The Smart Grid: A Use-Case for Large-Scale SDN Deployment

Felix Neumeister, Martina Zitterbart
Institute of Telematics, KASTEL Security Research Labs, KIT
Karlsruhe, Germany
felix.neumeister@kit.edu, martina.zitterbart@kit.edu

I. INTRODUCTION

The continued integration of distributed energy resources into the power grid is a well-known challenge. The increased variability in demand and supply causes frequent state changes. Consequently, more coordination between energy generation, energy storage, energy consumption, and the transmission grid is required. The lack of large rotating masses in the power grid further increases the timing requirements. All of this creates challenges with respect to a robust and resilient operation of the future smart grid. It also leads to enhanced requirements regarding the communication backbone of the smart grid [2]. Within this abstract, we outline SDN-SG, an SDN-based Smart Grid communication backbone for the middle and high voltage substations and equipment in the smart grid. SDN-SG provides highly reliably and timely communication.

In contrast to most literature discussing the application and advantages of SDN (Software-defined networking) in the smart grid (e.g. [3]), SDN-SG goes beyond small smart grid segments (e.g. [1]) targeting larger setups, e.g., spanning an entire country or continent. SDN-SG subdivides the communication backbone into SDN-based subnetworks called control domains. It enables highly reliable and timely communication between and across such control domains in order to provide a robust and resilient operation of the future smart grid.

This abstract presents a presumed topology of the communication backbone, outlines the main characteristics of SDN-SG and sketches the organization and operation of the network.

II. TOPOLOGY

Substations are equipped with more and more equipment to perform tasks such as protection and safety, remote monitoring and remote control. The adoption of such distributed mechanisms has been a driver to interconnect substations via dedicated fiber links, either independently built or directly placed along with the power lines. Due to the low additional cost, fiber links are placed together with most new or refurbished power lines. SDN-SG aims to use these links to build a communication backbone, which will likely have a topology that resembles the topology of the power grid.

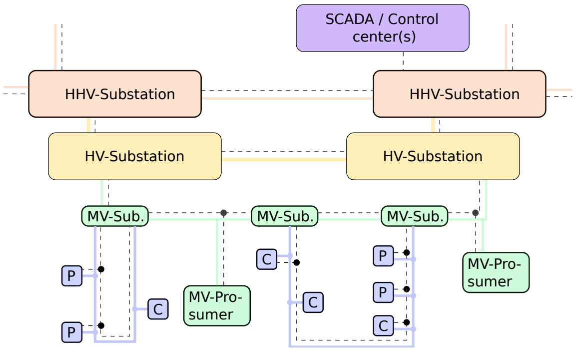

Fig. 1. Smart grid physical topology. Dashed lines represent fiber, solid lines power lines. Producers (P) and consumers (C) on lower levels. Colors show the different voltage levels. Communication across substations is possible.

Fig. 1 sketches a typical physical topology of a power grid. A redundant hierarchical topology with high voltage substations, interconnected over large distances. Lower voltage grid segments always have redundant connections to the higher voltage levels. For example, the high voltage (HV) segment (yellow) can be supplied by either HHV-Substation. This redundancy is compulsory in the power grid and is also utilized in SDN-SG, i.e., in the communication backbone. If a link fails, an alternative route to the higher level should always be available through other substations.

III. SDN-DEPLOYMENT

The most crucial requirements regarding the smart grid and, thus, for its communication backbone are robustness and resilience. Therefore, SDN-SG has to be built in such a way, that it can withstand large scale failures and can reorganize itself autonomously. The following main characteristics of SDN-SG support this: (i) autonomously operating control domains, (ii) topological and packet redundancy, (iii) unimpeded communication paths, and (iv) resource reservation and traffic differentiation.

SDN-SG organizes the communication backbone in so-called **control domains**, which are independently controlled, autonomously operating SDN-subnetworks. This way, a logically centralized SDN controller that could lead to a single point of failure is avoided for the overall smart grid. Even utilizing physically distributed controllers, requiring global,

This work was supported by funding from the topic 46.23.02 Engineering Security for Energy Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

consistent state bares the risk of proliferating crashes. Within SDN-SG, the SDN-controllers of the control domains are organized in a distributed peer-to-peer fashion.

A key challenge is to make SDN-SG scalable to span countries with thousands of domains. The separation into control domains is one step in this direction. In addition, SDN-SG moves away from a complete, shared view of the network and utilizes the topology to aggregate information hierarchically. This requires aggregation schemes for the distributed mechanisms fulfilling the above outlined characteristics. These schemes have to be self-organizing to fulfill the resilience requirements.

SDN-SG explores **redundancy** in order to provide zero-loss failover for critical power grid control functions such as protection or failure compensation mechanisms. Two types of redundancy are supported: **topological redundancy** as outlined in section II and **packet redundancy**, that can be achieved through packet (de-)duplication mechanisms.

In order to make use of topological redundancy, multipath routing is applied which establishes appropriate communication paths across multiple control domains. This includes path establishment and resource reservations along these paths to ensure availability in critical conditions. Additionally, packet (de-)duplication mechanisms are applied for the communication across control domains. Communication packets belonging to safety critical communications will be transmitted multiple times (i.e., duplicated) along these redundant paths. At the receiver, deduplication is needed in order to filter redundantly received packets. Keep in mind that this (de-)duplication is applied for communication across substations and not just within substations as done with current redundancy mechanisms such as HSR (High availability Seamless Redundancy). Altogether, the redundancy mechanisms of SDN-SG shall support zero-loss failover across domains.

The critical control functions will not only require the higher reliability offered by SDN-SG´s redundancy mechanisms, but also **timely delivery** of communication packets. In order to achieve this across substations, **unimpeded communication paths** are favorable, i.e. communication paths without any non-deterministic and latency-increasing devices, such as gateways and firewalls. SDN makes it possible to dynamically filter the incoming and outgoing traffic and direct it to a firewall or filtering gateway when necessary, without introducing additional delay for critical control functions. However, in order to achieve this across substations, deviations from the IEC 61850 standard and the expectation of isolated substations are necessary.

Typically, the station bus (as defined in IEC 61850) and the internal components are connected via a gateway and wide area network (WAN) to the global SCADA system (Fig. 2, left). This is currently sufficient, since substations handle most if not all control operation internally. For critical control functions, the dedicated links introduced in section II are used to enable dependable communication on the bay level, independently of the substation network and the connection to the central SCADA. With the increasing delay and coordination requirements of an increasing number of control functions, having dedicated links is no longer practical. SDN-SG intends to remove this distinction and utilizes the existing dedicated links to interconnect substations at station bus level - without a gateway (see Fig. 2, right) - to form SDN-SG.

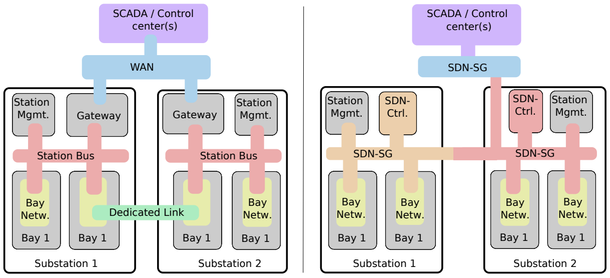

Fig. 2. Substation networks. Left similar to IEC-61850, right with SDN-SG: Gateway removed, controller added, previously dedicated link used as part of SDN-SG, replaces WAN for connection to SCADA.

Lastly, enabling time-critical, reliable inter-domain communication without dedicated links requires mechanisms to ensure that timing-requirements are met (or an inability to meet them is at least registered). With the SDN-SG managed paths, **traffic differentiation** in all parts of the network shall be possible. It is expected that, while intra-domain communication may require hard real time assurances and might require fine-grained mechanisms, such as the ones offered by TSN (Time Sensitive Networking), inter-domain traffic will have less stringent delay requirements. Applying TSN across domains might even have negative effects in cases of misconfiguration or time synchronization errors. The less stringent delay requirements shall be satisfied by employing the gained visibility and control of SDN-SG in combination with **resource reservation** to estimate the link utilization and provide soft real-time assurances. Specifically, high priority traffic has to be reserved on a per-flow basis including the desired assurances. The SDN-controllers involved would try to reserve the desired resources on applicable paths, indicate success or failure to the communicating devices and send periodic state updates.

REFERENCES

[1] Adam Cahn et al. “Software-defined energy communication networks: From substation automation to future smart grids”. In: *2013 IEEE Int. Conf. on Smart Grid Comm., SmartGridComm 2013* (2013), pp. 558–563. DOI: 10.1109/SmartGridComm.2013.6688017.

[2] H. Kazari et al. “Voltage stability improvement through centralized reactive power management on the Smart Grid”. In: *2012 IEEE PES Innovative Smart Grid Tech., ISGT 2012* (2012). DOI: 10.1109/ISGT.2012.6175622.

[3] Mubashir Husain Rehmani et al. “Software defined networks based smart grid communication: A comprehensive survey”. In: *arXiv* 21.3 (2018), pp. 2637–2670. ISSN: 23318422.