



QUALITY MANUALS | FIRST EDITION

IAF DIGITAL TWIN AND VIRTUAL COMMISSIONING MANUAL

Verified simulation and
controlled physical commissioning

STABLE RELEASE

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

Robot cells and assembly line simulation
PLC verification and cycle optimization
Model correlation and commissioning release

International Automotive Federation

English master text | 15 September 2026

iaf.com

Publication identity and use

IAF Digital Twin and Virtual Commissioning Manual

This manual defines how automotive engineering teams build, verify and maintain digital models of robot cells and production lines. It establishes evidence for virtual commissioning, PLC changes and transfer to physical equipment, with explicit model limitations and separate site safety release.

Control	Publication record
Document	IAF-MAN-DTV-001 IAF Digital Twin and Virtual Commissioning Manual
Edition / revision	First Edition Revision 01 Stable Release
Text issue	15 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	Accountable operating director and technical leads record the actual approval reference, scope and operational effective date.
Classification	Public core manual. Completed operational 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 required outcomes	5
2 Definitions and model use categories	6
3 Governance roles and project adoption	7
4 Requirements acceptance criteria and test oracles	8
5 Asset inventory and configuration baseline	9
6 Geometry coordinate systems and data preparation	10
7 Robot kinematics dynamics and collision fidelity	11
8 Conveyors buffers and assembly flow models	12
9 Human tasks access and maintenance representation	13
10 Signal mapping and interface contracts	14
11 Simulation clocks latency and determinism	15
12 Software in the loop commissioning	16
13 Hardware in the loop commissioning	17
14 Control sequences modes and recovery logic	18
15 Robot programme verification and transfer	19
16 PLC optimization and regression control	20
17 Fault injection and abnormal scenario campaigns	21
18 Safety related claims and physical validation	22

Contents - continued

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

19 Capacity studies and experiment design	23
20 Model correlation and uncertainty management	24
21 Virtual commissioning review and release	25
22 Transfer to physical commissioning	26
23 As installed configuration and handover	27
24 Operational synchronization and controlled updates	28
25 Cybersecurity access and intellectual property	29
26 Defects changes and evidence integrity	30
27 Competence metrics and management review	31
28 Document control and IAF interfaces	32
Annex A Model scope and fidelity record	33
Annex B Signal and interface mapping record	34
Annex C Virtual test scenario and result	35
Annex D PLC and robot optimization change record	36
Annex E Correlation and uncertainty worksheet	37
Annex F Virtual commissioning release record	38
Annex G Physical commissioning and twin reconciliation	39
Annex H Assurance and project learning review	40

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 required outcomes

1.1 This manual defines how automotive engineering teams create, verify and use digital models to commission production systems before physical installation. It covers robot cells, assembly conveyors, fixtures, material handling and the programmable logic controllers that coordinate them. It applies to new lines, major modifications and controlled improvements to operating equipment.

1.2 The required outcome is a reproducible body of evidence showing that the intended control sequence, layout and operating assumptions satisfy defined requirements within a declared model scope. The team shall identify which decisions the simulation supports and which still require physical measurement, safeguarding validation or product trials. A visually convincing animation is not sufficient evidence.

1.3 Virtual commissioning shall reduce uncertainty before equipment is built while preserving the separate authority for physical commissioning and safe operation. Passing a virtual test does not authorize energization, human entry into a robot cell or release of a production line. The responsible site specialists shall complete the applicable physical checks before those activities.

1.4 Use the manual across process engineering, controls, robotics, manufacturing, quality, maintenance and relevant suppliers. Include normal operation, setup, fault recovery, product variants and foreseeable interruptions. A model that represents only an ideal nominal cycle shall not be described as a complete commissioning model.

1.5 The requirements are independent of a particular simulation platform. Local instructions shall identify the actual software, adapters, controllers and versions used. Product specific limitations, licensing, export constraints and technical restrictions remain applicable even though this publication contains no named external product or standard references.

2 Definitions and model use categories

2.1 A digital model is a controlled representation of a process or asset. A digital twin adds a defined relationship to the intended or actual physical configuration and relevant data over its lifecycle. The project shall state the direction, frequency and purpose of data exchange rather than assuming that every three dimensional model is continuously synchronized with a factory.

2.2 Virtual commissioning tests control behaviour against a simulated plant before or alongside physical commissioning. A programmable logic controller is abbreviated PLC, and its human machine interface is abbreviated HMI. Input and output, abbreviated I/O, connect simulated or physical sensing and actuation to the controller under test.

2.3 Software in the loop uses simulated or emulated execution of relevant software with a plant model. Hardware in the loop uses actual controller hardware connected to a simulated environment. These are test arrangements with different timing and hardware coverage; neither automatically represents every feature of the final installation.

2.4 A test oracle is the independently defined expected result used to judge a test. Model verification asks whether the representation and implementation behave as specified. Model validation assesses whether the representation is sufficiently accurate for its intended decision. Calibration adjusts parameters using evidence; it shall not replace validation on separate relevant observations.

2.5 A baseline is an identified set of model, controller, robot, interface and test versions. A scenario specifies initial state, inputs, events and acceptance criteria. A limitation is an unrepresented or inadequately supported condition that restricts use of the evidence. These terms shall appear consistently in local test records and release decisions.

3 Governance roles and project adoption

3.1 The project owner shall appoint a model owner, controls lead, robotics lead, process owner and independent acceptance reviewer appropriate to the risk. The model owner maintains scope and fidelity evidence; each discipline verifies its contributed data and behaviour. Quality manages test disposition and evidence integrity without taking over the technical responsibilities of engineering.

3.2 The controls lead owns the PLC and HMI baseline, logic review and executable identity. The robotics lead owns robot configuration, tool and frame data and offline programme verification. The site machinery safety specialist owns the physical safeguarding acceptance and shall review any simulation claim that could influence a safety decision.

3.3 Suppliers shall agree deliverables, interface ownership, version control, intellectual property access and change notification before integration. An imported library or supplier model shall have a named owner and documented limitations. Acceptance of a purchase order does not establish that a model is suitable for every commissioning claim.

3.4 Adopt this manual through a project plan that defines equipment scope, decisions, risk, required fidelity, test stages, acceptance criteria and physical follow-up. Annex A records the basis and actual approvals. Missing requirements or safety critical interface information shall prevent the affected claim from being released.

3.5 IAF technical committees may review guidance and programme evidence within their remit. This manual does not change federation governance or confer recognition, accreditation or certification. Site and project authorities remain responsible for the actual equipment and operating decisions under the applicable IAF and local arrangements.

4 Requirements acceptance criteria and test oracles

- 4.1** Translate process requirements into testable statements before model execution. Each requirement shall have an identifier, owner, applicable variant, expected behaviour, acceptance criterion and verification method. Cover sequence, throughput, quality, operator interaction, recovery and interfaces rather than focusing only on cycle time.
- 4.2** Define expected results independently of the implementation being tested. A test that copies the same faulty PLC condition into its expected result can pass while preserving the defect. Review the oracle against process intent, mechanical constraints and the required response to invalid or missing information.
- 4.3** Separate design targets, mandatory release criteria and exploratory assumptions. A target cycle time may guide optimization, while a collision, wrong part routing or unsafe restart condition is a release blocker. The acceptance plan shall state which findings may be deferred, by whom and with what operating restriction.
- 4.4** Record quantitative limits with units, measurement location, time basis and applicable conditions. Define how uncertainty and model error affect the decision. Do not present a nominal simulated clearance, cycle time or response time as a universal physical acceptance limit.
- 4.5** Maintain traceability from each requirement to its model elements, test cases, results and unresolved physical verification. Annex C provides the scenario record. A requirement with no suitable test or supporting evidence remains unverified; marking a scenario executed is not the same as demonstrating that its requirement passed.

5 Asset inventory and configuration baseline

5.1 Create an asset and configuration register for robots, axes, tools, fixtures, conveyors, sensors, actuators, PLCs, drives and connected systems. Give each physical or planned item a stable identifier and map it to the corresponding model object. Similar equipment names shall not conceal differences in payload, stroke, firmware or installed options.

5.2 The baseline shall include geometry revision, kinematic data, physical parameters, controller programme, robot programme, HMI, interface mapping, simulator version, libraries, solver settings and test data. Record dependency versions and any local patches. The team shall be able to reproduce a released result from the retained package.

5.3 Distinguish planned, supplier confirmed, measured and assumed data. Assign an owner and resolution date to significant assumptions. When actual equipment differs from the planned configuration, assess the affected tests and claims before reusing earlier results.

5.4 Control common libraries and reusable components through review and change impact analysis. A corrected conveyor object can affect many lines, and a library update can change behaviour even where the project file is unchanged. Record which version each project uses and prevent uncontrolled automatic replacement during a test campaign.

5.5 Before a release run, freeze the configuration and record its manifest and integrity identifiers. Changes made during execution shall create a new identifiable baseline and invalidate the affected results until reassessed. A screenshot of a working model is not an adequate configuration record.

6 Geometry coordinate systems and data preparation

6.1 Import geometry through a controlled process that preserves units, coordinate systems, origins, handedness and relevant hierarchy. Verify scale with known dimensions and check that rotations and transforms match engineering intent. A millimetre to metre error can create plausible looking but unusable clearance and motion results.

6.2 Simplify geometry only with a documented purpose and effect on the decision. Retain collision relevant surfaces, tool envelopes, cable or hose allowances and access constraints where they influence acceptance. Decorative detail can be omitted; removing a bracket or protrusion that defines a collision boundary requires technical justification.

6.3 Identify reference frames for the factory, cell, robot base, tool and workpiece. Record calibration or measurement evidence when frames are tied to installed equipment. An offline coordinate transfer shall not be treated as a substitute for physical frame verification during commissioning.

6.4 Assess the quality of supplier computer aided design data, scans and manually created geometry. Record measurement uncertainty, hidden areas and outdated features. Use a controlled discrepancy process where the drawing, model and installed asset disagree rather than silently adjusting one representation to make a test pass.

6.5 Verify the imported assembly using dimension checks, known poses and interface positions before adding behavioural complexity. Retain the import settings and transformation history. Annex A shall identify the geometry evidence and limitations that affect the intended commissioning decisions.

7 Robot kinematics dynamics and collision fidelity

7.1 Define the robot type, axis limits, kinematic chain, mounting, payload and tool configuration from controlled data. Include external axes, grippers and workpieces where they affect reach or collision. Verify representative poses and trajectories against the intended controller behaviour before using the model to judge accessibility.

7.2 Distinguish geometric reach, collision checking and dynamic performance. A reachable pose may require an unsuitable configuration, pass near a singularity or exceed torque and acceleration capability. Where dynamic claims are made, represent mass, inertia, friction and relevant controller limits with a documented evidence basis.

7.3 Configure collision geometry and contact behaviour for the decision being made. Coarse meshes, missing flexible items and numerical penetration can produce false clearance or false interference. State what the collision model includes and use physical verification for residual uncertainties that matter to safe operation.

7.4 Select time steps, solver settings and tolerances appropriate to motion and contact. Verify stability and sensitivity across the tested range; increasing visual frame rate does not necessarily improve physical accuracy. Record any unsupported joints, controller functions or numerical workarounds as limitations.

7.5 Offline robot paths shall be reviewed for tool orientation, approach and retreat, cable routing, payload changes and process constraints. The simulated path is a candidate programme. Physical commissioning shall verify frames, mastering, load data, safeguarding and controlled motion before production use.

8 Conveyors buffers and assembly flow models

8.1 Represent conveyors, pallets, buffers, transfer stations and assembly resources with their actual routing and capacity constraints. Define carrier dimensions, occupancy, accumulation behaviour, transfer conditions and product identity. A material flow model shall not allow two items to occupy an impossible space merely because its event logic permits it.

8.2 Distinguish discrete event flow analysis from detailed motion and control simulation. A discrete event model can evaluate queues and utilization efficiently, while sensor timing and collision may need another representation. Document the interface between model levels so a result is not claimed beyond the fidelity used.

8.3 Include arrival patterns, product mix, operator availability, replenishment, quality holds, rework and equipment interruptions where relevant. Use justified distributions or measured data for variable events. Constant ideal cycle times shall not be used to claim robust capacity under variable production conditions.

8.4 Define buffer full, buffer empty, blocked, starved and unavailable states and the corresponding controller response. Test merge priority, product sequencing, carrier recirculation and recovery after a partial line stop. Ensure that product identity remains correct through diversion, rework and manual intervention.

8.5 Validate flow conservation and capacity constraints through simple known cases before complex campaigns. Reconcile items entering, completed, rejected and remaining in process. Unexplained creation or loss of simulated parts invalidates throughput results until the model defect is corrected.

9 Human tasks access and maintenance representation

9.1 Identify human activities that influence layout and operation, including loading, inspection, replenishment, cleaning, tool changes and fault recovery. Represent realistic task sequences and access needs. A human figure placed in a model is not, by itself, an ergonomic assessment or a demonstration of safe reach.

9.2 Consider the intended workforce, clothing, protective equipment, tools and product variants. Evaluate working space, visibility, posture, handling and escape with the appropriate ergonomics method. Record the supported population and the limitations of any digital human representation.

9.3 Model maintenance access and removal paths for foreseeable service tasks. Include lifting equipment, spare parts, opened panels and isolated work zones where they affect space. A line that can produce a part but cannot be maintained safely has not met a complete operational design requirement.

9.4 Simulation of a person near a robot or moving conveyor shall not establish a protective separation distance without the necessary engineering basis and physical validation. Safety related sensing, stopping behaviour and access control require their own acceptance evidence.

9.5 Use virtual reviews to identify concerns early and record actions for the physical station trial. Apply IAF-MAN-IHE-001 for industrial safety and ergonomics. Keep worker feedback and the actual site trial results linked to the digital model so design changes remain traceable.

10 Signal mapping and interface contracts

10.1 Define an interface contract for every connection between the model, controller, robot and supporting system. Record signal identifier, direction, data type, unit, range, polarity, initial value, update behaviour and quality or validity indication. Annex B provides the mapping record.

10.2 Map controller outputs to the intended simulated actuators and return simulated sensor states to the correct inputs. Verify mappings with controlled one-at-a-time checks and expected physical meaning. A tag name match does not prove correct address, direction, scaling or interpretation.

10.3 Represent sensor placement, switching behaviour, delay, noise or debounce where they affect sequence decisions. Define actuator response, completion feedback and fault state separately from the command. Setting a completion input immediately whenever a command is issued can conceal a real sequencing defect.

10.4 Specify handshake rules with robots, manufacturing execution, quality systems and material transport. Include sequence numbers or other correlation where needed, acknowledgement, timeout, retry and duplicate handling. A delayed response from an earlier cycle shall not be accepted as confirmation for the current part.

10.5 Validate invalid values, stale data, communication loss and restart behaviour. The controller shall respond according to the requirement rather than using the last good value indefinitely by default. Record forced signals and remove them before the release baseline is accepted.

11 Simulation clocks latency and determinism

11.1 Declare the time basis of each component: simulated time, controller scan, real time, event time and wall clock logging. Define how components advance and synchronize. A PLC connected to an accelerated model may behave differently if timers, communication and simulated process motion do not share a coherent time relationship.

11.2 Measure or justify scan intervals, communication delay, jitter, scheduling and processing overhead relevant to the test. Identify whether the simulator can maintain the required real time rate. If it falls behind, record the condition and invalidate timing claims affected by the loss of synchronization.

11.3 Use deterministic seeds and controlled initial states where repeatability is required. For stochastic studies, record seeds, distributions, warm-up, run length and replications. Repeatability does not prove realism; a deterministic model can reproduce the same incorrect result consistently.

11.4 Test boundary conditions around timeouts and simultaneous events. Evaluate event ordering, task priority and restart races. A visual replay can hide short signal transitions, so retain timestamped traces at a resolution suitable for the behaviour being assessed.

11.5 Document timing limitations of emulated controllers and hardware adapters. Hardware in the loop can improve coverage of actual execution but still depends on the simulated plant and I/O timing. Do not extrapolate a desktop simulation's average execution speed into a guaranteed physical response time.

12 Software in the loop commissioning

Use software in the loop to verify logic and interactions within the declared emulation scope. Keep the test environment isolated from production command paths and record the complete baseline.

Step / owner	Required action and evidence
1 Prepare baseline	Freeze requirements, model, PLC code, HMI, robot logic and mappings. Confirm the emulator supports the functions under test and record unsupported behaviour.
2 Verify interfaces	Check signal direction, scale, polarity, initial state and timing. Use simple known cases before running the complete sequence and retain the mapping evidence.
3 Run nominal cases	Execute representative variants, start-up, normal cycles, stops and completion handshakes. Compare results with the independent expected behaviour and product routing.
4 Challenge behaviour	Inject approved faults, late responses, missing parts, buffer limits and restart conditions. Keep fault injection confined to the simulation environment.
5 Review results	Record traces, findings, limitations and requirement coverage. Separate controller defects from model or test defects and assess any timing claims against emulator capability.
6 Release evidence	Approve only the demonstrated scope and identify tests requiring actual hardware or physical equipment. Archive the reproducible package and unresolved actions.

Do not replace an unsupported controller function with an idealized model and then claim the real function was verified. The release record shall state what was executed and what remains to be demonstrated.

13 Hardware in the loop commissioning

Use actual controller hardware only in a controlled test installation with physical outputs prevented from driving unintended machinery. The responsible controls and electrical specialists shall authorize the arrangement.

Step / owner	Required action and evidence
1 Secure test rig	Identify hardware, firmware, power, networks and interfaces. Separate the rig from production and prevent hazardous actuation through physical and network controls.
2 Load candidate	Verify the approved executable and configuration before loading. Record checksums or equivalent integrity identifiers and the actual controller settings used.
3 Connect model	Verify I/O mapping, update timing, clock behaviour and signal quality. Confirm that simulated feedback cannot be confused with a live production input.
4 Execute campaign	Run the planned normal, boundary and fault cases with actual hardware timing. Monitor scan load, communication and watchdog behaviour within the safe test arrangement.
5 Compare evidence	Review differences from software in the loop and expected behaviour. Investigate timing, hardware specific functions and model limitations rather than averaging away failures.
6 Close and control	Record accepted scope, defects and physical follow-up. Restore or secure the rig and retain the exact hardware and software baseline for reproducibility.

A passing hardware in the loop campaign does not verify real wiring, actuator behaviour or installed safeguarding. Those checks remain part of physical commissioning. Do not connect the test rig to a live line merely to make simulated results more realistic.

14 Control sequences modes and recovery logic

14.1 Define explicit states and transitions for automatic, manual, setup, stopped, faulted and recovery operation. Specify who may request each mode and the conditions for entry and exit. The model shall expose invalid transitions and conflicting commands rather than resolving them through an undocumented convenient assumption.

14.2 Test start-up from empty, partially completed and abnormal states. Verify initialization, retained data, part location and command ownership. A controller restart shall not assume that every physical actuator or workpiece returned to its initial position.

14.3 Verify handshakes and interlocks between stations so that transfer occurs only when the receiving condition is valid. Include delayed acknowledgements, duplicate requests, lost completion messages and a neighbouring station restarting independently. Test whether a fault can leave a part untracked or a resource permanently reserved.

14.4 Recovery sequences shall identify the actual safe state and required operator confirmation. Reset shall not silently resume hazardous motion or conceal an unresolved fault. Where physical access is required, the local procedure shall provide the applicable isolation and safe restoration controls.

14.5 Retain state and event traces that explain why each action occurred. HMI messages shall identify the condition and permitted response clearly enough for the operator. A simulated sequence that succeeds only because a test engineer forces internal bits is not an acceptable normal operating solution.

15 Robot programme verification and transfer

15.1 Manage offline robot programmes as controlled software linked to robot, tool, workpiece and fixture baselines. Verify motion instructions, coordinate frames, payload data, process commands and external axis coordination. A programme for a visually similar cell shall not be transferred without checking the actual configuration.

15.2 Review reach, configuration changes, singularity proximity, approach clearances and process orientation across the complete path. Include held parts, open grippers, dress packs and nearby equipment where relevant. Record any geometry or dynamics omitted from the model and the physical checks required to resolve them.

15.3 Test interactions with the PLC, tool controller and quality system, including start, complete, fault and abort conditions. Confirm that a stale completion signal cannot release the next station and that a interrupted process identifies the affected part for disposition.

15.4 Optimize motion only within the permitted process and equipment constraints. Shorter paths or higher speed may change settling, weld quality, adhesive application or collision margin. The robot and process owners shall review the complete effect before accepting a change.

15.5 Transfer the approved candidate through a controlled route and verify the loaded identity. Physical commissioning shall confirm mastering, frames, payload, tooling and protected test conditions before movement. Remove temporary simulation instructions and forced signals and retain the as-installed programme after authorized adjustment.

16 PLC optimization and regression control

16.1 Optimization shall begin with a measured problem and a preserved baseline. Identify whether the limitation is sequence waiting, unnecessary communication, resource contention, scan load or physical process time. Do not assume that shorter code or a lower average scan time automatically improves throughput or safe behaviour.

16.2 Record the proposed change, expected benefit, affected requirements and risks. Review timers, interlocks, task priorities, retained variables and error handling explicitly. Removing a wait is acceptable only where its original physical or process purpose is understood and an adequate replacement or justified removal is demonstrated.

16.3 Use controlled comparisons with the same model, inputs, timing basis and initial conditions. Run relevant variants and fault cases as well as the nominal cycle. A change that improves average performance but creates a rare deadlock, wrong sequence or lost traceability shall not be accepted.

16.4 Verify worst relevant execution and resource conditions rather than reporting only an average. Assess memory, communication and task scheduling constraints on the intended hardware. Where a requirement depends on real timing, confirm it through suitable hardware and physical evidence before making a final claim.

16.5 Annex D records the optimization decision and regression results. Release requires peer review, approved executable identity and a controlled rollback or recovery plan. Operators shall not alter timers or bypass conditions on the live line solely to reproduce a simulated cycle target.

17 Fault injection and abnormal scenario campaigns

17.1 Build a fault catalogue from the process risk assessment, equipment behaviour, incident history and interface analysis. Include sensor stuck states, missing or double parts, actuator noncompletion, communication loss, power restoration, full buffers and inconsistent product identity. Prioritize consequential combinations as well as individual faults.

17.2 Each injected fault shall have a defined location, trigger, duration, expected response and recovery condition. Record whether the fault represents a physical failure, communication defect or model assumption. An unrealistic fault can still explore robustness, but its result shall not be claimed as direct evidence for a different real failure.

17.3 Test detection, containment, operator information and recovery together. A fault that raises an alarm but still releases a defective part is not adequately controlled. Verify the disposition of material already in process and the prevention of unintended restart.

17.4 Run fault campaigns in isolated simulation or authorized test rigs. Do not inject faults into a live production network or defeat protective devices to validate an idea. Any physical fault test needs its own assessed method, authorization and protective conditions.

17.5 Retain unsuccessful runs and near boundary behaviour. A defect shall not disappear from the evidence because the next run passed. Use the issue process to identify the cause, change the relevant baseline and repeat the affected regression set after correction.

18 Safety related claims and physical validation

18.1 Simulation can help identify hazardous sequences and support design review, but its safety claims shall be limited to the evidence it can provide. Document the model of protective devices, stopping behaviour, access and control logic and identify which physical and hardware properties are not represented.

18.2 The machinery safety specialist shall define the physical validation required for guards, interlocks, emergency stops, protective sensing, safe motion and restart. Actual installation, wiring, response times and mechanical stopping behaviour can differ from the model. These checks shall not be waived because virtual tests passed.

18.3 Do not use a collision free robot animation to establish safe collaborative operation or human separation. Human exposure depends on the actual task, equipment, sensing and protective design. Apply the site's competent risk assessment and IAF-MAN-IHE-001 before allowing people within the relevant operating area.

18.4 Treat modeled safety signals separately from production authorization. A simulation adapter that forces a safe input for testing shall be identified and removed from the physical release configuration. Review temporary overrides and diagnostic modes explicitly before energization.

18.5 A failed or uncertain safety critical condition blocks the affected operating release. The project owner may not trade that condition for a schedule benefit. Record the required corrective action and the competent authority that verifies its closure using appropriate physical evidence.

19 Capacity studies and experiment design

19.1 Define the decision before selecting a simulation experiment: required throughput, buffer capacity, staffing, product mix or resilience to disruption. State the baseline and alternatives and identify the variables that will change. Use a representative operating horizon rather than selecting a favourable short interval.

19.2 For stochastic models, define input distributions, warm-up, run length, replications and seeds. Justify the input data and preserve correlations where they matter. Independent random values can misrepresent a process where breakdowns, product mix or operator delays are related.

19.3 Report variability and uncertainty alongside mean throughput or cycle time. Compare alternatives under consistent conditions and investigate sensitivity to uncertain assumptions. A narrow result range generated from unrealistically fixed inputs does not prove robust capacity.

19.4 Account for accepted output, rework, scrap, planned stops and resource limits in the reported metric. A simulated line producing 60 attempted units per hour with 6 rejected units delivers 54 accepted units per hour for that defined example. Do not report attempted output as accepted capacity.

19.5 Keep capacity evidence distinct from detailed controller verification and machine safety release. A flow model may show that a buffer improves output without proving that its actual controls, load support or access arrangements are acceptable. Record the follow-up engineering and physical checks for the selected design.

20 Model correlation and uncertainty management

20.1 Validate the model against independent evidence relevant to its intended use, such as supplier test data, measured component behaviour or physical commissioning observations. Reserve suitable data for validation rather than adjusting every parameter to the same observations later used to claim accuracy.

20.2 Define comparison metrics before reviewing the result. These may include cycle time, trajectory, sensor transition timing, queue behaviour or energy where the model supports it. Record units, conditions, measurement uncertainty and acceptable discrepancy, and distinguish systematic bias from run to run variation.

20.3 Illustrative comparison: a simulated cycle of 52.0 seconds and a measured cycle of 54.0 seconds differ by 2.0 seconds. Relative error using the measured value is 2.0 divided by 54.0, or about 3.70 percent. Whether that is acceptable depends on the predeclared decision tolerance and uncertainty; the example is not a universal acceptance limit.

20.4 Investigate discrepancies through geometry, process assumptions, timing, parameter values and measurement quality. Do not tune unrelated parameters solely to fit one output while damaging other behaviour. Record the reason for each calibration change and repeat relevant independent validation.

20.5 Annex E records correlation and permitted use. Where accuracy is inadequate, improve the model or restrict the claim. A model may be suitable for layout comparison while remaining unsuitable for a stopping time or precise throughput guarantee; its release shall state that distinction clearly.

21 Virtual commissioning review and release

The acceptance reviewer shall evaluate the complete evidence package for the declared virtual commissioning scope. This release authorizes the next controlled project stage, not unrestricted physical operation.

Step / owner	Required action and evidence
1 Confirm identity	Verify the model, PLC, robot, HMI, interface and toolchain baseline and the integrity of the archived executable and test package.
2 Review coverage	Reconcile requirements and scenarios, including variants, boundaries, faults and recovery. Identify unexecuted, failed and unsupported claims explicitly.
3 Assess fidelity	Review model verification, correlation, timing capability and uncertainty. Confirm that each accepted claim remains within the demonstrated model scope.
4 Resolve findings	Check defect closure and regression evidence. Record authorized noncritical deferrals with owner, restriction and due date; unresolved critical findings prevent release.
5 Define physical work	List installation, calibration, safeguarding, process and timing checks that remain. Assign each to the competent site owner and planned commissioning stage.
6 Approve package	Record the decision, approved scope, limitations and actual signatures in Annex F. Distribute the controlled package and prevent use of superseded candidates.

A release shall not be based solely on a presentation or video. The archived evidence must allow a competent reviewer to reconstruct what was tested and identify the exact candidate transferred to the physical project.

22 Transfer to physical commissioning

The site commissioning lead shall translate virtual evidence into a controlled physical test plan. Apply the actual equipment safety and isolation requirements before any energization or motion.

Step / owner	Required action and evidence
1 Verify installation	Check asset identity, mechanical assembly, wiring, utilities, frames, payloads and installed revisions against the released design. Record deviations before testing.
2 Establish protection	Confirm the required risk controls, guards, exclusion, emergency arrangements and authorized team. Complete the competent safety checks for the intended test stage.
3 Load and inspect	Verify the approved controller and robot package and actual settings. Remove simulation adapters, forced I/O and temporary overrides from the production configuration.
4 Test in stages	Perform approved static checks and controlled functional trials before integrated production. Verify actual sensors, actuators, timing and recovery within the protected test method.
5 Compare and correct	Correlate measured behaviour with the model and investigate deviations. Revalidate affected logic, model assumptions and product quality after any adjustment.
6 Release operation	Record safety, process and quality acceptance, remaining restrictions and the actual as-installed baseline in Annex G. Obtain the site authority's operating decision.

Unexpected motion, failed safeguarding, wrong I/O or unresolved product risk requires a hold. Physical commissioning adjustments shall be controlled changes and reflected in the model before it is reused for operational decisions.

23 As installed configuration and handover

23.1 At completion, reconcile the physical line with the digital baseline. Capture actual controller and robot programmes, hardware and firmware, frames, parameters, sensor locations and mechanical changes. The handed over twin shall represent the accepted installation within its stated scope rather than the earlier tender design.

23.2 Record deviations that remain intentionally different between model and plant, including simplified geometry and unmodeled behaviour. Explain their effect on permitted use. A maintenance team shall be able to determine whether a proposed analysis is supported without guessing which details were omitted.

23.3 Provide operating and maintenance owners with the model package, instructions, access rights, backup and restoration method and relevant training. Confirm that required software and data can be accessed over the planned lifecycle. An archive that cannot be opened or interpreted does not provide a usable handover.

23.4 Link the model to equipment records, spare parts information, risk assessments and commissioning evidence through stable identifiers. Avoid storing credentials or unnecessary personal data in the model. Document ownership and confidentiality restrictions on supplier contributions.

23.5 The receiving site owner shall acknowledge the actual handover and unresolved actions. Future modifications shall follow the controlled change process and trigger model impact assessment. The digital twin shall not remain labelled current after a material physical change that has not been evaluated.

24 Operational synchronization and controlled updates

24.1 Define which operational data enter the twin, why they are needed and how freshness and quality are assessed. Distinguish measured values, derived indicators and inferred states. A stale or missing signal shall be visible to the user and shall restrict analyses that depend on current conditions.

24.2 Begin operational integration with read-only data where that meets the intended use. Any command path from a model, optimizer or remote service to production requires separate engineering authorization, access control and protective design. A simulation result shall not automatically become a machine command.

24.3 Monitor drift in model predictions and underlying equipment behaviour. Define triggers for review such as changed cycle distributions, persistent parameter differences, maintenance modification or sensor replacement. Recalibration shall preserve version history and repeat the validation needed for the affected use.

24.4 If adaptive or learned models are used, control training data, model version, validation and deployment. Do not allow uncontrolled online learning to alter production behaviour or safety relevant assumptions. An updated model shall remain advisory until the defined review and authorization are complete.

24.5 Maintain a clear state of current, restricted, under revision or archived. Communicate restrictions to users and prevent obsolete analyses from being presented as current evidence. Record the time and physical configuration to which each operational result applies.

25 Cybersecurity access and intellectual property

25.1 Protect simulation assets, PLC code, robot programmes, factory layouts and production data according to their confidentiality and operational significance. Apply role based access, strong authentication, controlled sharing and audit records. Supplier collaboration shall expose only the scope necessary for the agreed work.

25.2 Separate development, simulation, test rigs and production networks through the approved architecture. Control adapters and remote connections that could bridge environments. A virtual commissioning tool shall not provide an undocumented route for writing to a live controller.

25.3 Verify imported scripts, libraries, models and executables before use. Treat active content and supplier packages as software supply chain inputs with known origin, integrity and dependency information. Do not run an unreviewed script merely because it is embedded in a plausible equipment model.

25.4 Protect secrets and credentials outside project files and shared logs. Use managed access for cloud resources and retain data residency and deletion requirements where applicable. A rendered image of a confidential factory layout can be sensitive even when the underlying model is not shared.

25.5 Use IAF-MAN-OTC-001 for connected factory controls and the IAF Data Protection and Privacy Policy for personal information. Define incident response, backup restoration and access revocation for the digital engineering environment and test that the retained project package can be recovered.

26 Defects changes and evidence integrity

26.1 Record a finding with the affected baseline, scenario, expected result, observed result, evidence and consequence. Classify whether the cause lies in the requirement, model, controller, interface, test or physical installation. Avoid assigning every discrepancy to the PLC before investigating the complete chain.

26.2 Prioritize defects by safety, product quality, availability and commissioning impact. Define release blockers and the authority for noncritical deferral. A frequent harmless visualization issue and a rare wrong-part release require different responses even if their defect counts are the same.

26.3 A change shall identify affected requirements, components and prior evidence. Perform peer review and an appropriate regression set before accepting the new baseline. Preserve the original failed run and link the corrected result rather than overwriting evidence to leave only passing records.

26.4 Control test logs, traces, screenshots and analysis calculations with timestamps and baseline identifiers. Record manual interventions and forced states. A result produced after an undocumented intervention shall not be treated as a clean execution of the approved scenario.

26.5 Use the IAF corrective action and complaints arrangements where appropriate and maintain impartial review under the Conflict of Interest Policy. Verify effectiveness after changes reach the physical line; a virtual fix that does not resolve the real problem requires further investigation.

27 Competence metrics and management review

27.1 Maintain a competence matrix covering modelling, controls, robotics, test design, statistical analysis, machinery safety and acceptance review. Practical evidence shall show that personnel can recognize model limitations and interpret failed tests, not only operate the software interface.

27.2 Define metrics that support decisions: requirement coverage, unresolved critical findings, repeated test reproducibility, model correlation, physical deviations and commissioning rework. Report test counts with scope and significance. A large number of trivial passing tests shall not conceal an untested consequential requirement.

27.3 Illustrative coverage: 92 verified requirements out of 100 applicable requirements is 92 percent. The remaining eight shall be listed with their risk and required action. If one is safety critical, the percentage does not justify operating release.

27.4 Management shall review assumptions, resources, supplier dependencies, fidelity gaps and physical follow-up at planned project milestones. Evaluate whether claimed benefits were achieved using consistent start and finish definitions. Avoid attributing all schedule improvement to the twin where other changes materially affected the outcome.

27.5 Annex H records assurance and learning. Share reusable findings with affected teams and update libraries through controlled review. Encourage reporting of model weaknesses and unexpected physical results; suppressing inconvenient discrepancies reduces the usefulness of the entire commissioning evidence.

28 Document control and IAF interfaces

28.1 Control models, code, test plans, reports and commissioning records through the IAF Documents and Records Guide. Assign owners, revisions, access, retention and disposal rules. Preserve the technical environment or an adequate reproducible export needed to interpret historical results.

28.2 This manual interfaces with IAF-QM-001, IAF-MAN-LMS-001 for lean production, IAF-MAN-GAA-001 for advanced assembly, IAF-MAN-OTC-001 for connected factory security and IAF-MAN-IHE-001 for industrial safety. IAF-MAN-NPI-001 governs pilot and new model introduction, while IAF-MAN-SDV-001 governs vehicle software quality.

28.3 Use the IAF In Line Quality and Computer Vision Manual where simulated sensors or quality systems are part of the project. Validation of synthetic or simulated inspection data shall remain distinct from physical sensor and product acceptance. Resolve shared interface ownership before the integrated release.

28.4 Revision proposals shall identify the affected requirement, reason, supporting evidence and transition needs. The competent IAF authority controls publication under the Constitution and document management arrangements. Sites shall assess the impact on local procedures, tools and active projects before applying a revision.

28.5 Annexes A to H are reproducible working templates. Enter actual values, evidence references and approvals; illustrative calculations and blank fields are not completed validation. Stable Release identifies the publication text and does not assert that any particular factory or simulation platform has already been technically approved.

Annex A Model scope and fidelity record

Complete before the main test campaign and update when the intended use or physical configuration changes. Attach the detailed model architecture and evidence register.

Field	Entry to complete
Project and scope	Project / line / assets / variants / model owner: _____
Intended decisions	Layout / logic / timing / capacity / other accepted uses: _____
Representation	Geometry / kinematics / dynamics / flow / human tasks included: _____
Data basis	Measured / supplier confirmed / planned / assumed data and owners: _____
Configuration	Model / controller / robot / HMI / adapter / solver versions: _____
Fidelity criteria	Required metrics / tolerances / uncertainty / evidence basis: _____
Limitations	Omitted behaviour / unsupported functions / restricted claims: _____
Physical follow-up	Installation, safety and process checks still required: _____
Approval	Technical reviewers / acceptance authority / date / next review: _____

Acceptance requires a clear relationship between each intended decision and the model evidence supporting it. Mark unresolved consequential assumptions as restrictions. A detailed visual model shall not be labelled validated solely because its appearance matches the planned factory.

Annex B Signal and interface mapping record

Use one controlled mapping row per signal or structured interface element. Expand the worksheet in the editable master and retain the completed mapping with the test baseline.

Mapping field	Entry to complete
Identity	Interface ID / controller tag / model object / owner: _____
Meaning	Physical meaning / source / destination / direction: _____
Data definition	Type / unit / range / polarity / invalid value: _____
Timing	Update interval / latency / timeout / timestamp basis: _____
State handling	Initial state / stale data response / restart behaviour: _____
Command and feedback	Command condition / completion evidence / fault indication: _____
Handshake	Correlation / acknowledgement / duplicate and retry handling: _____
Verification	Known stimulus / expected result / observed result / evidence: _____
Release	Mapping revision / reviewer / forced signals removed: _____

Verify scale and direction through controlled tests rather than tag names alone. Record simulated substitutes and their limitations. Before physical commissioning, confirm the actual wiring and remove any adapter or forced value that could conceal a missing or failed physical signal.

Annex C Virtual test scenario and result

Prepare expected results before execution and link them to requirements. Use separate records for materially different baselines or conditions.

Scenario field	Entry to complete
Identity	Test ID / requirement IDs / variant / risk priority: _____
Baseline	Model / PLC / robot / HMI / interface / toolchain: _____
Initial state	Part positions / resources / modes / retained data / seed: _____
Stimulus	Commands / events / fault location / timing / duration: _____
Expected response	Sequence / alarms / product disposition / recovery criteria: _____
Acceptance	Quantitative limits with units / logical conditions / oracle owner: _____
Execution	Operator / date / traces / manual interventions / actual result: _____
Disposition	Pass / fail / blocked / limitation / linked defect: _____
Review	Reviewer / repeat or regression needs / physical follow-up: _____

A test is blocked when the environment cannot represent the required condition reliably. Do not mark it passed through an idealized substitute. Preserve failed runs and identify whether correction changes the model, implementation or expected requirement.

Annex D PLC and robot optimization change record

Use for changes intended to reduce cycle time, scan load or other operating losses. Preserve the original baseline and evaluate functional and abnormal behaviour as well as performance.

Change field	Entry to complete
Problem	Measured limitation / affected process / baseline evidence: _____
Proposal	Code or path change / reason / expected benefit: _____
Impact	Timers / interlocks / quality / traceability / resource use: _____
Comparison	Same inputs, model, time basis and hardware conditions: _____
Performance	Before / after / variability / worst relevant condition: _____
Regression	Variants / boundary / fault / recovery cases and results: _____
Technical review	Controls / robotics / process / safety review as applicable: _____
Release	Executable identity / scope / restrictions / approving authority: _____
Recovery	Rollback or safe recovery package / trigger / owner: _____

Reject an optimization that gains average output by creating an unacceptable failure mode. A simulated improvement remains provisional where physical process timing, quality or hardware behaviour has not yet been demonstrated. Record the later physical result against the same change identifier.

Annex E Correlation and uncertainty worksheet

Use independent relevant observations to validate the model for its intended decision. Record calibration data separately from the data used for final validation.

Comparison field	Entry to complete
Use and metric	Decision / metric / unit / applicable conditions: _____
Evidence	Physical or supplier test / measurement method / uncertainty: _____
Model result	Baseline / simulation conditions / predicted value: _____
Observed result	Measured value / range / operating conditions: _____
Difference	Absolute error / relative error basis / systematic bias: _____
Acceptance	Predeclared tolerance / uncertainty treatment / pass or restriction: _____
Investigation	Cause / calibration change / independent revalidation: _____
Permitted scope	Accepted use / excluded claims / reviewers / date: _____

Illustrative comparison

Simulation 52.0 s; measurement 54.0 s. Absolute difference = 2.0 s. Relative error using the measured value = $2.0 \div 54.0 \times 100 = 3.70$ percent. The project must define whether this is acceptable before seeing the result; this example supplies no universal tolerance.

If measurement uncertainty or model simplification could change the decision, obtain better evidence or narrow the claim. Do not report more numerical precision than the underlying data supports.

Annex F Virtual commissioning release record

This record authorizes the stated virtual commissioning scope and next project stage. It does not authorize physical operation or replace site safety acceptance.

Release field	Evidence and decision
Identity	Project / package manifest / integrity IDs / review date: _____
Requirements	Applicable / verified / failed / blocked / deferred list: _____
Model suitability	Verification / correlation / timing / limitations accepted: _____
Functional evidence	Nominal / variants / boundaries / faults / recovery results: _____
Findings	Critical closure / noncritical restrictions / owners / due dates: _____
Physical plan	Outstanding installation, safety, process and timing tests: _____
Handover	Controlled package / supplier deliverables / receiving owner: _____
Decision	Release for stated stage / restricted release / hold: _____
Authority	Discipline reviewers / acceptance signature / date: _____

List each deferred requirement and its effect on the next stage. The acceptance authority shall not use a high aggregate pass rate to waive an unresolved critical condition. Preserve the exact tested candidate and the reason for every restriction.

Annex G Physical commissioning and twin reconciliation

Complete through the authorized site commissioning process. Attach detailed machinery, electrical, process and product test records rather than replacing them with general tick marks.

Commissioning field	Entry to complete
Installed identity	Assets / hardware / firmware / mechanical and wiring revisions: _____
Protection	Risk controls / guards / isolation / emergency arrangements: _____
Software identity	PLC / robot / HMI / parameters / simulation forces removed: _____
Static checks	I/O / frames / payload / utilities / inspection evidence: _____
Functional trials	Approved stages / measured behaviour / faults / recovery: _____
Quality evidence	Accepted trial product / process verification / restrictions: _____
Correlation	Differences from model / impact / corrective action: _____
As installed twin	Updated baseline / remaining limitations / handover owner: _____
Operating release	Safety / process / quality approval / scope / actual time: _____

A mismatch affecting a critical requirement requires a hold and technical resolution. Keep the model marked restricted until material installation changes are evaluated. The final handover shall identify the configuration actually operating at the site.

Annex H Assurance and project learning review

Review the quality of decisions and evidence rather than only the number of scenarios executed. Include supplier and physical commissioning feedback.

Review area	Result and action
Coverage	Verified requirements / applicable requirements / unresolved risks: _____
Reproducibility	Retained package reopened / repeat run evidence / exceptions: _____
Fidelity	Correlation results / significant assumptions / restricted uses: _____
Defects	Model, controls, interface and physical findings / recurrence: _____
Performance	Accepted output / cycle variability / actual commissioning rework: _____
Competence	Role assessments / training gaps / reviewer independence: _____
Actions	Owner / resources / due date / effectiveness evidence: _____

Illustrative metrics: 92 verified requirements out of 100 equals 92 percent coverage, with eight still requiring disposition. Sixty attempted units per hour minus six rejected units gives 54 accepted units per hour. Neither percentage nor output number overrides an unresolved safety or product requirement.

Review chair / participants / date: _____. Record improvements to libraries and procedures through controlled changes and verify that lessons are incorporated in the next project baseline.