SIEMENS
Ingenuity for life

Security for IEC/IEEE 60802

Goals, Constraints and Use Cases

K. Fischer, A. Furch, L. Lindemann, O. Pfaff, T. Pössler, G. Steindl

Problem Statement

- Establish the **goals** for a security contribution to IEC/IEEE 60802 (see [14])
- Identify the given **constraints** for this contribution
- Agree on the applicable **use cases** for it

Next Steps

1. Present on security for IEC/IEEE 60802 in the **IEC/IEEE 60802 track** of the IEEE Interim Session (May, 05 2021; 09:00-11:00 ET)
2. Provide an initial contribution proposal for the **next draft D1.3** in text form using inputs from
   - Goals, constraints and use cases (this deck)
   - Selected information from the presentations for the
     - IEEE Interim Session 2021-05-05 (forthcoming)
     - IEEE Plenary Session 2021-03-03
     - Weekly TSN working group call 2021-02-22

Scope

SIEMENS
Ingenuity for life

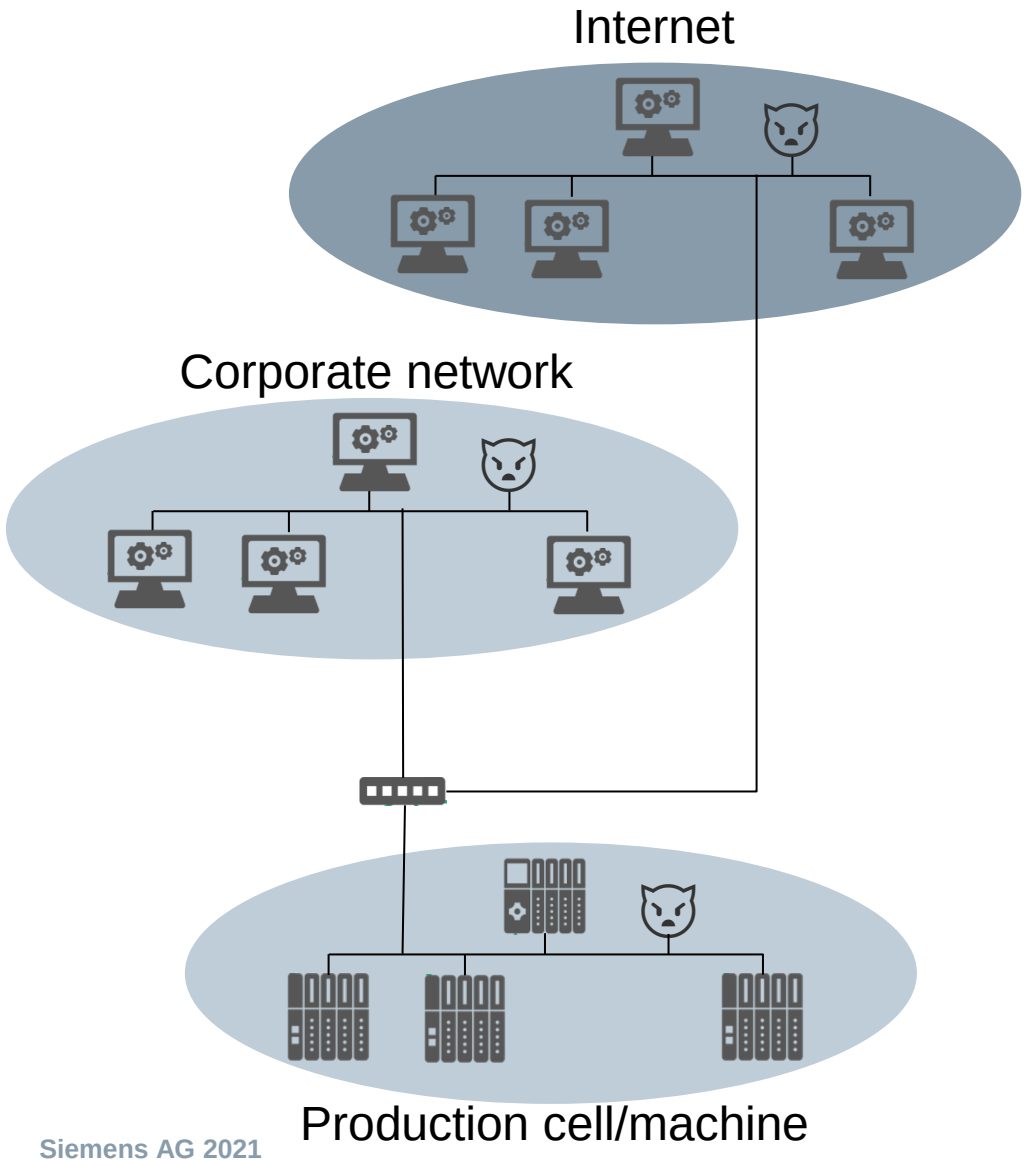
- **Security between stations**, in particular:
  - Discovering neighborhood relations
  - Provisioning of network configuration including TDMEs
  - Establishing streams including TDMEs
  - Synchronizing time
- **Shared security means** considering the joint use for IEC/IEEE 60802 security and application/middleware security on a single station, in particular:
  - Profiling the set of cryptographic algorithms, their usage (e.g. TLS record layer [11] or 802.1AE [7]) and protocols for managing this usage (e.g. TLS handshake layer or 802.1X [3])
  - 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

SIEMENS
Ingenuity for life

- 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*

To-Be-Assessed Security Threats: Scenarios



3. **Threats from the Internet:** attack vectors that apply when considering an Internet integration of production cells:
   - Exercised by (potentially) anyone
   - Exploiting remote access to the local network on layer 3-7

2. **Threats from local layer-3 networks**: attack vectors that apply when considering a production cell integration with corporate networks:
   - Exercised by e.g. staff employed by organizations that own/operate production cells
   - Exploiting remote access to the local network on layer 3-7

1. **Threats from the local layer-2 network**: attack vectors that apply when considering a production cell in isolation:
   - Exercised by e.g. staff with physical or local network access to the production cell e.g. service technicians
   - Exploiting physical access or remote access on layer 2

To-Be-Assessed Security Threats: Attack Vectors

SIEMENS
Ingenuity for life

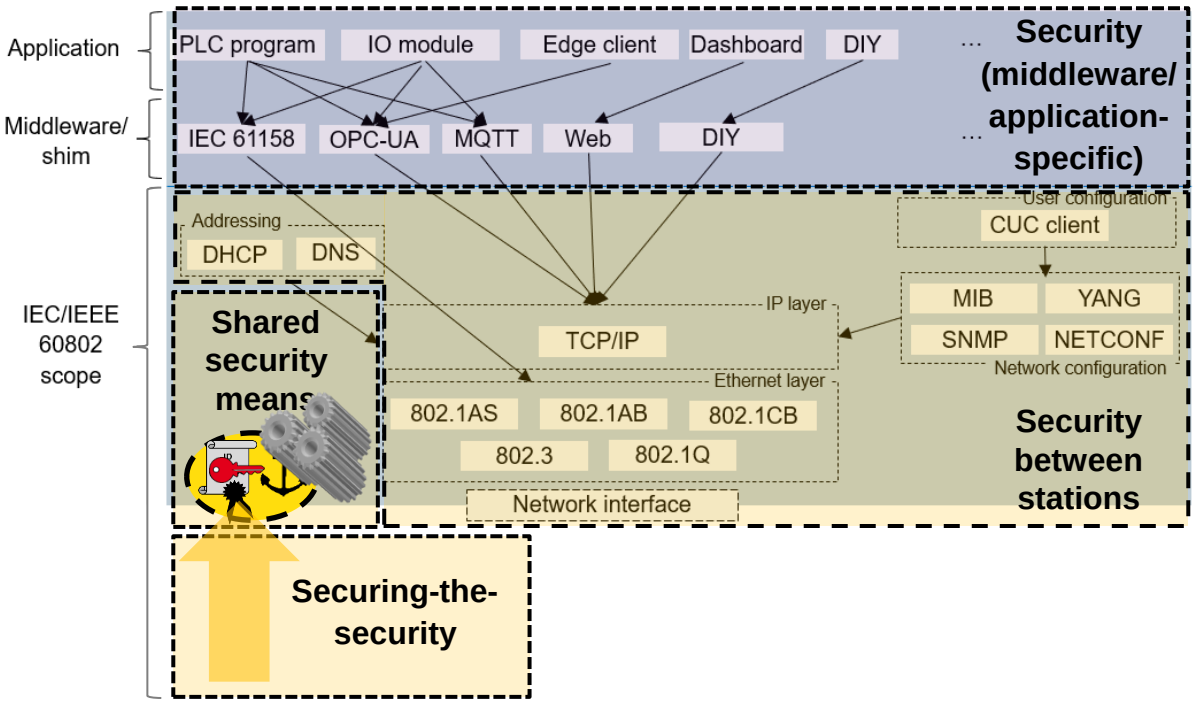
- Concerning individual physical entities (stations – as perceived in the network):
  a. **Impersonating/spoofing** of physical entities - e.g. forgery
  b. **Manipulating** of physical entities - e.g. corruption
- Concerning individual computing entities within a station (applications/middleware – as perceived in the network):
  c. **Impersonating/spoofing** of computing entities - e.g. forgery
  d. **Manipulating** computing entities - e.g. corruption
- Concerning communications between stations:
  e. **Insertion/manipulation** of individual messages or messaging contexts – e.g. tampering by manipulation or replaying, repudiation, denial-of-services
  f. **Reading** of message contents – e.g. eavesdropping
- Concerning accesses to (local) resources of a station by another (remote) station:
  g. **Abusing** (local) resources – e.g. accessing without privileges
  h. **Escalating** of privileges – e.g. accessing with inappropriate privileges

Functional Objectives

SIEMENS
Ingenuity for life

- **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 (see above for details)
- **Resource access authorization**:
  - Objective: protect system resources against **unauthorized access**
  - Features: authorization decision enforcement, making and policing
    - Prerequisite: message exchange protection, esp. (peer) entity identification and authentication
  - Scope: the system resources that are in-scope (see above for details)
- Note: message exchange protection plus resource access authorization allows to defeat/mitigate most attack vectors in the considered scenarios

Building Blocks



- In-scope (see Scope for details):
  i. **Security between stations**
  ii. **Shared security means**
  iii. **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

Respecting Industrial Automation

SIEMENS
Ingenuity for life

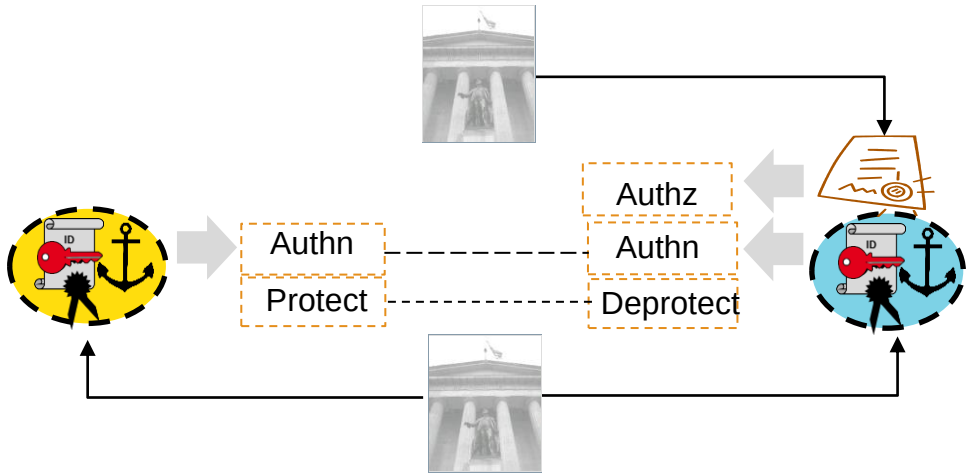
- IEC/IEEE 60802 security shall respect the essential characteristics/properties of industrial automation components/systems
- In particular characteristics/properties that differentiate industrial automation from IT must be addressed adequately. Differentiators from IT include:
  - Dedicated set of use cases (see [10]), 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

Covering IEC 62443

SIEMENS
Ingenuity for life

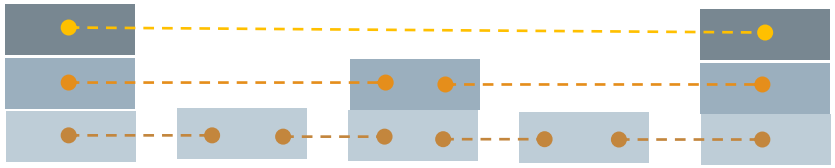
- IEC 62443-3-3 “System Security Requirements and Security Levels” (see [5]) and IEC 62443-4-2 “Technical Security Requirements for IACS Components” (see [13]) will be considered when creating the security contribution for IEC/IEEE 60802:
  - IEC 62443-3-3 and IEC 62443-4-2 **provide requirements** (from system and component perspective) to be addressed/considered by IEC/IEEE 60802 security (foundational requirements and security levels)
  - They do **not provide solutions** for their requirements, esp. do not provide a solution for IEC/IEEE 60802 security
- Applicability of further IEC 62443 documents for IEC/IEEE 60802 security needs further consideration
- Intended relationship with respect to IEC 62443:
  - IEC/IEEE 60802 security is **one building block** for the security of IEC 62443 IACS components
  - IEC/IEEE 60802 security shall **not conflict** with IEC 62443

Assigning Ownership for Keys/Authorizations



- Message exchange protection requires to assign authority for **keying control** e.g. keys for NETCONF message protection
- Resource access authorization requires to assign authority for **authorization control** e.g. for access control for NETCONF resources
- This aspect needs to be **balanced** by IEC/IEEE 60802 security, considering:
  - **Actors** in **industrial automation**: manufacturers, machine builders, distributors, system integrators, owners, operators…
  - **Lifecycle** of an individual **station**: manufacturing, bootstrapping, operating, maintenance, off-boarding (according [12])
  - **Use cases** for an individual **stations**: configuration update, SW/FW update….

Placing Security in the Protocol Stack



- Message exchange protection and resource access authorization require the allocation of **security mechanisms** in the **protocol stacks**
- This aspect needs to be **balanced** by IEC/IEEE 60802 security, considering:
  - **Going up/down**: there is no single, one-fits-all placement that can cover all demands
    - Going up a stack allows to granularly protect entities/ objects and lengthens the achievable security span but tends to increase the overall complexity
    - Vice versa for going down the stack
  - **Footprint**: multiple simultaneous stack placements of security can improve functionality/flexibility but also increases its price-tag

Given Rules for Security Contribution

SIEMENS
Ingenuity for life

- **Re-use** existing security mechanisms specified by IEC, IEEE and IETF
- **Identify** possible white-spots
- **Not invent** solutions for possible white-spots - if such need arises dedicated projects shall be considered

Overview

SIEMENS
Ingenuity for life

- **Automation-domain use cases** - that shall be matched by IEC/IEEE 60802 security:
  - Are provided in the document ‘Use Cases IEC/IEEE 60802 V1.3’ (see [10])
  - Action item: the security contribution to IEC/IEEE 60802 shall comment on the automation use cases. Note: comments for the use case 30 ‘Security’ in [10] are already provided below
- **Security-domain use cases** - that shall be identified and elaborated in the security contribution for IEC/IEEE 60802:
  - Candidates are proposed below
  - Action item: the security contribution to IEC/IEEE 60802 shall elaborate on the security use cases
- Constraint: **security** shall be added in a way that allows all **automation use cases** to still be **fulfilled**

Comments on Use Case 30 “Security”

SIEMENS
Ingenuity for life

- *Topping-up*: by adopting cryptographic security a whole set of **new security use cases** emerges and shall be considered (see below for candidates)
- *White-spot*: **authorization** is a fundamental goal of security and should be added
- *Refinements*: apart from spelling-out ‘*authorized system entities*’ (see Glossary), **availability** is a constraint for security and should be referred to as such
- *Scope*: albeit **protection against rogue/fake applications (running on authenticated stations)** is no sole deliverable of IEC/IEEE 60802 security it should be addressed as security threat/attack vector
- *Differentiation*: differentiate „**rogue**“ (*right entity behaving wrong*) and „**fake**“ (*wrong entity behaving right or wrong*)

Proposals for Security Use Cases (1)

SIEMENS
Ingenuity for life

1. **Checking the equipment under control**: serves to motivate/explain the checking (actual vs. expected) of IA components as prerequisite before imprinting keys/credentials for security (see [6] for an elaboration of this concern in case of natural persons)
2. **Imprinting during bootstrapping/commissioning**: serves to motivate/explain the supply of (initial) keys/credentials and differentiates according several credentialing modes e.g. human-operated/assisted vs. unattended/automated credentialing (see [1] for a basic model)
3. **Instructing equipment about security**: serves to motivate/explain the security instructions towards IA components:
   - Per owner/operator: security-only by default
   - Per individual IA component: security always-on or on/off, enabled ciphers….
   - Per application/communication relation: security on/off, authentication-only/authenticated encryption…
4. **Peer entity authentication:** serves to motivate/explain (peer) entity authentication and its inherited features e.g. key agreement or authorization including checking actual/expected (see [4] for an elaboration of this concern in case of IT)

Proposals for Security Use Cases (2)

SIEMENS
Ingenuity for life

5. **Message exchange protection:** serves to motivate/explain the protection of communications between stations including its prerequisites, in particular peer entity authentication (including identification)
   - Note: this security use case overlaps with use case 30 “Security” in [10]. It is proposed to serve a transfer
6. **Proving self-asserted information:** serves to motivate/explain binding between peer entity authentication and self-asserted information - applicable in case of such feature e.g. identification and maintenance data or topology discovery data
7. **Resource access authorization:** serves to motivate/explain access control and its prerequisites, in particular peer entity authentication (including identification)
8. **Credential/key update during operation**: serves to motivate/explain the handling of key aging, considers/establishes bumpless-ness
9. **Credential/key revocation/invalidation during operation**: serves to motivate/explain the handling of premature termination of key/credential lifetime
10. **Crypto algorithm-expiry/agility:** serves to motivate/explain the handling of the dawn of crypto algorithms

Abbreviations

SIEMENS
Ingenuity for life

Authn	Authentication
Authz	Authorization
DIY	Do It Yourself
DLL	Data Link Layer
E2E	End-to-End
EUC	Equipment Under Control
FW	FirmWare
HTTP	Hypertext Transfer Protocol
HW	HardWare
IA	Industrial Automation
IACS	Industrial Automation and Control Systems
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IT	Information Technology
JOSE	Javascript Object Signing and Encryption
MAC	Medium Access Control (networking) or Message Authentication Code (security)
OAuth	Open Authorization
OPC	Open Platform Communications
OT	Operational Technology
PLC	Programmable Logic Controller
SW	SoftWare
TDME	TSN Domain Management Entity
TLS	Transport Layer Security
TSN	Time-Sensitive Networking

Glossary (1)

SIEMENS
Ingenuity for life

Attack (RFC 4949, [2]): An intentional act by which an entity attempts to evade security services and violate the security policy of a system

Authorization (RFC 4949): An approval that is granted to a system entity to access a system resource

Availability (RFC 4949): The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system

Bridge (IEEE 802.3, [9]): A functional unit that interconnects two or more IEEE 802 networks that use the same data link layer (DLL) protocols above the medium access control (MAC) sublayer, but can use different MAC protocols. Forwarding and filtering decisions are made on the basis of layer 2 information

Computing entity (DIY): A system entity that has no own incarnation in the physical world e.g. PLC program/IO module

Credential (IEEE 802.1AR, [8]): Information that an entity (a person or device) possesses that allow it to make a verifiable claim of identity, i.e., to be authenticated

(Data) confidentiality (RFC 4949): The property that data is not disclosed to system entities unless they have been authorized to know the data

(Data) integrity (IEEE 802.1AE): A property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored

End station (IEEE 802.3): A functional unit in an IEEE 802 network that acts as a source of, and/or destination for, link layer data traffic carried on the network

Glossary (2)

SIEMENS
Ingenuity for life

Fake entity (DIY): A wrong system entity (incapable to authenticate itself – if that would be demanded) behaving right or wrong

Integrity (RFC 8446): Data sent over the channel after establishment cannot be modified by attackers without detection

Message authentication (IEEE 802.1AE): If the message arrives authenticated, the cryptographic guarantee is that the message was not modified in transit and that the message originated from an entity with the proper cryptographic credentials

(Peer) entity authentication (RFC 4949): The process of verifying a claim that a system entity or system resource has a certain attribute value. An authentication process consists of two basic steps:

> *Identification step*: Presenting the claimed attribute value (e.g., a user identifier) to the authentication subsystem
>
> *Verification step*: Presenting or generating authentication information (e.g., a value signed with a private key) that acts as evidence to prove the binding between the attribute and that for which it is claimed

Physical entity (DIY): A system entity that has an incarnation in the physical world e.g. station

Risk (RFC 4949): An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result

Rogue entity (DIY): A right system entity (authenticated or capable of authenticating itself) behaving wrong (because of e.g. being corrupted internally)

Glossary (3)

SIEMENS
Ingenuity for life

Secure element: (Global Platform): A tamper-resistant platform (typically a one chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities

Spoofing (IEEE 802.1AE): Claiming a fraudulent identity for purposes of mounting an attack

Station (IEEE 802.3): An end station or bridge

(System) entity (RFC 4949): An active part of a system -- a person, a set of persons (e.g., some kind of organization), an automated process, or a set of processes (see: subsystem) -- that has a specific set of capabilities

Threat (RFC 4949): A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm

References, Chronologically Ordered

SIEMENS
Ingenuity for life

1. Stajano, F.; Anderson, R: The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks, 1999
2. IETF RFC 4949: Internet Security Glossary, Version 2, 2007
3. IEEE 802.1X-2010: IEEE Standard for Local and Metropolitan Area Networks – Port-Based Network Access Control, 2010
4. IETF RFC 6125: Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS), 2011
5. IEC 62443-3-3: System Security Requirements and Security Levels, 2015
6. NIST SP 800-63: Digital Identity Guidelines, 2017
7. IEEE 802.1AE-2018: IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Security – Revision D 1.3, 2018
8. IEEE 802.1AR-2018: IEEE Standard for Local and Metropolitan Area Networks–Secure Device Identity, 2018
9. IEEE 802.3-2018: IEEE Standard for Ethernet, 2018
10. IEC/IEEE 60802: Use Cases IEC/IEEE 60802 V1.3, Draft (work-in-progress), 2018
11. IETF RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3, 2018
12. IETF RFC 8576: Internet of Things (IoT) Security: State of the Art and Challenges, 2019
13. IEC 62443-4-2: Technical Security Requirements for IACS Components, 2019
14. IEC/IEEE 60802: Time-Sensitive Networking Profile for Industrial Automation, Draft 1.2, 2020

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

Lars Lindemann, Siemens AG, DI FA CTR ICO ARC,
lars.Lindemann@siemens.com

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

Thomas Pössler, Siemens AG, RC-AT DI FA DH-GRAZ SAS,
thomas.poessler@siemens.com

Günter Steindl, Siemens AG, DI FA TI ART EA,
guenter.steindl@siemens.com