Briefing on IEC/IEEE 60802 Security

K. Fischer, A. Furch, O. Pfaff
Illustrating IA Devices/Controllers

- PLC program
- IO module
- Edge client
- Dashboard
- DIY

IEC/IEEE 60802 scope
- IEC 61158
- OPC-UA
- MQTT
- Web
- DIY

Middleware/shim
- User configuration
  - CUC client
- Network configuration
  - MIB
  - YANG
  - SNMP
  - NETCONF
- Addressing
  - DHCP
  - DNS

Ethernet layer
- 802.1AS
- 802.1AB
- 802.1CB
- 802.3
- 802.1Q

IP layer
- TCP/IP

Network interface

Application

Middleware/shim

IEC/IEEE 60802 scope
Scope of the Security Contribution

- **Security between stations**, in particular:
  - Discovering neighborhood relations
  - Provisioning of network configuration including TDMEs
  - Establishing streams including TDMEs
  - Synchronizing time

- **Shared security means**, considering the joint use for IEC/IEEE 60802 security and application/middleware security on a single station, in particular:
  - Profiling the set of cryptographic algorithms, their usage (e.g. TLS record layer or 802.1AE and protocols for managing this usage (e.g. TLS handshake layer or 802.1X)
  - Using a single security resource, e.g. (HW) secure element upon a single station for this purpose

- **Securing-the-security**, in particular:
  - Supplying/managing initial keys/credentials/security configuration to individual stations in a secure manner
Guiding Principle

- Converged networks need a ‘converged security’ model
- Converged security means:
  i. **An interoperable solution** for IEC/IEEE 60802 security - covering the above identified scope, especially *security between stations*
  ii. **Co-existence** of IEC/IEEE 60802 security with the security for application/middleware as (sub)components on the same physical entity (station) – a part of the above identified scope, especially *shared security means* and *securing-the-security*
Main Functional Objectives

• **Message exchange protection** between identified stations:
  
  • Objective: protect communications against *forgery*, *tampering*, and *eavesdropping*
  
  • Features: (peer) entity identification and authentication, (data) integrity and confidentiality, replay protection
  
  • Scope: the system communications that are in-scope

• **Resource access authorization**:
  
  • Objective: protect system resources against *unauthorized access*
  
  • Features: coarse-grained authorization e.g. network isolation, fine-grained authorization e.g. application/middleware or network configuration resources
  
  • Prerequisite: message exchange protection, esp. (peer) entity identification and authentication
  
  • Scope: the system resources that are in-scope
**Building Blocks**

- **In-scope:**
  1. Security between stations
  2. Shared security means
  3. Securing-the-security

- **Out-of-scope for IEC/IEEE 60802:** security between and at middleware/application components:
  - Protecting their message exchanges e.g. IEC 61158 communications between PLC programs and IO modules
  - Authorizing their resource accesses e.g. providing or changing instructions for the operation of an IO module

*: joined usage by application/middleware security is perceived but not shown here
Respecting Industrial Automation

- IEC/IEEE 60802 security shall respect the essential characteristics/properties of industrial automation components/systems

- In particular characteristics/properties that differentiate industrial automation from IT must be addressed adequately. Differentiators from IT include:
  - Dedicated set of use cases, e.g. ‘IA device replacement without engineering’, ‘machine cloning’
  - Embedded and constrained system components (lacking local user interfaces, limited computing power and memory, …)
  - System components that present physical entities and computing entities at the same time
  - Unattended operations
  - Undisturbed operations, e.g. bumpless key updates
  - Autonomy of production cells (with external cell control)
  - Deterministic communications particularly for time-aware streams
  - Physical world impacts, e.g. functional safety
Authors

Kai Fischer, Siemens AG, T RDA CST SES-DE,
kai.fischer@siemens.com

Andreas Furch, Siemens AG, T RDA CST SES-DE,
andreas.furch@siemens.com

Oliver Pfaff, Siemens AG, T RDA CST,
oliver.pfaff@siemens.com