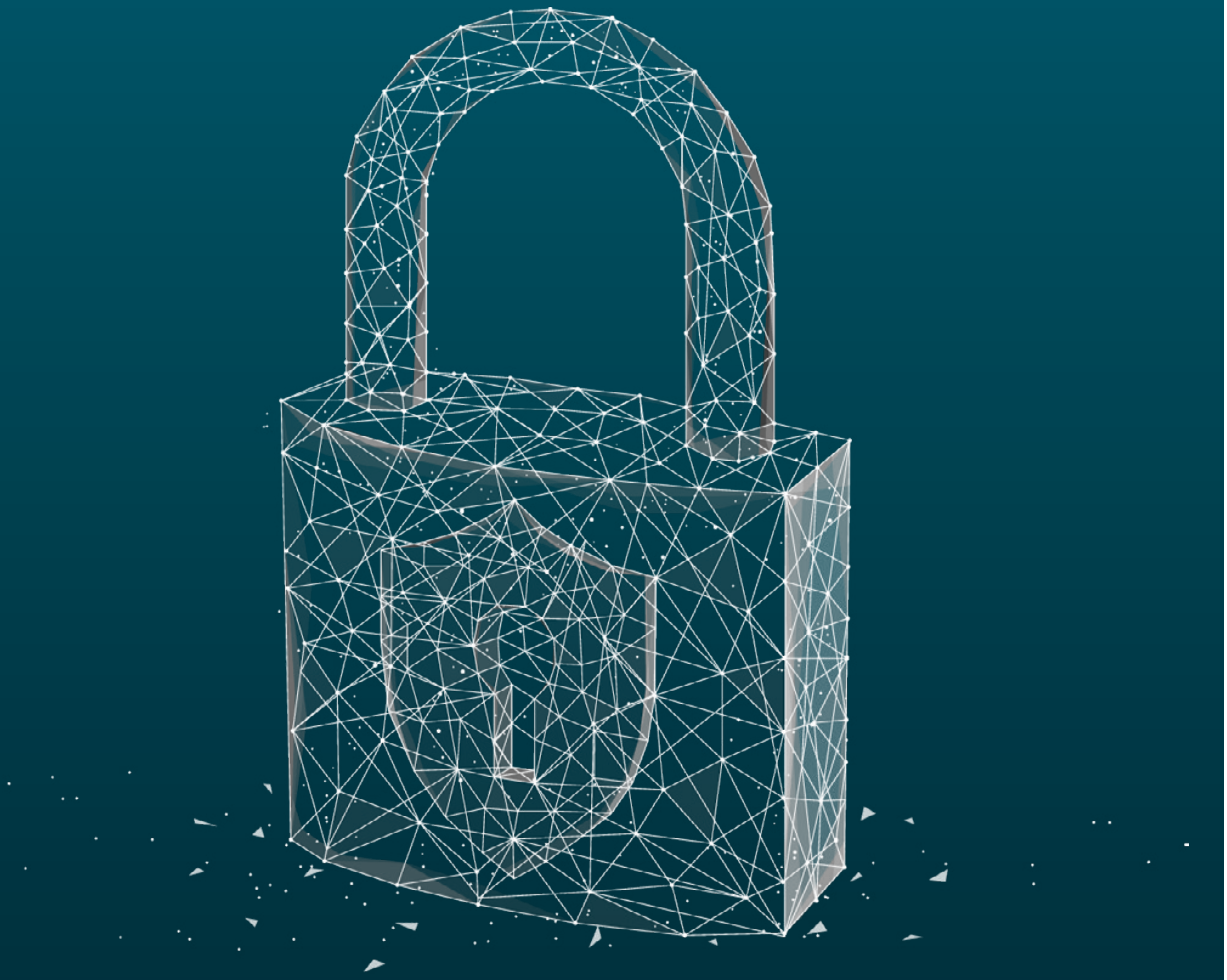


5G-ACIA White Paper

Security Aspects of 5G for Industrial Networks

5G Alliance for Connected Industries and Automation

Table of Contents

1 Abstract

5G is an enabler of both telecommunications and industrial use cases. The security requirements of telecommunications networks are well defined and have been widely published. This white paper concentrates on the security needs of industrial networks. Drawing on the use cases and network deployment models already developed within 5G-ACIA and other organizations, the paper focuses on the requirements of operational technology (OT) companies, on the degree to which these are already fulfilled by existing 5G features, and describes gaps between the two.

2 Introduction

Security requirements of public mobile telecommunication networks (public land mobile networks, PLMNs) have been extensively worked on, and the associated security features and functions have been specified by 3GPP as part of its standardization process for 5G and its predecessors. Telecommunications operator network architectures, designs and operating models are highly similar, and the threat and trust models and associated risk assessments also have similarities. This leads to a relatively uniform security response and toolbox, as defined in 3GPP standards [2, 3]. While optional features and extensions have been included in these standards, and there may be operational differences, the security architecture, functions and features used throughout PLMNs worldwide are relatively uniform. This enables seamless interoperability around the globe.

Industrial operators build their private communications infrastructures around their specific processes and operations. While the underlying technology components are similar and standardized, network architectures and their operating models can differ significantly. Moreover, the threats faced by each industry can be highly specific, too, with a variety of corresponding security objectives and requirements.

This diversity needs to be addressed without divergence in the underlying technologies and standards. While the individual threats and risks in each operational technology (OT) industry instance will be determined based on its own risk analysis, it is still possible to use a framework to manage the general security expectations and practices of current OT deployments.

Based on common best practices, the IEC 62443 series of standards provides a framework of functional and procedural requirements to address the issue of security for industrial automation and control systems (IACS). These requirements provide the baseline for assessment and certification, and each organization determines its security measures to meet these requirements from a security technology toolbox. The existing OT communications technologies have an associated security toolbox that represents the current security response of OT organizations. 5G comes with its own security features and functions, adding these to the OT security toolbox.

This white paper presents industrial network security requirements and current practices, and examines 5G security features and how well they match industrial needs. The paper also describes use cases and deployment scenarios to help to identify 5G-specfic security requirements. 5G-ACIA determined four major 5G deployment scenarios [1] for OT operators. Each scenario has its own implied requirements in terms of latency, availability, privacy and security.

The following section summarizes these scenarios and their associated risks. This is followed by a description of the most common security requirements of OT companies, as well as an introduction to the IEC 62443 standard.

Subsequently, the paper presents the 5G security toolbox and maps it to the network deployment scenarios. The conclusion considers how well the current 5G security toolbox meets OT requirements.

3 3GPP

The 3rd Generation Partnership Project (3GPP) is a collaborative project that brings together standardization organizations from around the world to create globally accepted specifications for mobile networks.

As its name implies, it was first created to establish such specifications for the third generation (3G) of mobile communication systems. It has continued its work for subsequent generations, including the one considered here, the fifth generation (5G).

4 5G-ACIA

The 5G Alliance for Connected Industries and Automation (5G-ACIA) was established to serve as the central and global forum for addressing, discussing, and evaluating relevant technical, regulatory, and business aspects with respect to 5G for the industrial domain. It reflects the entire ecosystem and all relevant stakeholder groups, ranging from operational technology (OT) players (industrial automation companies, engineering companies, production system manufacturers, end users, etc.), the ICT industry (chip manufacturers, network infrastructure vendors, mobile network operators, etc.), higher education, research, and other groups.

5 5G non-public network deployment scenarios

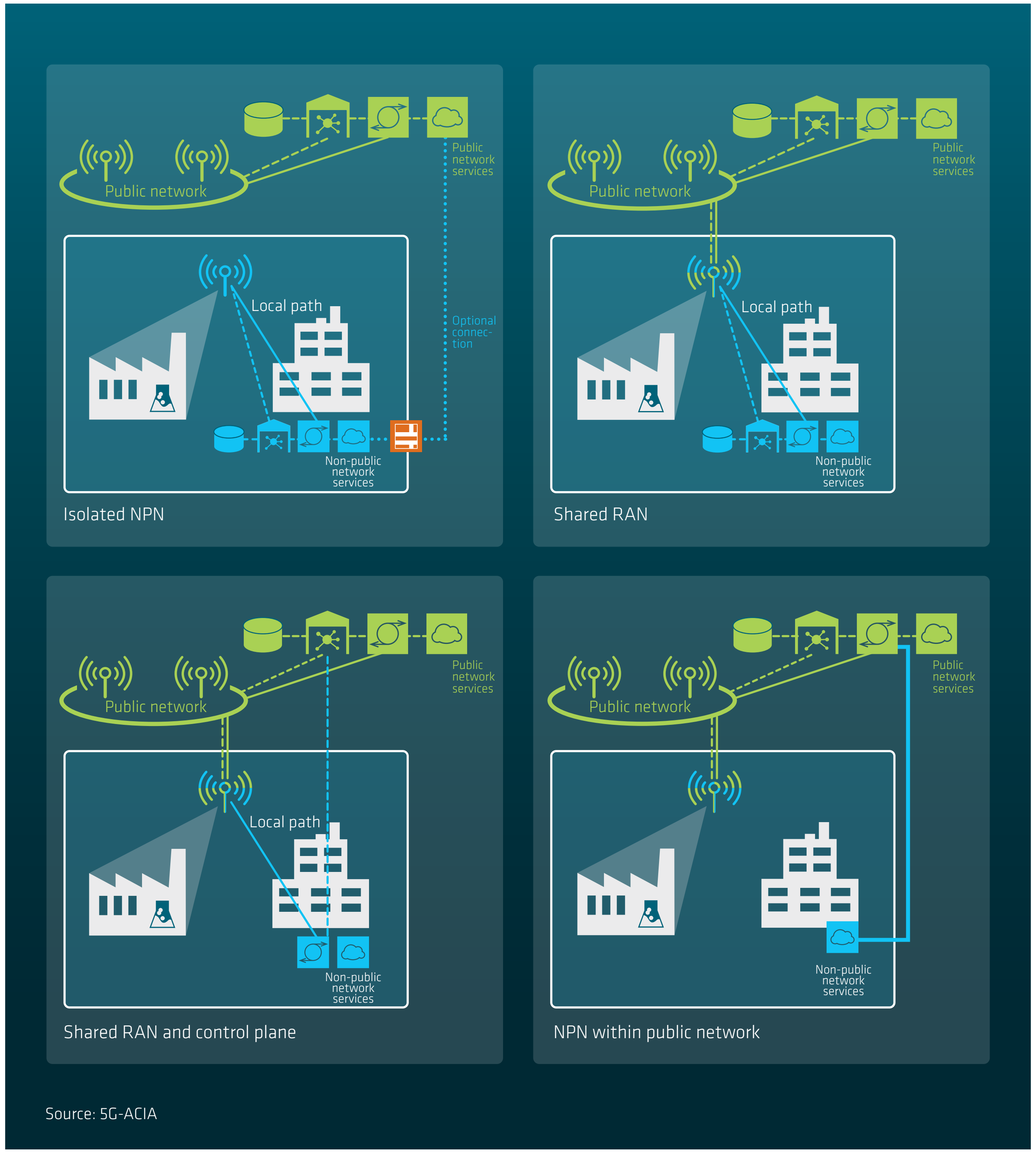
5G-ACIA identified four types of non-public network (NPN) deployment scenarios. They have differing levels of integration with the PLMN:

1. Standalone NPN: An isolated or standalone NPN (SNPN) does not share any resources with the PLMN but might have access to it via a firewall. In this scenario, the NPN is logically and physically separate from the public network and is typically operated by the OT operator on a shared spectrum such as citizens' broadband radio service (CBRS) or on an unlicensed spectrum. This scenario corresponds to the 3GPP SNPN specification.

2. Shared radio access NPN: In this scenario, the NPN only shares the radio access network (RAN) of the public network. All other control and user plane functions and network resources remain isolated. NPN data remains within the logical NPN perimeter. While it is possible to have either shared or dedicated base stations for the NPN, the RAN is operated by the public network operator. This scenario corresponds to the 3GPP SNPN specification. From a technical perspective, there is no difference for the PLMN between this scenario and the SNPN described above. From an OT operator point of view, since the PLMN base station is involved in authentication data exchange and has visibility into the user plane protection keys, the NPN operator needs to take this into account during their risk assessment.

3. Shared radio and control plane: Both the radio network and the control plane functions are shared between the NPN and the PLMN. The user plane is entirely within the NPN, supporting NPN data flow within the logical NPN perimeter. NPN devices are subscribers to the public

Fig. 1: 5G-ACIA NPN scenarios



Source: 5G-ACIA

network. This scenario would significantly benefit from 5G network slicing features for its implementation. 5G closed access group (CAG) functionality can be used for access control in this scenario [5].

4. Shared radio, control and user planes: In this scenario, the NPN is hosted by the public network and all NPN traffic is routed via the public network. NPN devices are subscribers to the public network. This scenario would significantly benefit from 5G network slicing features for its implementation, enabling separation between traffic and control plane functions of the NPN and PLMN. 5G closed access group (CAG) functionality can be used for access control in this scenario [5].

According to 3GPP, the first two scenarios are classified as SNPNs and the latter two are classified as public network-integrated NPNs (PNI-NPNs). Fig. 1 depicts the possible NPN deployment scenarios.

OT security requirements will differ according to the specific NPN deployment scenario and will be related to the security requirements of OT networks currently deployed. The most common security requirements and characteristics of OT networks are discussed in the following sections.

6 Security and privacy characteristics of OT networks

In order to assess the applicability of 5G security features in the future, it is necessary to first understand the most common security requirements and characteristics of OT networks today. There are a number of security and privacy characteristics of OT networks that distinguish them from PLMNs and traditional IT networks:

1. OT networks have traditionally been physically isolated. Perimeter protection and access control have been widely used to protect the confidentiality of processes, operational data, users and equipment. While access from outside is strictly controlled, operational data flows to the outside have also been restricted. With 5G, this physical isolation is no longer maintained and logical isolation mechanisms and physical radio layer protections (jamming protection) are needed.

2. Within the perimeter, the users, equipment and processes form a single trust domain. Third parties are not typically allowed within the perimeter, except for certain remote maintenance tasks that do not impact real-time operations. Further operational boundaries within factories may be used to ensure segregation of operational duties and to protect privacy (need-to-know principle) in accordance with regulatory requirements. A 5G telecommunications operator would not be part of this trust domain and additional end-to-end encryption and integrity protection mechanisms might therefore be needed. Access on the part of the 5G telecommunications provider to the OT's operational data must be prevented by data isolation between the data owner (OT operator) and the telecommunications service provider in the instance of PNI-NPN scenarios. Additionally, OT device access to NPNs and PLMNs needs to be controlled.

3. Due to the existence of physical perimeter security, state-of-the-art authentication mechanisms (such as those mandated by 3GPP) and secure hardware components for subscriber credentials' storage and processing have not generally been used in OT scenarios. PLMNs on the other hand require strict authentication mechanisms and secure credential storage and processing components, such as the UICC. OT devices that require PLMN access would need to comply with the PLMN's authentication and credential storage and processing requirements, be it via 3GPP or non-3GPP access.

4. Regulatory compliance and associated certifications are major business imperatives. Each network configuration change or update needs to ensure continuity of compliance. Otherwise, associated certifications could be lost. Some of these regulatory requirements relate to restrictions on data flows to the outside, and to other confidentiality and integrity protection mechanisms. 5G security features and functions would need to support compliance with these requirements, especially those defined in the IEC 62443 standard. By the same token, regulatory requirements within the PLMN, such as strong user authentication, access to emergency calls, and lawful interception, where applicable, would need to be met in the case of PLMN-integrated NPNs.

There are also operational requirements that need to be observed. OT 5G use cases are brownfield scenarios, where equipment and processes have long lifecycles. This means that any 5G security mechanisms being introduced need to interact with legacy systems and processes over a long transition period. There therefore may be a need to support interoperability between 5G security features and legacy OT security functions for operational flexibility. Usability and serviceability are of prime importance in OT operations, and various OT operational roles on the factory floor need to be considered when planning the introduction of 5G security mechanisms.

It can be observed that OT security objectives often differ from those in IT security generally, and so do the applicable security mechanisms and network design principles. In IT, the security triad (confidentiality, integrity, availability) describes the core requirements in their order of relevance. In OT scenarios, based on the specific deployment and risk assessment, availability and integrity of e.g. infrastructure might be prioritized, together with requirements related to safety, reliability and performance (latency) in order to maintain continuity of industrial operations. These differences must be considered when implementing 5G networks.

With the introduction of 5G into OT networks, the OT security toolbox needs to be expanded to include corresponding 5G security mechanisms that address the requirements outlined above. It is worth noting that the OT security toolbox contains numerous features that address security requirements at layers above the network layer. "Defense in depth" is also a common approach in OT networks. These features are discussed in greater detail in the following section.

7 Additional 5G-relevant security concepts in industrial networks

Not all security issues can or should be resolved at the level of 5G. This section therefore looks at other relevant security concepts in industrial networks.

A robust security architecture requires a combination of security controls and mechanisms in order to effectively protect industrial automation and control systems (IACS). In terms of technical security controls, the security means provided by 5G encompass the wireless part, frontand backhaul transmission as well as the corresponding configuration and management features.

Today's automation and control systems are based on standardized protocols. These are often embedded in an architecture that includes cryptographic protocols such as transport (TLS, DTLS) and application layer security, user authentication and authorization, including roles, key and certificate management, access control mechanisms, and auditing and logging. Prominent examples of such architectures are Ethernet/IP, Modbus-TCP and OPC UA.

Within the OPC UA framework, cryptographic protocols, certificate management and other security functions are specified within the standard series (IEC 62541) in the context of a security model in order to protect the target system. Security objectives defined by the standard include availability, integrity, auditability, confidentiality, non-repudiation as well as authentication and authorization. It is an agreed goal to provide such security services agnostic to the underlying communication system (wired, wireless) to enable end-to-end security for the entire installation.

A typical deployment use case scenario could comprise two devices (e. g. controllers) connected to each other via a path consisting of wired (e. g. Ethernet) and wireless (e. g. 5G) links. Independent from the physical layer, security objectives must be met, including manageability of the automation solution.

Several aspects of system design other than security also play an important role. In addition to availability and integrity, these include network bandwidth, reliability and latency – all of which are key concerns in industrial automation.

This must be considered when designing a security architecture, including the protocol stack(s) used within the scope of the automation solution. Security must not hinder the operation of the industrial automation and control system with regard to these important aspects of system design.

Furthermore, with new developments in the Industrial Internet of Things (IIoT) area, new applications and workflows are being deployed and integrated into existing automation solutions. This raises the bar for technical security controls and requires visibility, application flow control, and anomaly detection to address new threats. Any support the network infrastructure, wired or wireless, can provide, enables an additional layer of protection.

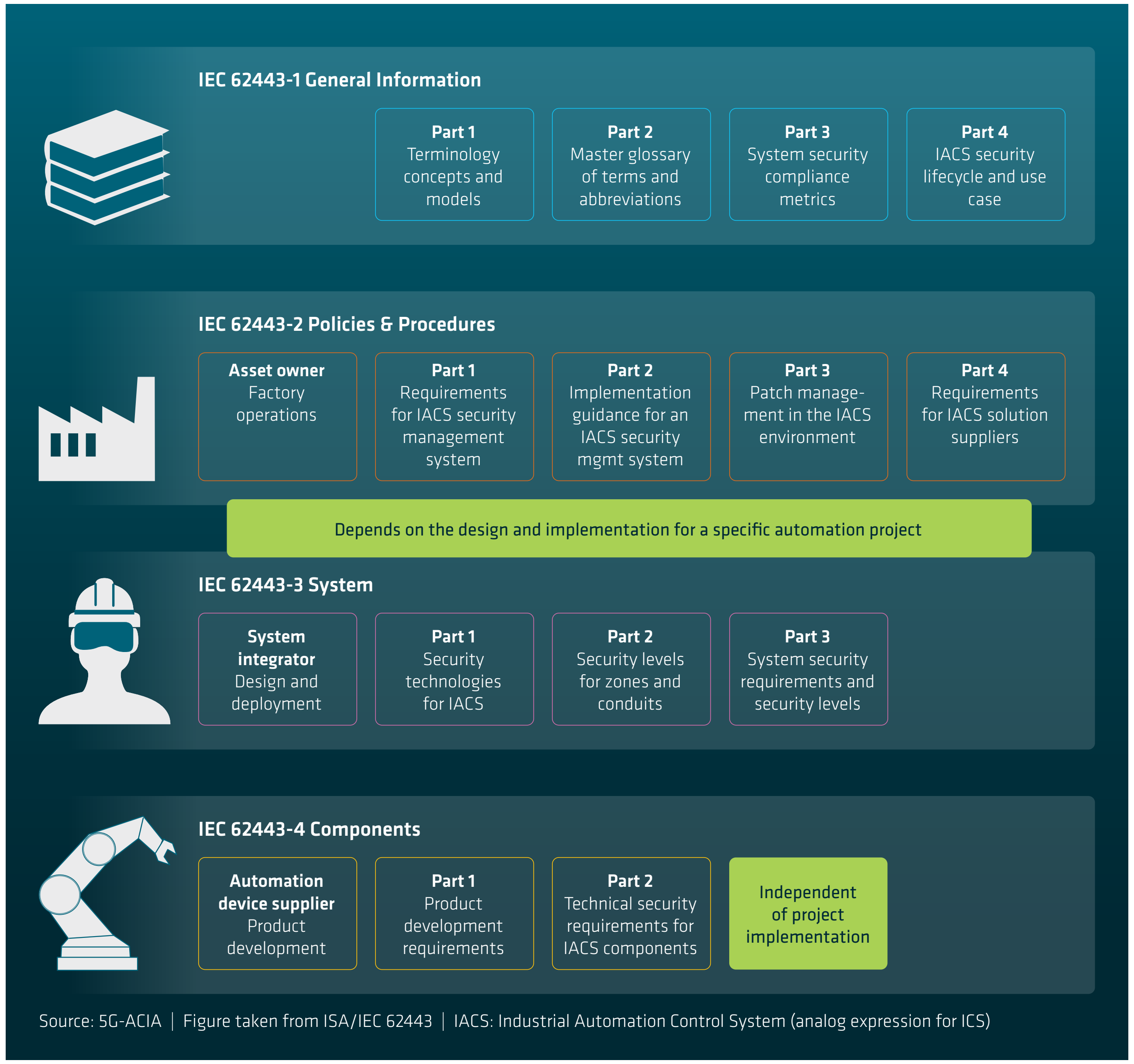
In this context, the IEC 62443 standard provides high-level guidance and methodology. It can be said that the technical security controls defined in various existing standards provide the technology-specific foundation (the toolbox) to meet the requirements defined in the IEC 62443 standard series. The following section looks at the IEC 62443 standard in greater detail to provide the context in which OT companies manage network security.

8 The IEC 62443 standard

The IEC 62443 standard addresses industrial automation control systems and is widely accepted as the most important standard for security management in this field. It is important to note that IEC 62443 takes into account established OT industry roles, namely, the OT manufacturers, integrators and operators, as given in the figure below. Each of these three may have their own specific security priorities and requirements. It is also important to understand who owns a certain risk and needs to mitigate it.

IEC 62443 includes a series of documents that are clustered in four parts: General Information, Policies and Procedures,

Fig. 2: IEC 62443 landscape



IEC 62443-1 General Information

Part 1 Terminology concepts and models

Part 2 Master glossary of terms and abbreviations

Part 3 System security compliance metrics

Part 4 IACS security lifecycle and use case

IEC 62443-2 Policies & Procedures

Asset owner Factory operations

Part 1 Requirements for IACS security management system

Part 2 Implementation guidance for an IACS security mgmt system

Part 3 Patch management in the IACS environment

Part 4 Requirements for IACS solution suppliers

Depends on the design and implementation for a specific automation project

IEC 62443-3 System

System integrator Design and deployment

Part 1 Security technologies for IACS

Part 2 Security levels for zones and conduits

Part 3 System security requirements and security levels

IEC 62443-4 Components

Automation device supplier Product development

Part 1 Product development requirements

Part 2 Technical security requirements for IACS components

Independent of project implementation

Source: 5G-ACIA | Figure taken from ISA/IEC 62443 | IACS: Industrial Automation Control System (analog expression for ICS)

Table 1: IEC 62443 security levels

Security Level	Means	Resources	Skills	Motivation
SL1	Casual or coincidental violation			
SL2	Simple	Low	Generic	Low
SL3	Sophisticated	Moderate	IACS-specific	Moderate
SL4	Sophisticated	Extended	IACS-specific	High

Source: 5G-ACIA

System, and Components. 62443-3-3 Security Requirements for Systems and 62443-4-2 Security Requirements for Components reflect the functional requirements from a design perspective. For maintenance aspects, 62443-2-4 list the requirements.

The standard defines seven foundational requirements (FRs) that need to be fulfilled to design a secure component/system:

- FR1: Identification and authentication control
- FR2: Use control
- FR3: System integrity
- FR4: Data confidentiality
- FR5: Restricted data flow
- FR6: Timely response to event
- FR7: Resource availability

For each foundational requirement, a list of system requirements (SR) and requirement enhancements (RE) are defined. The 5G security toolbox will be especially relevant for network- and data-related requirements such as, for example, visibility into communication flows at a given ingress or egress point of a network. Fulfillment of some requirements could potentially be left to higher layer functions

In addition to requirements, IEC 62443 defines four security levels (SL) that drive system security measures according to the attributes of potential attackers (table 1).

The following are instances of the various kinds of attackers:

- SL1: Any (Internet) user
- SL2: Hacker/company with generic security knowledge
- SL3: Expert/company with dedicated security knowledge that is willing and able to execute sophisticated attacks
- SL4: Government organizations/states

While security level 1 describes a system that is protected against casual or coincidental violation, level 4 assumes that the system implements mechanisms to counter adversaries that have sophisticated means, extended resources and an IACS-specific skillset. The required security level is subject to individual risk and threat analysis. In general, it can be assumed that level 2 attacks will always have to be considered for any industrial automation system. Since adversaries with IACS-specific knowledge may implement dedicated attacks, it is also advisable to contemplate level-3 defense mechanisms based on the risk assessment.

Table 2: IEC 62443 requirements reflect the security levels. Example with CR 1.9

IEC 62443 Requirement	SL1	SL2	SL3	SL4
CR 1.9 – Strength of public key-based authentication		x	x	x
RE(1) Hardware security for public key-based authentication			x	x

Source: 5G-ACIA

The security levels are also reflected in the Security Requirements for Systems and Security Requirements for Components parts of IEC 62443 referenced above. Some requirements only need to be fulfilled at higher security levels, while others are valid for all levels. For example, table 2 shows that requirement CR 1.9 Strength of public key-based authentication needs to be fulfilled to achieve SL2, SL3 and SL4. Moreover, for systems and components to achieve SL3 and SL4, there is a need for hardware security to protect keys and credentials.

As an example of how the 5G security toolbox would help fulfill these requirements, it is important to note that 3GPP-compliant 5G end-user devices store their security credentials on secure hardware, such as the (e)UICC for 3GPP-compliant PLMNs or secure hardware components in non-UICC based devices, which ensure compliance with high IEC 62443 security levels. This will be especially important for devices used in critical infrastructures. To ensure security for any of the 5G NPN scenarios would require consideration of which IEC 62443 security levels are pertinent. However, it might well be the case that differing parts of a network would have differing security levels. The following sub-section looks at such an architecture and how the IEC 62443 framework would apply.

8.1 Concepts of zones and conduits in the IEC 62443 standard series

It is not practical to apply a single security level to a large or complex IACS. The IEC 62443 standard series therefore describes the concept of a security zone, i. e. a logical grouping of physical, informational, and application assets that share common security requirements. A security zone has a clearly defined border that creates a division between included and excluded assets. Assets in differing security zones are usually isolated from each other.

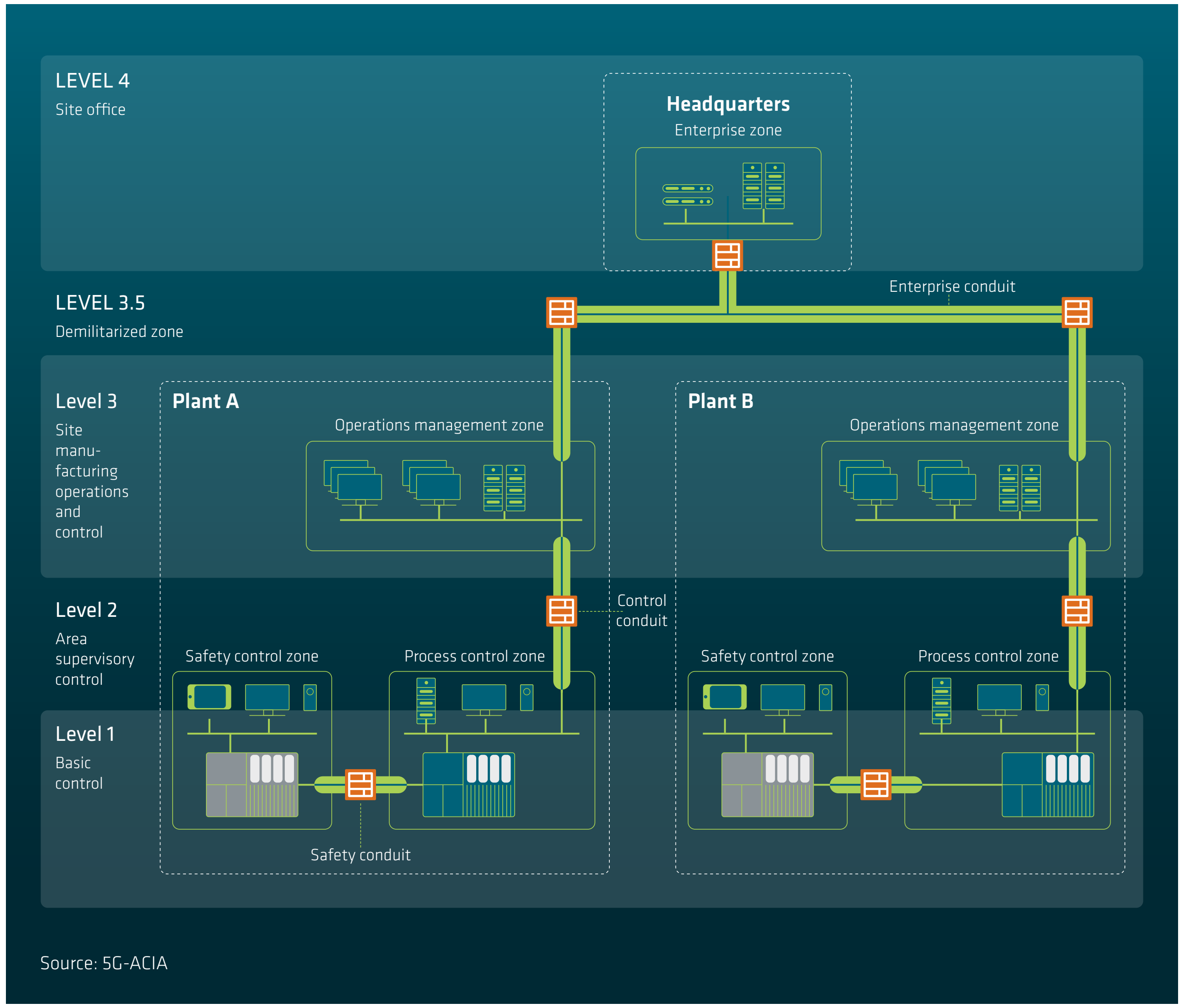
Figure 3 illustrates an example IACS based on the Purdue model and the IEC 62443 security design where two production plants are overseen by a headquarters. For this example, three security zones for process control, safety control and operations management have been created within the plants. Each zone has its own functionality and characteristics, and typically a dedicated owner, and therefore differing security requirements. In the example, some assets in level 1 and level 2 of the Purdue model could be included in one security zone, because it is assumed that these assets have the same security requirements and are owned by the same responsible organization.

For assets within a security zone to provide value, information usually needs to flow not only within the security zone, but also into or out of the security zone. The owner of the security zone needs to control the information flows entering and exiting the zone. To this end, the IEC 62443 standard series describes the concept of a conduit to cover the security aspects of the information flows. A conduit is a grouping of information flows crossing a border between security zones. The conduit can be physical or virtual, implemented via a network service, direct physical access (for a physically isolated system), or a combination of these. The conduit usually employs a firewall to validate any communications made via the conduit.

In the following figure, two conduits are defined for each plant, and there is an enterprise conduit connecting the headquarters and the plants, most probably via a public or private WAN service. The security design of this example prevents direct information flow over multiple levels of the Purdue model (for example, directly between level 1 and level 4 without passing through the intermediate levels).

Implementation of this architecture with 5G will depend on the existing network architecture and isolation requirements. Network slicing and closed access groups (CAGs) [5] could play a part in this architecture. Logical segmentation using virtual local area networks (VLANs) is another technique that could be used in conjunction with or in place of network slicing to implement security zones and conduits over the 5G network.

Fig. 3: Example of zones and conduits



Source: 5G-ACIA

Each zone can be treated as a separate network slice, i.e. headquarters, plant A and plant B would be separate slices with slice-specific authentication (on top of primary authentication). This provides logical separation between the member groups. The conduits can be implemented by means of WAN connections. Based on the security level of each zone, core network functions might have to be implemented separately for each slice.

It is worth noting that, since OT deployments are often brown-field projects, and many existing processes do not require modification, it may not be desirable to replace all of them with 5G. Slicing for each zone makes sense if the network offers differing types of services to each zone. On the other hand, if intra-zone and inter-zone communication is protected end-to-end at the application layer and the 5G network is only used for transport, then slicing may not be needed.

Now that the major security requirements and characteristics of OT deployments as well as their overarching standard security management framework have been described, this paper next looks at 5G security features that would be most relevant for the OT security implementation toolbox.

9 3GPP-defined 5G security features

This section provides an overview of the 5G security features defined by 3GPP that are most relevant for NPNs. A general overview of 5G security features can be found in the 5G Americas white paper, The Evolution of Security in 5G [4], and detailed requirements in 3GPP TS 33.501 [3].

9.1 5G authentication methods for NPNs

Authentication is fundamental to 5G in order to build trust between the user equipment (UE) and the network. 5G authentication mechanisms continue to fulfill the requirements from earlier generations/releases. With the introduction of NPNs and IoT use cases from Release 16 onwards, the 5G standard allows the use of authentication mechanisms that are different from 5G-AKA and EAP-AKA' for SNPNs.

3GPP TS 22.261 [2] states that the 5G system shall support operator-controlled alternative authentication methods with credentials that differ from 3GPP specifications for network access for IoT devices in isolated deployment scenarios, such as for industrial automation. Section 8.3 states that the EAP framework shall be supported to allow such alternative authentication methods with non-3GPP identities and credentials in SNPNs, provided that key-generating authentication methods are used [2]. In SNPNs, it is optionally possible to use 5G-AKA, EAP-AKA' or any other key-generating EAP method, for example, EAP-TLS. In 3GPP, TS 33.501, Rel-16, the normative Annex I on NPNs summarizes these updates.

3GPP currently mandates that in a 5G system a USIM in the UE must hold the shared secret (3GPP credentials) between the UE and the operator when using 5G-AKA or EAP-AKA'. Accordingly, when these two authentication methods are not used, such as in the case of other EAP authentication methods, for example EAP-TLS for SNPNs, the 3GPP standard does not specify how the credentials are stored and processed within the UE, leaving the choice to the SNPN operator.

For PNI-NPNs, since they will be connecting to PLMNs, the use of 5G-AKA and EAP-AKA' authentication methods are mandatory, together with the presence of USIMs in the UE for PLMN authentication. When the NPN is deployed as a slice, slice-specific authentication using EAP-based authentication can be optionally performed after primary authentication between the UE and the network. UEs can also authenticate to the 5G network via a non-3GPP access network in accordance with the procedure defined in section 7.2.1 of TS 33.501 [3].

9.2 Network slicing security

Next, this paper presents the most significant security features of network slicing in NPN scenarios, which will provide flexibility in OT networks.

Network slicing is a fundamental 5G innovation enabling the coexistence of significantly differing application/user group sub-networks on a single network infrastructure. This feature will have key implications for the OT industry, where multiple network slices may be deployed for various use cases. Securing and isolating the slices will be a fundamental requirement. This feature will be an important component of PNI-NPNs and therefore its security mechanisms will be essential to meeting OT security requirements.

A network slice provides an isolated, end-to-end network, optimized for a specific business purpose. These network slices support a wide range of services and applications, including as an NPN. Specific security features necessary for services and applications can be built into the network slice architecture.

In 3GPP Rel-15, network slice authentication and authorization are defined as part of primary UE authentication. When the UE is authenticated by the network upon initial access, a set of NSSAI (network slice selection assistance information) items denoting what is permissible is sent back to the UE. The serving network also receives a copy of the NSSAI which the UE is entitled to access. The UE can request to access any one of the permissible network slices (by including the corresponding NSSAI in the service request), but any request to access a network slice that is not part of the NSSAI item set is denied.

Table 3: Network slicing scenarios

NPN deployment scenario	Subscription owner	Default network/ slice interworking	Authentication method	Comments
Standalone NPN (SNPN) + shared RAN NPN	NPN operator	No interworking with any other PLMN network.	Multiple methods possible	Totally isolated NPN for an OT, with no interworking with external networks, providing total isolation.
Public network-integrated (PNI-NPN) (i. e. shared RAN and control plane or fully integrated NPN).	PLMN operator	Default network is PLMN, but certain users have access to NPN enterprise network acting as a separate slice.	Primary authentication by the PLMN using AKA-based authentication methods. The credentials for primary authentication are stored and processed within the USIM. But slice-specific authentication (EAP method) can optionally be performed between the UE and the NPN, if 3GPP Rel-16 is applied.	The subscription is owned by the PLMN. Access to PLMN is controlled by the PLMN operator.

Source: 5G-ACIA

Rel-15 therefore supports network slices by means of the UE's subscription information, and authentication and authorization for slice access is incorporated into primary authentication. It is also possible for the NSSAI to be concealed, and therefore not exposed in the radio layer, if it is considered sensitive.

In 3GPP Rel-16, support is included, in addition to the primary authentication for network slice access, for a slice-specific authentication procedure using the EAP authentication framework (RFC 3748).

Any EAP authentication method based on this framework could be used. When the UE is authenticated for network access, the serving network and the UE receives a list of permitted network slices, indicated by their NSSAIs. The permitted network slices may further require slice-specific authentication by the slice Authentication, Authorization and Accounting (AAA) function. This additional slice-specific authentication is indicated by the UE subscription information. If it is the case, the Access and Mobility management Function (AMF) in the serving network triggers the EAP authentication procedure for slice-specific access. This additional slice-specific authentication gives much more control to the NPN (enterprise) slice tenant in managing access to the slice instead of solely relying on the PLMN operator for access control.

A standalone NPN (SNPN) or public network-integrated NPN (PNI-NPN) can be built using Rel-15 and Rel-16 security procedures. It is up to the NPN operator or tenant to choose the appropriate NPN-PLMN interworking and level of authentication and authorization. A PLMN could deploy a PNI-NPN in such a way that the PLMN is the default network and the OT is a separate, dedicated slice. In this case, the PLMN would perform default authentication and authorization of the UE. Using Rel-15 and Rel-16 methods, the OT can create an additional security layer on top of PLMN authentication for more control and isolation.

Given the two choices, i. e. deployment as either an SNPN or a PNI-NPN, there are several possible slice configurations. The following table provides an overview:

9.3 Secure storage and processing of credentials

Another cornerstone of 5G security features is the secure storage and processing of credentials used in 5G security procedures, thereby ensuring their trustworthiness. This section outlines the options available for various NPN deployment scenarios.

3GPP has defined specifications for the secure storage and processing of subscription credentials within a tamper-resistant secure hardware component to ensure the security of the 5G system [3]. The secure hardware component is normally strongly linked to the platform hardware design, and a number of standardized solutions are available.

A secure hardware component can be used as the anchor for the network authentication application (NAA) employed for mutual authentication between the UE and the 5G System (5GS). TS 33.501 5G Security architecture and procedures for 5G System includes methods for authentication in NPNs, namely 5G-AKA, EAP-AKA', as well as any other key-generating EAP authentication method for SNPNs, for example EAP-TLS. The prerequisite for all methods is that the authentication key is protected.

For 5G AKA and EAP-AKA', 3GPP mandates usage of a USIM on a UICC to protect storage and processing of credentials. For SNPNs, other EAP methods than AKA are allowed. The choice of solution for the secure storage and protection of associated credentials is left to the SNPN operator(s).

The conventional solution for hosting the NAA is within a UICC. The UICC is a tamper-resistant hardware platform. Over time, the UICC has evolved from a credit card-sized smartcard to smaller form factors. With the current state of the art, one option is to solder the UICC to the printed circuit board (PCB). This is also known as an embedded UICC. Several standardization organizations are currently working on defining the evolution of secure hardware components. The following section will outline the activities of these organizations and how they relate to NPN deployment scenarios.

9.3.1 Standardization of secure hardware components

There are a number of components that are being standardized. The UICC is standardized by ETSI SCP, and 3GPP follows this standardization. The UICC platform hosts a file system and an authentication service used to authenticate towards the network. ETSI SCP also standardizes the alternative smart secure platform (SSP), which utilizes Global Platform (GP) VPP technology to support applications for various uses, such as network authentication and non-telecommunications applications e. g. banking, etc.

The Trusted Computing Group (TCG) standardizes two types of technology for the implementation of protected secure hardware components. The first of these two technologies, the trusted platform module (TPM), provides security services, such as attestation, key management and authentication from a tamper-resistant hardware component. The second, the device identity composition engine (DICE), addresses identity creation in resource-constrained devices, such as IoTs.

The Global Platform (GP) defines the GP trusted execution environment (TEE) and GP VPP technology. The difference between TCG and GP technologies is that TCG provides static services as defined by the standardization organization whereas Global Platform provides a framework within which applications can be hosted to provide the corresponding services. Key to evaluating secure hardware components is their certification on the basis of protection profiles. Standardization organizations develop schemes to help with this process.

9.3.2 Choice of secure hardware components for NPN

This section considers how to best choose a secure hardware component for an NPN. An NPN with a shared RAN and control plane, and an NPN hosted by a public network, needs to adhere to the security requirements set by the PLMN in accordance with 3GPP specifications. For the SNPN, including the shared RAN-only scenario, the choice of solution for credential storage and protection is left to the SNPN operator(s) by 3GPP specifications.

A standalone NPN hosts its own authentication and subscription services. This implies that a variety of solutions for credential storage and processing could be used. One example is the TPM module, which may already be employed during secure boot of the device, but can also be used to host the EAP-TLS keys for authentication to the network.

Table 4: Secure hardware component scenarios

Network configuration	Possible secure hardware components
Standalone NPN (SNPN) and shared RAN NPN	Alternative solutions: GP TEE, TCG TPM, etc. Conventional PLMN SE: (e)UICC, Future PLMN solution(s): iSSP, eSSP
PNI-NPN with shared RAN and control plane and fully integrated PNI-NPN	Conventional PLMN solutions: (e)UICC, PLMN future solution(s): iSSP, eSSP (not currently in 3GPP specifications although ETSI SCP has already published the standard)

Source: 5G-ACIA

It is recommended that NPN operators consider adopting and contributing to one of the available credentials management solutions and the organization(s) that maintain them, rather than creating a brand-new solution that is maintained separately. All these options need to be evaluated in addition to the security model and specific security requirements of the NPN operator before selection of the solution. NPN configurations and possible solutions are summarized in table 4.

For standalone NPNs (including the shared RAN-only scenario), OT operators can choose from the wide range of secure hardware components already on the market, or deploy a PLMN-proven UICC-based solution. The protection provided by the chosen solution must be in line with the requirements of the OT security risk assessment. For PNI-NPNs, a UICC is currently mandatory when it comes to primary authentication.

It is acknowledged that use of secure hardware components might not be common in current OT networks, and their introduction might seem like a challenge. As described in the following sub-section, there are initiatives to encourage the integration of secure hardware components into OT networks where they potentially interact not only with 5G systems but also with other networking and security technologies, such as OPC UA.

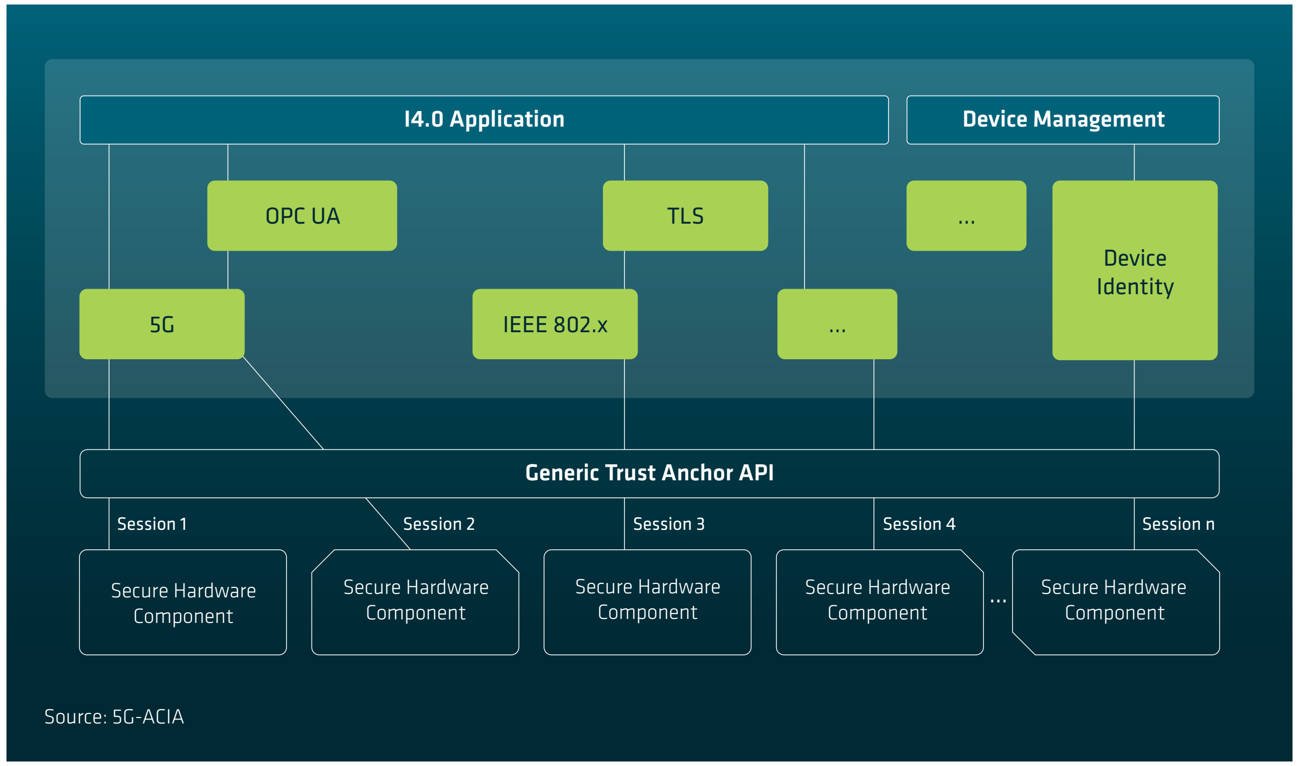
9.3.3 A conceptual framework for the usage of secure hardware components in OT networks

As described in the previous section, UICC has been used for secure credential storage and processing for a significant time in mobile communication networks. The use of secure hardware components by industrial communication protocols does not have such a long history but is clearly gaining momentum. With increasing connectivity and the introduction of new communication protocols, such as OPC UA, message security and device authentication have become more and more important. The level of protection afforded to keys and credentials is directly linked to the 5G system's level of security. The use of a secure hardware component is therefore advisable for industrial communication protocols as well.

In order to increase security by lowering the integration overhead, the German Federal Office for Information Security (BSI) has created a reference API for the usage of secure hardware components in OPC UA [6]. The goal was the definition of a standardized, vendorindependent API that allows the usage of various types of secure hardware components. As a result, higher layer applications can be developed independently of the cryptographic software libraries or hardware trust anchors underneath.

The importance of this BSI approach is widely accepted in the OT industry and standardization efforts are currently ongoing. A new ISO/IEC JTC1 SC41 work item for a Generic Trust Anchor Application Programming Interface for Industrial IoT Devices, supported by many OT companies, is scheduled to commence in the first half of 2020.

Fig. 4: Generic trust anchor API concept



Source: 5G-ACIA

Figure 4 shows the basic concept of the generic trust anchor API. The aim of standardization activities is to ensure that not only OPC UA and TLS but also other protocols and communication standards are supported by the API. One (or several) Industry 4.0 applications on a device could initiate a number of sessions with one (or multiple) secure hardware components. This way all cryptographic functions would be performed on the applicable secure hardware component. In Figure 4, session 1 would make use of one secure hardware component to offer cryptographic services for the 5G connection. Session 2 would use another secure hardware component for the OPC UA-related cryptographic functions. Session 3 could use a secure hardware component as cryptographic service provider for a TLS handshake.

In addition to supporting applications, the generic trust anchor API could be used for device identity and lifecycle management, as indicated in the figure by session n. Integration with 5G authentication methods for private networks should be considered to increase the usability of both the API and 5G-based solutions in OT networks.

This completes the overview of the 5G security features most relevant to NPN deployments. The following section provides an assessment of a physical layer security concept that is highly relevant for OT networks.

9.4 Protection against radio jamming in 5G

Industrial operations have little tolerance for disruption of production lines or operations due to the unavailability or unreliability of their communication channels. The possibility of radio level jamming has been a concern during the early adoption of wireless/mobile, mostly Wi-Fi-based, technologies within OT communication architectures.

There are numerous industrial use cases for 5G, such as autonomous guided vehicles (AGVs) and massive industrial IoT (IIoT) deployments where the mobility features (handover between base stations and roaming) of 5G play a central role.

For these use cases, it is important to evaluate the radio jamming risk.

Any risk assessment needs to consider not only the technical possibility of jamming, but also the feasibility of any attack being successful, both regarding executing such an attack (e. g. configuring and deploying the jamming device) and the limitations related to the radio environment and characteristics (such as radio propagation, path loss and penetration loss reducing the viability of indoor attacks, and jamming in unlicensed bands versus licensed bands).

Existing jamming detection techniques and 5G radio features such as beamforming, multiband carrier aggregation, and link adaptation can be adopted in 5G systems to increase reliability and reduce the probability of successful attacks. Mitigation of jamming can be achieved through a combination of existing 5G interference management features, careful network deployment strategies, and continual spectrum monitoring.

Having reviewed the OT network security requirements and the 5G security features most relevant to NPNs, the next section provides an overview of how the major OT security concepts could be implemented in each 5G NPN deployment scenario. Subsequently, an outlook for further developments is presented.

10 OT NPN security requirements and 5G NPN scenarios: the outlook

Table 5 compares how OT security attributes are handled by the four 5G-ACIA-defined NPN deployment scenarios.

Note that in the PNI-NPN cases, and the shared RAN SNPN case, the PLMN base station has visibility into authentication exchanges between the UE and the core network, and into the keys for user plane protection. This therefore differs from the isolated SNPN case.

In all PNI-NPN cases, and where the SNPN is operated by the PLMN, higher layer encryption functions are an option for OT operators.

Lawful interception requirements for the PLMN would generally not be applicable for SNPN scenarios, as there is no connection to the public network. With PNI-NPNs, lawful interception would apply to the PLMN interfaces and identities, but not to the NPN interfaces. In general, local regulato-

Table 5: NPN scenarios and OT security requirements

	SNPN		PNI-NPNs	
Security attribute	**Isolated deployment**	**Shared radio access network**	**Shared radio and control plane**	**NPN hosted by public network**
Isolation via network perimeter protection	Highly isolated: The network is physically and logically isolated.	High to medium isolation: The RAN is logically isolated but not physically. Control and user plane functions physically isolated but connected via the shared RAN.	Medium to limited isolation: The RAN and control plane functions are logically isolated but not physically. User plane physically isolated but utilizes the shared RAN.	Limited isolation: Only logical separation in radio, control and user planes that are managed by the PLMN. Physical resources might be shared.
Alignment with trust domains in OT networks	No link to PLMN operator. Trust domains as implemented in the legacy perimeter protection case.	Functionally no link to PLMN operator. PLMN has visibility into authentication exchanges and user plane keys, so multiple trust domains to	Subscriber information is shared with PLMN. PLMN operator implements the control plane functions. Multiple trust domains to be considered.	Subscriber info, control and data plane shared. Multiple trust domains to be considered.
Authentication and secure storage and processing of credentials	Highly flexible implementation. According to 3GPP specifications, it is permissible to use additional SNPN authentication and credentials management options (that are outside the scope of 3GPP specifications).	Highly flexible implementation. According to 3GPP specifications, it is permissible to use additional SNPN authentication and credentials management options (that are outside the scope of 3GPP specifications).	Choice is determined by 3GPP, PLMN authentication and credentials management requirements.	Choice is determined by 3GPP, PLMN authentication and credentials management requirements.
Regulatory compliance	Low effort for OT network regulatory compliance. PLMN regulatory compliance does not generally apply since the endpoints are not on the PLMN.	Low effort for OT network regulatory compliance. PLMN regulatory compliance does not generally apply since the endpoints are not on the PLMN.	Medium effort to ensure regulatory compliance for both OT and PLMN.	High effort for OT and low effort for PLMN. For PLMN, identical to public network compliance.

ry requirements vary from country to country in accordance with national legislation, and these variances are reflected in the options provided in 3GPP standards.

Where IEC 62443 security levels 3 and 4 apply, secure hardware components would be necessary for non-trusted elements of the network. This might be achieved by means of the 3GPP 5G-defined security features for mutual authentication of the UE and the network, or additionally at higher layers with necessary security assurance functions. Most likely, multiple layers of security would be deployed, reflecting a "security in depth" approach.

It can be concluded from the above table that the isolated SNPN deployment scenario is generally closer to the current OT network deployment characteristics while the fully integrated PNI-NPN scenario is closest to a PLMN architecture. Available 5G security features can be adapted to each deployment scenario to meet the security requirements of OT operators.

The outlook:
To enhance the 5G security toolbox even further, to meet OT-specific security requirements, the following steps could be taken. While these might not necessarily translate into 3GPP 5G specifications, their availability would enhance secure implementation of 5G in OT scenarios.

1. Visibility into network operations needs to be ensured in OT deployment scenarios, especially with PNI-NPNs, to ensure compliance with security policies and certification requirements. Suitable security monitoring capabilities, such as event and incident monitoring, e. g. by means of dashboards, and flow control at ingress/egress points need to be studied further and described. For example, the question needs to be considered whether or not such requirements would be addressed within the scope of 5G or in higher layers.

2. Radio level jamming remains as a major concern for many OT manufacturers, integrators and operators. 5G provides improvements over previous mobile technology generations in terms of jamming resilience. Furthermore, it is important to evaluate the risks realistically for any given scenario (indoor/outdoor, etc.). Additional measures can be developed at the implementation stage, and may not necessarily require changes to specifications. This is an area that calls for additional investigation and the development of robust solutions to alleviate persistent concerns.

3. It would be helpful to establish security profiles and implementation guidelines corresponding to each 5G-ACIA-defined deployment scenario. These would essentially make 5G security expertise and the toolbox widely available and deployed. Operational considerations and implementation options will be just as much key factors in such an endeavor as technology specifications. This work would need to be a joint effort on the part of operational experts in the ICT and OT domains, and may not necessarily be the remit of the standardization organizations.

11 Conclusions

3GPP 5G security features generally provide robust support for OT network deployments. These security features together form a toolbox that allows OT companies to address the varying security risks of the multiple OT 5G deployment scenarios described in this paper. The degree of involvement of the PLMN operator in implementation of the OT network plays an important part in determining which security features would be applicable.

The OT domain is characterized by the interdependence of companies with various industry roles, such as manufacturers, integrators and operators. The 5G security toolbox may be used differently by each of these. Additionally, as much as technology requirements, the OT field is characterized by operational and implementation-related requirements specific to each field deployment. Therefore, it will not be sufficient to select security features based on technical considerations alone. Thought will have to be given to operational and implementation-related constraints

In the IEC 62443 standard context, when the 5G network would be part of a critical industrial system, the administrators and operators of the 5G network must be trusted by the industrial systems operator. When security levels 3 and 4 are needed, higher layer protections (e. g. a secure application layer protocol such as TLS or IPsec) may have to be provided.

In a conventional OT deployment, all entities within a network or zone are assumed to be part of a single trust domain. In an OT 5G PNI-NPN, where a PLMN operator provides part of the network infrastructure or services, the PLMN operator is a new entity that the OT operator must trust with regard to its certification requirements. This new relationship could be compared to outsourcing. As in any outsourcing model, visibility and monitoring capabilities become key to establishing trust and verifying compliance.

In this context, the PLMN operator aims to maintain its trust relationship with the UE as before and the OT operator seeks to continue its conventional model of integral trust zones, perhaps through higher-level security functions, such as application layer encryption. Each will strive to minimize disruption to its existing mode of operation. It has been demonstrated that 5G security features form a toolbox that both OT and PLMN operators can use to manage the risks in the OT networks of the future.

12 Definitions

5G-AKA: Device authentication method defined by 3GPP and introduced for 5G.

5GS: Fifth generation system of the mobile network.

Constrained device: Small device with limited CPU, memory, and power resources. (RFC 7228)

EAP-AKA’: Device authentication method.

Network slicing: Network slicing is a specific form of virtualization that allows multiple logical networks to run on top of a shared physical network infrastructure.

Non-3GPP access: Access to the core network via connectivity other than the base station, such as Wi-Fi.

Non-public networks: A non-public (private) telecommunications network providing mobile cellular services.

PNI-NPN: A non-public telecommunications network integrated into a public network by sharing core functions.

Purdue model: A reference model for industrial control system (ICS) network segmentation, based on the Purdue Enterprise Reference Architecture (PERA).

Security controls: Countermeasures designed to manage security risks.

Trust anchor: A trust anchor is an authoritative entity for which trust is assumed and not derived. (RFC 5914).

Trust domain: A trust domain is a network area defined by its trust boundaries wherein mutual trust is assumed.

13 Abbreviations

3GPP	3rd Generation Partnership Project
5G-AKA	5G authentication and key agreement
AKA	authentication and key agreement
API	application programming interface
CAG	closed access group, as defined by 3GPP TS 23.501, V16.3.0, section 5.30.3
CBRS	Citizens Broadband Radio Service
DICE	device identity composition engine
DTLS	datagram transport layer security
EAP	Extensible Authentication Protocol
EAP-AKA‘	IETF RFC 5448: Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA‘)
EAP-TLS	IETF RFC 5216: The EAP-TLS Authentication Protocol
eSSP	embedded Smart Secure Platform
ETSI	European Telecommunications Standards Institute
eUICC	embedded UICC
GP	Global Platform
IACS	industrial automation and control system
ICT	information and communication technologies
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISO	International Organization for Standardization
iSSP	integrated smart secure platform
IT	information technology
NAA	network authentication application
NIST	National Institute of Standards and Technology (USA)
NPN	non-public network
NSSAI	network slice selection assistance information
OECD	Organization for Economic Cooperation and Development
OPC	object linking and embedding for process control (OPC Foundation)
OPC UA	OPC Unified Architecture
OT	operational technology
PCB	printed circuit board
PLMN	public land mobile network
PNI-NPN	public network-integrated non-public network
RAN	radio access network
SCP	smart card platform
SIM	subscriber identity module
SNPN	standalone non-public network
SoC	system on chip
TCG	Trusted Computing Group
TEE	trusted execution environment
TLS	transport layer security
TPM	trusted platform module
UE	user equipment
UICC	a smart card conforming to the specifications of the ETSI Smart Card Platform (SCP) project ref. TR 102 216
VLAN	virtual local area network
VPP	virtual primary platform
WAN	wide area network

14 References

[1] 5G-ACIA white paper "5G Non-Public Networks for Industrial Scenarios", https://www.5g-acia.org/fileadmin/5G-ACIA/Publikationen/5G-ACIA_White_Paper_5G_for_Non-Public_Networks_for_Industrial_Scenarios/WP_5G_NPN_2019_01.pdf, July 2019.

[2] 3GPP TS 22.261: "Service requirements for the 5G system; Stage 1", October 2019.

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system (Release 16)", September 2019.

[4] 5G Americas white paper, "The Evolution of Security in 5G", October 2018.

[5] 3GPP TS 23.501: "System architecture for the 5G System (5GS); Stage 2," December 2019.

[6] "SE API Reference for OPC UA Project 314", German Federal Office for Information Security (BSI), Draft v0.7, December 17, 2018.

5G-ACIA White Paper
Security Aspects of 5G for Industrial Networks

Contact
5G Alliance for Connected Industries and
Automation (5G-ACIA), a Working Party of ZVEI
Lyoner Strasse 9
60528 Frankfurt am Main
Germany
Phone: +49 69 6302-209
Fax: +49 69 6302-319
Email: info@5g-acia.org
www.5g-acia.org

Published by
ZVEI – German Electrical and
Electronic Manufacturers' Association
5G Alliance for Connected Industries and
Automation (5G-ACIA), a Working Party of ZVEI
www.zvei.org

February 2021
Design: COBRAND Berlin

15 5G-ACIA Members

As of February 2021

ABB
altran Part of Capgemini
arm
ASKEY

ASOCS
ATHONET
Audi
aurelis

BAYFU
BECKHOFF
Baicells
BOSCH

Canon
celona
中国移动 China Mobile
cisco

DASSAULT SYSTEMES
DENSO
Deutsche Messe
DFKI

NTT docomo
Endress+Hauser
EMERSON
ERICSSON

ETRI
FESTO
Fraunhofer
GHMT

HARTING
HIRSCHMANN A BELDEN BRAND
HMS
HUAWEI

IDLab INTERNET & DATA LAB
ifak
ifm
III

infineon
inIT
intel
ITRI Industrial Technology Research Institute

KETI
KEYSIGHT TECHNOLOGIES
LS telcom
MAVENIR

MC TECHNOLOGIES
MITSUBISHI ELECTRIC
MOXA
MUGLER TELCO NETWORKS

NOKIA
NXP
orange
Panasonic

PEPPERL+FUCHS
PHOENIX CONTACT
Qualcomm
Radisys

RELIABLE REAL-TIME RADIO
ROHDE&SCHWARZ
SAL SILICON AUSTRIA LABS
salzburgresearch

Schneider Electric
SICK
SIEMENS
SINTEF

SoftBank
SONY
ST life.augmented
T··

TRUMPF
TZi
ublox
verizon

VIAVI VIAVI Solutions
vodafone
WAGO
Weidmüller

XITASO
YOKOGAWA
ZTE

5GACIA

www.5g-acia.org