Prospects of Software-Defined Networking in Industrial Operations

György Kálmán

Centre for Cyber and Information Security
Critical Infrastructure Protection Group
Norwegian University of Science and Technology
mnemonic AS
Email: gyorgy.kalman@ntnu.no

***Abstract*—Software-Defined Networking (SDN) is appealing not only for carrier applications, but also in industrial control systems. Network engineering with SDN will result in both lower engineering cost, configuration errors and also enhance the manageability of control systems. This paper analyzes the different aspects of SDN in an industrial scenario, including configuration management, security, and path computation. It also shows the possible enhancements to mitigate the challenges related to network segmentation and shared infrastructure situations. The utilization of SDN in traffic-segregation and security measures is identified as one of the possible solutions for the challenges of an internet-connected automation world.**

***Keywords*—automation; infrastructure; manageability; configuration; life-cycle; DCS; SDN; engineering; path computation.**

I. Introduction

The following paper is the extended version of [1], Security Implications of Software Defined Networking in Industrial Control Systems. Industrial Ethernet is the dominating technology in distributed control systems and is planned to take over the whole communication network from office to the field level, with sensor networks being the only exception at the moment.

Since its introduction in time critical industrial applications, Ethernet's performance has been questioned, mainly because of the old, coax networks. Current networks are built using full duplex solutions and automation networks follow: these are built with switches, have plenty of bandwidth and the more demanding applications have their specific technologies. These solutions provide intrinsic Quality of Service (QoS), e.g., EtherCAT or try to implement extensions to the Ethernet standards with e.g., efforts to implement resource reservation like the IEEE 802.1 Time-Sensitive Networking Task Group.

Many of the issues the control system engineering is facing, are not new. From the advent of packet switched networks, QoS and resilience was a question. For metropolitan and Wide Area Networks (WAN), different solutions, like Asynchronous Transfer Mode (ATM) or Multiprotocol Label Switching (MPLS) were developed to allow creation of virtual circuits. These virtual circuits can be a natural representation of the control loops.

With the industry moving towards Commercial Off The Shelf (COTS) products in the networking solutions (both hardware and software) opened for direct interconnection of other company networks towards the automation systems [2], [3]. The problems associated with network performance and resilience are similar to the ones, which e.g., MPLS was built to solve.

The possibility to proceed further with adopting technologies developed for WAN or telecommunication use is in large part enabled by the extended use of COTS devices. The common technology enables efficient data exchange, but also opens the possibility to attack the previously island-like automation systems from or through the company network [4].

One of the aspects of such interconnection of systems is that the automation network might be attacked through other systems. For a more structured approach, a possible categorization of attackers is given by [5]:

- Hobbyists break into systems for fun and glory. Difficult to stop, but consequences are low.
- Professional hackers break into systems to steal valuable assets, or on a contract basis. Very difficult to stop, consequences usually financial. May be hired to perform theft, industrial espionage, or sabotage.
- Nation-States and Non-Governmental Organizations (NGOs) break into systems to gather intelligence, disable capabilities of opponents, or to cause societal disruption.
- Malware automated attack software. Intent ranges from building botnets for further attacks, theft, or general disruption. Ranges from easy to stop to moderately difficult to stop.
- Disgruntled employees, including insider threat and unauthorized access after employment.

Engineering efforts have been made to reduce the risks associated with this interconnection, but it only gained momentum after the more recent incidents of e.g., stuxnet and repeated cases of Denial of Service (DoS) incidents coming

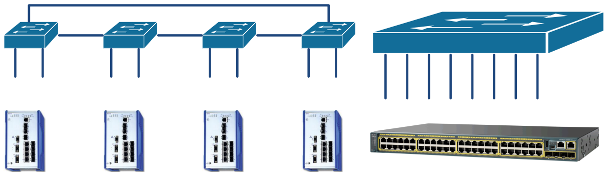

Fig. 1. Low port count switches in automation

from external networks. The first efforts were focused on including well-known solutions from the IT industry: firewalls, Intrusion Detection Systems (IDS), authentication solutions.

The challenge with these solutions is that they were designed to operate in a different network environment [6]. Amongst others, the QoS requirements of an automation system tend to be very different than of an office network. The protocol set used is different and the typical protocol inside an automation system runs on Layer 2 and not on the IP protocol suite [7].

Beside the efforts on adopting IT security solutions to industrial environments, several working groups are involved in introducing security features into automation protocols and protocols used to support an automation system (e.g., IEEE 1588v3 on security functions, IEC 61850 to have integrity protection). The necessity of network management systems are gaining acceptance to support life-cycle management of the communication infrastructure.

In this landscape, SDN is a promising technology [8], [9] to support automation vendors to deploy their distributed control systems (DCS) more effectively, to allow easier brownfield extensions and to have a detailed overview of the traffic under operation [10], [11].

The paper is structured as follows: the second section gives an introduction of Industrial Ethernet and SDN, the third provides an overview of DCS structures, the fourth provides an overview of the security landscape, while the fifth presents an analysis of the impact of SDN on the security controls. The last section draws the conclusion and provides an outlook on future work.

II. State of the Art

Industrial Ethernet is built often as a special mixture of a few high-end switches and a large number of small port count discrete or integrated switches composing several network segments defined by both the DCS architecture and location constraints.

Engineering of networks composed from small switches results in typically a magnitude more devices than a comparable office network (e.g., a bigger refinery can have several hundreds of switches with a typical branching factor of 4-7) as shown on Fig. 1. The engineering cost and the possibility of configuration-related delays has a big impact on competitiveness.

In the majority of cases, the actual configuration of the devices can be described with setting port-Virtual LAN (VLAN) allocations, Rapid Spanning Tree (RSTP) priorities, Simple Network Management Protocol (SNMP) parameters and performance monitoring [12]. These steps currently require manual work.

In a different setting, practically all of these problem scenarios were present previously in the backbone engineering of large networks. The centralized configuration management was present since ATM was launched, offering a control plane for making forwarding decisions and allowing simpler devices inside the network. At that time, the consideration was twofold: one for keeping QoS, but also to reduce complexity of the networking nodes on the transit path. This was at that time forced by the resources available in these nodes. In the current industrial case, the forwarding decision itself is not a resource problem for the local switch or router, but a policy question where resource usage and security considerations play a key role. As a less known alternative, Internet Engineering Task Force (IETF) has defined an entity in RFC 4655 and 5440, called Path Computation Element (PCE).

A. *Path Computation Element*

PCE is a visibility and control protocol for MPLS networks. The protocol partially moves the control plane of the head-end routers to define network paths. The problem for PCE to solve was that the head-end router is expected to both deal with internal routing and external connections. If a complex path computation algorithm is added, it might exhaust the resources of the device.

Compared to SDN, the PCE protocol presents an evolutionary approach. Although an SDN implementation like OpenFlow offers a wider feature set, PCE only requires a change in the head-end routers and not in all routers and switches.

The approach is noteworthy, because it splits the actual tasks of the central element of an Autonomous System (AS) in a way, which is transparent for the rest of the network and allows a change in algorithm complexity without the exchange of the central component. This can be beneficial in equipment with a long expected life, like most of the automation installations.

The focus on head-end routers however makes it less suitable for use in industrial networks, as the majority of communication is done on Layer 2 (in switches), which is outside the coverage of PCE. From the traffic viewpoint, the possibility of per flow control of switch forwarding makes SDN implementations more suitable.

B. *Software-Defined Networking*

The main difference from control systems perspective between PCE and a full SDN implementation is the support for Layer 2. Often, solutions developed for other fields of networking fail on this aspect. In a typical network case, where security, manageability and monitoring has key importance is on Layer 3. Although nodes in the industrial networks typically also have a presence on Layer 3, the focus of communication is on a lower layer [13]–[15].

There are also different driving forces in the centralization of the control plane. In a typical non-automation scenario, centralized flow management is driven by reaching higher forwarding efficiency and is applied in carrier networks [16]. Also, the network reaches higher flexibility by centralizing the forwarding decisions as e.g., QoS requirements might lead to different paths for flows with different requirements but the same source and destination.

SDN capabilities for separating traffic and control on carrier networks can be adopted to the control system scenario. The focus, although, in this case is more on management and the implementation of a call admission control-feature is more interesting. The possibility of deploying new services without disturbing the production network and the appealing possibility of having a full overview of network flows from one central controller is presenting a valid business case [17]–[19].

With SDN, a telecom-like network structure is introduced into distributed control systems with splitting the control and the forwarding plane. In such a network, the flows are programmable through a central entity on the control plane [20]. This allows testing and resource reservation for specific flows, not just at commissioning, but also during operation. The ability to isolate new traffic flows can be beneficial from both security and operational viewpoints. These possibilities are appealing for the industrial automation systems, as they are very much in line with the current trends of redundancy, QoS and shared infrastructure.

As defined by the Open Networking Foundation [21], SDN is or offers

- *Directly programmable* Network control is directly programmable because it is decoupled from forwarding functions.
- *Agile* Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs.
- *Centrally managed* Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch.
- *Programmatically configured* SDN lets network managers configure, manage, secure, and optimize network resources very quickly via dynamic, automated SDN programs, which they can write themselves because the programs do not depend on proprietary software.
- *Open standards-based and vendor-neutral* When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.

SDN architecture is typically represented with three layers, as show compared to a traditional network structure on Fig. 2 and on Fig. 3 by OpenFlow. Using several planes in a communication technology is not new, it was present both in ATM, SDH or all the digital cellular networks. What is new, that these management possibilities are now available also in a much smaller scale. It is expected that a network with a centrally managed control plane can better react on changes in traffic patterns and also be more flexible in network resource management [22]. The forwarding performance is expected to be very similar or equivalent to the current switches used. The industrial applications will be run without disturbance in a stable network state [23], [24].

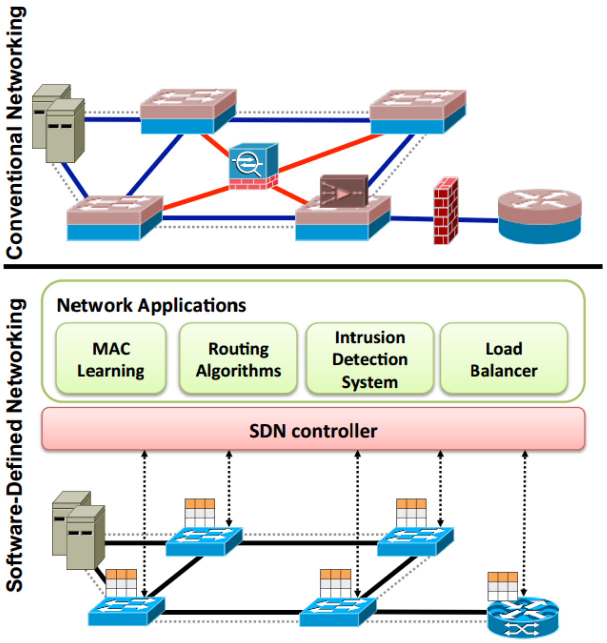

Fig. 2. Traditional network architecture compared to SDN [9]

The normal communication traffic is expected to be significantly larger than the control and signalling traffic generated by SDN and therefore not considered as a performance problem. Also the considered communication on an industrial network supports the mitigation of this performance threat, as most of the sessions are periodic machine to machine (M2M), which can be scheduled or event driven, with precisely defined transmission deadlines. The gaps between planned periodic traffic are rarely filled with event-driven communication.

III. DCS Architecture

Current DCS networks are a result of an evolution from analog wiring towards digital lines, buses and finally networks. Many challenges related to both engineering and operation of industrial networks originate from this evolution like the problematic expression of QoS parameters and the underestimated importance of the communication infrastructure.

The systems considered by this paper are primarily the current Ethernet-based solutions without special (e.g., EtherCAT, PROFINET IRT) hardware support. These networks

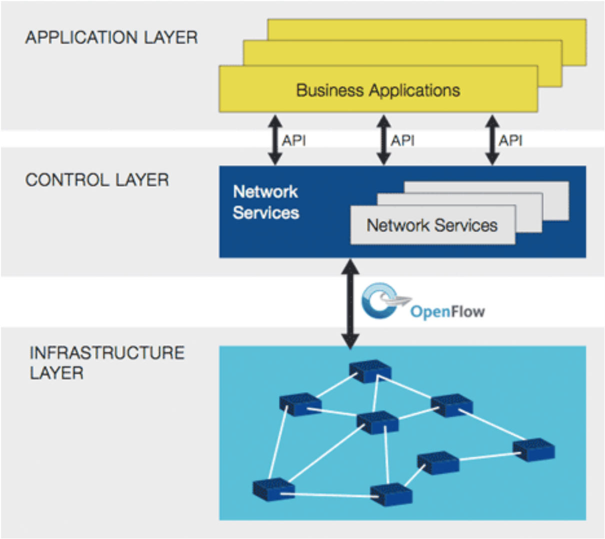

Fig. 3. Three layer SDN architecture [21]

are composed by standard equipment where both the QoS environment, protocols and capabilities used are similar.

The invisibility of the communication infrastructure in the DCS is a constant problem and source of challenges in both engineering and operations. Historically, this was not a seen as problematic, as first there was direct wiring between the components, so failure in the line resulted in immediate errors and typically had no impact on other parts of the system. There was also little change with the bus systems and serial solutions: the communication infrastructure got digitalized, but still it was more the task of an electric technician to create it than one of an IT network specialist.

Current engineering practices still follow manual methods with creating connection lists and per unit configuration. The methods used lead to problems when one has to express situations like shared infrastructure or formalized checking of redundancy.

Traditional Network Management Systems (NMS) are typically not present in industrial deployments, mostly as a result of cost pressure. The existence of the communication infrastructure both in DCS (LAN) or SCADA (WAN) cases is typically hidden from the automation tasks and operations. The separate operation and maintenance of the DCS and the communication infrastructure is inefficient in large scale. With the evolution of control systems, covering more and more processes with integrated solutions, the network complexity is only expected to grow. Thus the current practice of using command line or web interfaces on a per node basis. Even in case of managed equipment (switches, routers), the nodes are configured individually and the efficiency or in more serious cases, the stability of operation is dependent on the communication between the network specialist and the control engineer.

Control systems are traditionally built using a three network levels. The plant, the client-server and the control network. These levels might have different names, but they share the following characteristics:

- *Plant network* is home of the traditional IT systems, like Enterprise Resource Planning (ERP), office services and other support applications. It is typically under the control of the IT department.
- *Client-server network* is the non-time critical part of the automation system, where the process-releated work-places, servers and other support entities are located. It is firewalled from the plant network and is under the control of Operations.
- *Control network* includes everything close to the actual process: controllers, sensors, actuators and other automation components. Typically follows a strict time synchronization regime and contains the parts of the network with time-critical components. It is accessible through proxies from the client-server network and under the control of Operations.

There are some solutions, where network nodes can communicate status and errors to the DCS, but the possibilities are limited and typically the information conveyed is not enough to fully understand the situation. A possible way to reduce visible network complexity is to use unmanaged switches. These devices melt into the network fabric, but also remove the possibility to analyze the network status or troubleshooting of forwarding. In current engineering regimes, unmanaged devices have their usage areas limited to small installations, where managed equipment is prohibitively expensive or where very high reliability is required, as a typical unmanaged switch has nearly ten times longer Mean Time Between Failure (MTBF) time than its managed counterpart.

In most cases, the use of a programmable network is focusing on flow control. This is a typical efficiency-driven effort to ensure, that the network flows are utilizing the resources in an optimized or optimal way. An Internet Service Provider (ISP) or a carrier network will focus on such use. In case of an industrial deployment, the main motivation is not per flow control, although later a use case related to security will be shown. The main motivation however is the possibility to control the network from one centralized entity. This control functionality is expected to be easily understandable and acceptable by operations, as it can be compared to a Programmable Logic Controller (PLC), the very base of an automation system: an SDN controller operates in a very similar way, telling if the traffic should slow or take a different direction, than a PLC, which can tell a valve to open or close and can regulate the flow of materials or changing the speed of a drive.

SDN concepts have the possibility to streamline the network operations and enable diagnostics with more possible points of entry and a wider tool set [25]. With communication paths controlled through the vertical of the industrial network, it would be possible to create end-to-end QoS links within a system. This would allow more control and continuous monitoring of the network performance. The simplification of configuration and implementation of network architectures with possible use of templates and macro building blocks may both lower engineering costs and lead to higher performance. Also the need of network specialists in operations will be lower as the centralized control is assumed to require less (physical) presence than today's situation with may be hundreds of switches on the plant floor, each of them uniquely configured.

The transition to programmable network on the plant floor is expected to shorten the time needed to identify and locate a problem and to ease tension between operations and IT. With the control plane moved to a central entity, the technician can exchange the identified faulty unit with one having default configuration and, which can be configured by the SDN controller. The automatic configuration also represents a mitigation for some cases of physical misconfiguration of cables.

The centralized management of adding or removing network devices can enable currently unavailable dynamism in an industrial context: it would be possible to reconfigure the network topology to adopt to new situations or tasks.

Real-time Ethernet also represents an area, where SDN can have a positive impact. In the current situation, either an industrial Ethernet technology with intrinsic QoS is used or the network only can give a probabilistic guarantee on delivery. Current engineering practice is, that these network parts are configured once and run without reconfiguration for extended periods, only changed when necessary. This operational regime is acceptable with smaller network segments, but does not scale. Using SDN to control the forwarding of real-time flows can have definitive advantages: continuous evaluation of the Service Level Agreement (SLA), immediate reaction at link failure, prioritization of time sensitive traffic and the possibility to integrate new technologies in a transparent way (e.g., IEEE 802.1AV). To be able to give a deterministic guarantee (upper bound) on forwarding delays, the SDN controller needs to have a connection to real time. This is not a priority in a carrier environment and a feature, which needs to be developed. The main potential of SDN in this case is, that since the forwarding decisions are not being made on a per hop and per frame basis, the traffic situation of a switch has less influence on the jitter and delay of the communication.

The complete view of network paths also allows the controller to choose the optimal route per flow also in a larger environment: time sensitive traffic might be forwarded on an express path and less sensitive on a more economic path, very much implementing the different traffic classes of IntServ.

In case of link failure, the controller can reroute the flow (depending on the SLA) to a precalculated backup path or to a newly calculated alternate route. Precalculated backup paths can also be used as a hot standby with actual forwarding on two independent routes. Following the actual status of the network, an SDN controller can also monitor if the backup routes can still fulfill their tasks. This feature can protect again cascading effects of link failures: the backup routes shall be able to carry all the traffic they carry by default and in addition the traffic of the primary route.

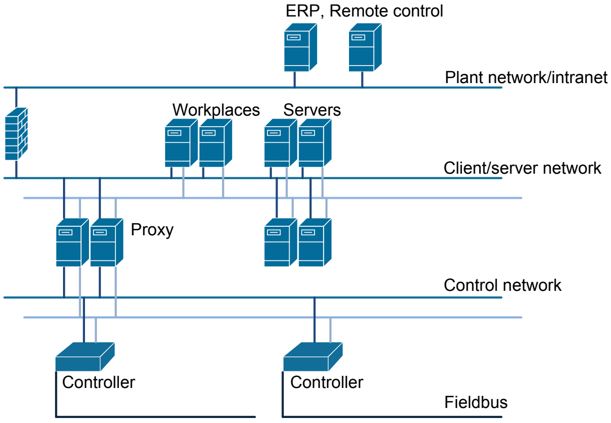

Fig. 4. Traditional DCS network architecture

Since the SDN controller also has a complete view of the network and enough resources, it might precalculate independent backup routes for most of the network flows. Having alternatives ready might considerably reduce the recovery time of the network.

Faster reaction times and status monitoring of the network is also useful in case of node failures. In this case, SDN can again provide better functionality than current solutions. It is not only possible to spot the problematic node, but the system can also show if it is possible to isolate the faulty device with keeping the current SLAs for the involved traffic flows or if now, then, which QoS parameters are achievable.

One of the possible limiting factors of SLA creation and QoS parameter setting is, that traditionally, parameters of a control loop are expressed with different measures.

A. *Control loop parameters*

Requirements definition for the communication network is one of the actual challenges in automation. An example IEC 61850 control loop would be defined as: having a sampling rate of 80 samples per cycle (4800 Hz for 60 Hz networks), with sampling 16 inputs, 16 bit per sample. Event-based traffic is negligible compared to the periodic traffic.

If there is a requirement for synchronous operation, time precision (quality) can also be a QoS metric. Redundancy requirements can lead to topologies, which are unusual in a normal network infrastructure: first, the use of Rapid Spanning Tree Protocol (RSTP) to disable redundant links, second the general use of loops (rings) in the network to ensure that all nodes are dual-homed. With dual-homing, the network can survive the loss of one communication link without degradation in the service level. Path calculation algorithms created for generic network use might not support such constellations.

From the network viewpoint, this control loop will introduce a traffic flow, with a net ingress payload stream of approx. 98Mbps. The sampling will generate 2560 bytes of traffic each second, which can be carried by at least two Ethernet frames, thus the system can expect at least approx. 10000 frames per second. The traffic will be forwarded on a horizontal path to the controller. On the ingress port to the backbone, it will enter with approx. 110 Mbps (header+payload). The traffic flow will be consumed at the egress port to the controller.

For SLA composition, either a definition of the traffic is needed in forehand or the classification at the SDN controller needs to be dynamic: the controller has no information at the first ingress frame, which frequency or payload length will be typical.

The information on the flows is not only beneficial for resource management. Precisely defined traffic flows (which is a possibility in industrial applications) can create an excellent base for configuring and implementing network security functions, like Intrusion Detection Systems or actual firewall configurations.

B. SCADA and grid operations

With interconnection of previously isolated locations, in addition to the traditional Supervisory Control And Data Acquisition (SCADA) operations, industrial wide area networks are being deployed.

Maybe the most important in the current European landscape is the effort to add more intelligence and dynamism into the electric grid control: creation of smart grids. Current grid communication networks are based on standard IP networking, where network parameters and configuration are defined at the design phase, the same process as in DCS. When the network is in operation, and in this sense, the grid control is always expected to be in operation with the possibility to have planned maintenance stops. Dynamic changes outside these planned stops tend to be problematic, both from economic and supply security viewpoint. Such a rigid setup on the other hand can be problematic in the expected dynamic environment of the smart grid: where plants and consumers should communicate about the power generation and usage, bandwidth and path selection parameters might change under operation.

SDN is expected to be able to deliver appropriate QoS, since the network parameters in steady state will not considerably differ from a static network. The more important aspect is how SDN could enhance system resilience. The features are similar of those in case of a DCS and show the scalability of SDN in this perspective. The first one is the possibility of precalculated backup paths, then the possibility to isolate a node if there is a chance, that it got compromised or failed. Then an additional feature might be to reroute the control information over the public internet. This possibility could give a highly independent backup route, where the necessary flows could be rerouted with applying appropriate encryption and integrity protection.

There is also a possibility for coordinated actions between the SDN controller, the security measures (firewall, IDS) and the SCADA control.

IV. Security landscape

Industrial deployments were built traditionally as isolated islands, thus security was more a question of doors and walls then IT [5]. Employees from the operations department had the responsibility to keep the communication network intact.

Security issues connected to computer networks came with, amongst others, the SCADA applications, where remote access to industrial deployments was granted. With the spread of Ethernet and IP-based communication, more and more automation networks could be connected to other networks, to allow easier management and new applications.

Threat analyses showed that industrial systems can be more prone to DoS and related attacks due to the more strict QoS requirements and lack of available processing power in the devices [26]. Typically the deployed network infrastructure can handle a magnitude higher traffic than the end-nodes. This helps in supporting the SDN operation with allowing the traffic, which does not match any of the forwarding rules to be sent to the controller in the normally unused bandwidth. The static traffic picture will also allow the use of sharp heuristics on new traffic, categorizing unknown traffic very early as malicious and drop it early.

DoS attacks require no knowledge of the automation system, only access to the infrastructure, which is a much larger attack surface this case as DCS and especially SCADA systems have a tendency to cover large areas, where enforcing of a security policy (both physical and cyber) is a hard task [27].

This properties have focused the security efforts on protecting the leaves of the network and also on creating policies to ensure the use of hardening practices.

Standard hardening procedures in current industrial deployments include:

- Creation of a *Security Policy* following e.g., the IEC 62443 standard. This allows to have a structured approach for operating the network.
- A standard way to introduce anti-virus solutions in the automation network using central management.
- Specific focus on the configuration of server and workstation machines with e.g., policies and additional software components.
- Access and account management: using Role-Based Access Control (RBAC), OS functions like the Group Policy Object (GPO) or tools like a trusted password manager.
- Backup and restoration as a part of disaster recovery.
- Network topology to support security levels in the IEC 62443, with using firewalls as separator.
- Specific remote access solution and whitelisting of both traffic and nodes.

These tasks show that the there is an understanding of the importance of security in this field and there are efforts on standardization.

The problematic part of the process is, where these guidelines, policies and physical appliances need to be deployed in a new or an existing installation.

Correctness of the implementation is crucial for future reliability of the system. In a typical current workflow, configuration and deployment of devices is a manual task together with the as-built analysis under or before the factory acceptance test (FAT). At the moment there is no merged workflow and software support for all of the steps mentioned earlier.

SDN can be part of the answer: the communication infrastructure, communication security and monitoring under operation can be implemented using SDN, where the whole or part of the tasks could be automated [28], [29].

V. SDN-related challenges

SDN changes the security model considerably. To enable automatic features, the operation and the way of controlling a SDN system has to be analyzed in the industrial context.

A. The plane structure

After the author's view, the introduction of the separated control and forwarding plane is the biggest enhancement for network security in this relation. In the telecommunication field, separated planes are used since decades to support secure service delivery with minimizing the possibility of a successful attack from the user side towards network management.

In an industrial context, the split planes mean, that the configuration of the devices is not possible from the network areas what clients can see, thus intruders getting access to e.g., the field network through a sensor, will not be able to communicate with the management interfaces.

Attacks at the data plane could be executed with e.g., gaining access to the network through a physical or virtual interface and try to execute a Denial of Service (DoS) attack or a type of fuzzing attack, which might exploit a flaw in the management or automation protocols.

An attacker could also leverage these protocols and attempt to instantiate new flows into the device's forwarding table. The attacker would want to try to spoof new flows to permit specific types of traffic that should be disallowed across the network [30].

B. The SDN controller

The first group of issues are related to the SDN controller. To allow a central entity to control and configure the whole network, it has to gain administrative access over the whole network infrastructure configuration and status. Thus the SDN controller's ability to control an entire network makes it a very high value target.

The SDN controller has predefined interfaces towards other systems:

- Northbound application programming interfaces (APIs) represent the software interfaces between the software modules of the controller platform and the SDN applications. These APIs expose universal network abstraction data models and functionality for use by network applications.
- East-West protocols are implementing the necessary interactions between the various controllers.
- Data plane and southbound protocols: the forwarding hardware in the SDN network architecture.
- Communicate with the network infrastructure, it requires certain protocols to control and manage the interface between various pieces of network equipment.

This can be problematic if the controller has to cross several firewalls to reach all nodes under its control. In the traditional DCS network architecture (Fig. 4) in order to gain control of the whole network, the controller has to pass the firewall between the plant and the client-server network, the proxy towards the control network and the controllers towards the field devices.

In a realistic situation, the controller of the DCS will not be allowed to control also the plant network, but is expected to reside inside the DCS, most probably on the client-server network. Inside the automation network, firewalls and the controllers can be configured so, that they pass the SDN signaling.

Network intelligence is being transferred from the network nodes to the central controller entity. This, if being implemented inside a switched network, might only be a semantic difference in network control, as it extends the possibilities of a NMS, but it does not need to integrate more sophisticated devices in an industrial situation.

It is expected that a network with a centrally managed control plane can better react on changes in traffic patterns and also be more flexible in network resource management.

In addition to the attack surface of the management plane, the controller has another attack surface: the data plane of the switches. When an SDN switch encounters a packet that does not match any forwarding rules, it passes this packet to the controller for advice. As a result, it is possible for an attacker who is simply able to send data through an SDN switch to exploit a vulnerability on the controller [31].

Attacks directed against the controller can for example aim to destruct the topology by taking control over the path calculation. A compromised SDN controller may change the configuration of the communication devices. This can put keeping the SLAs in danger.

The standard SDN controller behavior of getting all the frames forwarded, which were not classified already at ingress, can lead to DoS attacks.

To mitigate the single-point-of-failure what the SDN controller represents, in most installations, it will be required to deploy two of the controllers in a redundant installation.

Also shared infrastructure between different operators can be a problem in this case. Legal issues might arise if the audit and logging of SDN-induced configuration changes is not detailed enough.

C. Service deployment security

In an SDN case, the controller entity can change the configuration and forwarding behavior of the underlying devices. This possibility is a valuable addition to the existing set of features, because an SDN system could deploy a new service without disturbing the current operation, which would reduce costs related to scheduled downtimes.

Also, the fine-grained control of network flows and continuous monitoring of the network status offers a good platform for IDS, Managed Security Services (MSS) or a tight integration with the higher operation layers of the DCS.

D. Central resource management

Currently, SNMP-based NMSs are widely used for monitoring the health and status of large network deployments. Using SDN could also here be beneficial, as the monitoring functionality would be extended with the ability of actively changing configurations and resource allocations if needed.

One of the most significant technological and policy challenges in an SDN deployment is the management of devices from different providers. Keeping the necessary complexity and configuration possibilities is hard to synchronize with entities delivered from different providers.

With SDN's abstraction layer one can hide differences in features but also can introduce problems in logging and audit. Network equipment manufacturers are not supporting by default that their devices are managed by a third party.

Although, the rollout of new services would become safer, as the system could check if the required resources are available and the use of SDN is not expected to have a negative impact on the reliability of the network the problems related to shared infrastructure need to be elaborated further.

E. Security implications of shared infrastructure

As part of the universal use of Ethernet communication, it is now common for vendors to share the network infrastructure to operate different parts of an installation. An example is a subsea oil production platform, which is controlled through a hundreds of kilometers long umbilical, can have a different operator for the power subsystem, an other one for the process control and a third one for well control.

In the current operation regimes, the configuration of the networks is rarely changing and all vendors have a stable view of their part of the network shared with the one being the actual operator. With SDN, the network could be controlled in a more dynamic way.

From the technological viewpoint, the biggest challenge is to find a solution, where both the controller and the devices support encrypted control operations. If they support it, than the logging and audit system has to be prepared for a much more dynamic environment.

From a policy management viewpoint, the possibility of fast per-flow configuration opens for new types of problems: the valid network topology and forwarding situation might change fast and frequently, which is not typical in the industry. Logging has to provide the current and all past network configurations with time stamping to allow recreation of transient setups in case of communication errors.

In such a shared case, the use of SDN could reduce risk in topology or traffic changes, as vendors could deploy new services without an impact on other traffic flows in the network. It is possible to create an overlay network, which follows the logical topology of an application or subsystem. This would improve the control possibilities as the staff could follow the communication paths in a more natural way.

F. Industrial safety

Conversations on Safety Integrated Systems (SIS) mainly include questions on QoS. The cause is that these installations share the communication network between the automation task and the safety function (as they can also share infrastructure with the fire alarm system). In a safety sense, SIS have no QoS requirements. The safety logic is built in a way, that a communication error is interpreted as a dangerous situation and the safety function will trip. So the system avoids dangerous situations at the expense of lower productivity and availability.

Safety as such is an availability question and through availability, it implies QoS requirements on the automation system as any other communication task. Special treatment is not required.

Safety systems are classified into 4 levels, Safety Integrity Level (SIL) 1 to 4. The different levels pose well-defined requirements towards the system. These integrity levels cover all aspects of the system, including hardware, software, communication solution and seen in contrast with the application. A similar approach could be also beneficial for formalizing the relationship between the automation application and the bearer network.

The IEC 61508 standard requires that each risk posed by the components of the safety system is identified and analyzed. The result of the risk analysis should be evaluated against tolerability criteria.

Coverage of safety communication is not only important in itself, but also because many of the processes used in safety can be used effectively in deploying security measures, where the vocabulary and test methods of functional safety help.

G. Wireless integration

Another key field currently is the integration of wireless networks into industrial deployments. SDN could help with integration of wireless technologies by checking if the needs of a new service e.g., can be satisfied with a path having one or more wireless hops or a new rule has to be deployed into the network to steer the traffic of that service on a different path.

H. Integrating Security in the preliminary design

In the bidding phase, the control engineer could leave the planning of the network on a high level with having an SDN rule set to check if the network can be built. The needed security appliances and other entities would be added to the list of required components following rules developed using the relevant standards.

The control engineer could add the control processes and the SDN software will check if the required resources are available on the communication path. In contrast with current methods, the acceptance of a communication session would also give a proof that the required resources are available and the security requirements are met.

I. Network simulation and capacity estimation

The use of SDN and the central management entities will also lead to more detailed information on network traffic and internal states. The data gathered on operational network not only supports the management of the current network, but also can be used to fine-tune the models used in early steps of bidding and planning and can lead to a more lean approach on network resource allocation. SDN could provide better communication security by helping to avoid overloaded network situations.

J. Firewalls

A current limitation on the coverage of SDN is connected to accountability. While automatic changes in the forwarding table on layer 2 is not expected to cause big problems, automatic rule generation for firewalls and other higher layer devices might cause more problems than it solves.

Granting the control rights of network security devices to the SDN controller is necessary to gain full control over all network nodes. The challenge with this setup is, that L2 forwarding can be described with relative few properties, routing tables with some more, but still within a limited size, firewall rules can contain a lot more properties and values to fill. If automatic generation is disabled, then the SDN network split into several security zones can only be partially managed by the controller. If automatic generation is enabled, it can cause security breaches (e.g., the early implementations of Universal Plug and Play (UPnP)). This setup also potentially requires cooperation from several companies, e.g., an MSS provider running the security infrastructure and the operations staff at the location focusing on automation.

From the practical viewpoint, there are several issues. The first is that in most cases, management protocols only offer the implementation of security functions, but they are optional, so having a required encryption (one cannot avoid this when managing firewalls) might result in incompatibility already in the communication. The second is, that one needs much more complex support for firewalls in the management software than for switches or routers.

K. Intrusion Detection Systems

Running IDS in an SDN network is promising. The IDS can notify the SDN controller upon detecting anomalies in the traffic, so that the controller can reconfigure the network accordingly. In addition, the SDN controller can also feed information about legitimate flows to the IDS, enabling the creation of a detailed whitelist.

Current IDS implementations typically use distributed wiretaps or other traffic monitoring sources to watch for malicious traffic and might get aggregated traffic information (e.g., over NetFlow).

SDN can take this functionality into a whole new level. The controller has a complete view of the L2 traffic streams over the whole network, thus not only has a wiretap *everywhere*, but also has the control of the forwarding entities: it can make changes in the forwarding decisions in real time. In extreme cases this can result in, that the malicious packet cannot even travel through the network to its destination, because at the entry the IDS system classifies it as potentially malicious and in transit redirects it into an isolated network.

Industrial deployments are an excellent basis to develop such a fast-reaction IDS: the communication is typically M2M, the network traffic is stationary (whole-new traffic flows are not typical) and the topology is mostly static. The heuristics of the IDS could be as a result, very sensitive on non-planned traffic, thus reacting fast on potential hazards.

If the SDN infrastructure is available because of network management, the extension of providing IDS and firewall management can also lead to cost reduction compared to deploying and operating a separate solution for both.

L. Protecting the SDN controller

As it was mentioned earlier, the SDN controller represents a single-point-of-failure in the network. As most of the industrial deployments are redundant, it is natural to require also a redundant deployment of the SDN controller.

This redundancy is required both from the availability viewpoint (all crucial components have redundant counterparts in most deployments) and also from network security: protection from e.g., DoS attacks.

Transport security shall be ensured with up to date standard protocols, e.g., TLS for web access or SSH for shell. An effort shall be used to keep the cryptographic suites, which are used by these protocols updated.

VI. Conclusion

SDN is very likely to be the next big step in industrial networks, both on LAN and WAN level. It offers exactly the functionality automation engineers are looking for: hiding the network and allowing the planning and deployment of network infrastructure without deep technical knowledge, based only on definition of network flows and automatic dimensioning rules.

With a complete view over the current network traffic situation, QoS parameters can be checked in a formal way with the help of the central management entity and as such, provide a proof in all stages of the engineering work, that the infrastructure will be able to support the application.

In brown field extensions SDN can reduce risks associated with deploying new equipment and extending the current infrastructure because of the isolation of traffic flows and the complete control over the forwarding decisions.

Network security is the other main area, where, if properly planned and implemented, SDN can provide a big step forward in both security and operational excellence. With the real-time overview on the network infrastructure, an SDN-based IDS could react much faster on attacks.

Technological advancements are clearly moving towards a more automated network infrastructure and in the industrial case, SDN is a promising technology, which has to be taken seriously.

REFERENCES

[1] Gy. Kalman, ”Security Implications of Software Defined Networking in Industrial Control Systems,” IARIA ICCGI 2015, St. Julians, Malta

[2] N. Barkakati and G. C. Wilshusen, ”Deficient ICT Controls Jeopardize Systems Supporting the Electric Grid: A Case Study,” Securing Electricity Supply in the Cyber Age, Springer, pages 129-142, e-ISBN 978-90-481-3594-3

[3] Gy. Kalman, ”Applicability of Software Defined Networking in Industrial Ethernet,” in Proceedings of IEEE Telfor 2014, pages 340-343, Belgrade, Serbia

[4] ABB, ”Security for Industrial Automation and Control Systems,” White Paper, ABB, Doc. Id. 3BSE032547

[5] M. McKay, ”Best practices in automation security,” White Paper, Siemens, 2012.

[6] Cisco, ”Secure Industrial Networks with Cisco,” White Paper, 2015., http://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/white-paper-c11-734453.pdf, Accessed 30.08.2015.

[7] C. Alcaraz, G. Fernandez, and F. Carvajal, ”Security Aspects of SCADA and DCS Environments,” In Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense, LNCS 7130., Springer, pp. 120-149, September 2012.

[8] M. Jammal,T. Singh, A. Shami,R. Asal, and Y. Li, ”Software-Defined Networking: State of the Art and Research Challenges,” ArXiv e-prints 1406.0124, May 2014.

[9] D. Kreutz, F. Ramos, P. Verissimo, C. Rothenberg, S. Azodolmolky, and S. Uhlig, ”Software-Defined Networking: A Comprehensive Survey,” Proceedings of the IEEE, Volume: 103, Issue: 1, January 2015

[10] D. Cronberger, ”The Software-Defined Industrial Network,” The Industrial Ethernet Book, Issue 84, Pages 8-13, 2014.

[11] D. Cronberger, ”Industrial Grade SDN,” Cisco, 2013, http://blogs.cisco.com/manufacturing/industrial-grade-sdn, Accessed 28.05.2015.

[12] A. Gopalakrishnan, ”Applications of Software-Defined Networks in Industrial Automation,” https://www.academia.edu/2472112/Application_of_Software_Defined_Networks_in_Industrial_Automation, Accessed 28.05.2015.

[13] M. Robin, ”Early detection of network threats using Software Defined Network (SDN) and virtualization,” Master’s thesis, Carleton University, Ottawa, 2013

[14] B. Genge and P. Haller, ”A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems,” IFIP Networking Conference and Workshop, 2016

[15] G. Ferro, ”SDN and Security: Start Slow, But Start,” Dark Reading Tech Digest, 2014, http://www.darkreading.com/operations/sdn-and-security-start-slow-but-start/d/d-id/1318273, Accessed 28.05.2015.

[16] D. D’souza, L. Perigo, and R. Hagens, ”Improving QoS in a Software-Defined Network,” University of Colorado, Boulder, Capstone 2016 Interdisciplinary Telecom Program, 2016, http://www.colorado.edu/itp/current-students/capstone-and-thesis/spring-2016-capstone-team-projects/capstone-2016-improving-qos, accessed 08.09.2016

[17] Fujitsu White Paper, ”Software-Defined Networking for the Utilities and Energy Sector,” 2014

[18] X. Dong, H. Lin, R. Tan, R. Iyer, and Z. Kalbarczyk, ”Software-Defined Networking for Smart Grid Resilience: Opportunities and Challenges,” Position Paper on CPSS 2015, April 14-17. 2015, Singapore

[19] D. Cronberger, ”Software-Defined Networks,” Cisco, 2014, http://www.industrial-ip.org/en/industrial-ip/convergence/software-defined-networks, Accessed 28.05.2015.

[20] HP, ”Network functions virtualization,” White Paper, Hewlett-Packard, 2014

[21] Open Networking Foundation, ”Software-Defined Networking: The New Norm for Networks,” white paper, https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf, Accessed 28.05.2015.

[22] W. Braun and M. Menth, ”Software-Defined Networking Using OpenFlow: Protocols, Applications and Architectural Design Choices,” Future Internet, Volume 6, Issue 2, Pages 302-336, 2014

[23] P. Hu, ”A System Architecture for Software-Defined Industrial Internet of Things,” IEEE International Conference on Ubiquitous Wireless Broadband, ICUWB, 2015

[24] T. Mahmoodi, V. Kulkarni, W. Kellerer, P. Mangan, F. Zeiger, S. Spirou, I. Askoxylakis, X. Vilajosana, H. Einsiedler, and J. Quittek, ”VirtuWind: virtual and programmable industrial network prototype deployed in operational wind park,” Transactions on Emerging Telecommunications Technologies, Volume 27, Issue 9, Pages 1281-1288, Wiley, 2016

[25] J. Du and M. Herlich, ”Sofware-defined Networking for Real-time Ethernet,” 13th International Conference on Informatics in Control, Automation and Robotics, July 2016, Lisbon, Portugal

[26] R.C. Parks and E. Rogers, ”Best practices in automation security,” Security & Privacy, IEEE (Volume:6 , Issue: 6), pages 37-43., 2009.

[27] I. Fernandez, ”Cybersecurity for Industrial Automation & Control Environments,” White Paper, Frost&Sullivan and Schneider Electric, 2013.

[28] R. Millman, ”How to secure the SDN infrastructure,” ComputerWeekly, 2015, http://www.computerweekly.com/feature/How-to-secure-the-SDN-infrastructure, Accessed 28.05.2015.

[29] Open Networking Foundation, ”Solution Brief: SDN Security Considerations in the Data Center,” ONF, 2013, https://www.opennetworking.org/images/stories/downloads/sdn-resources/solution-briefs/sb-security-data-center.pdf, Accessed 28.05.2015.

[30] S. Hogg, ”SDN Security Attack Vectors and SDN Hardening,” Network World, 2014, http://www.networkworld.com/article/2840273/sdn/sdn-security-attack-vectors-and-sdn-hardening.html, Accessed 28.05.2015.

[31] D. Jorm, ”SDN and Security,” The ONOS project, 2015, http://onosproject.org/2015/04/03/sdn-and-security-david-jorm/, Accessed 28.05.2015.