Cybersecurity Integration with IEC 61850 Systems

6

Dennis Holstein, Mark Adamiak, and Herbert Falk

Abstract

In this chapter, a coherent methodology to seamlessly integrate cyber-physical security (CPS) systems with IEC 61850 protection, automation and control systems (PACS) is described. To do, one needs to understand how adversaries gain access and use of mission-critical protection and control devices and the digital communication networks that connect these devices. For all the right business and technical reasons, IEC 61850 systems have leveraged digitisation and ubiquitous connectivity technologies to enable today's operational systems. The same technologies have offered an open attack surface to adversaries with the skills to develop new tactics to interfere with, disrupt or disable PACS functions. The chapter concludes with the top six cyber-physical response actions to protect IEC 61850 protection, automation and control systems and a list of future study topics and objectives to improve this protection.

Keywords

IEC 61850 • Cyber-physical security • Advanced persistent threats • Risk assessment • Risk mitigation

D. Holstein (✉)
OPUS Consulting Group, Seal Beach, CA, USA
e-mail: holsteindk@ocg2u.com

M. Adamiak
Adamiak Consulting LLC, Paoli, USA
e-mail: adamiakconsulting@aol.com

H. Falk
OTB Consulting Services LLC, Troy, USA
e-mail: herb.falk@otb-consultingservices.com

P. Bishop and N.-K. C. Nair (eds.), *IEC 61850 Principles and Applications to Electric Power Systems*, CIGRE Green Books, https://doi.org/10.1007/978-3-031-24567-1_6

6.1 Cybersecurity Imperatives

To understand what is needed to protect IEC 61850 PACS assets and networks, one must have some understanding of the threats and how they are executed. To do this, the approach is to focus on well-resourced adversaries such as nation-states or criminal organisations. Thus, the security levels as described in IEC 62443-3-3 [1] only provide basic understanding for addressing the threats and vulnerabilities. The approach to rank order the cyber-physical security (CPS) solutions for PACS based on the perceived consequences of a successful attack provides a more holistic approach.

6.1.1 The Onset of Advanced Persistent Threats

Software and malware attacks on industrial control systems (ICS) have been evolving since 2009 [1]. For example, nation-state-sponsored terrorism is using advanced spy-craft technology [2] to find and exploit vulnerabilities inherent in open system communication networks, such as those deployed in IEC 61850 PACS architectures. For example, Fig. 6.1 describes Deloitte's analysis of the cyber threat profile for the US electric power sector [3]. The attacks on the Ukraine power grid in 2015 (BlackEnergy) and 2016 (CrashOverride) are excellent illustrations of Advanced Persistent Threats (APT) which target PACS to seriously disrupt the power services to a large service area.

An in-depth analysis of the Ukraine attacks shows how a well-financed adversary can patiently perform the reconnaissance to identify the vulnerability of the open system network to gain access to and control of the protection relays. This was not a simple one-off attack. The attack exercised was practised multiple times over 6 months to ensure that it would achieve the desired objective. Only when the adversary had confidence in its success was the attack executed.

What is learned from these APT attacks?

1. Endpoint detection and response systems are not effective because security information and event management technologies provide event notifications and alerts after the fact. This does little to trap and isolate the impending attack on PACS assets and networks during the reconnaissance phase.
2. Firewalls, anti-virus, intrusion detection systems and data loss prevention systems depend on existing signatures and rules. APTs use new and creative techniques developed during the reconnaissance phase. Therefore, their signatures and rules are unknown.
3. If Ukraine had a highly trained staff with high-powered analytical tools to recognise the reconnaissance activity, it could have taken timely action to forestall the attack. Reference is made to the discussion of maturity models and their metrics in Sect. 6.2.1.

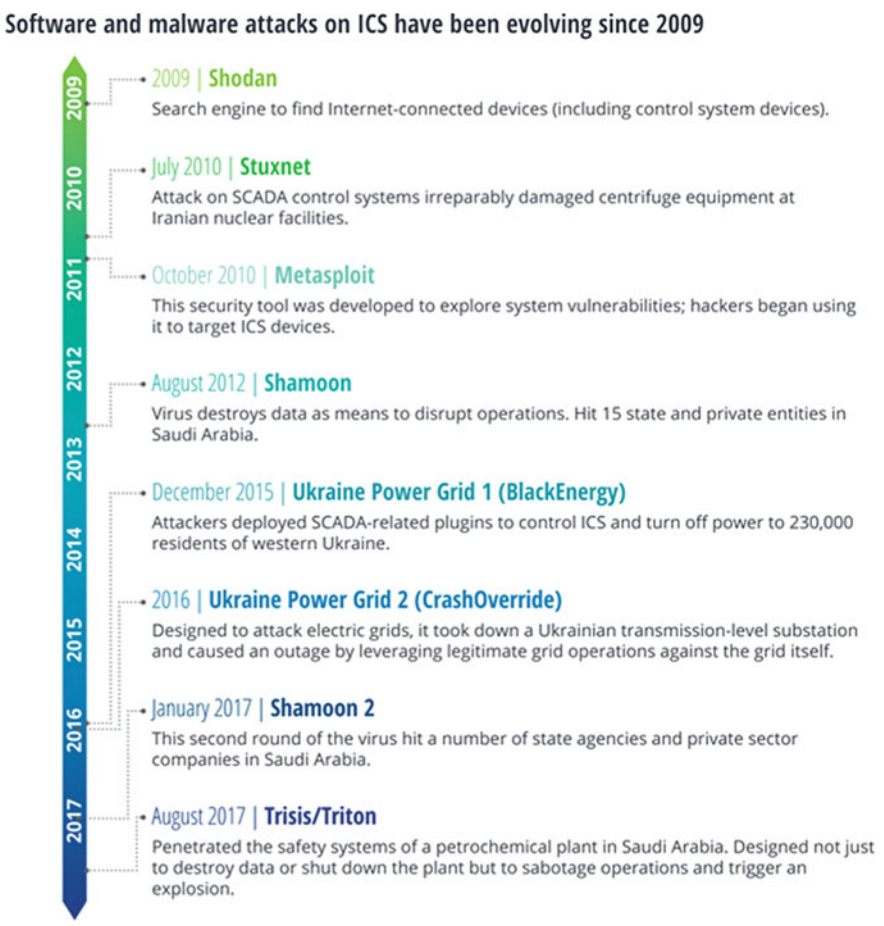

Fig. 6.1 An evolution of cyber threat on the electric power sector

One could argue that the adversary needs to have a comprehensive understanding of the targeted PACS operation including applicable settings in the protective relays and related intelligent electronic devices (IEDs). They also need to know how to penetrate or circumvent the cyber defence mechanism deployed by the utility. This issue is addressed in previous CIGRE studies [4–6]. Figure 6.2 is used to explain how the adversary can use an insider to facilitate the attack on PACS assets and networks.

Threats are described in terms of their type, their objective, their location and success criteria. Three special threats of interest are those executed remotely (external threats), those executed internally by employees or contractors and those that require collaboration between internal organisations. This threat model is commonly known as the "insider threat". Nation-states and criminal organisations have demonstrated a meticulous plan of action to cover every possibility and sequence

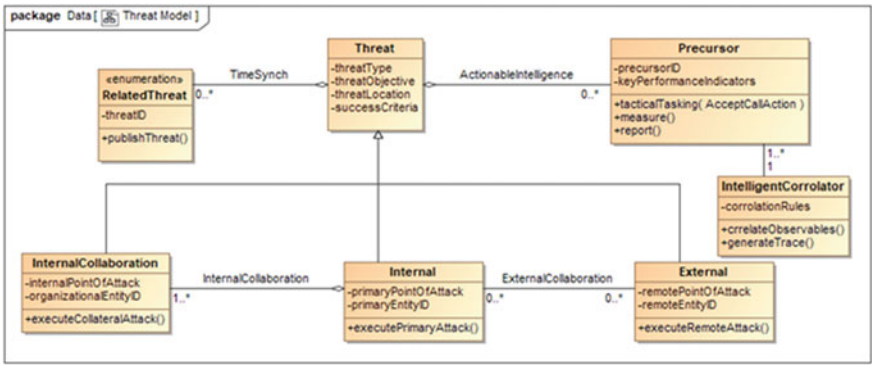

Fig. 6.2 Insider threat collaboration

of events needed to effectively compromise utility employees, support contractors and supply chain providers.

As described in [7], establishing contact with potential targets for compromise is often difficult. It requires finding a likely candidate, getting to know him or her ascertaining the candidate's interest, uncovering exploitable vices, and possible Achilles' heel requires a great deal of patience, time and resources. It is not unusual to take 6 months to 1 year to develop the rapport. It is important to understand the targets of compromise rarely if ever, succumb because of ideology. Personal reasons usually prevail, and ideological justifications often come after a decision has been made to cooperate with the adversary. Thus, models for responses and future actions are designed to cover many long-term, high-risk scenarios by focussing attention on precursors to track key performance indicators (KPIs) describing behaviour patterns developed by an analytical tool called "intelligent correlator" in Fig. 6.2. Unfortunately, most utilities poorly address this process because they have neither adequate staff skill nor analytical tools.

Some APT cases may be time synchronised with other related threats to add more confusion to the situation, in which case an instance of the related threat is modelled as part of the primary threat shown in the centre block [1]. The cardinality notation (0..*) simply indicates that an instance of threat knows about no related threat (0) or it may include many related threats (*).

Figure 6.2 also shows that no precursors or many precursors are part of the threat (0..*). This relationship identifies the actionable intelligence available to the utility organisations with staff skills and advanced analytical tools described by at least one instance of an intelligent correlator that provides the rules to correlate data from disparate sources. This correlation is known as data fusion which uses raw data to generate actionable intelligence. But that is a complex capability for another day.

The open literature is rich with examples that describe how employees and support contractors can be compromised by a well-financed adversary, e.g. nation-state or criminal organisation. Thus, there may be a collaboration between an external

adversary with remote access privileges and an internal adversary who knows the nuances of the deployed protection system and its settings.

Given the advanced digitisation and ubiquitous connectivity inherent in 61850 protection and control schemes, there are usually multiple organisations that manage silos of operation. If these organisations have a heightened awareness of the potential attack, they will receive observable alarms initiated by the attack scenario during the reconnaissance phase of the attack and the end-game attack. In this case, the adversary needs to compromise internal employees and contractors within the applicable silos of operation.

6.1.2 Time on Target Doctrine

When CIGRE study committee D2 (Information Technology and Telecommunications) studied future threats and their impact on electric power organisations and operations, they identified "time on target" as a new doctrine to increase the effectiveness of a well-planned attack scenario [5]. The basic idea is to time the cyberattack vectors to create a saturation scenario. These attacks would come from multiple locations and gain access to the PACS assets and networks through multiple entry points.

For example, in the substation, there are access points on the process bus and the station bus that can be exploited. The exploit can be initiated by an insider threat agent or remotely by an external insider threat agent or by an external threat agent. For example, PACS network access ports that are disabled can be enabled at the prescribed time. The same is true for disabling alarm setting to ensure that those monitoring the system operation are not alerted to any anomalous behaviour.

Lastly, attack vector migration can be dormant and awakened by a timed trigger or event or a combination of both. The dormant vector can be installed early in the supply chain and not be detected during the supplier's bench testing, factory acceptance testing, utility quality assurance testing, site acceptance testing and maintenance testing.

6.1.3 Fundamental Response Strategies

Faced with the rapid development and deployment of APTs, the utility must design a highly agile response strategy to better anticipate and proactively defend against unknown APTs before they evolve. This requires PACS and network engineers to use several new technologies such as artificial intelligence, machine learning and deep learning techniques. Because IEC 61850 protection systems are highly automated, they can readily incorporate these new technologies.

IEC 61850 PACS is enabled to provide data on demand to all applications that need the data. Put another way, data no longer travels from point A to point B, rather data has a point of presence that can be accessed promptly using multicast and publish and subscribe methods. Thus, the availability of these data provides the

means to correlate the sequences of PACS network traffic, log data, asset metadata and federated intelligence to provide a context to the behaviour in your system and pinpoint the exact threat. PACS engineers have intimate knowledge of their networks and settings in PACS IEDs which can be leveraged against APT agents.

While standards such as IEC 62443 [1, 8, 9] and IEC 62351 [10–14] give rise to significant advances in mitigating APTs, operational maturity is the key to success. For this reason, we focus on response strategies that are indexed to a simple maturity model.

6.2 Understanding Cyber-Physical Security Issues

This section examines the cyber-physical security issues as they relate to the aforementioned maturity assessment schemes. The objective is to shed light on the complex nature of standing up and maintaining an effective response strategy.

6.2.1 Focus on Maturity Assessment Challenges

In response to the emerging threat landscape of well-financed advance persistent threats, there is an imperative need for utilities to assess the maturity of their security policies, procedures and organisational directives (PP&ODs). Based on their risk assessments, funding is allocated to upgrade the capabilities of PACS staff, processes, operational processes and automation technologies. To justify the allocation of resources, it is helpful to use a maturity assessment to identify and prioritise the investment in people, processes and technology. IEC standard 62443 is a multipart standard that provides a life-cycle framework to address operational requirements for industrial automation and control systems (IACS).

Maturity models allow an organisation to assess their capabilities and maturity level in many practice areas and assign a Maturity Indicator Level (MIL) to those practice areas. Typically, maturity models have 4 levels (MIL0-MIL3), where MIL0 indicates no or minimal maturity in the area, MIL1 indicates basic maturity, MIL2 indicates intermediate maturity, and MIL3 indicates advanced maturity. Some models provide additional levels indicating finer-grained advancement, with the highest MIL always indicating advanced maturity.

To achieve a particular level, all practices must be at or above the indicated level. For example, in an assessment of 10 practices, if nine of the practices are rated at MIL3, but one is rated at MIL1, the overall assessment is rated MIL1. Using the weakest MIL rating for reporting is a common approach. As discussed later, only MIL 1 needs attention.

Organisational directives assign responsibility and accountability to responsible PACS-related organisational units (ROUs) for properly executing maturity improvements and continuously managing and maintaining the needed level of maturity for the deployed cyber-physical security solutions. This requires a

high degree of cooperation between operational personnel, including well-aligned enabling processes and procedures to maintain an effective defence posture.

By identifying specific practices that do not meet each organisation's goals for achieving a particular maturity level, resources may be effectively and prudently applied to improve those specifically identified areas to achieve the desired maturity level. In the preceding example, resources could be focussed on improving only the one practice area requiring improvement since the others have already been assessed at the desired levels. The process can then be repeated over time in a continuous improvement cycle to increase the maturity level.

Next is some insight into the available maturity assessment schemes available to support a utility's allocation of funding over the planning horizon, measurement of improvement effectiveness and adjustments needed to improve staff skills, operational processes and technical capabilities. Three maturity assessment schemes considered are as follows.

(1) Carnegie-Mellon Model (CMM) [15],
(2) DOE's Cybersecurity Capability Maturity Model (ES-C2M2) [16] and
(3) Nemertes Maturity Model (NMM) [17].

In the development of IEC 62443, ISA99 reviewed the general-purpose CMM and its use to assess the maturity of IACS solutions. They concluded this multi-dimensional model was far too complex and too difficult to align with the standard's approach to an effective security strategy.

ES-C2M2 is a well-understood scheme. It was released in 2012 after joint development between DOE, DHS and utility experts was piloted by over a dozen utilities during development and has since been updated and used by many other utilities. It has expanded from its initial electricity sector approach to include a natural gas version and a generic version. It is currently undergoing another revision. Computer-assisted tools have been developed to streamline the data gathering and analysis process making it easier for organisations to self-assess their maturity under the ES-C2M2. The Electric Power Research Institute (EPRI) uses this model to develop a set of metrics [18]. This is also a work in progress and needs to be tested and vetted by utility stakeholders.

The Nemertes maturity model is a simplified maturity assessment scheme that is closely aligned with the kill-chain model [19]. CIGRE working group D2.46 reviewed Nemertes' assessment methodology and found it to be easily aligned with IEC 62443 requirements for different levels of security posture [5]. This approach has not been tested or vetted by utility stakeholders. Because it is well-aligned with the kill-chain model and IEC 62443, it warrants further attention.

This simplified model has a few advantages over CMMI v2.0 and ES-C2M2. The simplicity of this approach is captured in Fig. 6.3, which aligns well with IEC 62443's focus on people, process and technology. PACS organisations can use a simple index (0.1.2.3) to rate the maturity of their staff's ability to address the evolving cyber threat landscape. In concert with staff, skills are the need for well-defined policies, procedures and organisational directives that can be

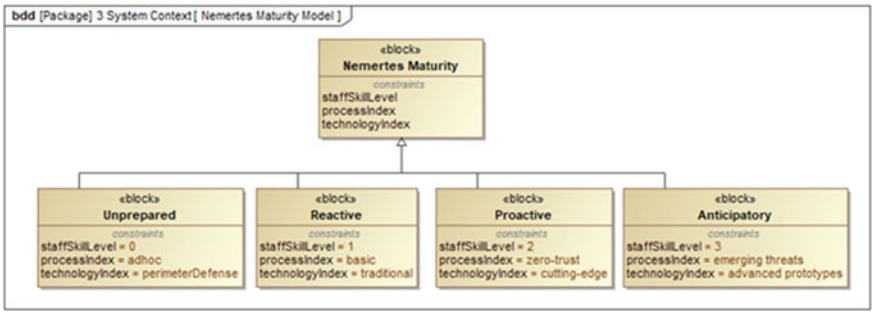

Fig. 6.3 Nemertes maturity model

indexed in terms of processes. Furthermore, staff skills also need to be aligned with technologies deployed by the utility.

At the lowest level (unprepared) is when the PACS staff skill level is rudimentary, processes are for the most part ad-hoc, and cybersecurity protection relies on perimeter defence in the form of firewalls and air gap between the operational networks and the business networks.

When examined in some detail, most PACS organisations fall into the "reactive" category of maturity. Their staff is periodically updated on the threat landscape to improve their awareness of the cybersecurity threats of interest. They do have approved policies, procedures and organisational directives that reflect the requirements imposed by local laws and regulations, such as the NERC CIP and EU's general data protection regulation (GDPR). Most cybersecurity protection is deployed in terms of traditional systems, such as firewalls, demilitarised zones (DMZ) and some features of IEC 62351 that are available from IEC 61850 solution providers.

Many of the larger utilities have stood-up versions of an integrated security operations centre (ISOC). But due to the high cost of operating an ISOC, many utilities need an alternative security operation centre, to share the cost—a federated security operations centre (FSOC). The idea behind the FSOC is to use many of the cloud computing services. However, extreme care is needed to guard against abuse of authentication mechanisms.

The U.S. National Security Agency (NSA) published Detecting Abuse of Authentication Mechanisms which discusses how malicious cyber actors are abusing trust in federated authentication environments to access protected data. The exploitation occurs after the actors have gained initial access to a victim's on-premise network. The actors leverage privileged access in the on-premise environment to subvert the mechanisms that the organisation uses to grant access to cloud and on-premise resources and/or to compromise administrator credentials with the ability to manage cloud resources. The actors demonstrate two sets of tactics, techniques and procedures (TTP) for gaining access to the victim network's cloud resources, often with a particular focus on organisational email [5].

There may be a few "proactive" PACS organisations that have invested in personnel with specialised cybersecurity skills and have updated their policies, procedures and organisational directives to reflect the guiding principle of zero trust. This requires the latest cutting-edge technologies to adequately ensure that only authorised entities (person or computer) have access to and use mission-critical assets. For example, identity and authentication management (IAM) relies on the use of digital signatures and implied trust in the selected certificate authority (CA).

The goal is to reach the "anticipatory" maturity level. At this level, the key is to provide skilled staff and the use of advanced cybersecurity prototypes to address the emerging threats, such as zero-day threats.

6.2.2 How Utilities Address APT Challenges

IEC 62351 standard has been published to provide security recommendations for different power system communication protocols including IEC 61850. In [20], detailed analysis of security threats, possible attacks and security requirements for IEC 61850 communication is presented. Building on this, the security considerations presented in IEC 62351 for securing different IEC 61850 messages such as Generic Object-Oriented Substation Events (GOOSE), Sampled Values (SV), Routable-GOOSE (R-GOOSE), Routable-SV (R-SV) and Manufacturing Message Specification (MMS) messages are discussed in [21] and summarised in an IEEE paper [22].

PACS use cases being considered include the following:

- Transfer trip from one to multiple terminals,
- Remedial action schemes (RAS) from a central controller to multiple remote controllers,
- Synchrophasor transmission,
- Surgical load shedding,
- Grid forming controls and
- Inverter-based black start.

Continuing with [21] and [23], experiments and laboratory demonstrations by a US utility have implemented R-GOOSE for their centralised-RAS; however, the security elements (authentication and encryption) are pending. Their major concern is the additional end-to-end communication message latency (about 1 ms) induced by the encryption mechanism. The encryption mechanism is discussed in Kanabar's paper [22].

A series of webinars [23] addresses security configuration and maintenance, which, in many cases, is viewed as complex and represents an impediment for adoption and deployment. The use of R-GOOSE/R-SV requires that the pairing of published information to subscribers of that information (e.g. a publication group) shares a common symmetric key that utilises a key distribution mechanism as specified in IEC 62351-9. The experiments and demonstrations rely on vendor tools

to configure the security policies and manage the certificates. CIGRE Technical Brochure 427 raised several concerns that these configuration tools, testing tools and data collection tools are vulnerable to compromise by insiders including support contractors [6, 24]. Thus, there is a need to seamlessly integrate CPS solutions into proprietary tools discussed in Chap. 10. Protection and automation engineers need to be concerned with the security of engineering tools used to configure IEDs and to manage mission-critical technicians' settings. No standard explicitly addresses the security requirements imposed on IEC 61850 tools. Of concern are the security vulnerabilities introduced when attaching field technicians' notebooks or another device (e.g. portable media) to the substation LAN. For this reason, strong security for both local as well as remote access and use control is most important.

Another issue that needs attention is patch management. No standard or guideline provides sufficient technical detail to effectively address patch management on time. Although this is a general security problem, more research is needed to develop a concrete specification for patch management in IEC 61850 operating systems, protocol stacks and applications. The only work on this issue is the work in ISA99 and IEC TC65 WG 10 to develop IEC/ISA 62443-2-3 [8]. However, this is a general standard for Industrial Automation Control Systems (IACS) and there need to be some more specifications to tailor parts 2–3 for IEC 61850 systems.

No standard or guideline provides sufficient detail to effectively address the timely reporting of events (TRE); e.g. NERC CIP requires a report within 24 h from event notification. Intrusion detection and reporting systems are currently designed to look for known scripts but are woefully lacking in their ability to learn from attack patterns on time. More research is needed to develop derived requirements for IEC 61850 to ensure that cybersecurity events are reported to the proper authority promptly.

Including conformance statements in a standard is still a thorny issue. The best attempt to do this is specified in IEC 62443-2-4 [9]. Parts 2–4 need to be tailored for IEC 61850 systems.

The good news is the availability of applicable standards (IEC 61850-90-5, IEC 62351-9, RFC 6407) and experiments in work by a major US utility. The bad news is the sparse deployment of IEC 62351 implementations in PACS assets and networks. Without these deployments, there is a lack of assessments by PACS organisations that address both management and engineering challenges for an embedded solution. Therefore, PACS organisations must continue to rely on traditional security mechanisms which are reflected in a "reactive" maturity posture described in Fig. 6.3.

Until cybersecurity is integrated into the logical nodes of PACS assets and networks, some utilities are improving their maturity posture to a proactive level by standing up an integrated security operations centre (ISOC). CIGRE Technical Brochure 796 [5] provides a good summary of the capabilities provided by an ISOC. One major benefit to PACS organisations is the offloading of cybersecurity responsibilities for threat awareness, internal and external reporting and specialised skills needed to use the advanced analytical tools.

6.2.3 Security Testing Needs Attention

Functional testing is discussed in Chap. 9, but these tests should include cyber-physical security (CPS) testing as an integral part of the test program. PACS management should use rigorous methods to validate their models and document those methods and results. Using a variety of commercial tools for penetration testing, they should routinely perform tests to assess and determine if any open communication ports third-party not used. If so, they should be disabled. If required, third-party testing is recommended to obtain an unbiased assessment of the CPS solution. These tests should utilise real threats and attack methods that are being used by cybercriminals and other threat actors. The threat scenarios should be based on attacks collected from a recognised global threat intelligence network. Using automated and manual threats, three key capabilities need to be stress tested.

- Inbound threat detection and prevention (before execution),
- Execution-based threat detection and prevention (during execution) and
- Continuous monitoring post-infection and ability to act in the event of compromise (post-execution).

NSS laboratories, located in Fort Collins, Colorado (USA), have been proofing a wide range of product testing and evaluation services. For example, Check Point has actively participated in NSS labs testing since 2011 and has achieved NSS Labs recommendation in firewall, next-generation firewall and Intrusion Prevention System (IPS) group test.

6.3 Leveraging IEC 61850 for Early Threat Detection

The underlying capabilities designed into IEC 61850 logical nodes provide the structure to seamlessly integrate cybersecurity protection solutions. With this in mind, the next step is to explore some of these solutions.

6.3.1 Understanding the Kill Chain

The Law Enforcement Cyber Center uses the “kill-chain” model to define the cyberattack life cycle. The cyberattack on PACS assets and networks is straightforward; hence, any attacker can attack this system soon after getting access and escalating the privileges within the targeted system of interest. In such a case, the attacker must design the site-specific attack and test the attack before finally getting on with the actual attack; otherwise, there are high chances of failure. CIGRE survey, reported in [5], reveals that cybersecurity breaches are active on an average of 200 days in a critical infrastructure before they are discovered.

There are eight stages in the life cycle. For a cyberattack to be successful, the attacker must successfully execute all eight stages of the cyberattack life cycle;

therefore, to prevent a successful cyberattack from being successful, it is imperative to thwart the attack at any of the phases, or break the chain, in the life cycle. The eight stages of the life cycle are as follows:

- Perform initial reconnaissance. The attacker identifies PACS assets and networks and determines operating systems, security, applications, protocols, addresses and other runtime characteristics.
- Make an initial compromise. The attacker uses an exploit or attack to probe and break through PAC network cybersecurity system defences. This compromise could be achieved through social engineering, phishing, extortion or other means.
- Establish a foothold. The attacker establishes or creates persistence on a PACS asset or network, perhaps by installing a backdoor or installing utilities or malware to maintain access.
- Escalate privileges. The attacker gains greater access to PACS assets and data by obtaining credentials, leveraging privileges, belonging to an application or service or exploiting vulnerable software.
- Perform internal reconnaissance. The attacker explores other PACS assets and networks to map the entire environment, identify the roles and responsibilities of key operational staff and locate interesting or valuable data needed to execute the attack scenarios.
- Move laterally. The attacker jumps from one PACS asset to another asset on PACS networks, using network shares, scheduled tasks and remote access tools or clients.
- Maintain a presence. The attacker maintains ongoing access and activity on the PACS assets and networks using backdoors or remote access tools.
- Complete the mission. The attacker achieves his attack objectives, such as stealing sensitive data or executing a scenario that interferes with, disrupts or disables PACS functions.

Solutions to detect threats resident in PACS assets and networks are either anomaly-based or deception-based.

Anomaly-based detection creates a behaviour baseline of hosts, data access, network traffic, user behaviour, etc. Commonly, any activity that is inconsistent with the baseline is flagged as an alert to PACS responsible organisational unit and subsequently to EPU's security team. Anomaly-based solutions have two significant drawbacks:

- Capturing, storing and associating data from disparate sources are complex, expensive and time-consuming. It requires highly sophisticated tools and skilled analysts that are not usually common in PACS engineering organisations.
- False positives occur at a high rate, which can degrade the confidence in the assessment tools and security team.

Deception-based detection is an alternative to anomaly-based detection. Many of the PACS assets (multifunction relays, merging units, etc.) can be used for deception-based detection. The deceptions are not part of the normal operations and are revealed only by a cyberattack. When an intruder spends the time and effort to locate and access a deception that is set up to invite an attack, it is a positive affirmation of a compromise or a highly positive anomaly.

Deceptions take many forms to detect and engage threats at every step of the kill chain. Deceptions are broadly grouped into four types:

- Decoys: A decoy is a fabricated system or software server that presents an attractive target to an attacker. A decoy is usually more attractive to an attacker than a PACS asset or network because it is seeded with interesting (but fake) data and known vulnerabilities are left open.
- Breadcrumbs: Breadcrumbs are used to lead an attacker to a decoy. When an attacker does reconnaissance, breadcrumbs are placed on the endpoints and the PACS network points to create an interesting target.
- Baits: Baits are honey tokens such as counterfeit data or fake PACS operating credentials to a service that the attacker finds valuable. Baits are laid so that ordinary IT and OT procedures or normal user behaviour do not reach them. An attack can be detected by monitoring the access or usage of the bait.
- Lures: A lure makes a decoy, a breadcrumb or a bait more attractive than the actual PACS network assets. For example, to make a software service decoy attractive, it can be set with factory default credentials.

To address the insider threat, decoys, breadcrumbs, baits and lures must be closely guarded. They should not be known to each PACS organisation performing 24/7/365 operations.

6.3.2 Data Fusion in IEC 61850 Systems

If detection of the attack early in the kill chain is disrupted, or used to set traps, it can be used to thwart the adversary's intrusion objectives. Defenders can then implement appropriate countermeasures to protect their mission-critical functions. The fundamental elements of intelligence are the three types of indicators: atomic (source addresses, vulnerability identifiers), computed (derived data involved in an incident) and behavioural (tactics used by the adversary).

Tracking the deviation of a given indicator from its predecessors in the kill chain is the challenge. Connecting the indicators is difficult because the raw data comes from disparate sensors and is subject to unverified assumptions. In military intelligence terms, this process is known as tactical data fusion (TDF). At each stage of the kill chain, the outcome of TDF analysis can be catalogued as follows:

- Reconnaissance to identify and select PACS asset and network targets for intrusion.
- Weaponisation by exploiting a selected vulnerability to deliver a payload using an automated tool.
- Delivery of the weapon to the targeted environment.
- Exploitation to trigger the weapon's action by direct command or by auto-execution.
- Installation to maintain a persistent presence inside the selected PACS asset or network target to manage the attack.
- Command and control (C2) for the adversary to maintain positive control over the weapon's actions.
- Actions on objectives to execute the attack and adjust the tactics to achieve their ultimate objectives.

Two observations are derived from analysis of successful adversary campaigns and extrapolation to existing PACS environments: (1) adversaries have highly sophisticated tradecraft tools and expertise to perform and engage in each of the categories and (2) defenders need to significantly raise their maturity levels with advanced tools and strategies to perform the TDF functions in each category. In short, PACS managers need to migrate from a purely defence-in-depth (DiD) siege mentality to a proactive and anticipatory response strategy.

This dramatic shift in response strategy requires well-defined metrics to measure the performance and effectiveness of defensive actions at each stage of the kill-chain intrusion. As noted by Hutchins [24], framing metrics in the context of the kill chain, defenders have the proper perspective of the relative effectiveness of defence of their defences against the intrusion attempts and where there were gaps to prioritise remediation. Furthermore, there is a clear need to use advanced analytical tools to reconstruct the intrusion scenario at each stage of the kill chain. Without this reconstruction, it is nearly impossible to anticipate the next steps by the attacker. This projection is needed to establish the mitigation strategy to either disrupt, degrade, deceive or destroy the attacker's kill-chain strategy and tactics. One approach called intrusion reconstruction, promoted in several CIGRE technical brochures, is to define model-based systems engineering (MBSE) descriptions of the problem domain in terms of black-box and white-box relationships of the PACS system of interest (SoI). In turn, these logical architectures that emulate the SoI can be used to simulate (with live data feeds) the progression of the kill-chain scenario. Various mitigation options can then be examined to determine which approach is most effective to deny the attackers ultimate objectives. MBSE analysis focuses attention on the behaviour of the attackers, their tactics, techniques and procedure to determine "how" they operate, not specifically "what" they do.

For example, consider the case that from a remote workstation a targeted malicious agent containing a weaponised application installs a backdoor for outbound communications. Access to and execution of the weaponised application may be controlled by a means known only to the attacker. If so, this will be important information for the defender to select the appropriate mitigation option. Due to

the reuse of known indicators collected over several weeks/months, the agent is blocked. Furthermore, analysis of the remaining kill chain reveals a new exploit or backdoor to PACS operational network. Without this knowledge, future intrusions from remote workstations delivered by other means may go undetected. This example illustrates the importance of the speed of response to deploy countermeasures, which gives the defender a tactical advantage. Background for this example is discussed at length in CIGRE Technical Brochure 762 [25].

This example illustrates the need for highly specialised training and tools to detect, process and reach an actionable conclusion. It also emphasises the need for timely coordination and cooperation between those responsible for operating the PACS assets and networks. Additionally, a well-defined situation assessment that can be shared with external agencies is needed. If the attack employs a combination of threat agents, selecting and executing the best response option are even more complicated. This further supports the need for a well-defined MBSE model of the SoI to select the best response and to avoid unintentional consequences.

6.3.3 New Crypto-Based Technologies for IEC 61850 Systems

Most physical PACS network links provide ill-defined and uneven guarantees of confidentiality and privacy or data integrity. Industry networks are increasingly wireless, and wide area networks are impossible to physically secure against pervasive surveillance. Therefore, any information from a user to a service or between users should preferably be encrypted at the object level using standards-based cryptographic techniques to render it unintelligible to eavesdroppers while at the same time offering the data integrity/trust model necessary as actionable information.

All types of communications from the user, customer or function should be protected: personal information, found at the organisational level or sensitive sensor inputs, should be encrypted to preserve privacy and control (and security). However, even access to otherwise public resources should be obscured through encryption to prevent an eavesdropper from inferring users' patterns of browsing, profiling, service use or extracting identifiers that may be used for future tracking. This assurance is even more necessary in the cloud environment where all service level agreements (SLAs) state that data security is the responsibility of the data owner, not the cloud provider.

Information security techniques should be considered to achieve a logical state of "safe harbour" throughout the entire engineering process beginning at the earliest design stages to the operation of the productive system if possible. Using appropriate techniques such as encryption, data must be persistently protected in all phases of its life, in transit, at rest and overtime.

Data protection is the responsibility of the PACS data owner, not the infrastructure in which the data exists. Data protection must persist and travel with the data object, indifferent to network topography, supporting persistent protection of data regardless of data location, use and reuse.

Information security techniques must be consistent with and address the protection goals of availability, confidentiality and integrity. All of these goals are important from privacy and data protection perspectives that specifically require that unauthorised access and processing are prevented and that also ensure accuracy and protection from manipulation, loss, destruction and damage.

At the same time, however, the organisational and technical processes must be in place to allow appropriate handling of the data and provide the possibility for individuals to exercise their rights while only accessing data when necessary. This principle calls for appropriate technical and organisational safeguards and access management. To achieve information stability, data accountability is required, to ensure, and to be able to demonstrate, compliance with privacy and data protection principles (including legal requirements). This requires clearly defined responsibilities, internal and external auditing and controlling all data processing. In some organisations, data protection officers are installed to demonstrate compliance, perform data protection impact assessments and internal audits and handle complaints.

Data protection providers need to regard the entire life-cycle management of sensitive data from collection, processing, to deletion, systematically focussing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of sensitive data.

The responsible party, which could be a data protection provider, is responsible for carrying out a data protection impact assessment based on published standards (e.g. NIST/ISO/ANSI), and the results referenced when developing those measures and procedures.

6.3.4 Understanding Role-Based Access Control (RBAC)

As suggested earlier, RBAC and Attributre Based Access Control (ABAC) are the common means to enforce the limitation of access and use by the requesting organisation. RBAC is most discussed in applicable standards and supporting reports with the parameters shown in Fig. 6.4. Examples of roles and permissions are identified in the two enumeration blocks. These parameters are specified by the project manager and specified in the digital certificates discussed earlier.

ABAC parameterisation, shown in Fig. 6.5, is equally important but has received less attention in the applicable standards and supporting reports, the exception being IEC 62351-90-19 which gives it proper attention. What ABAC provides to augment RBAC are location, device and time of when the access and use privileges are enabled. Again, ABAC parameters values are set by the project manager.

Details about how RBAC can be implemented are discussed in Sect. 6.4.4.

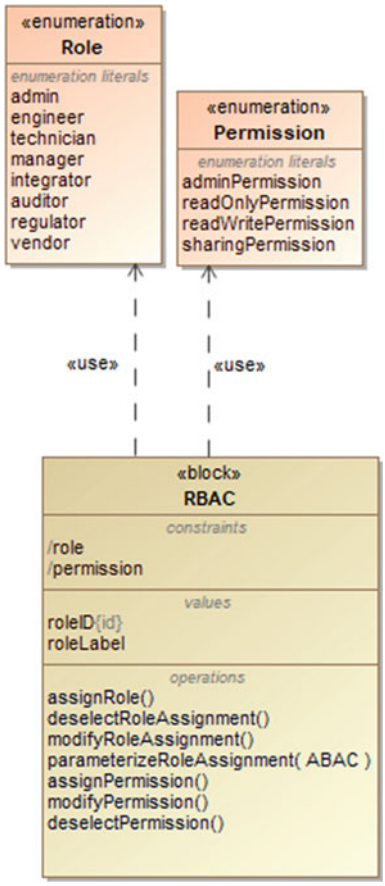

Fig. 6.4 Role-based access control parameterisation

6.3.5 Extended Access Control Mechanisms

Information security techniques must play a central role, and these same information security techniques can also include actions that eliminate old and unnecessary data, thereby preventing unnecessary or unwanted processing of that data, without the loss of the functionality of the information system.

Attribute-based access control (ABAC) enforced by cryptography, at the object level, is an example of an approach that could be implemented to meet these objectives. This object-level ABAC process, (defined by NIST in SP800-162, SP1800, and by ANSI in X9.69 and X9.73 as well as ISO 11568) can achieve the declared objectives.

Protected messages are represented as extensible markup language (XML) markup using the canonical XML encoding rules (cXER) or represented in a binary format that is backward compatible with existing deployed systems. These systems rely on cryptographic message syntax, using the basic encoding rules (BER) or the canonical subset of BER, the distinguished encoding rules (DER).

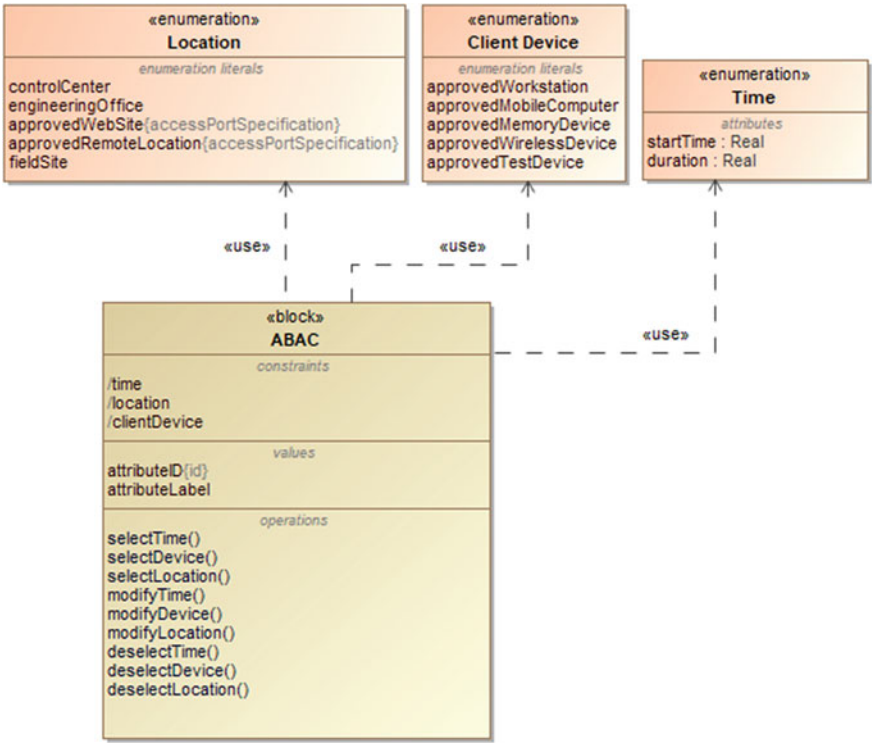

Fig. 6.5 Attribute-based access control parameterisation

Messages and objects are protected independently. There is no cryptographic sequencing (e.g. cipher block chaining) between messages or objects. There need not be any real-time connection between the sender and recipient of the message. This makes the syntax suitable for use over store-and-forward systems.

Standard attributes are defined using an extensible design to allow any organisation with a need to define additional attributes for any purpose. Attributes are defined that allow security assertion markup language (SAML) and XML's key management specification (XKMS) content to be carried in each of the cryptographic types defined in X9.73, supported by the key management defined in X9.69.

The syntax is cryptographic algorithm independent and extensible. It supports the provision of data confidentiality using encryption and tokenisation techniques, data integrity, data origin authentication and non-repudiation services. Any algorithm may be used for message or object encryption, digital signature, signcryption and key management. A variety of key management techniques are supported, including key exchange, key agreement, password-based encryption and constructive key management.

1. Selective field protection can be provided in two ways. First, they can be protected by combining multiple instances of this syntax into a composite message. Second, they can be protected in a single message by using identifier and markup tag names and content-specific manifests that are cryptographically bound to content to select message components. This approach allows reusable message and/or object components to be moved between documents without affecting the validity of the signature.
2. Precise message and object encoding, and detailed cryptographic processing requirements of binary and XML markup message representations are provided.

Simple Object Application Protocol (SOAP) message extensions are defined for each of the cryptographic types defined in X9.73 to enable the protection of financial services information in Web Services environments. The typical application of the enveloped-data content type will represent one or more recipients' digital envelopes on the content of the data or signed-data content types.

6.3.6 Security Requirements for Remote Services

Chapter 14 describes access to PACS network and devices from a remote (outside the substation security perimeter). Several CIGRE technical brochures developed by Study Committees B5 and D2 have addressed the security risks and practical solutions for remote services to mitigate that risk. Figure 6.6 identifies the local laws and regulations that must be satisfied in the PACS-centric policies, procedures and organisation directives (PP&ODs). In turn, the basic CPS objectives for remote services must satisfy the PP&ODs.

This led to the identification of two parts of IEC 62443 that address the issues. Figure 6.7 illustrates the interaction of parts 2–4 requirements imposed on the solution providers, and parts 2–3 identify the need for system segmentation such as the use of a demilitarised zone (DMZ). These are best described in terms of the multiple requirements for access control, use control, data confidentiality, data integrity, restraints on data flows (interfaces), resource availability and timely reporting of events. These CPS requirements should be seamlessly integrated into the remote access services described in Chap. 14.

6.3.7 The Need for Security-Smart PACS Data Objects

IEC 61850 introduced the concept of smart PACS objects. IEC 62351 overlays the cybersecurity requirements onto the IEC 61850 objects. CIGRE Technical Brochure 790 [26] introduced the concept of "security-smart" objects for PACS applications. The basic idea is to use a standards-based specification for secure, self-protecting data objects (SSDO), that are data-label aware with services based on that awareness. When properly implemented, SSDO provides differential access and use control that is independent of network configuration.

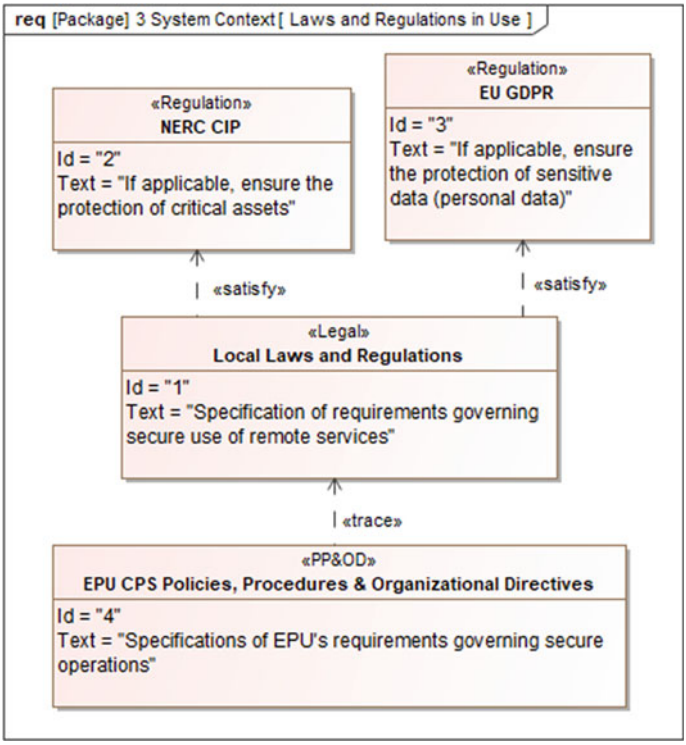

Fig. 6.6 Local laws and regulations that must be satisfied in a PACS-centric environment

Cryptographic key management for PACS is also comprehensively addressed in the IEC 62351-9 standard "key management". This part forms a basis for handling keys at the client, server and key generation/distribution and is referenced by other IEC 62351 parts that use key management to address secure process communication (parts 3 through 7) and RBAC (part 8). Digital certificate management is addressed in Sect. 6.3.8.

The good news is commercial solutions are available. However, PACS stakeholders must evaluate and compare different implementations to determine which solution best fits their PACS-centric SSDO protection mechanisms. As a minimum, the evaluation should include the following:

- A well-defined process to designate roles and credentials that are seamlessly integrated with job responsibilities. Specifically, the role is defined by the credentials where each credential represents an attribute of the data described in the underlying information classification model.
- The information classification model should be aligned with local laws and regulations and well-specified in PACS sensitive security policies, procedures and organisational directives.

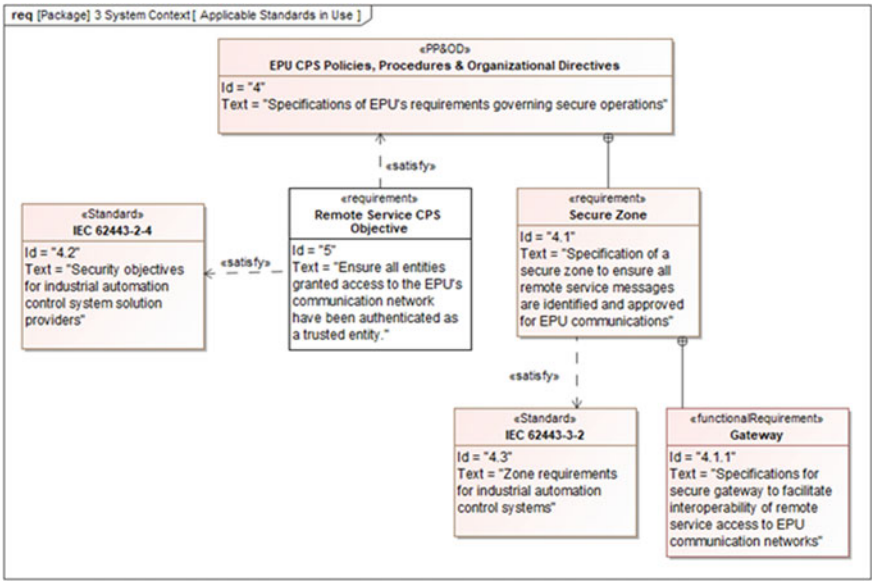

Fig. 6.7 IEC 62443 requirements for remote services

- A federated management system to securely generate, distribute, recover and dispose of cryptographic keys and key fragments.
- Unique communication requirements for distribution of keys and digital credentials. The best solutions do not require encrypted communication of keys and digital credentials.
- A trusted certification authority to authenticate digital certificates (credentials) that describe access and use privileges.
- Every authorised user and PACS application must have a digital credential when they issue their first request.
- Solution providers must conform to the standards to ensure consistency between versions released and interoperability between SSDO management systems and embedded solutions in PACS devices. PACS managers should insist that all stakeholders enforce conformance to a well-defined interface control document (ICD).

Secure PACS applications require management of intelligent electronic devices (IEDs) such as network devices and protective relays shown in the SysML-based model, see Fig. 6.8. Of interest in this example are two IED types: network devices and protection and control relays. Management of these devices is the responsibility of an authorised user, e.g. network engineer or technician, or relay engineer or technician. Security requires access control specified in RBAC and ABAC privileges assigned to the authorised user. For this example, the authorised user logs on to an EPU controlled workstation that has the responsibility to verify access

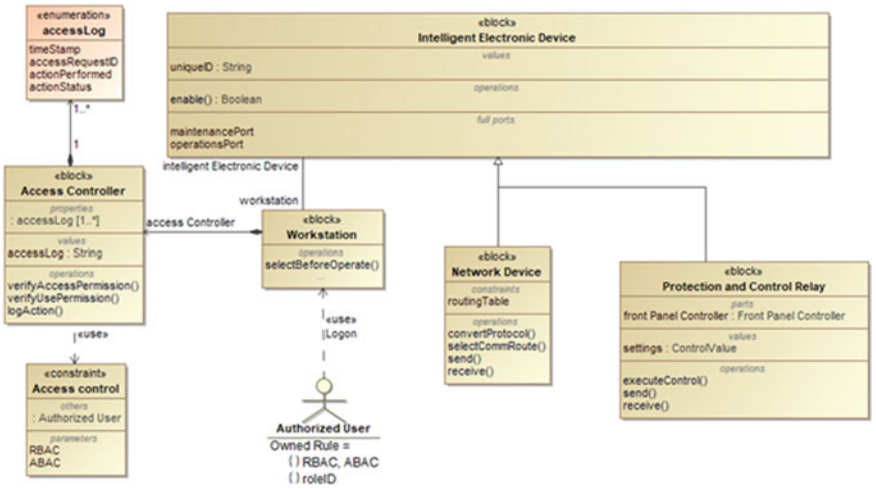

Fig. 6.8 Typical participants in PACS applications

permissions and use permissions. Once verified, the process then proceeds as a select-before-operate sequence of transactions.

6.3.8 Digital Certificate Management

Multiple PACS functions use digital certificates to enable access control (RBAC) and use control privileges (ABAC). IEC 62351-8 and IEC 62351-9 describe the semantics for smart data objects contained in these certificates. An understanding of the life cycle of digital certificates provides the proper context for PACS applications.

Digital certificates including their keying materials can be used to identify and authenticate an entity (human or IED) access authority and use privileges for managing a network device, workstation or a power system device. These privileges include generation, exchange, storage, safeguarding, use, vetting revocation and replacement or renewal of certificates. Successful digital certificate management is critical to the secure use of certificates to provide protection and control data confidentiality and in some cases data integrity.

Figure 6.9 is an overview of the certificate life cycle. Elements of the process are labelled to facilitate cross-referencing and to help identify the logical sequence flows. A "+" symbol is used to note that a task may be complex and require multiple iterations and coordination between stakeholders. The dashed connector is used to identify a data association. The red association connector is used to highlight specific actions required to update or revoke a digital certificate.

In summary, the management of these certificates requires the following capabilities.

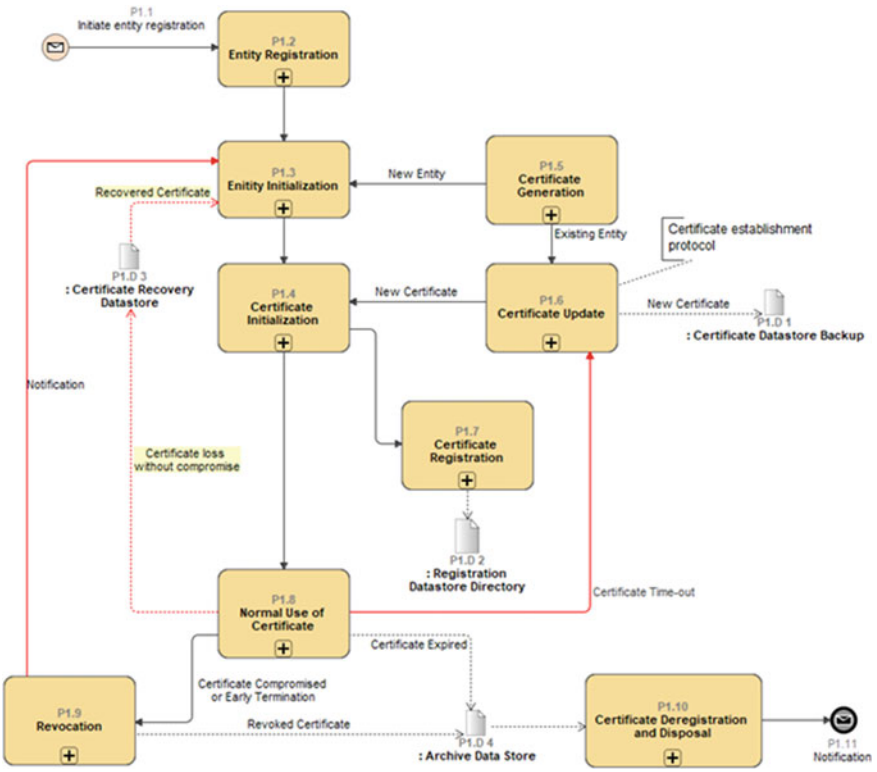

Fig. 6.9 Overview of the digital certificate life cycle

- The digital certificate management system shall provide the capability to generate and distribute digital certificates that maintain the secret values on time to support operations. Note: timeliness requirements imposed by critical operations that require high security determine the means to distribute the digital certificates.
- The certificate management system shall prove the capability to periodically update the digital certificates. Note: the period for certificate use varies based on the need to limit an entity's time of access and use. For some situations, a persistent digital certificate is appropriate with no time-out specified.
- The certificate management system shall provide a secure means to maintain the digital certificates to support certificate recovery when the certificate management system fails and becomes disconnected, or the certificate is lost but not compromised.
- When applicable, the certificate management system shall encrypt the certificate data from end to end, so it is protected when at rest or in transit. Note: security through encryption needs to be efficient and transparent to some operation

functions, e.g. protection and control. Other functions may not need encryption, e.g. sample data streaming.
- The certificate management system shall provide the capability to revoke a digital certificate if it is compromised or its time of effectiveness expires.

6.3.9 Leveraging Self-Protecting Data Objects

Leveraging the SSDO capabilities requires modification to existing components of the protection and control IED. The example shown in Fig. 6.10 identifies three subsystems of the protection and control relay that require consideration: data handling subsystem, P&C logic subsystem and P&C data management subsystem. The new participant is the crypto-content management subsystem, which is logically part of the data handling subsystem. To perform its encryption and decryption function, the crypto-management subsystem needs access to information owned by the P&C data management subsystem, which in turn needs access to data owned by the P&C logic subsystem.

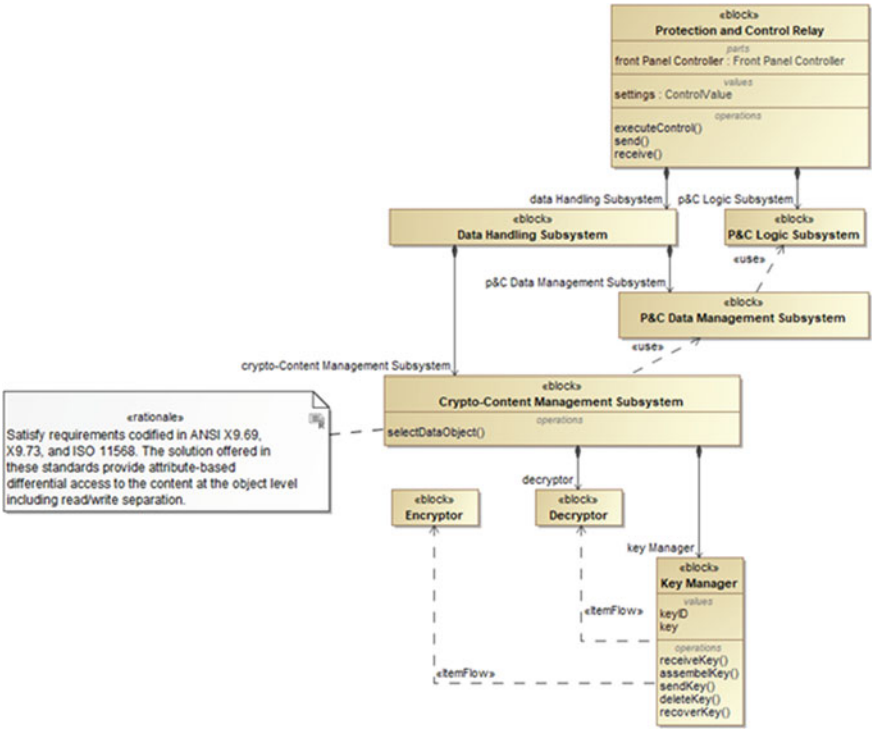

Fig. 6.10 SSDO participants in PACS applications

Part of the crypto-management subsystem is the key manager that is responsible for receiving keys (or key fragments, assembling keys from key fragments and sending the keys to the encryptors and decryptors. In addition, the key manager is responsible for the secure deletion of keys and key recovery.

Control of keys is critical because in a PACS environment multiple parties are likely to have the same key pairs. It is a better design to have dynamic certificates that can be rekeyed. Furthermore, this key management scheme requires that connectivity be ensured.

6.3.9.1 A Means to Improve Front Panel Access Control

Figure 6.11 focuses attention on local access to the front panel of the protective relay. An access controller (a part of the front panel controller) provides the capability to verify access permission and verify use permission, time stamps the action and logs the status of the request (0: denied, 1: approved).

Local access to changing settings on a protective relay front panel needs attention. One approach is to use a radio-frequency identification (RFID) smart card enabled with access and use control privileges to gain local access to the protective relay. To implement defence-in-depth, the RFID smart card could be used to

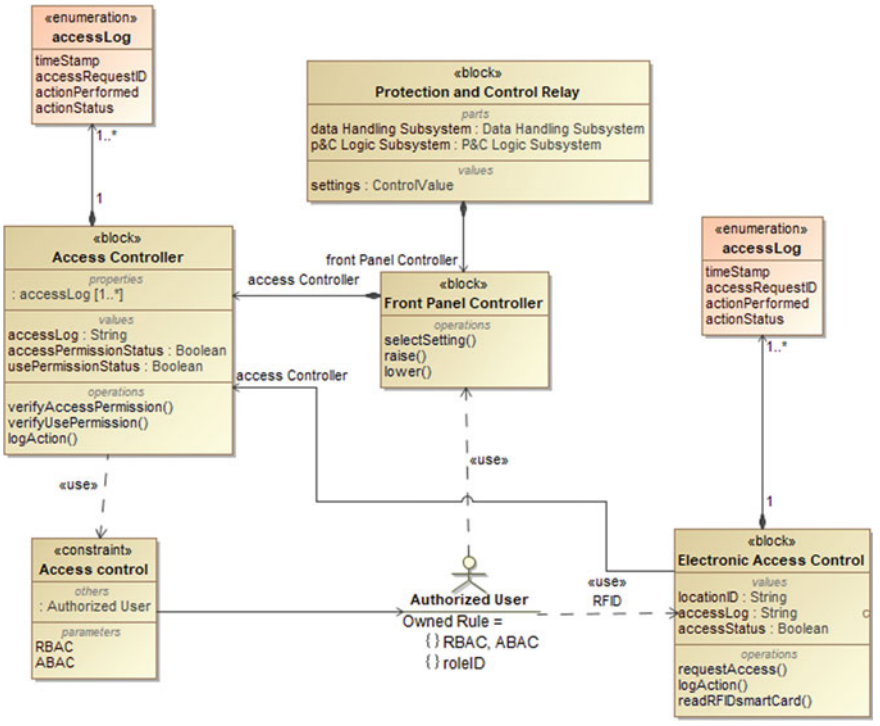

Fig. 6.11 Local access control to change settings

gain access to the substation yard, access to the substation house, access to the substation cabinet and access to the front panel reads of a protective relay. In each case, the block electronic access control in Fig. 6.11 reads the RFID smart card with the access request information and logs the action. Each instance of the read action is time-stamped and includes the location (substation yard gate, substation house, substation cabinet and protective relay front panel) and logs the access status (0: denied, 1: approved).

Another approach is to have the IED/relay authenticate the user with a numeric ID and passcode, both of which are centrally managed in a RADIUS/LDAP server with centrally enforced account management policies. This approach also works with existing IEDs where a numeric keypad and a screen are available on the front panel and does not increase the attack surface by, e.g. introducing a new RFID interface.

6.4 Security Implementation in R-SV and R-GOOSE

6.4.1 Message Security

In today's utility environment, wide area secure communication is a requirement. The ability to secure R-SV (Routable Sampled Values), R-GOOSE, GOOSE and SV is defined in the IEC 61850 and IEC 62351 standards (appropriate parts). The security goals that were identified are as follows:

- Ability to provide Information authentication and integrity (e.g. the ability to provide tamper detection). The use of authentication is required for operational systems.
- Figure 6.12 Confidentiality (via encryption) in R-GOOSE and R-SV is optional.

Message authentication is achieved through the calculation and inclusion of a secure Hash (Message Authentication Code—MAC) that is computed using data from the entire message except for the part of the message that contains the MAC (Fig. 6.13). This signature is referred to as a Message Authentication Code or MAC, and given that a Hash algorithm is used, the term Hashed Message Authentication Code or HMAC is used. A Hash is an amalgam of all bytes that make up the message and is combined with a secret key to encrypt the Hash.

Since the IEC 61850 messages can be sent to many receivers, all members of the publish-subscribe group must be able to encode and decode a message. To implement this functionality, a Symmetric Key is used and is distributed to all members of the publish-subscribe security group. A key is a large number—typically 16 to 32 bytes long (directed by policy) and is generated with cyber randomness (e.g. normal random functions do not have enough entropy to satisfy this requirement). The secure distribution of the Symmetric Key is performed by a function/device known as a Key Distribution Centre (KDC). Distribution over the wire to members of the security group is performed by a protocol known

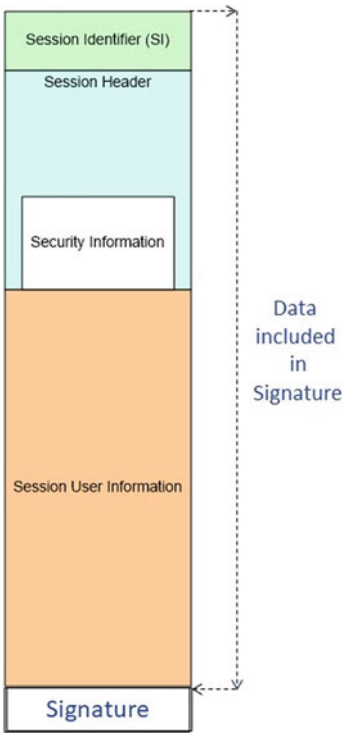

Fig. 6.12 R-SV and R-GOOSE message structure

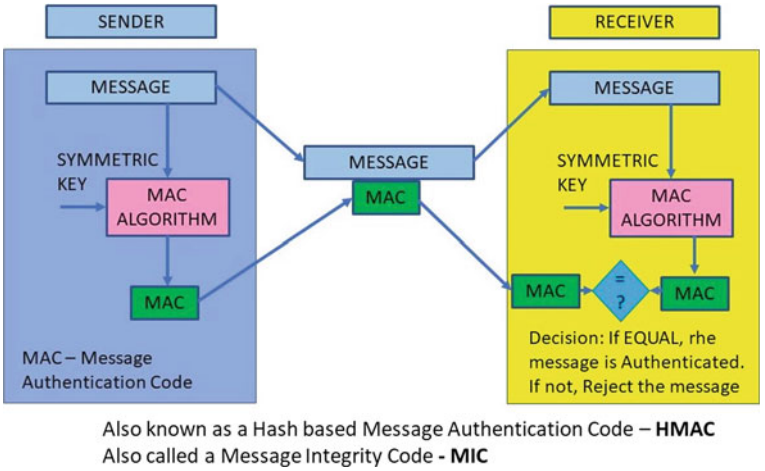

Fig. 6.13 Message authentication process

as the Group Domain Of Interpretation (GDOI) as defined in IEC 62351-9 [13] which refers to several Internet Request For Comments (RFCs) including RFC 6407 [27]. The same Symmetric Key is used to compute the message signature and to encrypt the message. If encryption is selected by policy (set in the KDC), only the payload of the message is encrypted. Further details regarding the KDC follow in this section. The message authentication "Hash" is appended to the end of the published message (see Fig. 6.12). Upon receipt, the subscriber re-computes the message Hash using the same algorithm and key. If the received Hash is the same as the re-computed Hash, the message is declared to be authenticated (see Fig. 6.13).

As with all GOOSE communication exchanges, the exchange is configured in the SCD or publisher's CID file (note: a device may belong to multiple groups). IEC 61850-6 also has elements that allow the KDC(s) to be defined and allows configuration of which KDCs an IED/Application should communicate with to receive keys and policies. In addition, subscribers can identify their publisher's source and destination address. This allows anti-replay to be implemented per IEC 62351-6.

6.4.2 Key Distribution Centre—KDC

As noted above, implementation of security on R-GOOSE, R-SV, GOOSE and SV requires that asymmetric key be distributed to all members of a publish-subscribe group, also known as a security group. Membership in a security group is usually defined by the Substation Configuration Description (SCD) file. Members of a security group and the KDC must be provisioned X.509 identity certificates and can validate other X.509 identity certificates from one or more X.509 certificate authorities. On the start-up of the KDC, the identity certificates are exchanged and authenticated by both the group members and the KDC. If the identity of the Group Member is authenticated, and it has been granted rights to obtain the keys and policies, the KDC will deliver these to the Group Member. The Symmetric Key is delivered to the members of the security group through a protocol, as noted above, known as the Group Domain of Interpretation (GDOI). As an example, in the case of an SV message, the security group includes the publishing merging unit (MU) and all subscribers to the MU's dataset. It should be noted that all security implementations are based on existing Internet standards and RFCs (albeit, one was created to meet 61850 needs). The KDC is also responsible for the periodic re-keying (re-key time is user selectable) of all members of a security group. Keys should be periodically changed as the longer a key is in use, the higher the probability (albeit still small) of the key is cracked.

Note: PKI provides policies, and procedures needed to create, manage, distribute, use, store and revoke identity digital certificates. These include the following:

- The ability to request identity and certificate authority X.509 certificates through the use of Simple Certificate Enrolment Protocol (SCEP) or Enrolment of Secure Transport (EST).
- The ability to determine if an X.509 certificate has been revoked through the use of the Online Certificate Status Protocol (OCSP).

Symmetric Key Delivery, through GDOI, can be performed by the KDC via two different mechanisms known as PUSH and PULL. In both modes, there are two sets of keys/policies delivered to be utilised by the exchange of GOOSE, R-GOOSE, SV or R-SV. These are known as Traffic Encryption Key (TEK) payload. This set is provided in order to provide cybersecurity for two key rotation periods even if KDCs are offline. Additionally, the key/policy to be used to protect the PUSH is exchanged. This is known as the Key Encryption Key (KEK) payload. In PULL mode, a Group Member PULLs or requests a key from the KDC. Before a key is delivered, the KDC validates the certificate of the requesting Group Member. Group members must execute a PULL request on start-up to request keys to synchronise key usage or to address lost keys when a PUSH is not able to be received or authenticated. When PUSH is set by policy in the KDC, the KDC sends or pushes a new key to the Group members.

When the KDC policy is set to PUSH, keys to the Group Members are sent from the KDC to the security group members. In this mode of operation, the group member can acknowledge receipt of a key to the KDC (set via policy). In the re-keying process, events on the grid may inhibit the delivery of a new key. When security is implemented on functions such as transfer trip and remedial action, failure to deliver a new key must not be known to inhibit the operation of the function. To address this scenario, a policy is known as Key Delivery Assurance (KDA—specified in IEC 62351-9) can be utilised. With KDA enabled, the KDC can ascertain if key delivery attempts to a user-set percentage of the group members (policy set in the KDC) are reached, and permission to change keys to the publisher is inhibited. Alternatively, if key delivery to the user-set number of group members is successful, a KDA message is sent to the publisher of the group which allows the publisher to change keys at the specified time. KDA should only be utilised if the publisher supports PUSH; otherwise, the operational integrity of KDA is questionable.

The recommended rotational period is twenty-four hours. With two keys being delivered at one time, there are enough keys delivered to allow key rotation (e.g. between the two keys) for forty-eight (48) hours even without KDA.

The KDC function should be extensible to meet the needs of most any size domain of management including, but not limited to, enterprise, control centres, substations, generation facilities, distributed energy resources (DER), distribution networks and home meter communications.

Recently, IEC 62351-9 has been extended to provide key management for Precision Time Protocol as specified in IEEE 1588:2019 and the emerging power profiles IEC/IEEE 61850-9-3 and IEEE C37.238.

6.4.3 IEC 61850 Client–Server Security

In client–server security, a "secure" message transfer is to be established between a function like a SCADA Master and the "server" or SCADA remote in the field. IEC 62351-6 allows several different combinations of transport-level and application-level security—two of which are shown in Fig. 6.14.

There are differences between Information Technology (IT) and Operational Technology (OT) cybersecurity priorities. OT Security concentrates on availability, integrity and confidentiality (AIC). Authentication is becoming more important so AICA (adds authentication) is becoming more important. The selection of the appropriate options for each client/server security profile is policy decisions to achieve the identified utility security policies.

The IEC 62351-4 security profile requires the use of Transport Layer Security (TLS) to provide confidentiality and integrity. Mutual authentication of the connecting nodes is also performed within the context of TLS. Application-level authentication is provided through the exchange of PKI certificates within the application layer.

IED 62351-4 end-to-end (E2E) security can provide confidentiality, integrity and authentication within the application layer depending upon the negotiated policies. This means that the use of TLS is optional for this security profile.

Authorisation is achieved through local means. As of this writing, the Role-Based Access Control (RBAC) configuration mechanism for IEC 61850 is still under development (e.g. IEC TR 61850-90-19).

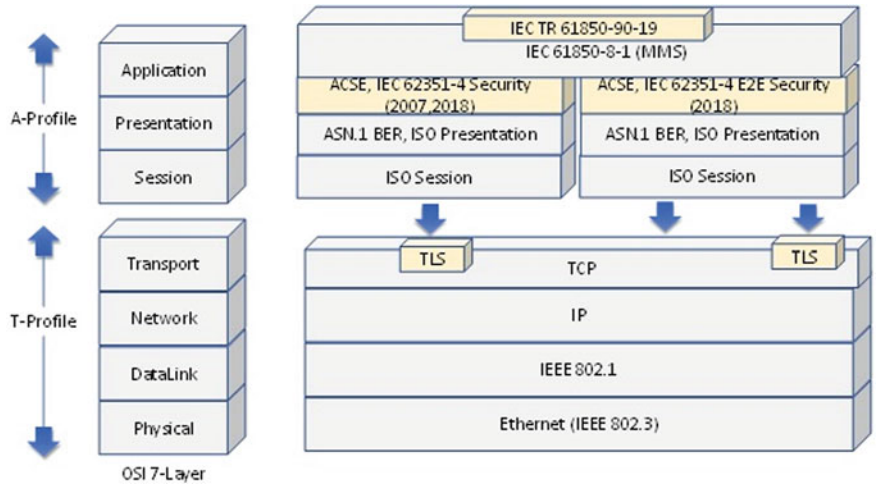

Fig. 6.14 TLS security options in IEC 61850

6.4.4 Role-Based Access Control—RBAC

As explained in Sect. 6.3.4, RBAC is a security mechanism that restricts user access to a system at a level needed to achieve a specific function. IEC TR 61850-90-19 leverages the RBAC constructs outlined in IEC 62351-8. Within IEC TR 61850-90-19, it is possible to grant/deny access to IEC 61850 services as well as access to IEC 61850 objects, including but not limited to Logical Nodes, data objects (DOs) and Functionally Constrained Data Attributes (FCDAs). Access control can also include conditions based upon IEC 61850 object values or Areas of Responsibilities (AORs). AORs can be geographical areas, IED mode based (e.g. local and remote) and other constructs. AORs and roles can be embedded in an identity certificate or via the preferred mechanism of a digital attribute certificate.

There are predefined role vs right bindings that can be found in IEC 62351-8. IEC 62351-8 also specifies how to create custom role vs right binding. IEC TR 61850-90-19 goes beyond IEC 62351-8 and allows the specification of rights to permit/deny access to specific IEC 61850 objects and services. The object permissions can be based upon a wildcard, Logical Node, Functionally Constrained Data (FCD) or Functionally Constrained Data Attribute (FCDA) down to the lowest definition in a data object. There is also a mechanism to utilise values to control security configuration as may be required for environmental emergency conditions (e.g. fire or earthquake) where normal security restrictions are relaxed to allow service restoration (shown as the stoplight in the Fig. 6.15).

The RBAC abstract model is serialised into a subset of the eXtensible Access Control Markup Language (XACML) per https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf. The support of XACML is anticipated

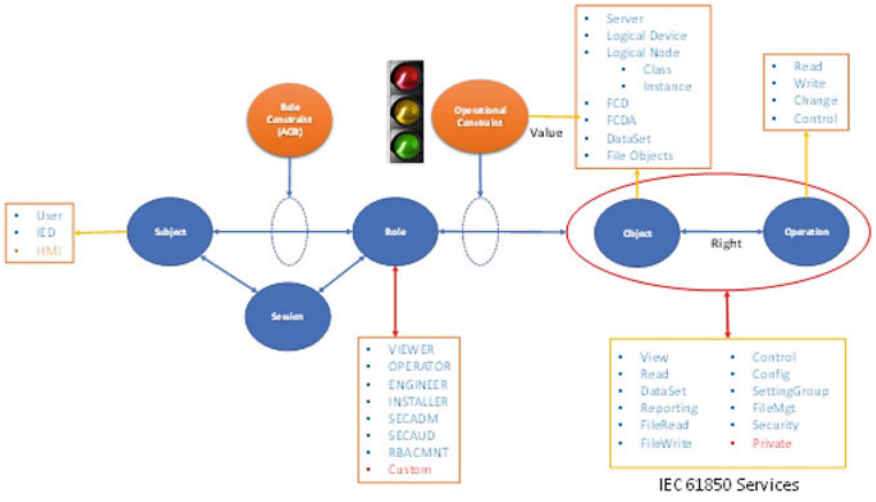

Fig. 6.15 RBAC concept

to be mandatory with the second serialisation being based upon an IEC TR 61850-90-19-specific XML Schema Language (XSD). The resulting serialisations result in an XML file that must be transferred securely to the Point of Enforcement (POE) such as an intelligent electronic device (IED).

6.5 Conclusions (Call to Action)

6.5.1 Top 6 CPS Actions to Protect IEC 61850 PACS

- It is imperative that CPS requirements be baked into every process of the IEC 61850 life cycle. This includes the supply chain of all components included in the solution (for example, see U.S. Executive Order 13920, effective January 16, 2021). It also includes each stage of configuring and testing at the component, subsystem and systems levels. Last is the need to address CPS requirements for decommissioning and disposal activities.
- Deploy software- or hardware-based collectors to ingest network traffic, log data, PACS asset and user metadata to learn the behaviours of PACS network while identifying and classifying the consequence of an APT on your system.
- Provide PACS-related organisations with advanced analytical tools to discover and prioritise anomalous behaviours through a combination of machine learning and deep learning algorithms.
- Provide visualisation mapping to understand a time-based narration of how an APT is evolving in your PACS network and to enable the protection engineers to drill down into the details of the threat.
- Integrate cybersecurity orchestration and incident management tools to provide semi-automatic or fully automatic response and remediation.
- Tools needed to configure security policies, perform testing and collect data need to be vetted to ensure they do not expose the PACS assets and networks to cyberattack, see [6].

6.5.2 Future Study Topics and Objectives

Study committees B5 and D2 need new cooperative, or joint working groups, to identify and assess emerging cyber-physical security issues related to IEC 61850 systems. These assessments should address the full life cycle of the design, development and qualification of systems, subsystems and components that comprise an IEC 61850 system deployed and operated in a live environment. For example, these studies should address migration solutions to update IEC 61850 systems in use. Following are the high-priority topics.

- Emerging laws and regulations, such as the general data protection regulation (GDPR) or variations of the GDPR defined by the local authorities. These

requirements and constraints should be applied to all IEC 61850 sensitive data, such as IED settings, configuration tools and testing tools.

- Emerging NERC CIP requirements should be addressed in all future studies. There will be a need to reconcile the NERC CIP emerging requirements and the emerging laws and regulations.
- Digital certificate management schemes, including but not limited to IEC 62351's approach, should be addressed to better understand both client-side and server-side certificate management mechanisms in IEC 61850 systems for various authentication, encryption and secure communication protocols. Cross-signing by multi-utility and supporting organisation certificate authorities (CAs) also needs attention to avoid abuse.
- Software-defined measures, the networking (SDN) and network function virtualisation (NFV) are emerging technologies for IEC 61850 systems (see Chap. 11). An assessment of SDN/NFV implementation and lessons learned from early deployments is needed to identify the potential improvements in cybersecurity protection. NFV brings into play the potential of virtualising selected IEC 61850 functions. Such an approach needs further study to identify CPS risks and viable solutions to mitigate those risks.
- More work is needed to identify a measure of effectiveness (MoEs) and metrics for various CPS maturity schemes. Specifically, assessment needs to identify costs, benefits and challenges to implement and manage each candidate maturity scheme in an IEC 61850 operating environment.

References

1. Industrial communication networks—Network and system security—Part 3-3: System security requirements and security assurance levels, Standard 62443/FDIS-3-3 (ISA-99.03.03), TC65WG10, January 2013
2. Cherkashin, V., Feifer, G.: Spy Handler: A Memoir of a KGB Officer: The True Story of the Man Who Recruited Robert Hanssen and Aldrich Ames. Basic Books (2008)
3. Livingston, S., Sanborn, S., Slaughter, A., Zonneveld, P.: Managing cyber risk in the electric power sector. Deloitte. As of 17 (2019) [Online]. Available: https://www2.deloitte.com/us/en/insights/industry/power-and-utilities/cyber-risk-electric-power-sector.html
4. CIGRE WG D2.38: TB 698—framework for EPU operators to manage the response to a cyber-initiated threat to their critical infrastructure. CIGRE, Technical Brochure #698 (2017) [Online]. Available: https://e-cigre.org/home.asp
5. CIGRE WG D2.46.: TB 796—cybersecurity: future threats and impact on electric power utility organisations and operations. CIGRE Study Committee D2, CIGRE, 21, rue d'Artois, 75008 Paris, FRANCE, Technical Brochure 796 (2020) [Online]. Available: https://e-cigre.org/home.asp
6. CIGRE WG B5.38.: TB 427—the impact of implementing cybersecurity requirements using IEC 61850. Technical Brochure #427 (2010) [Online]. Available: https://e-cigre.org/home.asp
7. Schwartz, H.A.: Significant cyber incidents since 2006. Center Strateg. Int. Stud. (2020) [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/200626_Cyber_Events.pdf

8. TC65WG10.: Security for industrial automation and control systems—network and system security—Part 2-3: patch management in the IACS environment. Int. Electrotech. Comm. Draft Tech. Rep. IEC/DTR 62443-2-3 (ISA-99.02.03), 2014-01-07
9. IEC 62443-2-4: 2015 Industrial communication networks—network and system security—part 2-4: security program requirements for IACS service providers, Standard, IEC 62443-2-4: 2015, TC65WG10, Geneva CH, 2015–06–30
10. IEC 62351-3 + AMD1: 2018—Power systems management and associated information exchange: data and communication security—Part 3: profiles including TCP/IP, IEC 62351-3 + AMD1: 2018, TC57WG15 (2014)
11. IEC 62351-4: 2018—Power systems management and associated information exchange: data and communication security—Part 4: profiles including MMS and derivatives, Standard IEC 62351-4, TC57WG15 (2018)
12. IEC 62351-6: 2007—Power systems management and associated information exchange: data and communication security—Part6: security for IEC 61850 (note: new edition under development). Standard IEC 62351-6, TC57WG15 (2007)
13. IEC 62351-9:2017—Power systems management and associated information exchange—data and communications security—Part 9: cyber security key management for power system equipment. Standard IEC 62351-9: 2017, TC57WG15 (2017) [Online]. Available: https://webstore.iec.ch/publication/30287
14. IEC 62351-8: 2011—Power systems management and associated information exchange: data and communication security—role-based access control (note: new edition under development). Standard IEC 62351-8: 2011, TC57WG15 (2011)
15. CMMI_Institute.: CMMI v2.0: online capability maturity platform accelerates speed to performance, resiliency, and scale (2019)
16. Stevens, J.: Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)(Case Study). DTIC Document (2014) [Online]. Available: http://www.energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model-es-c2m2
17. Johnson, J.T.: Cybersecurity by the numbers: maturity metrics of successful security organisations. Presented at the SAI education at ISC, Las Vegas NV, 9 April 2019, Presentation (2019)
18. Suh-Lee, A.A.C., Rasche, G., Wakefield, M.: Cyber Security Metrics for the Electric Sector, vol. 3.0. Electric Power Research Institute (2017) [Online]. Available: https://www.epri.com/#/pages/product/3002010426/?lang=en-US
19. Zhou, X., Xu, Z., Wang, L., Chen, K., Chen, C., Zhang, W.: Kill chain for industrial control system. In: MATEC Web of Conferences, vol. 173, p. 01013. EDP Sciences (2018)
20. Hussain, S.S., Ustun, T.S., Kalam, A.: A review of IEC 62351 security mechanisms for IEC 61850 message exchanges. IEEE Trans. Ind. Inf. (2019) [Online]. Available: https://www.researchgate.net/
21. Holstein, D.: Logical node implementation of cybersecurity in IEC61850 PAC assets and networks. In: Mark Adamiak, R.M., Falk, H., Cease, T.W. (eds.) PACS Use Cases of Actual Implementations of Cybersecurity in the Logical Nodes and Lessons Learned from these Implementations. Email exchange (2020)
22. Kanabar, M., Cioraca, A., Johnson, A.: Wide-area protection and control using high-speed and secured routable goose mechanism. In: 2016 69th Annual Conference for Protective Relay Engineers (CPRE): IEEE, pp. 1–6 (2016) [Online]. Available: http://ieeexplore.ieee.org
23. Triangle_Microworks.: Simplifying Secure Routable GOOSE & Sampled Values. 2020–07–30 Webinar
24. Hutchins, E.M., Cloppert, M.J., Amin, R.M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lead. Issues Inf. Warfare Secur. Res. Tech. **1**(1), 13 (2011) [Online]. Available: https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
25. CIGRE WG D2.40.: TB 762—remote service security requirement objectives. CIGRE, Technical Brochure 762 (2019) [Online]. Available: https://e-cigre.org/home.asp

26. CIGRE WG B5.66.: TB 790—Cybersecurity requirements for PACS and the resilience of PAC architectures. CIGRE, Technical Brochure (2020) [Online]. Available: https://e-cigre.org/publication/790-cybersecurity-requirements-for-pacs-and-the-resilience-of-pac-architectures
27. RFC 6407 Group Domain of Interpretation
28. Aleksandraviciene, A., Morkevicius, A.: MagicGrid Book of Knowledge. Vitae Litera, UAB, Kaunas, Lithuania, p. 170 (2018)
29. Industrial communication networks—network and system security—Part 3-2: security levels for zones and conduits, standard 62443/CD-3-2 (ISA-99.03.02), TC65WG10 (2013)
30. CIGRE JWG B5/D2.46.: TB 603—APplication and management of cybersecurity measures for protection and control. Technical Brochure #603 (2014) [Online]. Available: https://e-cigre.org/home.asp
31. Weis, B., Rowles, S., Hardjono, T.: The group domain of interpretation. Internet Req. Comm. **6407** (2011) [Online]. Available: https://tools.ietf.org/html/rfc6407