IEC/IEEE 60802 Ed2

Open topics

2026-05-11

Günter Steindl, Siemens AG

Content

- Status
- Cell/Machine vs. Aggregation & Factory Backbone
- From deterministic QoS to deterministic Trust
- Constraint Devices / Proxy / Onboarding
- Wireless Integration
- Seamless Redundancy
- Conclusion

Status

Great progress, adoption is happening

Status

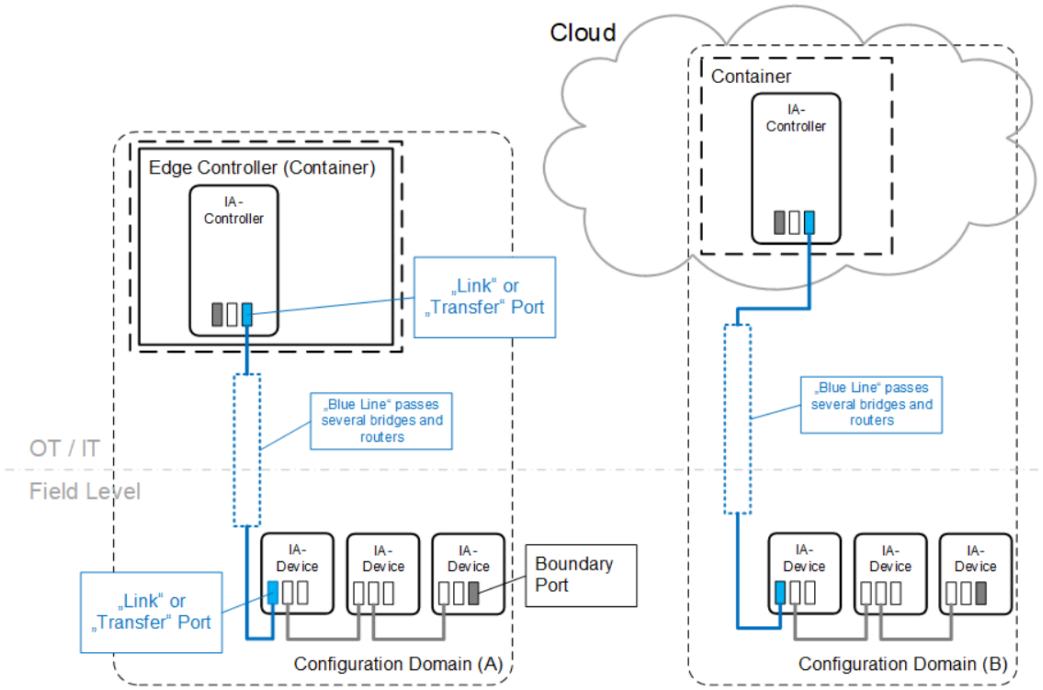
- IEC/IEEE 60802 ED1 is approved and being published
  => Great work — this will be used
- Example
  - PROFINET V2.5 positions IEC/IEEE 60802 as a referenced foundation for TSN
  - Interoperability was demonstrated: PROFINET devices combined with IEC/IEEE 60802(-like) bridges were shown as a technology demonstration at SPS 2025 and HMI 2026 fair
  - IEC/IEEE 60802-capable silicon fits PROFINET stations, even if not all TSN capabilities are used on day one, headroom enables future-proof evolution

=> Great progress, adoption is happening

=> Now we must keep momentum and drive the Edition 2

Reference for the "Blue Line"

IA-Controller – Cloud solutions – Problem statement



Reference for the contribution defining the "Blue Line" in this contribution:

[60802-Steindl-Proell-IA-Controller-ConfDomain-Cloud-0725]

Cell/Machine vs. Aggregation & Factory Backbone

Solving the responsibility assignment challenge

Keeping the Converged Network: Cell/Machine vs. Aggregation & Factory Backbone

- IEC/IEEE 60802 ED1 defines the Configuration Domain for Automation Cells or Machines
- In modern deployments, the IA-Controller may run at the OT/IT level (edge) or in the cloud, creating a logical distance (“Blue Line”) to IA-Devices
- The Blue Line crosses bridges and routers that are not part of the Configuration Domain → therefore it needs a Quality of Service

=> Key question: How do we preserve determinism when control/engineering spans beyond the Configuration Domain?

=> Without a standardized inter-domain model, we risk losing the just-achieved converged network properties

Standardized Inter-Domain Model: SLA + OAM + “Virtual Bridge” Abstraction

- Use OAM mechanisms (ITU-T Y.1731) as the toolbox for OAM and SLA thinking in Ethernet networks
- The SLA separates responsibilities between IT and OT
- The model expects OT to specify the acceptable Min/Max Delay for the Blue Line for the Configuration Domain, while IT can set a tunnel consistent with the Min/Max Delay requirements
- Engineering abstraction:
  - A tunnel with two tunnel endpoints (TEP) can make the remote IA-Controller appear as part of the Configuration Domain
  - The Blue Line looks like a bridge with two ports and offers Min/Max Delay characteristics

=> Suggestion: Standardize the abstraction (Virtual Bridge/OAM Port), not a single vendor tunnel technology

Service Level Monitoring (SLM): prove the SLA continuously

- Monitoring the Blue Line connection between IA-Controller and IA-Devices
- Suggestions:
  - Latency envelope (min/max one-way delay) per “virtual bridge” / per path segment
  - Jitter bound relevant for isochronous tasks
  - Time sync quality (e.g., offset/GM stability) when sync crosses domain boundaries
  - Availability / outage budget for the Blue Line + fault localization hooks (OAM)

=> SLM allows responsibility assignment between IT and OT

Time Synchronization across Domain Boundaries (Isochronous Applications)

- Find a solution for “Time sync” for the SLA/OAM/tunnel setup
- What is the standardized contract between Configuration Domain and Edge/IA-Controller regarding time?
- How to solve the “802.1AS Hop Count ~64…100” limit together with the Blue Line for synchronization

=> Do we need a normative “Time Gateway”?

Suggestion

- We need a standardized inter-domain model connecting IA-Controller and the IA-Device over the “Blue Line”
- SLA + OAM/Virtual Bridge + Time Sync are to be solved topics

=> Otherwise, we will re-fragment the converged network

=> Standardize an abstraction of the “Blue Line”, not a single vendor technology

From deterministic QoS to deterministic Trust

“Blue Line QoS” to “Blue Line Trust” — don’t lose convergence

“Blue Line QoS” to “Blue Line Trust”

- Once control/engineering spans beyond the Configuration Domain, the “Blue Line” crosses infrastructure outside the domain and therefore needs QoS + monitoring
- The same boundary immediately becomes a trust boundary: crossing it requires a security model (not only latency/jitter guarantees)
- If we standardize QoS/SLA but not security, the converged network will fragment again (operators will fall back to ad-hoc VPNs, blocked protocols, or isolated islands)

Secure Cell / Defense in depth: Perimeter protection + scalable security model

- Secure Cell / Defense-in-Depth is a recognized setup: segmentation into zones; firewalls/access control restrict traffic at the cell boundary
- “Secure Access” adds secure device access into the cell via a secure mechanism; e.g., Netconf or for PROFINET “Secure SXP over TCP”
- Clear distinction helps scoping:
  Secure Cell / Defense in depth = inside a protected perimeter, whereas secured access crosses a trust boundary (tools from outside)

Peer-to-Peer / Control-Plane protocols: required, but security is unclear

- Open question to IEEE 802.1 / IEC/IEEE 60802:
  - How to secure LLDP, gPTP, MSTP, … in the IEC/IEEE 60802 configuration domain?
  - How to secure ARP, ICMP, … in the IEC/IEEE 60802 configuration domain?
- This is not theoretical: these protocols are needed for engineering/operation scenarios and are repeatedly raised as requirements

=> Secure Cell / Defense in depth – how to secure essential protocols?

=> What is the role of IEEE 802.1AE and IEEE 802.1X for the Configuration Domain and its boundaries?

Constraint Devices / Proxy / Onboarding

Convergence must include constrained devices

Constrained Devices: Why this matters

- Convergence must include constrained devices, otherwise we re-fragment the Configuration Domain
- Many industrial devices are constrained in code/data size; available NETCONF/YANG implementations may not fit their footprint
- Requirement: keep the IEC/IEEE 60802 Configuration Domain model intact while accommodating constrained implementations

=> Integrate constrained devices into the IEC/IEEE 60802 configuration model without losing interoperability

Path forward:
Proxy onboarding now, standard lightweight later

- Edition 1 (pragmatic):
  - Keep the NETCONF/YANG domain; integrate constrained devices via a configuration proxy that translates CNC's NETCONF/YANG bidirectionally into the constrained device's organization/manufacturer-specific protocol
  - Proxy operating model: once discovered, constrained devices are assigned a proxy by the CNC; the proxy accepts configuration requests via dedicated YANG models and performs protocol translation (resource-heavy work stays on the ccA/proxy side)
- Edition 2 (strategic):
  - Evaluate whether a standardized, cheaper integration path is possible by leveraging CBOR/YANG-CBOR/CDDL
  - Can we replace the proxy with a simpler and cheaper protocol gateway?
  - Protocol gateway replaces the proxy southbound; CNC view remains NETCONF/YANG

=> Can we find a standardized solution for an easier/cheaper to integrate constraint devices?

Wireless Integration

Wireless is a trend we cannot ignore

Wireless Integration

- Strong market trend toward wireless industrial automation; if not integrated into the standard, parallel incompatible architectures will emerge
- How to handle Access Point + clients which are part of the Configuration Domain?
- How to handle an 5G factory backbone scenario
  - Access Point(s) outside, Blue Line, of the Configuration Domain
  - Clients are part of the Configuration Domain
  - 5G system as abstracted as Virtual Bridge?

=> How should Access Point and wireless clients be modeled as part of the Configuration Domain?

Seamless Redundancy

A solution covering all application traffic (not only streams) is needed

Seamless Redundancy

- HSR and PRP are widely deployed in industrial automation; they define protocol-independent node roles such as DAN and SAN
- HSR/PRP define node roles (DAN/SAN) and operational expectations for seamless redundancy across application traffic
- FRER seems to need further specification to substitute HSR and PRP in all use cases

=> Does FRER cover the operational scope expected of automation systems for all traffic types, including non-stream traffic?

=> Can automation systems migrate from HSR/PRP to FRER due to functional equivalence?

=> If not, what is missing? Or should we allow/profile HSR and/or PRP, too?

Conclusion

Momentum: „Great work, don’t slow down“

Don’t lose convergence

Industrial adoption pressure: Cost (constrained devices) + Wireless + Redundancy

Preserve Convergence

- ED1 is approved; adoption is happening → keep momentum
- Boundaries (“Blue Line”) need a standard model:
  SLA + OAM/Virtual Bridge + Time
- The same boundary is a trust boundary:
  without security model, convergence fragments
- Industrial adoption requires:
  constrained devices + wireless + redundancy without losing interoperability

Conclusion

- ED2 work items:
  - SLA/SLM/OAM,
  - time contract,
  - secure cell/defense in depth / essential protocols,
  - constrained device path,
  - wireless model,
  - redundancy clarification.

=> How to continue?