Additional TSN Industrial Automation Use Cases v0.4

Potential Use Case Targets for a future version / edition of IEC/IEEE 60802 [2026]

Contributors

This Use Case Document

McCall, David david.mccall@intel.com
Proell, Dieter dieter.proell@siemens.com

Initial Use Case Document from 2019

Belliardi, Rudy rudy.belliardi@schneider-electric.com
Dorr, Josef josef.dorr@siemens.com
Enzinger, Thomas thomas.enzinger@br-automation.com
Essler, Florian f.essler@beckhoff.com
Farkas, János janos.farkas@ericsson.com
Hantel, Mark mrhantel@ra.rockwell.com
Riegel, Maximilian maximilian.riegel@nokia.com
Stanica, Marius-Petru marius-petru.stanica@de.abb.com
Steindl, Guenter guenter.steindl@siemens.com
Wamßer, Reiner Reiner.Wamsser@boschrexroth.de
Weber, Karl karl.weber@beckhoff.com
Zuponcic , Steven A. sazuponcic@ra.rockwell.com

Abstract

This document describes use cases for industrial automation, which may be covered by a future project or projects to add functionality to IEC/IEEE 60802 TSN Profile for Industrial Automation. These use cases can guide a specification process: a selection of these use cases would determine WHAT shall be enabled by a future project or projects that specifies HOW to achieve the use cases at the system level of an IA system. Even if a project does not cover the overall system level, the project can enable, or at least does not prevent, the features described in a use case.

Log

Version	Date	Description
0.1	2025-11-10	Working Draft – Reviewed during Nov 2025 IEEE 802 Plenary
0.2	2026-01-25	Working Draft – Following review during Nov 2025 IEEE 802 Plenary. Minor updates. Group consensus from meeting was to “start fresh” rather than try to edit the original Use Case document from 2018. There will therefore be a more major update prior to the next review.
0.3	2026-01-25	Working Draft – “Start fresh” document. Clean sheet with use cases that, from previous discussion, it was decided to include for consideration; a mix of “old” use cases from discussions as part of developing IEC/IEEE 60802, but are not (fully) addressed by the published specification, and “new” use cases from contributors.
0.4	2026-01-28	Working Draft – Minor update following discussion during IEEE 802.1 TSN task group. Table of contents update and minor edits to text in a few use cases to improve clarity.

References

[1] "Use Cases IEC/IEEE 60802 v1.3", group contribution to IEC/IEEE 60802, September 2018

[2] "Review of potential use cases for a potential amendment to IEC/IEEE 60802 version 2", contribution to IEC/IEEE 60802 by David McCall, September 2025

[3] "Security Use Cases IEC/IEEE 60802", group contribution to IEC/IEEE 60802, April 2022

[4] "IEC/IEEE 60802 amendment brainstorming: IA-Controller – Cloud Solution – Configuration Domain", contribution to IEC/IEEE 60802 by Günter Steindl and Dieter Proell, June 2025

[5] "IEC/IEEE 60802 Edition 2 Topics", contribution to IEC/IEEE 60802 by Mark Hantel, July 2025

[6] "Management proxies for ccA", contribution to IEC/IEEE 60802 by Thomas Enzinger, May 2025

[7] "60802 – Edition 2 – Some Topics", contribution to IEC/IEEE 60802 by Marius-Petru Stanica, May 2025

[8] "Kick-off for Brainstorming on Potential Amendment to IEC/IEEE 60802", contribution to IEC/IEEE 60802 by János Farkas, May 2025

[9] "Other considerations for IEC/IEEE 60802, Edition 2", contribution to IEC/IEEE 60802 by Jordon Woods, May 2025

[10] "Simplified Standardization Workflows, ISA/IEC 62443 Security for industrial automation and control systems and Mapping of Standards to 62443", contribution to IEC/IEEE 60802 by Dieter Proell, May 2025

[11] "FRER Improvements Elimination of Contradicting Design Requirements", contribution to 802.1 TSN TG by Balázs Varga and János Farkas, September 2025

[12] "Overview of known issues for IEEE 802.1CB FRER…and next steps", contribution to 802.1 TSN TG by Dr. Lisa Maile, November 2025

Contents

<Figures – Placeholder for Table of Figures>

<Tables – Placeholder for Table of Tables>

Introduction

The document should be read in conjunction with IEC/IEEE 60802 TSN Profile for Industrial Automation (1st Edition; in a late draft, pre-publication stage at the time of writing v0.3 of this document). IEC/IEEE 60802 defines terms used in this document and provides context for many of the use cases. Some use cases are extensions of those covered by IEC/IEEE 60802 and described in early documents (see references) that drove development of the specification. Others are use cases defined in those documents, but not addressed in the specification (i.e. “left over” from its development). The remaining use cases are new to this document and based on contributions from the IEEE 802.1 TSN group.

Use Case 01: Deterministic Wireless Communications

Use Case

See [1] Use Case 9.

Wireless communications can be used in multiple scenarios. For example:

- Autonomous Mobile Robots (AMRs) and other mobile applications.
- Sensors and actuators where wired communications are impossible due to environmental conditions or movement.
- Communications where wired connectivity is expensive and wireless offers cost saving.

Within these scenarios, the ability to easily build heterogeneous networks with wired and one or more wireless technologies is desirable. The industrial automation use cases often require the same or similar capabilities from wireless connectivity when it comes to determinism and reliability. The use of existing wireless technologies is preferable. For example:

a) IEEE 802.11
b) IEEE 802.15.1
c) IEEE 802.15.3
d) IEEE 802.15.4
e) 5G / 6G

Existing Support & Potential Additions

IEC/IEEE 60802 is silent on wireless technologies. It only provides explicit support for wired (IEEE 802.3) connections.

Relevant Specifications

Besides those listed above:

- 802.1Q
- 802.11ax (Wi-Fi 6)
- 802.11be (Wi-Fi 7)
- IETF RAW (part of IETF DetNet)

Use Case 02: Redundant Communications (FRER for Relays)

Use Case

See [1] Use Case 7.

For critical applications, where loss of communication is unacceptable, networks are constructed to provide redundant paths. Data is replicated at one point in the network; copies of the data travers redundant pathways across the network; at a later point in the network, the pathways join and redundant data is eliminated.

The points of replication and elimination can be at the source (talker), sink (listener), or any point between (e.g. a bridge).

Existing Support & Potential Additions

IEC/IEEE 60802 1st Edition includes optional support for replication and elimination at an End Station (ccA or ccB), but not at a bridge (see 5.10.1b and 5.10.1c). Support for replication and/or elimination at a bridge is a possibility for 2nd Edition.

Relevant Specifications

- IEEE 802.1CB Frame Replication and Elimination for Reliability

Use Case 03: Virtual PLCs (FRER; Virtual NICs)

Use Case

Historically, Industrial Automation (IA) workloads have executed on PLCs running RTOSs. In the future it is expected that some workloads will execute on virtual PLCs (vPLCs) in containers or Virtual Machines (VMs) running general purpose OSs (e.g. Linux) with real-time capabilities.

The latter architecture enables distributed control systems that are much more dynamic, with workloads potentially being short-lived and/or rapidly moving from one location in a network to another. The network itself may also include a combination of physical NICs and virtual NICs, the latter running as part of a virtual machine.

The network protocols, and network configuration and management tools need to cope with the dynamic orchestration of workloads and nature of virtual NICs, specifically the fact that multiple virtual NICs' capabilities may be constrained by the resources available in a single physical NIC.

Existing Support & Potential Additions

IEC/IEEE 60802 1st Edition includes optional support for replication and elimination at an End Station (ccA or ccB), but not at a bridge (see 5.10.1b and 5.10.1c). Concerns have been raised that some aspects of the current FRER recovery algorithms may be problematic for dynamic, virtual environments (see [11]) and may be addressed by maintenance actions that the 802.1 TSN TG is currently considering (see [12]).

Contributions would be appreciated on the challenges and potential solutions related to the uses of virtual NICs.

Relevant Specifications

- IEEE 802.1CB Frame Replication and Elimination for Reliability

Use Case 04: Remote Virtual PLCs (Multi-subnet Operation)

Use Case

Architectures that support consolidation of workloads from multiple PLCs to a single, higher-powered industrial PC (see Use Case 03) also enable the physical location of the PC and it's workloads to be more easily moved away from the production line to, for example, and on-premises data centre or the Cloud. This location is typically not on the same IP subnet as the production line. Thus, network traffic from the workload to the production line has to traverse multiple subnets.

There are two potential use cases:

a) Integration of determinitstic IETF, IP-Level, cross-subnet, dynamic routing (DETNET)

b) Ability to set up a cross-subnet, QoS "tunnel" that can be comprehended and used by dynamic routing that is otherwise restricted to single subnet operation.

Existing Support & Potential Additions

IEC/IEEE 60802 is silent on multi-subnet operation. It only provides explicit support for operation within a single subnet.

IETF DETNET defines technologies that provide deterministic data paths that operate over Layer 2 bridged and Layer 3 routed segments.

See [4] regarding Use Case 04(b).

Relevant Specifications

IETF DETNET

Use Case 05: Bumpless Joining of Two Machines

Use Case

See [1] Use Case 21.

In some production environments, machines can connect and disconnect to and from multiple different networks during normal operation. For example, multiple AGVs (automatic guided vehicles) accessing various docking stations to communicate with a supervisory PLC. At times, an AGV may operate as a self-contained CPS (Cyber-Physical System). At other times, an AGV may act as one part of a larger CPS.

As networks are separated and joined, the operation of the AGVs must not be interrupted, i.e. there can be no “bump”; the separation and joining must be “bumpless”.

Existing Support & Potential Additions

IEC/IEEE 60802 1st Edition covered alignment of a 2nd machine's time domain with a 1st machine's in a bumpless manner (see D.2.3). It also states that if 2nd machine's time domains ceases to exist (i.e. replaced by first machine's) "Typically, in this case, the second machine is not operational while it is joined to the first.", i.e. BUMP!

Discussions in IEC/IEEE 60802 have included suggestions that further informative guidance could be provided on how to enable bumpless separation and joining either with or without normative additions to the specification.

Relevant Specifications

?

Use Case 06: SECURITY - Maintain security during Device Replacement and Modular Machine Assembly

Use Case

See [3] Use Case 2.

a) **Device replacement without engineering**: an owner/operator wants to (ad-hoc) replace a broken IA device and needs to equip the replacement IA device with keys/credentials that are specific for the production site or cell – without using engineering (or similar) tools.

b) **Modular machine assembly**: an owner/operator wants to (ad-hoc) re-use a priorly deployed IA device in another machine and needs to equip the re-used IA device with keys/credentials that are specific for the new production cell – without using engineering (or similar) tools.

Existing Support & Potential Additions

Use case for Taking Posession was covered in detail (trust on first use model) in IEC/IEEE 1st Edition; Device Replacement and Modular Machine Assembly are not elaborated on, i.e. the specification is silent. Both would probably use a lot of what was defined for Taking Possession but were regarded as out of scope for 1st Edition.

Relevant Specifications

?

Use Case 07: SECURITY - Resilience Against Attacks via LLDP

Use Case

See [3] Use Cases 3, 5 & 7.

Deployments of Industrial Automation technology must be secure against attack to ensure safety, performance, and continued operation. Compliance with the EU Cyber Resilience Act (CRA) (Regulation 2024/2847) is also a requirement for many deployments.

LLDP (IEEE 802.1AB) is an important enabling technology for IEC/IEEE 60802.

Existing Support & Potential Additions

IEC/IEEE 60802 1st Edition includes security for configuration, but not LLDP (or Time Sync; all are part of the Control Plane).

Note that security of Data Plane is expected to be managed via Industrial Automation protocols.

Relevant Specifications

- IEEE 802.1AB

Use Case 08: SECURITY - Resilience Against Attacks via Time Sync (Control Plane)

Use Case

See [3] Use Cases 3, 5 & 7.

Deployments of Industrial Automation technology must be secure against attack to ensure safety, performance, and continued operation. Compliance with the EU Cyber Resilience Act (CRA) (Regulation 2024/2847) is also a requirement for many deployments.

Time Synchronization (IEEE 802.1AS) is an important enabling technology for IEC/IEEE 60802.

Existing Support & Potential Additions

IEC/IEEE 60802 1st Edition includes security for configuration, but not Time Sync (or LLDP; all are part of the Control Plane).

Note that security of Data Plane is expected to be managed via Industrial Automation protocols.

Relevant Specifications

- IEEE 802.1AS

Use Case 09: SECURITY - Resilience Against Increasingly Sophisticated Attacks (excluding Quantum Computing)

Use Case

See [3] Use Cases 10.

Deployments of Industrial Automation technology must be secure against attack to ensure safety, performance, and continued operation. Compliance with the EU Cyber Resilience Act (CRA) (Regulation 2024/2847) is also a requirement for many deployments.

Over time, threat vectors change and protective actions must evolve to mitigate the threats.

Note: this use case is for threats excludes threats from quantum computing, which are sufficiently different and novel to warrant a separate use case.

Existing Support & Potential Additions

IEC/IEEE 60802 1st Edition includes security for configuration. It is best practice to periodically evaluate whether the supported approaches and algorithms continue to provide sufficient protection against current and future, expected threats.

Relevant Specifications

?

Use Case 10: SECURITY - Resilience Against Attacks Using Quantum Computation

Use Case

See [3] Use Cases 10.

Deployments of Industrial Automation technology must be secure against attack to ensure safety, performance, and continued operation. Compliance with the EU Cyber Resilience Act (CRA) (Regulation 2024/2847) is also a requirement for many deployments.

Over time, threat vectors change and protective actions must evolve to mitigate the threats. Recent advances in Quantum Computing suggest that, if the current pace is maintained, quantum computers might become capable of breaking many existing, widely used encryption protocols within a few years. It is therefore desirable to have encryption protocols that are robust against quantum computing available.

It may also be advisable to start using “quantum-safe” encryption algorithms in advance of quantum computing achieving the capability to break existing encryption algorithms. This protects against the possibility of sensitive, encrypted data being captured and stored until the capability is available.

Existing Support & Potential Additions

IEC/IEEE 60802 1st Edition includes security for configuration, but only against “traditional”, i.e. non-quantum, attack vectors.

Relevant Specifications

?

Use Case 11: SECURITY - Robust Supply of Security Core Function

Use Case

See [3] Use Case 11.

Deployments of Industrial Automation technology must be secure against attack to ensure safety, performance, and continued operation. Compliance with the EU Cyber Resilience Act (CRA) (Regulation 2024/2847) is also a requirement for many deployments.

Most Industrial Automation approaches to security, including IEC/IEEE 60802, rely on a solid foundation of underlying core capabilities. For example:

- **Authenticated encryption (AEAD)** vs. classical schemes (first-sign-then-encrypt or first-encrypt-then-sign; sidenote: encrypt-only is no safe harbor)
- **Key protection**
- **Randomness** for symmetric and asymmetric keys, nonces
- **Dedicated HW** for accelerating cryptographic operations and protecting keys/credentials, especially long-lived ones

Manufacturers, machine builders, system integrators and owners/operators need to be able to rely on these core functions.

Existing Support & Potential Additions

Considered out of scope for IEC/IEEE 60802 1st Edition, but the specification does rely on the robust supply of security core functions. Might not need details included in the specification, but might be good to add some references on how to do it (e.g. IEC 62443)?

Relevant Specifications

?