accountability and decision rights	7
4 Scope, inventory and criticality assessment	8
5 Risk assessment and treatment	9
6 Zones, conduits and network architecture	10
7 Identity, privilege and account lifecycle	11
8 Supplier and remote maintenance access	12
9 Engineering stations and endpoint hardening	13
10 PLC, SCADA and robot change control	14
11 Patch, vulnerability and legacy management	15
12 Removable media and artifact transfer	16
13 Logging, monitoring and detection	17
14 CAD, engineering IP and digital twins	18
15 Secure software supply and release packages	19
16 Signing keys, credentials and trust stores	20
17 EOL provisioning architecture and prerequisites	21
18 Secure first-flash operating procedure	22

Contents - continued

Every entry links to its section. Page numbers include the cover.

19 Interrupted flashing, recovery and final security state	23
20 Secure testing, quality data and release integrity	24
21 Incident readiness, classification and reporting	25
22 Incident containment and evidence preservation	26
23 Backups, recovery objectives and restoration	27
24 Reconnection and production recovery gate	28
25 Assurance, suppliers and personnel	29
26 Implementation, review and continual improvement	30
Annex A OT asset and dependency register	31
Annex B Zone and conduit authorization	32
Annex C Remote access and change record	33
Annex D EOL flash and provisioning traveller	34
Annex E Incident and product containment log	35
Annex F Backup restoration and restart test	36
Annex G Readiness and document interfaces	37

Using the annexes

Enter actual values, evidence references, names and dates in the worksheets. A blank, unsigned or illustrative record is not proof of completion. Retain the record with its governing instruction and revision.

1 Purpose, scope and security objectives

1.1 This manual governs the cybersecurity of connected automotive manufacturing operations and the integrity of first software provisioning to vehicles and components. It covers PLCs, SCADA, HMIs, robots, engineering stations, industrial networks, historians, manufacturing interfaces, test equipment and supporting services within the declared site scope.

1.2 The objectives are safe and reliable operation, integrity of production commands and records, controlled availability, protection of intellectual property and trustworthy product software. Cybersecurity decisions shall consider physical consequences. A technically effective network action can be unsafe if it removes essential monitoring or interrupts a hazardous process.

1.3 The site shall define boundaries with enterprise IT, suppliers, cloud services, development environments and vehicle systems. Factory network security, product cybersecurity and functional safety are related but separate responsibilities. Completion of this manual does not establish a vehicle cybersecurity approval or validate a safety function.

1.4 All testing and administrative actions shall be authorized for the actual asset and operating condition. This manual provides defensive controls and operating procedures. Production systems shall not be subjected to uncontrolled scanning, exploitation, stress testing or disruptive demonstrations.

1.5 Apply IAF-MAN-LMS-001 to manufacturing control and safe restart, IAF-MAN-GAA-001 to battery, high-voltage and robotic hazards, and IAF-GUI-DOC-001 to records. Applicable legal, customer and product requirements shall be identified by the responsible organization.

2 Terms, trust boundaries and asset states

2.1 Operational technology (OT) monitors or controls physical processes. A programmable logic controller (PLC) executes control logic; SCADA coordinates supervisory monitoring and control; a human-machine interface (HMI) provides operator interaction. A manufacturing execution system (MES) manages production information and may exchange commands or recipes with OT.

2.2 A zone groups assets with compatible security needs and trusted relationships. A conduit is a controlled communication path between zones. A demilitarized zone (DMZ) hosts intermediary services that separate enterprise access from plant control. Network labels alone do not enforce these boundaries.

2.3 A baseline is an approved and identifiable configuration, including relevant software, logic, parameters, accounts and network rules. A hash can detect change but does not by itself establish the source's trustworthiness. A digital signature verifies an artifact against a trusted key and validation policy; authorization to deploy remains a separate decision.

2.4 End-of-line (EOL) first flash is the controlled initial loading or configuration of production software on a vehicle or component. Provisioning can also establish identity, certificates, keys and security state. Those steps shall be individually identified even where one automated workflow performs them.

2.5 Asset states shall distinguish planned, received, quarantined, tested, production-approved, restricted, incident-contained and retired. An asset restored from backup is not automatically production-ready. The owner shall verify software integrity, process configuration and physical readiness before reconnection or release.

3 Governance, accountability and decision rights

3.1 The Site Director owns operational risk and resources. The OT Security Lead owns the security programme and coordinates with enterprise security. The asset owner owns the supported process and approves operating impact. Control Engineering owns logic and configuration. Production owns plant state; Quality owns product containment and release.

3.2 The product software authority owns released vehicle software, compatibility, signing policy and allowed recovery. The key-management authority controls cryptographic lifecycle. These roles shall be separated sufficiently that one uncontrolled account cannot develop, approve, sign and deploy a production image without independent checks.

3.3 Maintenance and suppliers may perform only the tasks and access explicitly authorized. IT support shall not patch, isolate, reboot or scan a plant asset solely under a general enterprise policy without the relevant OT coordination. Urgent incident actions shall follow the predefined safe containment playbook.

3.4 Named deputies and emergency contacts shall cover all shifts. The incident commander coordinates response; Production and safety specialists determine safe physical actions; Security assesses cyber containment; Quality determines suspect product boundaries. One shared event record shall preserve each decision and its authority.

3.5 Good-faith reporting of weaknesses, mistakes and suspicious activity shall be protected. Investigations shall separate immediate protection and evidence collection from personnel decisions. Commercial pressure shall not suppress a vulnerability, alter a failed test or approve unsupported vehicle release.

4 Scope, inventory and criticality assessment

4.1 The asset register shall identify owner, location, function, vendor, model, serial or unique ID, network identity, operating system or firmware, support status, software dependencies and approved connections. Include safety controllers, engineering laptops, test stands, gateways, switches, wireless devices and temporary equipment.

4.2 Use existing engineering records, configuration exports and approved passive observation to establish the inventory. Active discovery shall have a tested method, asset-owner authorization, maintenance window where required, monitoring and an abort plan. A general-purpose scanner may disrupt fragile control equipment.

4.3 Classify assets by consequences of loss or manipulation: personnel safety, environmental harm, product defects, line availability, genealogy, software integrity and IP disclosure. Record dependencies such as time, identity, licensing, virtual hosts, DNS, certificate validation and power. A small supporting server can be a critical single point of failure.

4.4 Validate inventory during commissioning, significant change, incident recovery and periodic review. Reconcile physical assets with network observations and purchase or retirement records. Unknown devices shall be assessed and controlled without unsafe disconnection of an unidentified process.

4.5 Annex A provides the minimum asset fields. Missing owner, unverified support status or unknown network dependency shall generate an action with a due date and interim risk controls. Inventory completeness shall be measured against a defined population, not asserted from one discovery tool.

5 Risk assessment and treatment

5.1 Assess credible scenarios such as unauthorized logic change, compromised remote support, ransomware on engineering stations, recipe manipulation, forged quality data, stolen CAD files and malicious or incorrect vehicle software. Evaluate exposure, existing controls, detectability and physical or product consequences.

5.2 For each significant risk, identify the asset and process, threat route, consequence, preventive and detective controls, response and residual exposure. Include accidental change, supplier errors, service outages and insider misuse as well as external attacks. A vulnerability score alone does not express manufacturing consequence.

5.3 Select treatment through engineering and security review: remove an unnecessary connection, strengthen access, isolate a legacy device, improve detection, add recovery capability or replace the asset. Define a responsible owner and evidence of implementation. Compensating controls shall address the specific uncorrected exposure.

5.4 Risk acceptance shall identify scope, reason, residual consequence, expiry and the accountable business authority. It cannot waive mandatory obligations or permit a known unsafe operation. Reassess after incidents, changed connectivity, supplier advisories, new products or expired support.

5.5 Maintain a plant security plan linking risks to assets, network architecture, access rules, changes, backups, incident playbooks and assurance. Use it to prioritize work that reduces real consequence rather than producing a high count of completed administrative controls.

6 Zones, conduits and network architecture

6.1 Define separate zones for enterprise services, industrial intermediaries, plant supervision, process cells, engineering access and vehicle provisioning according to risk. Safety-related systems require assessed separation and tightly controlled dependencies. A flat network that gives every workstation access to every controller is not an acceptable default architecture.

6.2 Conduits shall permit only documented source, destination, direction, protocol and service relationships. Record the business purpose, owner, approval and review date. Deny unnecessary paths and test rules safely. A VLAN is useful organization but does not by itself prove isolation; enforcement and permitted routing must be verified.

6.3 Use intermediary services to exchange production data without direct unrestricted enterprise access to controllers. Where consequences justify it, consider one-way transfer or equivalent restrictions. Validate latency, fail behaviour, logging and recovery; a security appliance shall not silently become a process reliability hazard.

6.4 Keep production programming and maintenance paths distinct from ordinary data collection. Remote access shall terminate at the approved gateway and jump environment. Direct internet exposure of PLC, SCADA or robot management interfaces is prohibited under this manual.

6.5 Protect configuration backups and maintain current diagrams showing actual routes, including cellular modems, wireless bridges, dual-network laptops and vendor appliances. Unauthorized secondary connectivity shall be removed through a safe coordinated change, with investigation of how it was introduced.

7 Identity, privilege and account lifecycle

7.1 Use named accounts for personnel wherever supported, with privileges limited to their authorized role and assets. Separate operator use, engineering change, security administration and software release. Shared interactive administrator accounts shall be replaced; unavoidable legacy use requires controlled checkout, attribution and compensating monitoring.

7.2 Approve access before activation and review it periodically and when employment, role or supplier assignment changes. Remove obsolete accounts promptly under the site's defined service targets. Time-limited access shall expire automatically where supported; an account with no current owner shall not remain enabled by default.

7.3 Apply strong authentication, including multi-factor authentication to remote and privileged access where supported. Where a controller cannot support it, enforce protection at the approved access gateway and restrict the local route. Do not implement a login control that prevents required safe emergency operation without an approved alternative.

7.4 Service accounts shall have a named owner, defined function, minimum privileges and protected credentials. Prevent interactive use where unnecessary. Rotation shall be planned with dependency checks so that it does not unexpectedly stop production or disable a protective monitoring service.

7.5 Emergency access shall be individually accountable, limited to the incident, recorded and reviewed after use. Keep recovery credentials in a controlled vault or equivalent protected arrangement. Passwords, private keys and reusable vehicle secrets shall not appear in tickets, screenshots, source repositories or routine logs.

8 Supplier and remote maintenance access

Owner: asset owner approves work; OT Security approves the access route; Production authorizes the plant state. Access approval is not permission to change logic or move equipment.

Step / owner	Required action and evidence
1 Define the work	Record supplier identity, named engineer, purpose, assets, permitted actions, schedule and local contact. Verify contractual confidentiality, competence and approved support tools.
2 Assess impact	Identify whether work can affect movement, process parameters, safety functions or product release. Require an approved change or diagnostic plan and establish the safe operating state.
3 Open bounded access	Use the approved remote gateway, strong authentication and controlled jump host. Limit reachable assets and privileges. Avoid direct inbound controller access and unmanaged remote desktop products.
4 Supervise and record	Maintain a local accountable contact. Record session metadata and relevant actions; record session content where lawful and appropriate. Stop the session if scope or plant conditions change.
5 Validate results	Review changed files, settings and device states. Perform the required technical, security and product checks before normal operation. Preserve the original and updated baselines.
6 Close access	Terminate sessions, revoke temporary rights and verify that no persistent route or account remains. Attach the work report, evidence and local acceptance to the access record.

Emergency supplier access follows the same minimum identity, scope and safe-state controls with a documented urgent approval. An always-on vendor tunnel shall not substitute for controlled authorization.

9 Engineering stations and endpoint hardening

9.1 Engineering workstations shall be dedicated or equivalently controlled for their production role. Maintain approved software, configuration, patch state and access. Restrict ordinary email, web browsing and untrusted tools in the engineering environment where they create unnecessary exposure.

9.2 Use least privilege, suitable application control and endpoint protection that have been tested for compatibility. Security agents shall not be installed on a controller or legacy host without evaluating resource use and process impact. Exceptions require a documented protection plan and review date.

9.3 Control project files, libraries, macros, scripts and compiler or vendor-tool versions. Verify artifact provenance before opening or executing them in the production engineering environment. Preserve a reproducible relationship between source project, compiled or downloaded object and deployed revision.

9.4 Physical access to cabinets, local ports, panels and engineering laptops shall be controlled. Lock unattended sessions where compatible with operations; maintain a safe method for operator access during urgent conditions. An unlocked maintenance laptop can bypass otherwise strong network controls.

9.5 Build replacement endpoints from approved images and verify software licences, drivers, interfaces and project compatibility. Keep a tested recovery method for critical stations. Asset retirement shall revoke credentials, remove trusted device entries and sanitize media using an approved method appropriate to its data.

10 PLC, SCADA and robot change control

Trigger: logic, recipe, HMI, robot path, firmware, network rule, test limit or related configuration change. Emergency changes remain traceable and subject to prompt review.

Step / owner	Required action and evidence
1 Request and scope	Identify the reason, assets, products, current baseline and proposed difference. Assess safety, quality, cybersecurity, timing, communication and recovery effects.
2 Prepare and review	Create the controlled change artifact. Independently review logic and parameter differences, especially release, interlock and test functions. Confirm supplier approval where needed.
3 Test off line	Use a suitable test environment or simulation where possible. Define positive, negative and failure cases and acceptance criteria. Record limitations that require controlled site verification.
4 Authorize deployment	Approve the change, maintenance window, plant state, backup, rollback conditions and responsible personnel. Notify affected operators and freeze unrelated changes where necessary.
5 Implement and verify	Deploy through the controlled engineering route. Confirm actual device configuration against the approved artifact. Validate affected functions and product checks before production release.
6 Close the record	Record actual time, performer, reviewer, results and first affected unit. Update baseline, inventory, instructions and backups. Monitor for specified adverse effects and close only with evidence.

Online edits and temporary forces can create immediate physical consequences. Use them only under a specific approved method and record every applied override and its removal. A hash match does not replace functional validation.

11 Patch, vulnerability and legacy management

11.1 The OT Security Lead shall monitor relevant vendor notices and vulnerability information for the installed inventory. Determine affected versions, exposure, exploitability in the local architecture, available mitigations and operational consequence. Record the evidence and prioritization decision.

11.2 Before patching, verify authenticity, compatibility, support conditions and recovery. Test representative hardware, drivers, engineering tools and process functions. Approve the deployment window and rollback plan with the asset owner. "Install all updates immediately" is not a sufficient OT change procedure.

11.3 Where immediate patching is unsafe or unavailable, define time-limited compensating controls such as restricting access, disabling an unnecessary service, enhanced monitoring or separating the asset. Verify their operation and assign a review deadline. An indefinite exception with no owner is unacceptable.

11.4 For unsupported equipment, maintain a replacement or risk-reduction plan with budget and milestones. Retain compatible spares, configurations and recovery knowledge where lawful. Isolation reduces exposure but does not make an unsupported device inherently trustworthy.

11.5 Vulnerability testing shall have authorization, scope, method, safe timing and an abort route. Production exploitation or denial-of-service testing is not permitted without a specific specialist-controlled plan and demonstrated safeguards. Prefer non-disruptive verification and representative test environments.

12 Removable media and artifact transfer

Applies to USB devices, portable disks, supplier laptops, transferred project files and offline update packages. The transfer route shall preserve both malware controls and artifact provenance.

Step / owner	Required action and evidence
1 Request the transfer	Identify source, owner, purpose, destination assets, file types and classification. Confirm that transfer is necessary and that the recipient has authority to use the data.
2 Use approved media	Use inventoried media or an approved transfer service. Do not connect unknown devices directly to production. Separate supplier media from the accepted production copy.
3 Inspect in quarantine	Use a controlled scanning and review environment. Check malware findings, expected contents and file provenance. A clean scan alone does not establish that logic or software is authorized.
4 Verify release	Check the approved manifest, signature where available, hash and intended version. Resolve unexpected files, macros, tools or configuration before import.
5 Transfer with control	Use the authorized endpoint and required plant state. Restrict write access and preserve the accepted artifact. Record who transferred what to which destination and when.
6 Close and retain	Verify import results, remove media and revoke temporary access. Store required evidence and sanitize or return media through the approved process. Investigate detected malicious or unexplained content.

Offline transfer shall not become a route around change control or data classification. The same software-release approval applies whether an artifact arrives through a network or removable media.

13 Logging, monitoring and detection

13.1 Define monitoring for unauthorized access, new devices, unusual conduits, logic or recipe changes, safety-setting modifications, failed provisioning, clock drift and abnormal production behaviour. Collect information with methods appropriate to the system's capacity and safety constraints.

13.2 Logs shall identify event time and time zone, source asset, actor or service, action, result and relevant change or product reference. Protect central records against unauthorized alteration and restrict sensitive content. Do not log passwords, private keys or reusable diagnostic secrets.

13.3 Use a controlled time service and monitor synchronization. Document how unsynchronized events will be correlated during investigation. A timestamp without a known time basis can undermine both security analysis and product containment.

13.4 Assign alert priorities, response owners and escalation periods based on consequence. Test routing during ordinary and out-of-hours conditions. An alert that no one receives is not an effective control. Tune noisy detections through documented review without hiding meaningful events.

13.5 Correlate cyber indicators with physical conditions such as unexpected rejects, motion, test failures or parameter drift. Preserve evidence before routine cleanup where safe. Monitoring shall support legitimate operational and security purposes with appropriate privacy, access and retention controls.

14 CAD, engineering IP and digital twins

14.1 Classify CAD models, drawings, bills of materials, process recipes, simulation models and digital-twin data according to sensitivity and permitted use. Assign an owner and identify customer, supplier and licence restrictions. Public product information shall be separated from manufacturing know-how and restricted design details.

14.2 Control access through project and role membership, approved repositories and authenticated transfer. Limit supplier access to the relevant project and version. Protect exported files, including neutral CAD formats and screenshots; a secure source repository does not protect uncontrolled copies.

14.3 Maintain revision, provenance and validation state for digital-twin models. Simulation output shall identify assumptions, parameter sources and uncertainty. A twin may support planning and diagnosis but shall not directly authorize a safety-critical change or override an interlock without an approved engineered control path.

14.4 For cloud, analytics or AI services, approve what information may be sent, the purpose, location and retention, provider access and permitted secondary use. Do not upload restricted drawings or production data to unapproved services. Review integrations and plugins for unexpected data flows.

14.5 When collaborating externally, record the agreement, recipient, data scope and return or deletion obligations. Use audit trails and suitable technical restrictions. On project closure or departure, revoke access and assess retained copies; confidentiality obligations do not replace practical access control.

15 Secure software supply and release packages

15.1 The software authority shall define a controlled route from source and dependencies to build, test, approval, signing and distribution. Separate development and production credentials. Protect build systems and dependencies against unauthorized changes and preserve evidence of provenance.

15.2 Each release package shall identify product family, hardware compatibility, software and calibration versions, dependencies, security state, manifest, hashes, signature validation requirements, test evidence and authorized deployment population. Include the intended recovery behaviour and rollback restrictions.

15.3 Obtain supplier information needed to evaluate components and vulnerabilities, including a software bill of materials where appropriate. A component list is not proof of security. Review supplier support, vulnerability notification, update availability and responsibility for addressing defects.

15.4 Test functionality, integration and security-relevant behaviours in representative conditions. Resolve or explicitly accept residual issues through the proper authority before release. Signing shall be restricted to approved artifacts; a valid signature on an unreviewed build is not a production approval.

15.5 Publish packages to a controlled repository with version and access protection. Retain the superseded release and its allowed-use status. Disable obsolete or compromised packages through a traceable decision that includes already provisioned products and downstream service implications.

16 Signing keys, credentials and trust stores

16.1 The key-management authority shall define key purpose, owner, generation, storage, use, rotation, backup where appropriate, revocation and destruction. Separate code signing, device identity, transport authentication and diagnostic authorization. Keys shall not be reused across unrelated purposes for convenience.

16.2 Protect production private keys in an approved hardware-backed or equivalently controlled cryptographic service suitable to the risk. Restrict signing operations, apply independent authorization for sensitive lifecycle actions and log use without recording secrets. A signing service shall authenticate the caller and verify the approved artifact scope.

16.3 Device provisioning shall create or install credentials through a controlled per-device process. A credential from one vehicle shall not grant equivalent privileged access to the rest of the fleet. Record public certificate or key identifiers and provisioning outcomes; keep private material out of ordinary manufacturing records.

16.4 Trust stores and validation policy are controlled configurations. Define accepted signers, certificate validity and revocation handling, offline behaviour and time dependencies. Production shall stop affected provisioning if trust cannot be established; operators shall not click through a signature error.

16.5 Prepare a tested compromise response: suspend affected signing or access, identify packages and devices, rotate or revoke trust through an approved recovery design and notify responsible parties. Consider products already shipped and legitimate service access. Certificate expiry and revocation distribution shall be monitored before they disrupt production.

17 EOL provisioning architecture and prerequisites

17.1 The EOL system shall separate software approval, package distribution, station operation, device identity and key services. A station shall receive only the permissions needed for its assigned product and job. Production software and credentials shall not be copied from an engineer's personal laptop.

17.2 Before flashing, verify station integrity, supported tool versions, trusted package source, authenticated operator or service, correct vehicle or component identity and current build order. Bind the job to the physical ECU identity and hardware configuration; a manually entered VIN alone is insufficient where stronger verification is available.

17.3 The vehicle shall be in the approved commissioning state, with required power stability, controlled movement and electrical precautions. The fixture and connection sequence shall be validated. Software loading shall not interrupt an active safety-relevant test or charging operation without an approved process.

17.4 The approved manifest shall determine image, configuration, calibration, security mode and anti-rollback policy for that hardware and product. Check available storage, bootloader compatibility and prerequisites. A valid image for another model remains an invalid deployment.

17.5 Station failures, package mismatches, unavailable identity services or signature failures shall prevent an automatic pass. Define a safe held state and a controlled offline mode only where it has been specifically validated. An operator override shall not bypass authenticity, identity or required product-release checks.

18 Secure first-flash operating procedure

Owner: manufacturing software operations. Prerequisites: approved release package, trusted station, correct physical device, safe commissioning state and authorized job. Use Annex D.

Step / owner	Required action and evidence
1 Bind the job	Read and reconcile build order, vehicle or component identifier, ECU identity and hardware version. Record the intended manifest and station. Stop on missing, duplicate or inconsistent identity.
2 Verify the artifact	Validate package provenance, signature, trusted signer, integrity, compatibility and permitted security version. Confirm that the release is approved for this population and has not been withdrawn.
3 Establish the session	Authenticate the station and device using the approved protocol. Obtain only the required time-limited authorization. Verify stable power, fixture readiness and allowed vehicle state.
4 Load and provision	Execute the validated loading sequence and device-specific credential process. Record progress and result identifiers without exposing secrets. Enforce approved anti-rollback and configuration rules.
5 Verify the outcome	Verify installed software and configuration, boot or attestation evidence where supported, provisioning status and required diagnostic or functional tests. A successful file transfer alone is not a pass.
6 Close and release	Remove temporary privileges and establish the approved production security state. Reconcile the record to the unit; Quality releases only after all required tests and holds are resolved.

If power, communication or verification fails, place the unit on hold and follow Section 19. Preserve failed attempts and actual state. Do not retry blindly, disable signature checking or substitute an unapproved image.

19 Interrupted flashing, recovery and final security state

Trigger: incomplete loading, wrong configuration, rejected signature, failed boot, provisioning mismatch or unexpected device security state. Recovery shall use the product's validated method.

Step / owner	Required action and evidence
1 Hold the product	Prevent shipment and uncontrolled further programming. Record unit, station, package, error, last completed step and observed state. Maintain the safe physical condition.
2 Determine scope	Establish whether the issue is unit-specific, station-related, package-wide or a trust-service incident. Hold related units where evidence cannot exclude common impact.
3 Authorize recovery	The product software authority selects the approved recovery image or process for this exact hardware and security version. Check anti-rollback restrictions and key or certificate implications.
4 Execute safely	Use an authorized station and competent personnel. Follow the validated sequence and preserve the original failure. Repeated failures or an unexpected state require engineering escalation.
5 Verify production state	Confirm installed versions, required protection, credential status and restricted developer access. Remove temporary accounts, test modes and access rights according to the approved serviceability design.
6 Release with evidence	Repeat affected functional and security checks. Quality records disposition, recovery reference and final configuration. Link all attempts to the same unit and retain package-level corrective actions.

Recovery shall not defeat the approved rollback protection or create a shared fleet secret. Necessary legitimate service access shall remain available through authenticated and controlled mechanisms rather than hidden unrestricted debug interfaces.

20 Secure testing, quality data and release integrity

20.1 Protect test limits, station recipes, calibration references and pass/fail logic under change control. The person operating a production test shall not freely edit its acceptance criteria. Record the exact version used for each test result.

20.2 A result shall bind the physical unit, station, method, configuration, time and actual outcome. Prevent duplicate identifiers, replayed receipts and reuse of another unit's pass. Reconcile counts and sequence where automated systems exchange results.

20.3 Preserve original failures, retries, manual interventions and concessions. A passing retest shall be linked to the approved reason for retest and previous outcome. Do not overwrite a failure or delete a record to satisfy a delivery target.

20.4 Where a test system or data store is compromised or unreliable, Quality shall identify affected units from the last trustworthy point. Missing integrity evidence may require a hold even if no physical defect has yet been observed. Define additional testing or other disposition with the product authority.

20.5 Production release shall require the complete approved evidence set, including software configuration and unresolved holds. System downtime or an interface fault shall not convert missing results into automatic acceptance. Any continuity route shall preserve the same essential identity, evidence and approval controls.

21 Incident readiness, classification and reporting

21.1 The site shall maintain playbooks for ransomware, unauthorized logic change, supplier account compromise, lost engineering data, suspicious devices and software-signing or provisioning incidents. Define contact routes, authority, safe containment options, evidence sources and recovery dependencies.

21.2 Classify incidents by actual or plausible consequence to people, environment, product, operations and information. Unknown scope with credible high consequence shall receive urgent assessment. Do not delay protective action while waiting for a perfect technical classification.

21.3 Train operators to report unexpected motion or logic behaviour, unexplained parameter changes, unusual logins, inaccessible files, signature errors and abnormal test results. Reporting shall capture what was observed without requiring the operator to diagnose the attack.

21.4 Maintain protected communications and an offline contact list for a loss of enterprise systems. Predetermine how suppliers, customers, authorities and product-safety teams will be notified when required. External messages shall be accurate and authorized; confidentiality shall not be used to conceal a required notification.

21.5 Exercise the plan with Production, Engineering, Quality, EHS, Security and relevant suppliers. Tabletop and test-environment exercises shall include safe isolation decisions and suspect-product handling, not only IT restoration. Record lessons, owners and evidence that corrective actions work.

22 Incident containment and evidence preservation

The incident commander coordinates this procedure. Physical safety and emergency actions take precedence. Security containment shall be selected with the process owner's knowledge of the plant state.

Step / owner	Required action and evidence
1 Establish command	Record the event, affected area, immediate hazards and responsible contacts. Use trusted communications. Preserve a timeline of decisions and avoid uncontrolled parallel changes.
2 Stabilize the process	Production and safety specialists determine whether to continue in a controlled state, stop or use emergency procedures. Do not indiscriminately power off controllers, cooling or monitoring systems.
3 Contain access	Use the approved route to restrict compromised accounts, remote sessions or network paths. Select boundaries that reduce exposure while maintaining essential safe functions. Record each containment change.
4 Preserve evidence	Collect relevant logs, configurations and other evidence using authorized competent methods where safe. Record source, time, collector and handling. Avoid altering fragile equipment solely to acquire more data.
5 Contain product	Quality identifies units, batches and software jobs potentially affected since the last trustworthy state. Block shipment and preserve original production results pending assessment.
6 Plan recovery	Determine trusted sources, affected dependencies, credential actions and required validation. Obtain accountable approval before rebuilding, reconnecting or restarting the process.

If malicious logic or a safety-related change is suspected, involve Control Engineering and the relevant safety authority. A clean antivirus result alone does not establish that the controller configuration or manufactured product is trustworthy.

23 Backups, recovery objectives and restoration

23.1 Identify recovery requirements by process consequence. Define the maximum tolerable interruption, recovery time objective (RTO) and recovery point objective (RPO) for each critical service and its dependencies. These are site decisions; a single universal target is not imposed on all controllers, historians and provisioning systems.

23.2 Back up approved logic, recipes, robot programmes, safety configuration, network rules, workstation images, software repositories, certificates where appropriate, and required production data. Preserve compatible tools, licences and recovery instructions. Protect secrets according to the key-management policy rather than placing them in ordinary backup folders.

23.3 Maintain protected recovery copies with access and separation suitable to ransomware and insider risks. Test whether attackers using production credentials could alter or delete the backup. Monitor job failures and incomplete copies; a successful scheduler message does not prove usable recovery.

23.4 Test restoration in a safe representative environment and verify content, configuration and required function. Measure actual time against RTO and recovered data against RPO. A file-open check is insufficient for a critical PLC, safety system or vehicle-provisioning service.

23.5 During incident recovery, identify a trustworthy baseline, remove persistence through competent rebuilding or remediation, address exposed credentials and verify dependencies. Reconnection and production restart require Section 24 acceptance. Retain the evidence that establishes why the restored state is trusted.

24 Reconnection and production recovery gate

Applies after cyber containment, rebuild, significant security change or loss of trusted configuration. System availability and production readiness are separate acceptance decisions.

Step / owner	Required action and evidence
1 Verify the baseline	Confirm restored software, logic, parameters, accounts, trust stores and network rules against the approved state. Review unexplained differences and unresolved compromise indicators.
2 Validate dependencies	Check time, identity, certificates, licensing, databases, communications and required monitoring. Verify that protection has not been lost through an emergency workaround.
3 Test in a bounded state	Engineering performs the approved functional and failure tests. Validate affected safety functions through the competent process. Keep identified trial units separated from releasable product.
4 Reconcile production data	Quality verifies genealogy, test results and software receipts across the outage. Resolve missing or duplicate records and determine disposition of affected stock.
5 Approve restart	Security accepts containment and trust evidence; Engineering accepts configuration; Production accepts plant readiness; Quality accepts product controls. Obtain relevant EHS or electrical acceptance.
6 Monitor and close	Reconnect in the approved sequence with heightened monitoring. Define rollback or renewed containment triggers. Close only after the stated observation and evidence criteria are met.

A restored server that responds to login is not proof of a safe or correct line. Use the manufacturing restart gate in IAF-MAN-LMS-001 and relevant battery or robot controls in IAF-MAN-GAA-001 alongside this record.

25 Assurance, suppliers and personnel

25.1 The audit programme shall examine actual assets, access, network paths, configurations, release packages and recovery evidence. Sample changes, remote sessions, failed flashes and exceptions as well as normal successful cases. Review all relevant shifts and contractors.

25.2 Suppliers shall receive security, support, vulnerability notification, remote access and change-control requirements proportionate to their role. Contracts shall establish ownership of configurations, required recovery information, data use, incident cooperation and end-of-support notice. A confidentiality agreement alone is insufficient.

25.3 Train operators, engineers, administrators, software release personnel and managers for their distinct responsibilities. Verify practical response to identity mismatch, suspicious access, failed signature and incident containment. A general awareness course does not establish competence to change control logic or manage signing keys.

25.4 Track overdue privileged-access reviews, unsupported critical assets, untested restores, unapproved connections, unresolved high-consequence vulnerabilities, failed provisioning and overdue corrective action. Each metric shall identify population, source, owner and response rule. A high patch percentage can conceal the single asset with the greatest consequence.

25.5 Investigate findings through IAF-QM-001 processes and relevant reporting policies. Independent technical judgment shall be protected from production or commercial pressure. Close findings through evidence of effective control, not only revised documentation.

26 Implementation, review and continual improvement

26.1 Implementation begins with ownership, inventory and a current network and data-flow map. Prioritize exposed remote access, uncontrolled engineering privileges, missing backups, untrusted software routes and unknown release logic. Stabilize the highest-consequence gaps before expanding connectivity.

26.2 Deploy controls in tested stages with operating-owner involvement. Pilot authentication, network restrictions, monitoring and application control on representative systems. Record performance and recovery effects before rollout. The security team shall not introduce unassessed latency or downtime into a critical control path.

26.3 Use Annex G to confirm minimum readiness: accountable roles, risk register, controlled remote access, approved change route, trusted first-flash process, recoverable baselines, incident playbooks and product containment. An unresolved critical gate prevents activation of the affected connection or service.

26.4 Management shall review effectiveness at least annually and after a significant incident, technology transition or material connectivity change. Examine risk, resource adequacy, supplier support, recovery tests, product incidents, assurance and emerging dependencies. Record decisions, owners and completion evidence.

26.5 The document controller shall maintain actual adoption and revision records under IAF-GUI-DOC-001. Changes to this publication do not silently change a plant's safety configuration or vehicle software. Each affected implementation shall receive its own impact assessment, approval and controlled release.

Annex A OT asset and dependency register

Form reference: OTC-A. Use one record per asset or a clearly justified managed group. Do not enter passwords or private keys.

Field	Entry / evidence
Asset identity	ID / location / serial / owner / function: _____
Platform	Vendor / model / firmware / OS / approved software: _____
Network	Zone / IP or other identity / permitted conduits: _____
Criticality	Safety / quality / availability / IP consequence: _____
Dependencies	Power / time / identity / licence / host / database / gateway: _____
Access	Operator / engineering / service accounts / remote route: _____
Baseline	Configuration and project references / approval: _____
Support	Vendor status / lifecycle / relevant vulnerabilities: _____
Recovery	Backup reference / tools / RTO / RPO / last restore test: _____
Operational state	Approved / restricted / quarantined / retired: _____
Review	Reviewer / date / gaps / next review: _____

Discovery method and safety authorization: _____

Reconcile this register after commissioning, material changes, incident recovery and retirement. Include indirect and temporary connections; an asset without an ethernet address can still depend on or affect the control network.

Annex B Zone and conduit authorization

Form reference: OTC-B. Architecture version: _____ Request: _____ Business purpose: _____

Control item	Entry
Endpoints	Source zone / asset: _____ Destination zone / asset: _____
Permitted traffic	Direction / protocol / port or service / data type: _____
Business necessity	Process dependency and reason alternatives are insufficient: _____
Enforcement	Gateway / firewall / identity / filtering controls: _____
Plant impact	Latency, availability, fail behaviour and safety review: _____
Monitoring	Log source / alert owner / review interval: _____
Validation	Test method, approved window, result and rollback: _____
Approval	Asset owner / OT Security / Engineering where relevant: _____
Validity	Start / expiry if temporary / next review: _____
Closure	Removal evidence or approved continuing baseline: _____

Architecture verification

Confirm the actual route, including wireless, cellular, vendor appliances and dual-network endpoints. Verify that the intended restriction is enforced. A diagram, VLAN name or firewall rule entry does not by itself prove that an unwanted route is blocked.

Evidence location and unresolved restrictions: _____

Annex C Remote access and change record

Form reference: OTC-C. Access event: _____ Linked change / work order: _____ Asset / production scope: _____

Stage	Required entry
Requester	Organization, named person, competence and contact: _____
Scope	Purpose, permitted actions, assets and prohibited actions: _____
Time and route	Approved window, gateway, jump host and authentication: _____
Operating approval	Local contact, plant state and protective arrangements: _____
Change basis	Current baseline, proposed artifact and review evidence: _____
Recovery plan	Backup, abort criteria and approved rollback method: _____
Execution	Actual session / performer / changes / deviations: _____
Verification	Configuration comparison, functional tests and product impact: _____
Access closure	Session ended, temporary rights removed, route checked: _____
Acceptance	Asset owner / Security / Production / Quality as applicable: _____

Incident or unexpected outcome reference: _____

Signature / authenticated approval and date: _____

Access, change and product release are distinct approvals even when recorded on one form. Preserve the original and deployed configuration and the first affected product boundary.

Annex D EOL flash and provisioning traveller

Form reference: OTC-D. One traceable record per unit and attempt. Store secure evidence references, never private keys or reusable diagnostic secrets.

Gate	Entry / result
Physical identity	Vehicle / component / ECU ID / hardware revision: _____
Authorized job	Build order / variant / manifest / intended population: _____
Station readiness	Station ID / software version / operator or service identity: _____
Artifact checks	Package ID / hash / signer ID / trust and compatibility result: _____
Safe state	Power, fixture, vehicle state and commissioning authorization: _____
Provisioning	Public credential identifier / protected service receipt / result: _____
Flash outcome	Attempt number / start-end time / installed versions / result: _____
Verification	Boot or attestation evidence and required functional checks: _____
Final security state	Temporary access removed / approved debug state / policy result: _____
Disposition	Pass / hold / recovery reference / release authority and date: _____

Failed attempts and linked incident or recovery: _____

Before release, reconcile the physical unit, approved manifest, installed configuration and test results. Do not accept a file-transfer success, station completion flag or another vehicle's receipt as the required evidence.

Annex E Incident and product containment log

Form reference: OTC-E. Incident ID: _____ Commander: _____ Initial time / time zone: _____
Trusted communication route: _____

Decision point	Record / owner / time
Initial observation	What was seen, by whom, asset and process condition: _____
Safety assessment	Hazards, safe state and responsible production / safety decision: _____
Cyber scope	Accounts, devices, conduits and plausible exposure: _____
Containment	Action, authorization, expected impact and verification: _____
Evidence	Source, time basis, collector, storage and handling record: _____
Product population	Last trustworthy point, units / lots / jobs / destinations: _____
Notifications	Recipient role, legal or contractual basis, approver and time: _____
Recovery basis	Trusted baseline, credential actions and validation plan: _____
Release	Security, Engineering, Production and Quality decisions: _____
Lessons	Cause, corrective actions, owners, deadlines and effectiveness: _____

Restrictions and unresolved uncertainty: _____

Retain decisions and original records. Do not delay necessary product hold or safety protection while investigating root cause. Evidence collection shall not create a new physical hazard.

Annex F Backup restoration and restart test

Form reference: OTC-F. Service / asset: _____ Test owner: _____ Date: _____
 Environment and authorization: _____

Test field	Entry / evidence
Objectives	RTO: _____ RPO: _____ Process consequence: _____
Recovery copy	Source / date / integrity / access separation: _____
Dependencies	Tools, licences, firmware, identity, certificates and data: _____
Procedure	Approved recovery instruction / personnel / safe state: _____
Restoration	Actual start-end time / issues / recovered data point: _____
Technical validation	Configuration and required functional / failure tests: _____
Security validation	Accounts, trust, monitoring, clean baseline and connectivity: _____
Product validation	Genealogy, test results, provisioning and held units: _____
Outcome	RTO / RPO achieved? Restrictions / corrective actions: _____
Restart decision	Security / Engineering / Production / Quality approvals: _____

Next test trigger and responsible owner: _____

A backup job success is not a restore test. Reconnection to live production is a separate authorized step and shall follow the approved sequence with monitoring and abort conditions.

Annex G Readiness and document interfaces

Readiness gate	Required evidence
Ownership and scope	Named roles, current inventory, criticality and approved architecture.
Access and connectivity	Bounded remote access, privileged-account control and verified conduits.
Changes and integrity	Reviewed baselines, tested changes, protected recipes and release logic.
Vehicle provisioning	Trusted artifacts, controlled credentials, identity binding and final-state verification.
Resilience	Recoverable copies, demonstrated restores, incident playbooks and safe restart.
Assurance	Competent personnel, supplier controls, corrective actions and management acceptance.

Controlled document interfaces

IAF-QM-001 provides institutional quality controls. IAF-GUI-DOC-001 governs records and revisions. IAF-MAN-LMS-001 governs manufacturing control and restart; IAF-MAN-GAA-001 governs battery, electrical and robot application conditions. IAF privacy, whistleblowing, complaints and conflict policies apply to relevant information and decisions. Membership, recognition and mark rights remain separate approval routes.

Record retention and operational acceptance

Classify inventories, diagrams, access logs, configurations, CAD exports, releases, provisioning receipts and incident evidence. Set retention by legal, contractual, product and operational needs; preserve relevant evidence under legal or investigation hold. Restrict access to sensitive architecture and personal data. Verify archive readability and approved disposal.

Scope / open actions / acceptance reference: _____

Accountable approver / actual effective date: _____