SIEMENS
Ingenuity for life

Security for IEC/IEEE 60802

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

Executive Summary

SIEMENS
Ingenuity for life

- *Goal*: propose a security contribution to IEC/IEEE 60802 covering
  i. **Security for shared resources**
  ii. **Shared security means**
  iii. **Securing-the-security**
- *Constraints*:
  - **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

Problem Statement

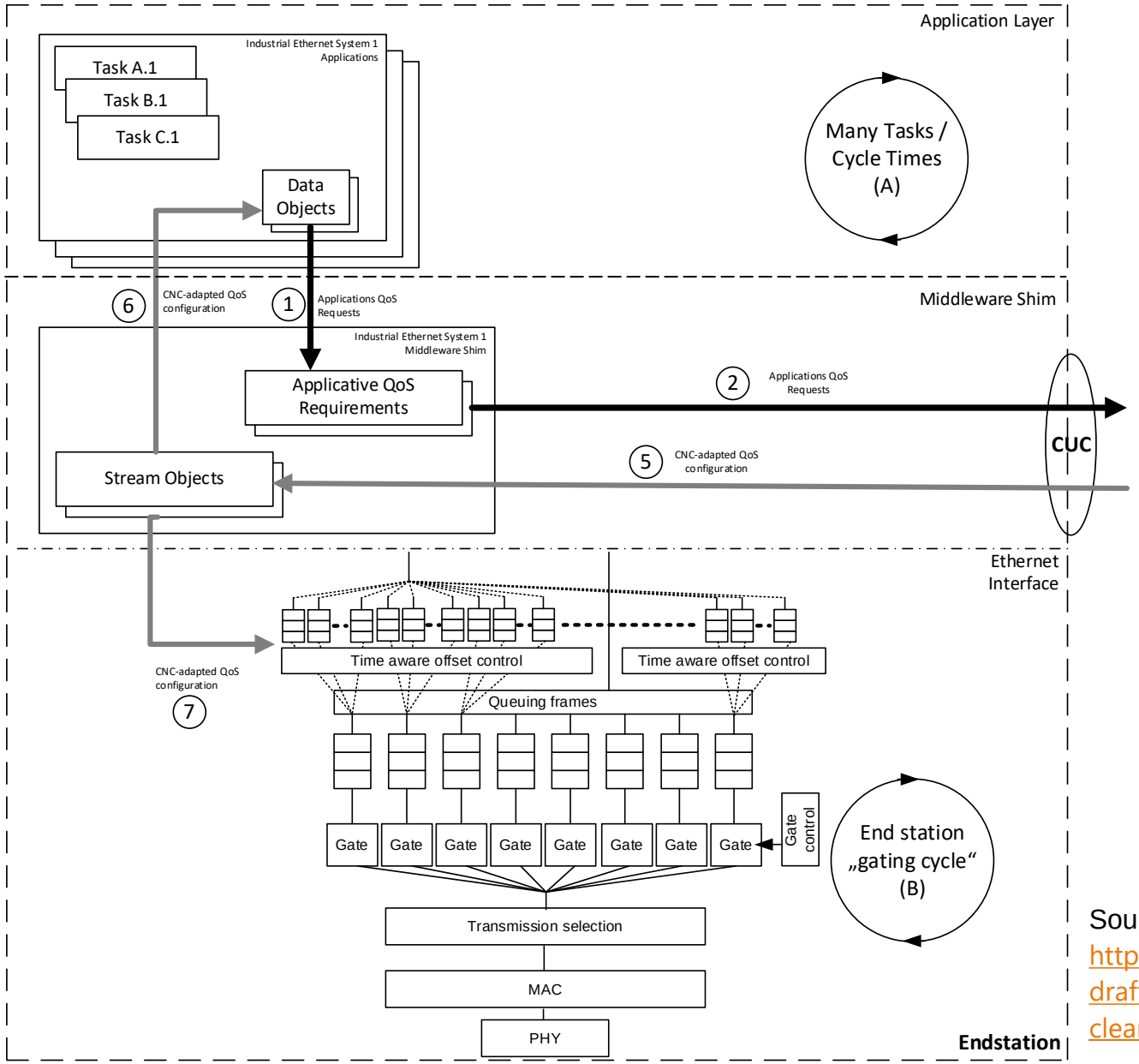
SIEMENS
Ingenuity for life

- IEC/IEEE 60802 specifies TSN profiles for **IA devices**: a single IA device is assumed to host middleware/applications from **one or more domains** e.g. IEC 61158, OPC-UA, Web…
- Security historically emerged **per domain,** in a somewhat **isolated fashion** and backed by **IT-specific needs**
  - *The Good*: the originating domain knows its resources best; no other domain can design resource protection details better
  - *The Bad and the Ugly*: the common security mechanisms depend on fundamental tasks such as "*check the entity before attaching a key*". That would happen for **each domain** i.e. multiply for a single component – unless an over-arching integration happens

Security fulfilment disciplines*	Best done by	Industry status quo
Protection of domain-specific resources	Domain-specific security	Largely addressed
Establishment of security associations between domain-specific endpoints on IA devices	Domain-specific security	Largely addressed
Management of initial credentials and overall security configuration for individual IA devices	Overarching security	**White-spot and/or plethora of bits&pieces**

*: to achieve message exchange protection and resource access authorization

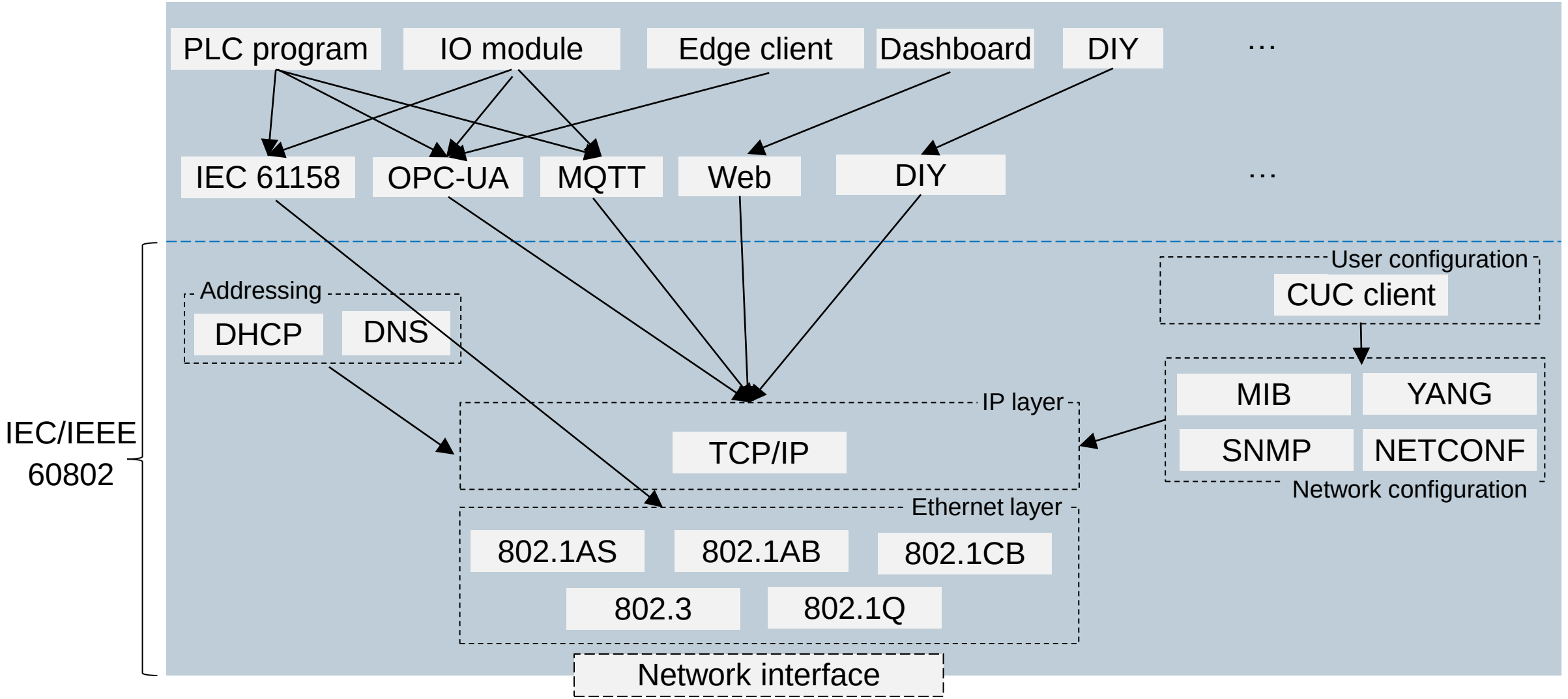
IA Device - Recap



Source: Figure 2 – Industrial Automation in https://www.ieee802.org/1/files/private/60802-drafts/d1/60802-Steindl-Clause4-0121-v17-clean.pdf (modified)

IA Device – Zoom-in & Zoom-out

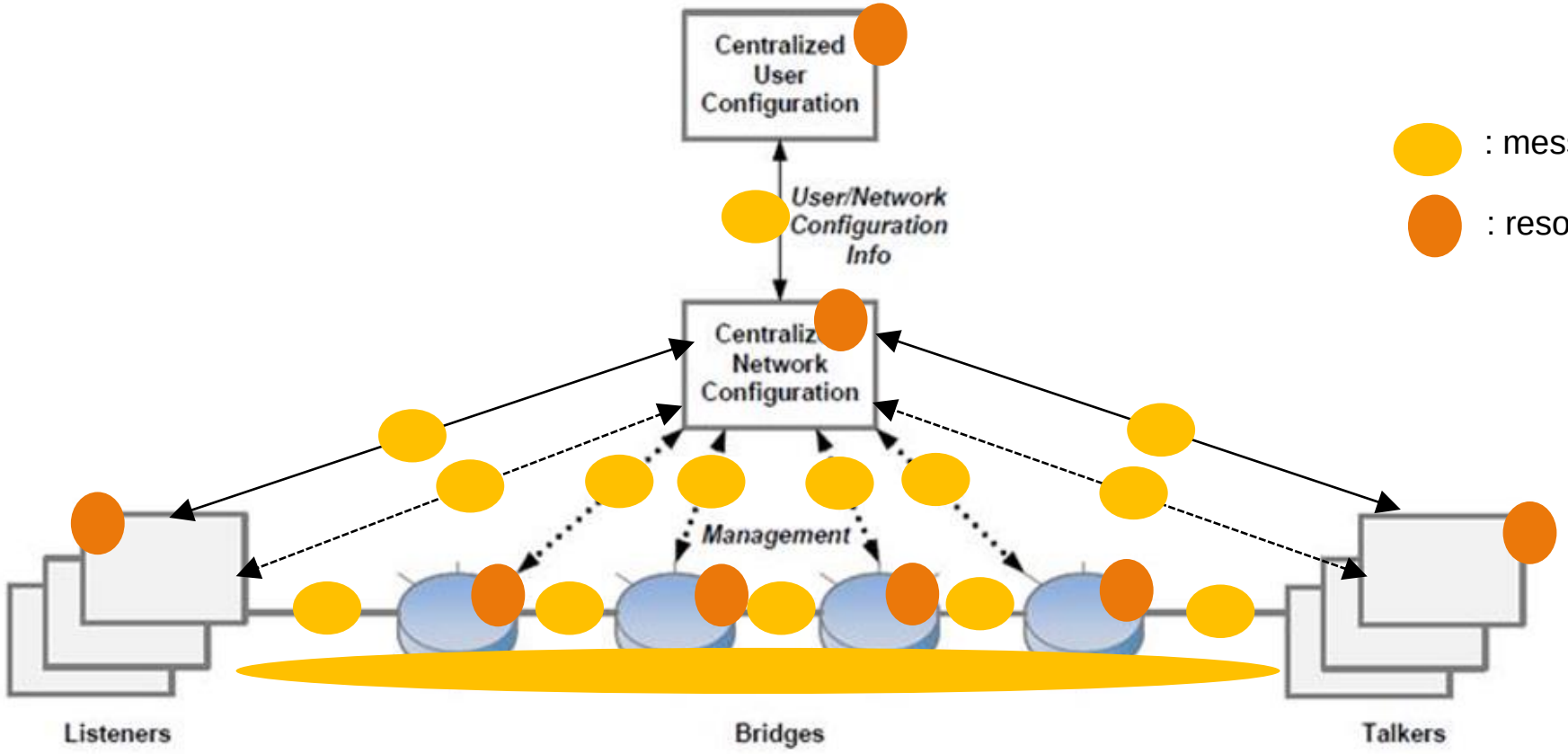
SIEMENS
Ingenuity for life



Security Demands in Distributed Systems

SIEMENS
Ingenuity for life

- **Protect message exchanges**: depends on (mutual) entity authentication, depends on entity identification
- **Authorize resource accesses**: depends on entity authentication of the caller, depends on entity identification
- Illustrated for IA systems (also translates to decentralized model):



Source: Figure 46-3 – Fully Centralized Model in IEEE 802.1Qcc:2018 (modified)

Physical Entity Identification State-of-the-Art

SIEMENS
Ingenuity for life

- **One or more identifiers** apply to **one IA device instance** as a physical entity e.g.

Origin	Instance identifiers	Values controlled by	Notes
IA device (IEC/IEEE 60802)	MAC address	Manufacturer	Globally unique form of MAC addresses
IEC 61158, (here: type 10, PROFINET)	NameOfDevice: manufacturer ID/product type/product serial number	PI: manufacturer ID Manufacturer: product type and product serial number	Also imprinted to device body (electronic reading)
OPC-UA	ProductInstanceURI	Manufacturer/machine builder	Also imprinted to device body (electronic reading)
OEM sub-components	(Manufacturer ID)/product type/product serial number	Misc. entities: manufacturer ID Manufacturer: product type and product serial number	OEM sub-component: part of an IA device e.g. network card (reflected by best-current-practices)

Computing Entity Identification State-of-the-Art

SIEMENS
Ingenuity for life

- **One or more identifiers** apply to **one IA device instance** as a computing entity e.g.

Cluster	Origin	Instance identifiers	Values controlled by
Application/ middleware	**IEC 61158,** (here: type 10, PROFINET)	NameOfStation	Owner/operator
	OPC-UA	Application name/URI	Owner/operator
	MQTT	IP address and/or DNS name, UDP or TCP port number	Owner/operator
	Web	IP address and/or DNS name, TCP port number	Owner/operator
Network	**IP layer**	IP address and/or DNS name, UDP or TCP port number	Owner/operator
	Ethernet layer	MAC address	Manufacturer
	Configuration	IP address and/or DNS name, UDP (or TCP) port number (NETCONF/SNMP)	Owner/operator
	Addressing	IP address and/or DNS name, UDP or TCP port number	Owner/operator

Security State-of-the-Art

SIEMENS
Ingenuity for life

- **One or more security offerings** apply to **one IA device** as an instance in a distributed system e.g.

Cluster	Domain	Message exchange protection	Resource access authorization
Application/ middleware	**IEC 61158**	Supported by some types e.g. types 2/10	Supported by some types e.g. type 10
	OPC-UA	UASC or TLS-based secure channel (client/ server), application object-level security (PubSub)	Role-based, resource consumers call authorization services
	MQTT	TLS-based secure channel and/or application object-level security	Not specified (left to MQTT technology suppliers/users)
	Web	TLS-based secure channel	Not specified for legal entity-owned resources (elaborated (OAuth, UMA) for the individually-owned resource space)
Network	**IP layer**	IPsec/IKE-based secure packets (network layer)	Identifier-based, resource providers call authorization services (RADIUS etc.)
	Ethernet layer	MACsec-based secure frames (802.1AE, 802.1X)	Identifier-based, resource providers call authorization services (RADIUS etc.)
	Configuration	TLS or SSH-based secure channel, mutually authenticated, dedicated checks (NETCONF). Application object-level security (SNMP)	Not elaborated (NETCONF and SNMP)
	Addressing	DNSSEC-based object-level security	N.a. (resources are regarded public)

State-of-the-Art Shortcomings

SIEMENS
Ingenuity for life

- Security:
  i. **Security for shared resources:** known solutions exist in IT (e.g. DNSSEC, NETCONF/SNMP security [IETF]). Their fitness for IA devices is unclear. At least, resource access authorization is under-illuminated
  ii. **Shared security means**: commonly known solutions are subject to IT (e.g. PKCS#11 [OASIS] as an interface standard). With respect to IA devices these solutions come with undesired complexity.
  iii. **Securing-the-security**:
    - Known solutions from IT (e.g. ACME/CMC/CMP/EST/SCEP [IETF]) do not translate into solutions for IA devices – by copy&paste
    - Emerging solutions from middleware/application initiatives in the OT domain (e.g. OPC-UA security) lead to a plethora of approaches, possibly resulting in multiplication of work for a single IA device
- Identification: the evolution of security (in 'isolated fashion') could end in *schizophrenia* in case of IA devices*

*: identification information in multiple forms for a single entity (for human beings e.g. nickname/full name, driver license/passport/tennis club card…) is okay if there is an understood way of correlation

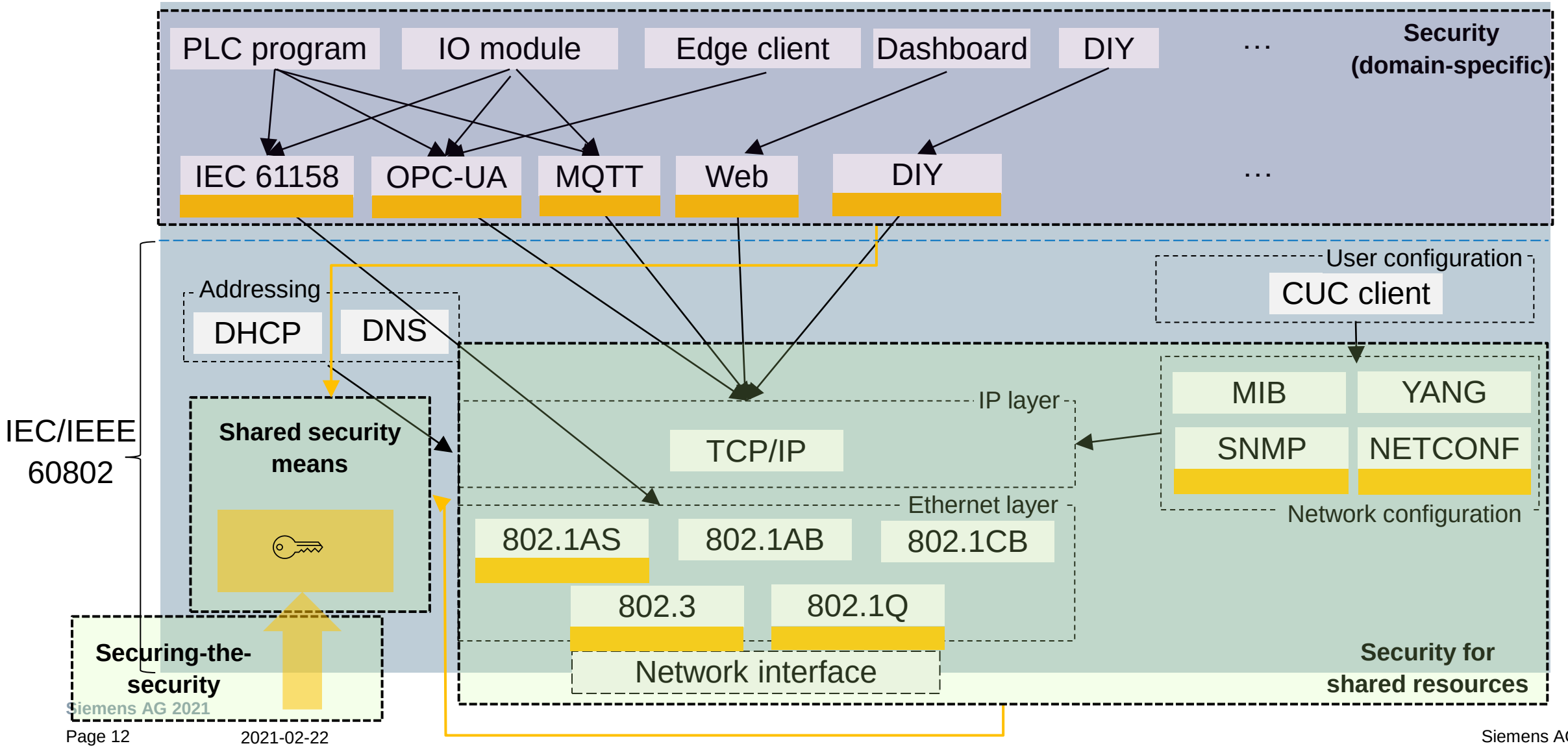
Proposed Scope of Security Contribution

SIEMENS
Ingenuity for life

- Security:
  i. **Security for shared resources:** *how to protect resources upon IA devices that are shared among multiple middleware/application domains?* Especially:
    - Stream establishment
    - Network management
  ii. **Shared security means**: *how to facilitate the joint use of singleton means for security upon the IA device?* Especially:
    - Secure elements providing secure storage and execution environment for keys/credentials
  iii. **Securing-the-security**: *how to protect the management of IA device resources underpinning the security)?* Especially:
    - Component-global security configuration
    - Entity/key bindings esp. proving the correctness of identifier(s)/entity association
    - Equipment originality checking
- Identification: *how to deal with existing forms of identification to deliver a sound security experience?*

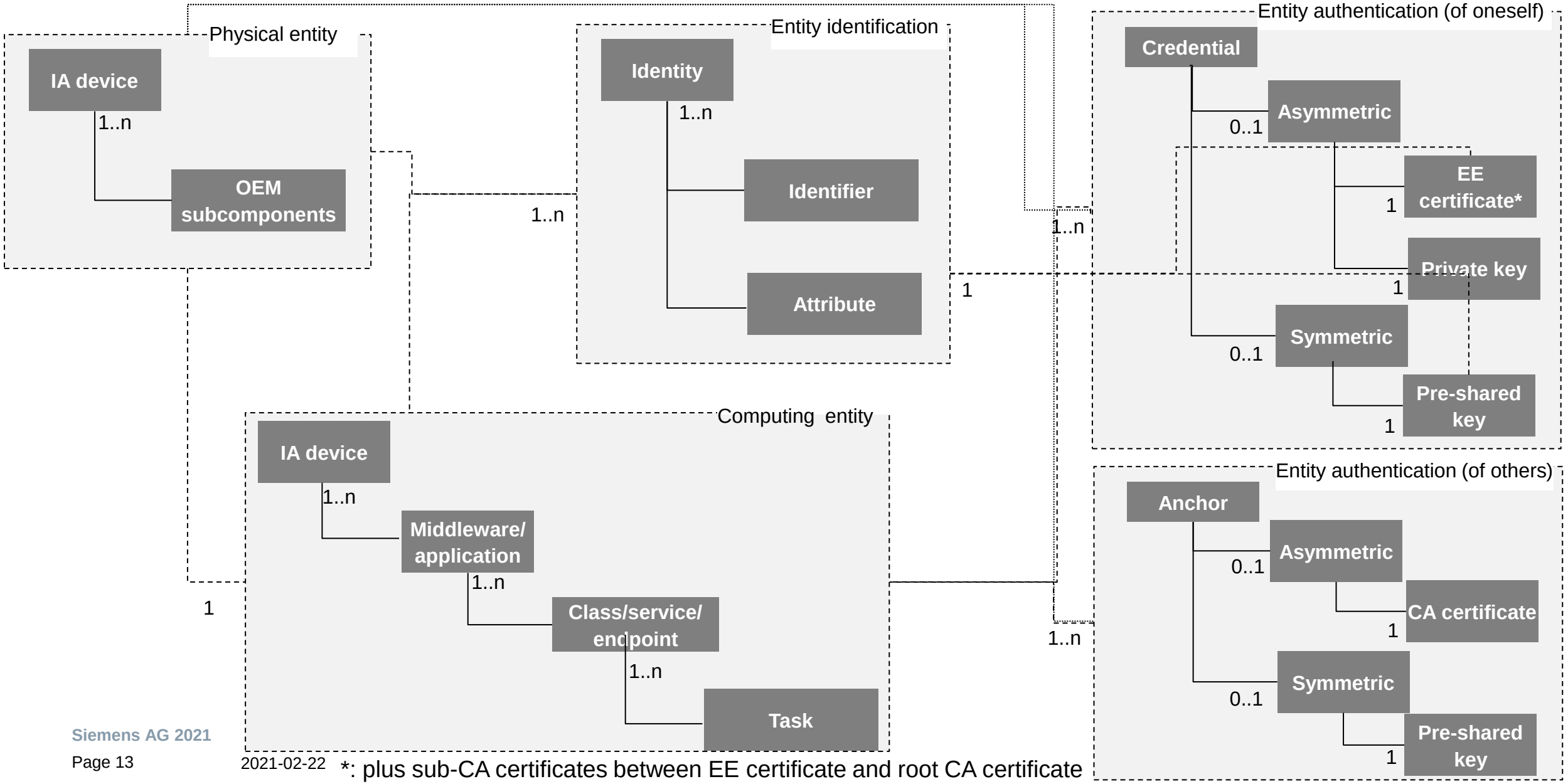
IA Device with Security

SIEMENS
Ingenuity for life



Entity/Identification/Authentication for IA Devices

SIEMENS



*: plus sub-CA certificates between EE certificate and root CA certificate

Abbreviations

SIEMENS
Ingenuity for life

CUC	Centralized User Configuration
DHCP	Dynamic Host Configuration Protocol
DIY	Do It Yourself
DNS	Domain Name Service
DNSSEC	DNS SECurity Extensions
HW	HardWare
IA	Industrial Automation
ID	IDentifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IO	Input Output
IP	Internet Protocol
IPsec	IP security
MAC	Media Access Control (networking)
MACsec	MAC security
MIB	Management Information Base
MQTT	Message Queuing Telemetry Transport
NETCONF	NETwork CONFiguration
OASIS	Organization for the Advancement of Structured Information Standards
OAuth	Open Authorization
OEM	Original Equipment Manufacturer
OPC	Open Platform Communications
OT	Operational Technology
PHY	PHYsical
PKCS	Public Key Cryptography Standards
PLC	Programmable Logic Controller
PROFINET	PROcess FIeld NETwork
RADIUS	Remote Authentication Dial In User Service
SNMP	Simple Network Management Protocol
SW	SoftWare
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TSN	Time-Sensitive Networking
UA	Unified Architecture
UASC	UA Secure Communication
UDP	User Datagram Protocol
UMA	User-Managed Access
URI	Uniform Resource Identifier
YANG	Yet Another Next Generation

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