AI FOR MANUFACTURING
WORKSHOP

IEC TC 65

Industrial-process measurement, control and automation

Extract from Standards Landscape, Ongoing Activities & Strategy covering Cyber security, Functional safety

Rudy Belliardi

IEC TC 65 Secretary

Disclaimer: While the author is the IEC TC 65 Secretary, opinions in the presentation and extract are of the author, not of the IEC/TC 65.

May 27–28, 2026 · NIST, Gaithersburg, Maryland

IEC TC 65 Overview, organisation with 4 subcommittees and 69 groups

IEC TC 65 INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION

Horizontal function for OT security

Chair	Rainer SCHRUNDNER (DE)	Technical Officer	Ms Marlene Maillet
Secretary	Rudy BELLIARDI (FR)	Std. Project Admin	Ms Lori Werner
Assist. Sec.	Adam GAUCI (FR)	Editor	Ms Maria-Elena Volet

AG14: Chair's advisory group
Convenor: Rainer Schrundner (DE) 17

SC 65A SYSTEM ASPECTS

Horizontal function for Functional Safety

Chair Koji DEMACHI (JP)
Secretary Stephanie Lavy (GB)
SPA Lori Werner
Editor Maxine Jost

- WG 4: EMC. Requirements — Convenor: Jochen Guethe(DE) 40
- WG 14: Functional Safety Guide — Convenor: Ron BELL (GB) 32
- WG 15: Alarm systems — Convenor: Donald G. DUNN (US) 20
- WG 16: IEC 61069 — Convenor: Kaoru ONDERA(JP) 15
- WG 18: FS Defence Applications — Convenor: Katia POTIRON (JP) 46; Convenor: Phil WILIAMS (GB)
- WG 19: HMI — Convenor: Maurice WILKINS(GB) 18; Convenor: David BOARD (GB)
- AG 20 Chair's advisory group — Convenor: Koji Demachi(JP) 18
- JWG 21 AI for FS — Conven:Canning(UK),Mariani(IT) 64
- WG 23 Continuous ProcessOperation — Convenor: Nazer(CA),Wilkins(UK) 11
- WG 24 Hum-Machine Collaboration — Convenor: K. TSUKIYAMA 14
- MT 61508-1/2 FS Maintenance — Convenor: Holger LAIBLE (DE); Convenor:Riccardo MARIANI (IT) 129
- MT 61508-2-1 FS Maintenance — Convenor:Tom Meany (IE) 31
- MT 61508-3 FS Maintenance — Convenor:Audrey CANNING(GB) 122
- PT 61508-3-2 FS FM Software — Convenor: Peter LADKIN (DE) 19
- MT 61511 FS for Process Ind. — Convenor: Dirk HABLAWETZ(DE) 94
- WG 25 Batch Control systems — Convenor: David BOARD (GB) 17

P 32
O 17

SC 65B MEASUREMENT & CONTROL DEVICES

Chair Tim LESSAU (DE)
Secretary Wallie ZOLLER (US)
Assist. Sec Chao Feng (US)
SPA Lori Werner
Editor Esther Monet

- WG 5: Temperature Sensor — Convenor: Masahiko GOTOH(JP) 30
- WG 6: Testing & Evaluation — Convenor: Marco Casati (IT) 30
- WG 7: Programmable control sy. — Convenor: Rene SIMON (DE) 60
- WG 9: Final Control Elements — Convenor: Sekhar SAMY (US) 25
- WG 14: Analyzing Equipment — Convenor: A.L.M.ADRICHEM(US) 27
- WG 15: Function Block — Convenor: Alois ZOITL (AT) 16
- WG 16: Power sources — Convenor: Ludwig WINKEL (DE) 6
- WG 65B/1302/NP (temporary) — Convenor: TBD
- MT 61131-9 IO-Link — Convenor: TBD 6

P 23
O 20

SC 65C INDUSTRIAL NETWORKS

Chair Ian VERHAPPEN (CA)
Sec. Alexandre NABAIS MORENO (FR)
Assist. Sec Carl SCHUMAKER (FR)
SPA Lori Werner
Editor Maxine Jost

- WG 9: Fieldbus Maintenance — Conven: Proell (DE), Winkel(DE) 82
- JWG 10: Industrial Cabling — Conven:Russo(IT),Hormeyer(DE) 53
- WG 12: FS for fieldbus — Convenor: Xiaoling ZHANG (CN) 51
- WG 15: High Availability network — Convenor: G. HOERCHER (DE) 39
- WG 16: Wireless — Convenor: Hideo Nishimura(JP) 55
- WG 17: Wireless Coexistence — Convenor: Ludwig WINKEL (DE) 36
- WG 18: TSN for IA — Convenor: Dieter PROELL (DE) 56
- MT 63444: Ethernet-APL — Convenor: Ludwig WINKEL (DE) 20
- ahG 19:Security for Communication — Conv:Micaela Caserza Magro (IT) 22
- JWG 20: Commnic. Tech+Arch — Conv: YC Hu(DE), Min Wei(CN) 26

P 23
O 21

SC 65E DEVICES AND INTEGRATION IN ENTERPRISE SYSTEMS

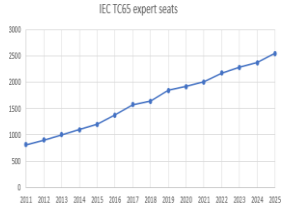
Chair Patrick LAMBOLEY(FR)
Vice-Chair Lu DING (CN)
Secretary David Richmond (US)
SPA Lori Werner Ed Maxine Jost

- WG 2: Prod. Dev. Eq. Proc. Func. — Conv:Dickmann(DE),Kesten(DE) 50
- WG 3: Commissioning — Convenor: Marco BOLL (DE) 13
- WG 4: Field Device Tools — Convenor: C.DIEDRICH (DE) 11
- JWG 5: Enterprise Control Sys Int — Convenor: C. MONCHINSKI (US) 24
- WG 7: Function Block + EDDL — Convenor: C.DIEDRICH (DE) 17
- WG 8: OPC — Convenor: Ingo WEBER (DE) 34
- WG 9: Automation ML — Convenor: Nicole SCHMITD (DE) 29
- WG 10: Intelligent Device Mgmt — Convenor: Ian VERHAPPEN(CA) 14
- WG 12: Predictive Maintenance — ConvenorChengchengWANG(CN) 18
- WG 13: 3D plant models — Convenor: Carsten BÖDEGE (DE) 7
- WG 14: Modul Type Package — Conv:S.Wang(CN),B.Martinez(FR) 23
- WG 15: Servitization of Manuf. — Convenor: DING, Lu 8

P 23
O 12

- WG 1: Terms & Definitions — Convenor: P.ZIMMERMANN(DE) 13
- WG 10: Security — Neitzel(US), Faifman(CA), Nicoll(US) 185
- WG 12: P&ID, CAEX — Conv: Mayr(DE), Ingebrigtsen(NO) 21
- JWG 13: Safety requirements — Convenor: Juergen MEIER (DE) 50
- JWG 14: Energy Efficiency(EEIA) — Convenor: R. BELLIARDI (FR) 54
- WG 15: Documents for Industry — Convenor: Matthias KIBLER(DE) 9
- WG 16: Digital Factory — Convenor:Thomas HADLICH (DE) 34
- JWG 17: Sys. Interf. En. Sys. /OT — Chen(CN),Ikeyama(JP),Verhappen(CA) 36
- WG 18: Cause and Effect Table — Convenor: Dieter GOLTZ (AT) 9
- WG 19: Lifecycle Mgmt. — Convenor: Detlef Winkel (DE) 12
- WG 20: Framework Safety & Security — Convenor: Koji DEMACHI (JP) 57
- JWG 21: SM Reference Model(s) — Conv:BRANDL(US), KIMURA(JP) 109
- WG 22: Reliability — Convenor: Lu DING (CN) 20
- WG 23: SM Framework +Concepts — Convenor: Weber(DE), Heidel(DE) 72
- WG 24: Asset Admin. Shell — Convenor: M.HOFFMEISTER(DE) 55
- JAG 25: Collaboration JTC1 SC27 — Conv: WEBER (DE), WOLF(ISO) 16
- JAG 26: Horizontal Security for OT — Convenor: Ingo WEBER (DE) 34
- JAG 28:Collaboration w. JTC 1/SC 41 — Conv: Schrundner(DE),Coallier(CA) 8
- JWG 29:Industrial Aut. Product Data — Conv:Weber(DE), Barnstedt(DE) 27
- ahG 30: AI in Industrial Autmation — Convenor: Riccardo MARIANI (IT) 22
- WG 31: Ind Agent Multi-Agent Sys — Proj.Leader: Christoph Legat (DE) 28

P 30
O 19



Additional information Including SCs

(2026-03-01)

- ~510 Publications
- ~95 Work items
- ~69 Groups
- ~1250 experts
- ~2647 seats incl. liaisons
- ~37 countries having experts

Cyber security and functional safety standards and AI in Manufacturing

LANDSCAPE

AI in Manufacturing still needs to fulfill the current standards in Cyber security and Functional safety.
The landscape just gets more complicated.

General concerns [from IEC 62443-1-1, new edition under development]

- The cyber security and functional safety disciplines have similar and even common concerns. An automation and control system cannot be deemed to be safe if it is not also secure. While each discipline has its own concepts and terminology, the imperative is the same. Prevention or mitigation of negative consequences is essential whether they are related to safety or cyber security.

- While the cyber security response is often based on risk assessment that includes threat, vulnerability and consequence, functional safety response typically includes detailed hazard analyses. Each discipline has defined a set of levels to provide guidance on selecting the most appropriate response for a given situation.

- When addressing functional safety, it is necessary to include cyber security in the overall hazard analysis work process, addressing cyber security throughout the entire safety lifecycle. Similarly, a comprehensive cyber security program must also consider implications for functional safety

Cyber security and functional safety standards definitions

LANDSCAPE

Security definitions [IEC 62443-1-1, new edition under development]

Security

condition of automation and control solution being free from unauthorized access and from unauthorized or accidental change, destruction or loss

Note: types of security are cyber security and physical security

Cyber security

set of actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, or damage to systems or informational assets

Note: Cyber security includes the concepts of identification, authentication, accountability, authorization, availability, privacy, and confidentiality.

Safety definitions [IEC 61508-0]

Safety

freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.

Functional safety

part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

Cyber security standards recent and in progress

IEC TC 65/WG 10 Security for industrial automation and control systems

Recent publications (IEC 62443 ‘Security for industrial automation and control systems series’ parts)

- IEC TS 62443-1-5 ED1 Scheme for IEC 62443 security profiles
- IEC PAS 62443-1-6 ED1 Application of the 62443 series to the Industrial Internet of Things (IIoT)
- IEC 62443-2-1 ED2 Security program requirements for IACS asset owners
- IEC PAS 62443-2-2 ED1 IACS security protection scheme
- IEC 62443-2-4 ED2 Security program requirements for IACS service providers
- IEC TS 62443-6-1 ED1 Security evaluation methodology for IEC 62443-2-4
- IEC TS 62443-6-2 ED1 Security evaluation methodology for IEC 62443-4-2

In progress (IEC 62443 Security for industrial automation and control systems series parts)

- IEC 62443-1-1 ED1 Overview and Guidance for the IEC 62443 Series (replaces TS)
- IEC 62443-2-1 ED3 Security program requirements for ACS asset owners
- IEC TS 62443-2-3 ED1 Patch management in the ACS environment [replacing TR]
- IEC 62443-2-4 ED3 Security program requirements for ACS service providers
- IEC 62443-3-1 ED1 Use of security technologies in the ACS environment
- IEC 62443-3-3 ED2 System security requirements and security levels
- IEC 63441-4-1 ED2 Secure product development lifecycle requirements
- IEC 63441-4-2 ED2 Technical security requirements for ACS components
- IEC TR 63441-4-3 ED2 Security programs lifecycles and roles
- IEC TR 63441-4-4 ED2 Security lifecycle details for automation and control solutions
- IEC 62443-6-1 ED1 Security evaluation methodology for IEC 62443-2-4 [replacing TS]

Most development done in liaison with ISA99

Documents in progress, including part # and title, are subject to change

Functional safety standards recent and in progress

IEC TC 65/SC 65A MT 61508-1-2, MT 61508-3, MT 61508-3-2

Recent publications (IEC 61508 series 'Functional safety of electrical/electronic/programmable electronic safety-related systems' parts and others based on IEC 61508)

- IEC TS 61508-3-2 ED1 Requirements and guidance in the use of mathematical and logical techniques for establishing exact properties of software and its documentation
- IEC TR 61508-3-3 ED1 Object-oriented software in safety-related systems
- IEC TR 5469 ED1 Artificial intelligence – Functional safety and AI systems (ISO/IEC JTC 1/SC 42 in liaison with MT 61508-3)

In progress (IEC 61508 series 'Functional safety of electrical/electronic/programmable electronic safety-related systems' parts)

- IEC 61508-1 ED3 General requirements
- IEC 61508-2 ED3 Requirements for electrical/electronic/programmable electronic safety-related systems
- IEC 61508-2-1 ED1 Requirements for semiconductors
- IEC 61508-3 ED3 Software requirements
- IEC 61508-4 ED3 Definitions and abbreviations
- IEC 61508-5 ED3 Examples of methods for the determination of safety integrity levels
- IEC 61508-6 ED3 Guidelines on the application of IEC 61508-2 and IEC 61508-3 (see Functional Safety and IEC 61508)
- IEC 61508-6-1 ED1 Treatment of hardware or software developed to ISO 26262
- IEC 61508-7 ED3 Overview of techniques and measures

Documents in progress, including part # and title, are subject to change

Functional safety standards in progress

IEC TC 65/SC 65A JWG 21 Artificial intelligence – Functional Safety and AI systems – Requirements linked to ISO/IEC JTC 1/SC 42

In progress

ISO/IEC 22440-1 ED1 Artificial Intelligence – Functional Safety and AI – Part 1: Requirements

ISO/IEC 22440-2 ED1 Artificial Intelligence – Functional Safety and AI – Part 2: Guidance

ISO/IEC 22440-3 ED1 Artificial Intelligence – Functional Safety and AI – Part 3: Examples of applications

ISO/IEC 25223 ED1 Information technology — Artificial intelligence — Guidance and requirements for uncertainty quantification in AI systems

Joint development with
ISO/IEC JTC 1/SC 42

Documents in progress, including part # and title, are subject to change

Cyber security and Functional safety (both concurrently) standards in progress

IEC TC 65/WG 20 Framework to bridge the requirements for safety and security

In progress

IEC TS 63069 ED1 Framework for safety and security

This work is a challenge by itself. Done in liaison with ISA84.

Documents in progress, including part # and title, are subject to change

Smart Manufacturing

IEC TC 65/WG 23 Smart Manufacturing Framework and Concepts for Industrial-process measurement, control and automation

IEC 63283 series Industrial-process measurement, control and automation – Smart manufacturing

Published:
Part 1: (TR) Terms and definitions
Part 2: (TS) Use cases
Part 3: (TR) Challenges for cybersecurity
Part 5: (TR) Market and innovation trends analysis

In progress:
Part 4: (TR) Usage of new technologies and standardization.
Part 6: (PAS) Valuation of intelligence properties for smart manufacturing system [not yet a project]

Considerations on AI.

Documents in progress, including part # and title, are subject to change

IEC TC 65/WG 24 Asset Administration Shell for Industrial Applications

Many parts, some published, others in progress. Some parts for cyber security.

Published: IEC 63278-1 ED 1 Asset Administration Shell for industrial applications - Part 1: Asset Administration Shell structure

Following are in-progress.

IEC 63278-2 ED1	Asset Administration Shell for Industrial Applications – Part 2: Information meta model.
IEC 63278-3 ED1	Asset Administration Shell for Industrial Applications – Part 3: Security provisions for Asset Administration Shells.
IEC 63278-4 ED1	Asset administration shell for industrial applications - Part 4:Applications of Asset Administration Shell.
IEC 63278-5 ED1	Asset Administration Shell for industrial applications – Part 5: Interfaces.

Some use of AI.
Great contribution for digitization, with high potential for AI.

Documents in progress, including part # and title, are subject to change

IEC TC 65/JWG 21 Smart Manufacturing Reference Model(s) linked to ISO/TC 184

Published:
IEC TR 63319 ED1 A meta-modelling analysis approach to smart manufacturing reference models
IEC 63339 ED1 Unified reference model for smart manufacturing

In progress
IEC TR 63597 ED1
Application of IEC 63339 to Smart Manufacturing Reference Models.

Considerations on AI.
Great contribution for digitization, with high potential for AI.

Joint development with
ISO /TC 184

Documents in progress, including part # and title, are subject to change

Agents in Industrial Automation

IEC TC 65/WG 31 Industrial Agent and Multi-Agent Systems

In progress

IEC 63718 Industrial Agent and Multi-Agent Systems
A series, expected to grow. The initial 5 parts are:

- Part 1: Fundamentals

(The following projects are in preparation)

- Part 2: Development
- Part 3: Application
- Part 4: Design Patterns
- Part 5: Key Performance Indicators

Cyber security and Functional safety considerations needed from the start.

Documents in progress, including part # and title, are subject to change

SC 65E WGs for Identification, tool exchanges, interfaces

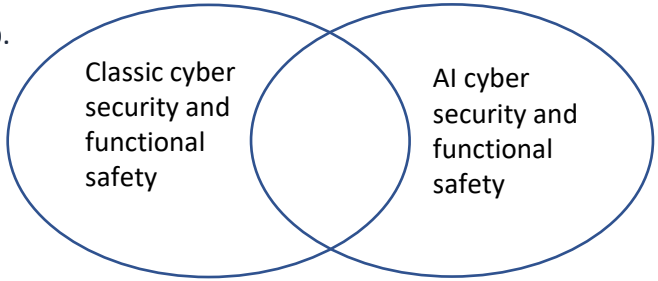
WG 2	Product, device, equipment, processes and functional descriptions
WG 3	Commissioning
WG 8	OPC
WG 9	AutomationML - Engineering Data Exchange Format
WG 10	Intelligent Device Management
WG 12	Predictive Maintenance
WG 13	Representation of electrical & instrument objects in digital 3D plant models during engineering
WG 14	Modular Type Package (MTP)
WG 15	Service-Oriented Manufacturing Resources and Capabilities

Great contribution for digitization, with high potential for AI.

AI Security and Safety are not the same as Security and Safety

Implications introduced by machine learning and fully autonomous agents

There is an overlap.
Both are needed.



Machine learning and types of agents, from deterministic workflow to fully autonomous, have great implications on the ‘classical’ approach to cyber security and functional safety for industrial automation.

In the early days of artificial intelligence, with automation realized via rule-based expert systems, the saying was that knowledge is power, but the problem was that there weren’t good ways to capture knowledge; today we know, via trained neural-networks, but often we cannot explain the consequence of that power.

We are now dealing with probabilistic systems, where outputs can change even with the same inputs.

AI Security and Safety are not the same as Security and Safety

Implications introduced by machine learning and fully autonomous agents

Classical cyber security and functional safety are formalized around roles, tolerable risk, requirements, reproducible incidents, and compensating measures, often via patches.

When dealing with machine learning and in particular with autonomous agents:

- Agents can change roles.
- The probabilistic behavior makes it difficult to quantify the risk.
- Auditing may not be possible.
- Often changes need to be made via curated data sets and tests, as it is difficult to interpret and reverse-engineer the output behavior.
- Incidents may not be reproducible.
- Patches cannot be performed on single components, it may be necessary to retrain the model on a new data set.
- Components come from many sources, some via 3rd party libraries, not fully vetted at this time.
- Availability, the most important factor of the Availability, Integrity, Confidentiality industrial automation triad, is difficult to assess.
- Protocols for communicating agents haven’t yet been fully exercised.
- Terminology is still not standardized, hampering the communication between field practitioners, and proper documentation.
- Need to give the model examples of bad input.
- Need to provide guardrails.
- In addition to cyber security for AI, there is the new challenge of AI used for adversarial attacks.
- Testing is still in its infancy.

Standardization

There is a need to standardize around AI used for Manufacturing, with times to be discussed, not only to allow communication and comparisons between users, but also to bootstrap the SDO standardization cooperation itself.
Successful systems have high content of custom work to compensate: time-consuming, expensive, fragile, does not transfer.
Missing standards are needed

- terminology
- communicating protocols, brokers
- methodologies
- tests
- models
- evaluations
- humans in/on the loop
- configurations for real time communication
- log and audit support, rationale

While both cyber security an functional safety are challenging and related, at this time it seems that standardization of cyber security for manufacturing systems that make heavy use of AI technology is more urgent, demanding, and behind the work done for functional safety. Moreover, cyber security is needed to protect functional safety.

If in the future all is done with AI, a secure and safe AI is all what is needed.

Standardization considerations

- Can we ‘migrate ‘ standards currently in development?
  - There has been a large investment on current standardization projects. Digitization has already injected several changes. AI is yet another wave, and can leverage digitization. Cyber security, Functional safety, OPC UA, Asset Administration Shell, Models …
- Defense in depth, also regarding development lifecycle.
- Determinism for real time, delegation
- Determinism for introspection and reinforcement learning
  - macro logging of decisions
  - documentation of rationale
  - aid for auditing, and for the broker receiving feedback loops
- Voting, including digital twin
- Canonical forms for testing
- DPP (TC 65/JWG 29) as a source of data, Evolution for optimization, Fail safe and restart