Hochschule Bremen
City University of Applied Sciences

HSB

Automated Monitoring of Operational Technology Security and Compliance for Power Grids

Bastian Fraune, M.Sc. Computer Science

The Motivation

→ Increasing digitization in the energy domain
→ Prosumers: Producing and consuming energy (at the same time)
→ Production and consumption needs to be balanced all time!
→ Requires highly automated coordination of consumption and production in future (smart grid)
→ Vision: Compliance status of security configurations of smart grid devices in a monitoring system

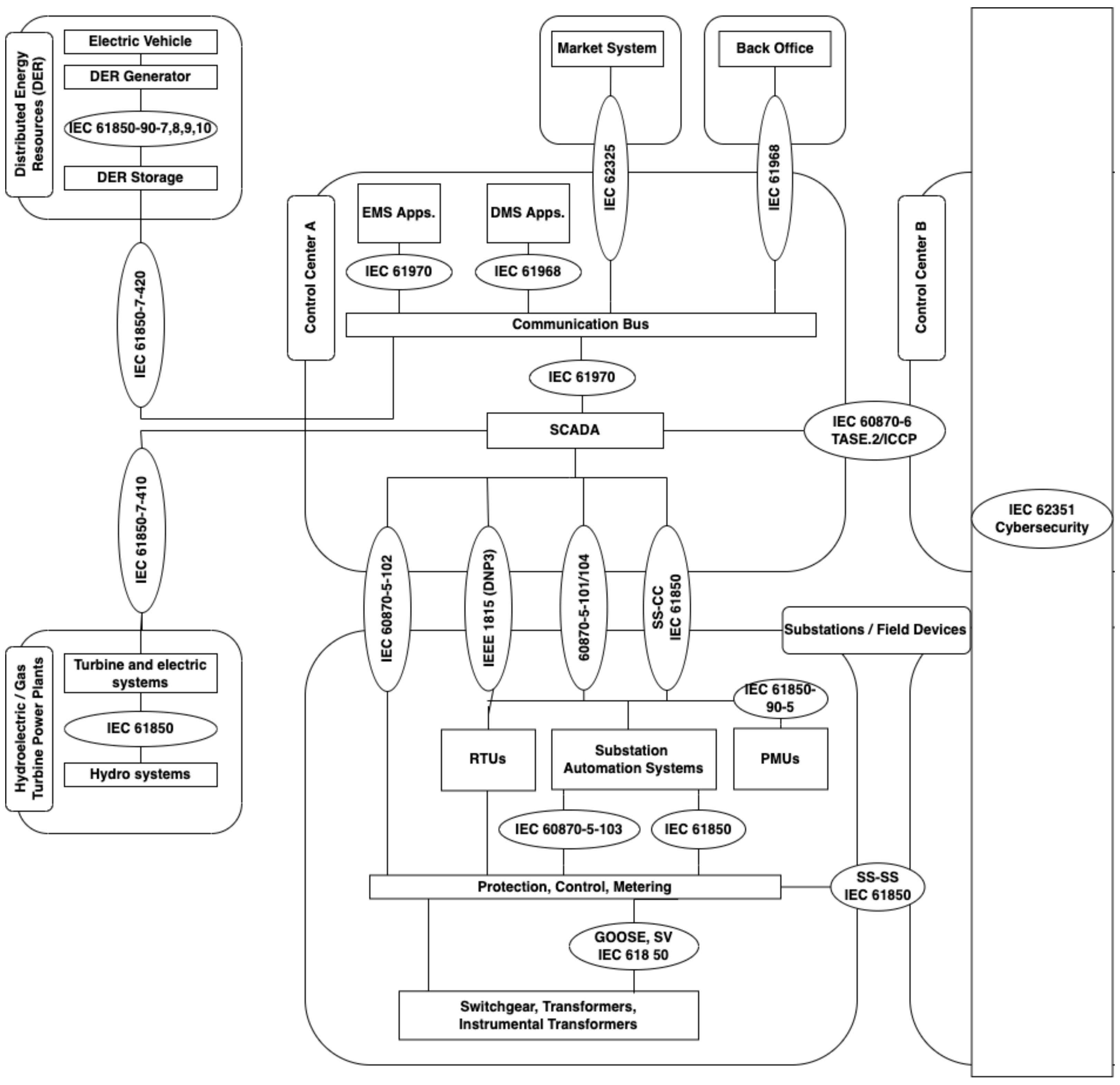

Figure 1: IEC TC57 Communication Standards Architecture, own depiction of [IEC12],

What is the Problem?

The increasing amount of smart grid components will increase and at the same time their administration in terms of software maintenance and configurations is not under control of the grid operator. Because most of the components are not owned or under physical control of the grid operators. Those devices need to be monitored, to know their security configurations and thus to be able to check their compliance.

Typical issues in industrial control systems according to BSI [Bu21]:

→ Insecure configuration
→ Insufficient documentation
→ Manipulation and sabotage of ICS components
→ Insufficient user- and authorisation management

Typical issues within the OWASP Top 10 year 2021 [OWA21]

→ Security Misconfiguration
→ Security Logging and Monitoring failures
→ Software and Data Integrity failures

The Challenge in this PhD Project

Audits are a typical way to inspect the compliance of standards and is done by third parties. In future, it will not be possible to audit all devices that are part of the smart grid and under control of the grid operator. For instance, it is simply not possible to check whether an IED controlling household's PV meets current security requirements.

To support a higher security of the smart grid and enable grid operators to know the current security state, **this PhD-project aims to enable an automated monitoring of security configurations**. Such monitoring needs to be integrated into established and current communication standards of the power grid.

Figure 1 shows a (simplified) reference architecture of power grid communication: At the bottom, substations represent a typical part of local power distribution nets. On the left side of the figure, distributed energy resources (DER) are depicted. Communication with other substations or control centres can be seen on the right side.

" How can existing information models from ICT component monitoring be considered?

This question aims to explore the extent, to which existing protocols for monitoring can be incorporated. The TC 57 is a technical committee of the International Electrotechnical Commission (IEC). TC 57 prepares and proposes standards for "Power systems management and associated information exchange" [In]. Many standards have been released and are currently in use (see figure 1). To be able to integrate the idea of the research project into the power grid, their standards have to be considered. Therefore an investigation driven by use cases is necessary in order to identify the required and applicable protocols. Suitable protocols shall be able to transport the monitoring data from the process level up to the operation and enterprise level.

" Which security features are relevant from the view of existing domains standards?

As the basis on the way to automate security configurations, it needs to be investigated what is required. To collect requirements, typical security standards in the power grid have to be identified. The standard IEC 62351 is made to secure protocols and communication within the TC 57 and shall be investigated in terms of requirements and missing requirements. In order to extract the correct requirements, it is important to analyse which requirements are applicable in which context and thus necessary for this PhD project. It is expected that typical security requirements are also included in industry standards such as the IEC 62443 series, those requirements will be considered, too.

" How can concepts of trusted computing support automated monitoring?

To enhance the trust of such monitorable security configurations an integration of hardware based trust anchors will be investigated. Trusted Computing concepts which allow to enable measured boot and remote attestation in combination with a hardware security module (HSM) are part of the research. The HSM specified by the Trusted Computing Group (TCG) is the Trusted Platform Module 2.0 (TPM2). Such an integration into the monitoring of security configuration allows to ensure that the devices authenticity can be proven.

[BU21] Bundesamt für Sicherheit in der Informationstechnik (BSI): , IT-Grundschutz- Kompendium, 2021

[OWA21] The Open Web Application Security Project, A. van der Stock, B. Glas, N. Smithline, and T. Gigler, "OWASP Top 10 - 2021," 2021.

[In] International Electrotechnical Commission (IEC): , IEC - TC 57 Scope.

[IEC12] IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure, Frances Cleveland, WG15 Convenor Xanthus Consulting International, 2012

Contact
Bastian.Fraune@hs-bremen.de