Cyber Security Considerations for Self-healing Smart Grid Networks

Martin Gilje Jaatun*, Marie Elisabeth Gaup Moe*, Per Erik Nordbø†
*SINTEF Digital, NO-7465 Trondheim, Norway
†BKK Nett, Bergen, Norway

***Abstract*—Fault Location, Isolation and System Restoration (FLISR) mechanisms allow for rapid restoration of power to customers that are not directly implicated by distribution network failures. However, depending on where the logic for the FLISR system is located, deployment may have security implications for the distribution network. This paper discusses alternative FLISR placements in terms of cyber security considerations, concluding that there is a case for both local and centralized FLISR solutions.**

I. Introduction

The modern power system consists of 4 main actors: 1) The power generators (hydroelectric, nuclear, fossil fuel etc.), 2) the Transmission Service Operators (TSOs) that do longhaul transportation of electricity to the 3) Distribution Service Operators (DSOs), who distribute electricity to the 4) consumers (see Fig. 1). Considering the increasing pressure on DSOs to operate their distribution network efficiently, and the trend towards zero tolerance among customers that blackout events occurs, automated Fault Location, Isolation and Service Restoration (FLISR) solutions, and in particular Fast Local FLISR solutions, are attractive in areas where local energy storage / production is not available or practical (FLISR systems also contribute positively to field service personnel safety, but that is not the focus of this paper). This in turn requires that FLISR solutions must be built on best practice cyber security principles and organizational security procedures to prevent cyber-attackers from taking down large portions of well-functioning parts of the distribution network.

Supervisory Control And Data Acquisition (SCADA) networks in power distribution networks have traditionally been isolated, making cyber-attacks if not impossible, then at least very improbable. The last decade's developments in Smart Grid technology have however changed this, and it can no longer be assumed that there is no communication link to the outside world, as illustrated in Fig. 2. The admin network serves functions such as network planning, customer relations, and field service management. Of particular interest is the current reliance on Network Information Systems (NIS)/Geographic Information Systems (GIS), which contain crucial information on the physical topology of the distribution network; NIS/GIS solutions are typically sourced from third-party providers, but need to be imported to a DSO-specific NIS variant connected to the DMS. This implies that there is a connection from the admin network to the DMS network, as illustrated on the right of Fig. 2.

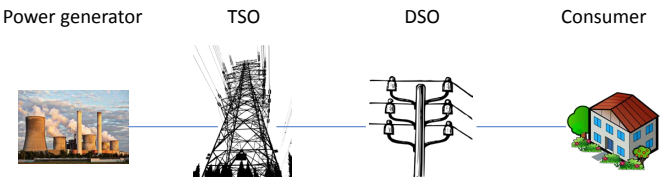

Fig. 1. The modern power system

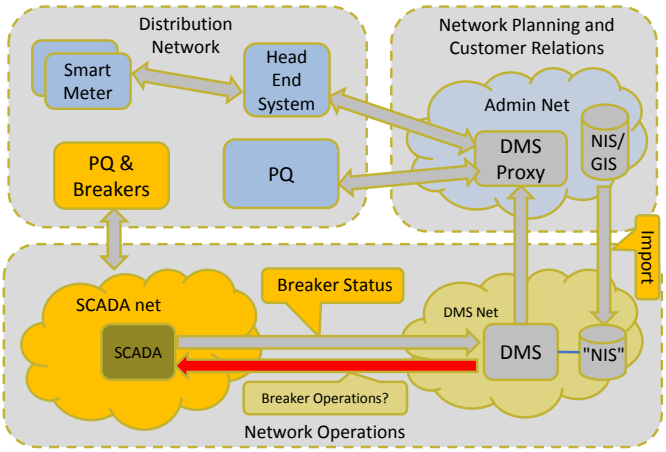

Fig. 2. Network architecture

Smart Grid networks are facing many cyber security challenges [1], [2], and increased interconnection will inevitably add to these challenges. SCADA systems with remote connectivity can be compromised and infected with malware, as demonstrated in the Ukraine power grid cyber-attacks[3].

The Distribution Management System (DMS) is the workhorse of the DSO, enabling real-time monitoring and control of the distribution grid, typically from the DSO control room. In this paper, we address the particular challenge of how self-healing mechanisms affect the cyber security of the SCADA and DMS. We will discuss pros and cons of three alternative configurations:

- Centralised self-healing
- Decentralised self-healing

- Local self-healing

The research has been carried out in collaboration with Distribution Service Operators (DSOs) that are in the process of evaluating different future Smart Grid solutions for FLISR systems, where how to implement cyber security and data protection is a key issue.

II. Background

In this section we will first briefly cover existing work on cyber security relevant to the power grid, and then provide a primer on FLISR.

A. Related Work on SCADA Cyber Security

The first incident that brought SCADA cyber security to the forefront of public attention was the Stuxnet compromise at Iran's Bushehr nuclear power plant in 2010 [4], where uranium enrichment centrifuges were rendered inoperable after malware modified vital parts of the Human-Machine Interfaces (HMIs) and Programmable Logic Controllers (PLCs). However, even before that there were plenty of "Chicken Littles" pointing out potential weaknesses [5] and the need for heightened vigilance in process control networks [6].

One problem that has been observed by many [7], [8], [2] is that there seems to be a cultural divide between people working in the traditional safety domain and their counterparts in IT security. SCADA security straddles these two domains, and successful solutions cannot ignore one or the other. The cultural divide is also a source of many misconceptions; Pietre-Cambacedes et al. [9] point out that many still believe Industrial Control Systems (ICSs) are isolated (they are not, as Stuxnet proved), nobody really wants to attack ICSs (Stuxnet and others), nobody understands our obscure ICS protocols (yes they do), and so on. Nicholson et al. [10] conclude that there is still a lot of work to be done in SCADA security, and particularly when we consider the probable involvement by nation states in several of the more publicised incidents later years, the prospect of cyber war seems to loom on the horizon. The argument that SCADA networks somehow should be exempt from active attacks is also refuted by Line et al. [11], who advocate increased efforts into incident detection and response in this domain.

Once the misconceptions identified by Pietre-Cambacedes et al. [9] are acknowledged, it is important that SCADA networks are subjected to cyber threat modeling [12], in order to make informed decisions regarding prioritisation and implementation of cyber security countermeasures.

B. A Motivating Recent Example from Ukraine

Just before midnight on the day before Christmas Eve 2015, around 230 000 Ukranian power customers suffered a total blackout. The reason turned out to be a cyber-attack [3], where intruders had succeeded in remotely accessing the SCADA security zone where they issued commands to open the breakers, taking at least 27 substations offline. At the same time, recovery was delayed by the uploading of malicious firmware to the serial-to-ethernet gateway devices, so that when the operator's workstations were up and running again, remote commands to bring the substations back online could not be issued.

To obtain the unauthorized access, the attackers first compromised the administration network by the use of spear phishing emails containing malware, later identified as BlackEnergy3 [3]. The malware collected usernames and passwords that allowed the attackers to enter the SCADA systems by existing remote access tools through a Virtual Private Network (VPN). The breaker settings were manipulated via the SCADA HMI on operator workstations, where the operators could detect the attack by seeing a "ghost mouse" clicking around on the screen.

Almost exactly a year later, it was "déjà vu all over again" for the Ukrainians, when the Pivnichna transmission substation outside Kiev was taken offline for an hour just before midnight December 17th [13], leaving parts of Kiev without power. Initial analysis of the attack concluded that it was similar to what had happened last year, but there were indications that some new malware had been involved. There were also speculations that this was more of a proof-of-concept than an attack in earnest.

The following summer, a new type of malware known as Industroyer [13] or CRASHOVERRIDE [14] was described by anti-virus firm **eset** and the security company Dragos, respectively. The documentation concluded that this was the same type of malware that had been involved in the December 17 Kiev incident. The analysis determined that Industroyer had native support for a number of Industrial control protocols, including IEC 60870-5-104 (also known as IEC 104) and IEC 61850, which are popular in European power systems. Even more worrying, the Industroyer malware had a modular architecture, allowing rapid deployment of new plugins supporting other protocols. This is reminiscent of the Havex/Energetic Bear malware used in the 2013 Dragonfly campaign [15], which also had a remote update feature. It is thus reasonable to expect that this malware will re-emerge in different markets in the future.

C. Fault Location, Isolation and Service Restoration

The functional steps in FLISR solutions are as follows:

Step 1: Based on sensor input automatically detect the Fault Location

Step 2: By means of breakers – automatically Isolate the faulty component/segment

Step 3: Maximum Service Restoration by energizing the new topology of the net.

An example of a FLISR system is illustrated in Fig. 3, where a distribution network is organised as a ring network, with a default partition implemented by a breaker. Sections with power are illustrated with green circles. There are several breakers (B) distributed along the ring,

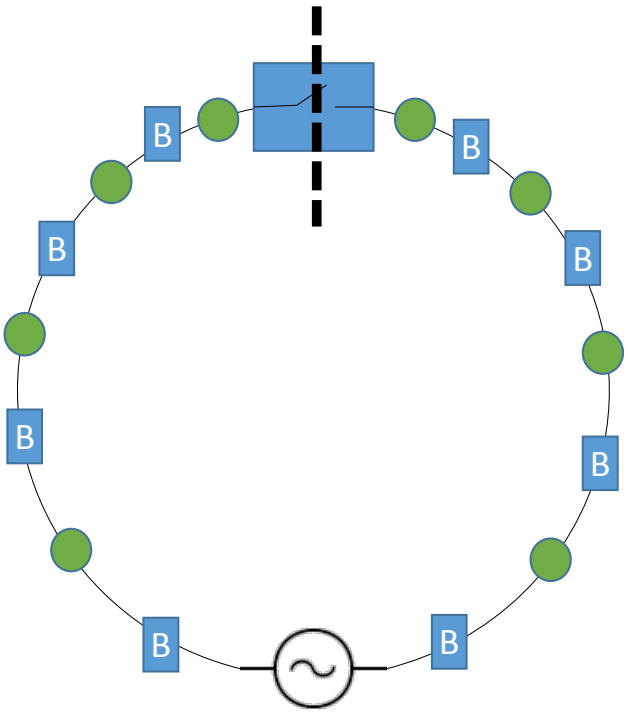

Fig. 3. Example FLISR configuration

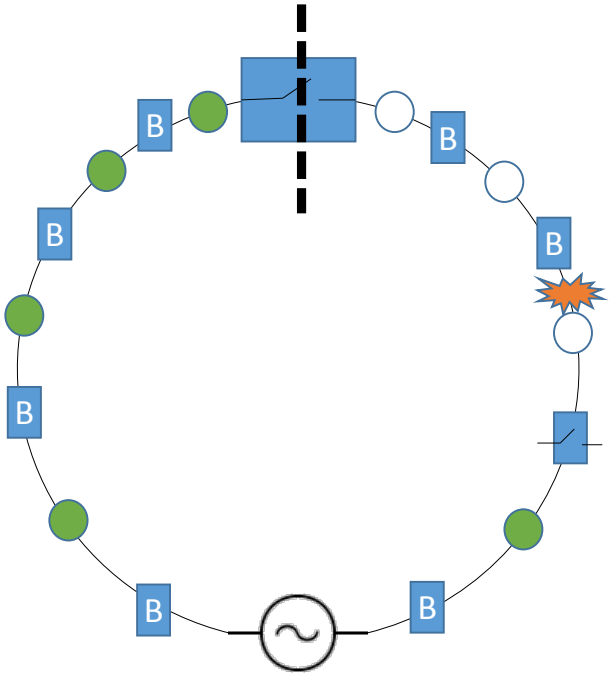

Fig. 4. Fault triggering a breaker

and when a fault is detected, these will trigger automatically, as shown in Fig. 4 (there are different types of breakers with different properties applicable to different situations, but that is beyond the scope of this paper). The precise fault location might not have been identified before the breaker is triggered, however, and it is thus likely that a larger portion of the network than necessary is left without power, indicated in Fig. 4 by white circles.

Timing is critical for a well-functioning FLISR, and it is required that the entire re-partitioning can be completed within 300ms of the first breaker being tripped. This is fast enough that most consumers only will experience a brief dip in voltage before they are restored to full power.

By communication with sensors and breakers, it is possible to pinpoint the fault location, and re-partition the network as illustrated in Fig. 5. In this example, the repartitioning can restore power to two of the three sections that were cut off automatically due to the initial fault.

The ring network is pedagogical for explaining FLISR, but the concept is equally applicable to other configurations, such as illustrated in Fig. 6. In this case, when a fault is detected, the substation B breaker will be triggered, as shown in Fig. 7, leaving all customers served by this substation without power. The FLISR solution will then work its magic in a completely analogous way as in Fig. 5, ensuring that only the rightmost section in Fig. 7 is left without power.

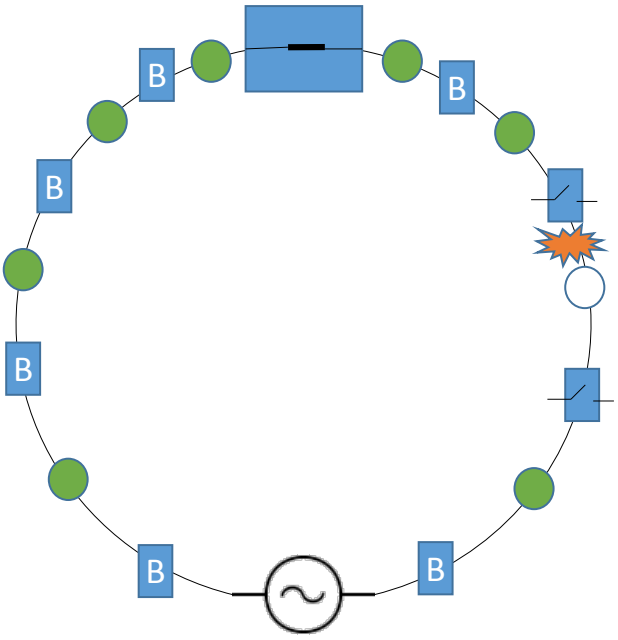

Fig. 5. FLISR minimizing outage

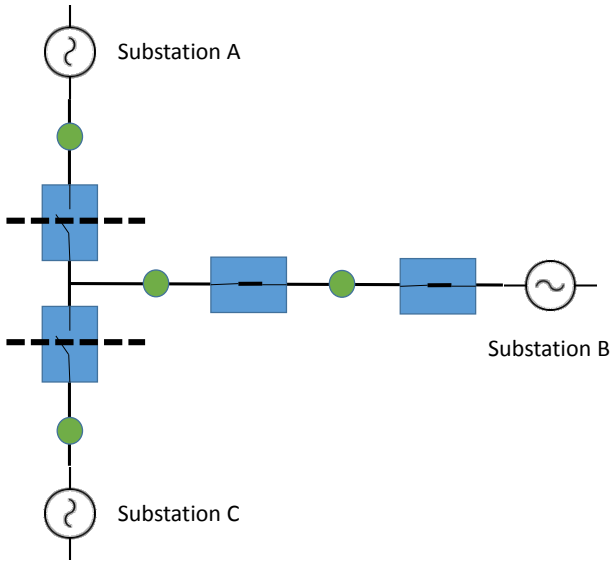

Fig. 6. Alternative FLISR configuration (adapted from [16])

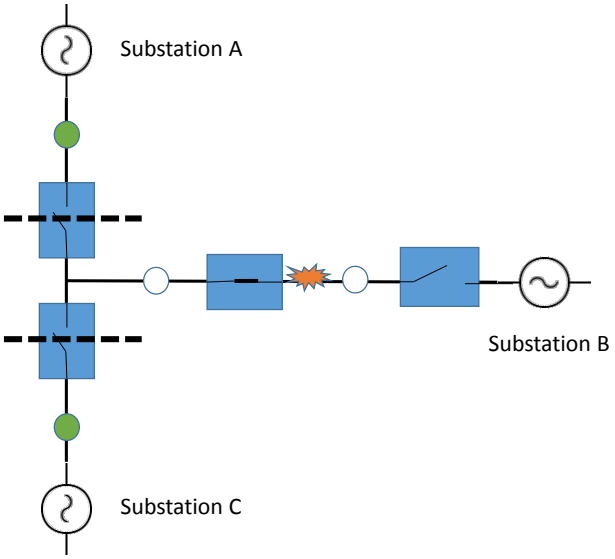

Fig. 7. Substation B breaker triggered by fault

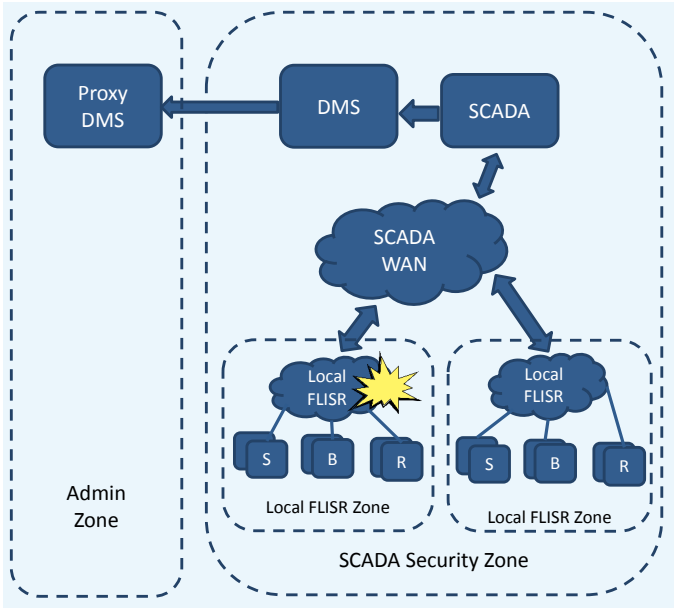

Fig. 8. Local FLISR

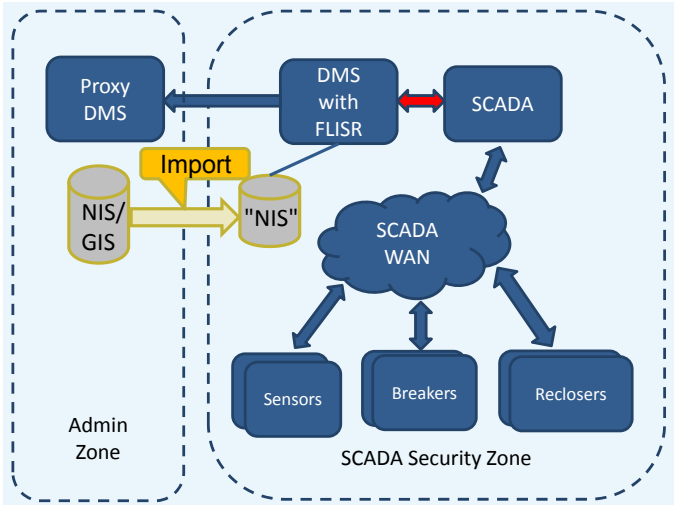

Fig. 9. DMS-based FLISR

The detailed operation depends on whether the FLISR is local, decentralized or centralized.

III. Placement of FLISR

As mentioned in the introduction, self-healing (FLISR) logic can conceivably be placed in different parts of the distribution network.

A. Autonomous Local FLISR Solutions

The fastest FLISR solutions typically operate locally on a predefined autonomous region of the distribution network, as illustrated in Fig. 8. The local FLISR controllers are collectively in charge of carrying out breaker and recloser operations until service is restored. Only breaker status is reported back to the SCADA system, describing the new topology of the autonomous area.

Since messages sent to the SCADA system are status messages, the SCADA system can protect itself from local FLISR domains by only accepting status messages. This implies that this solution is less vulnerable to cyber-attack than solutions that require DMS to be able to modify breakers directly.

If sensor data have been manipulated in a local FLISR solution, malicious/wrong commands can be sent to breaker/reclosers, but the problem would not spread since the autonomous region only reports status to the central SCADA system.

In case of physical topology changes that affect the

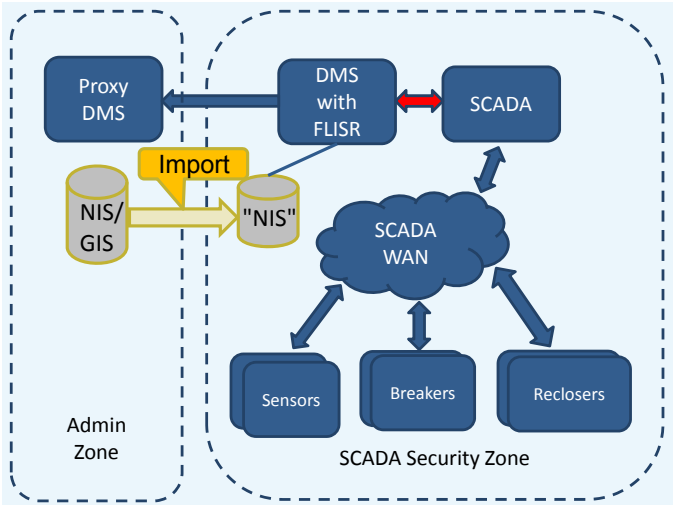

Fig. 10. DMS-based FLISR

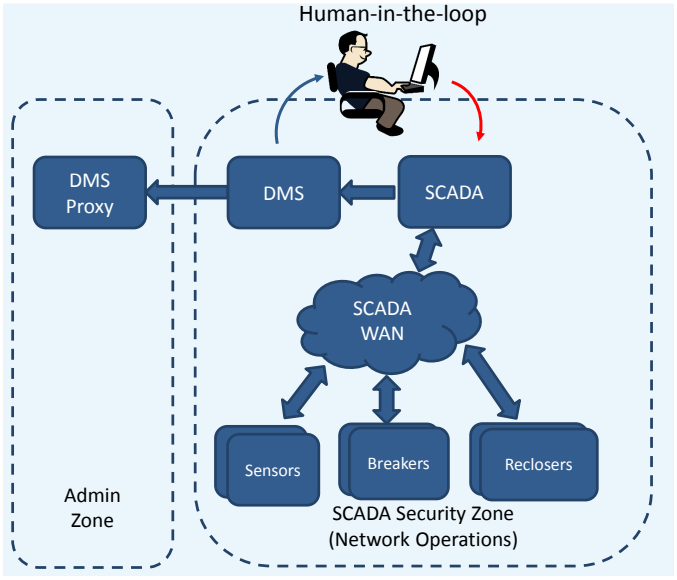

Fig. 11. Manual self-healing with human-in-the-loop

FLISR functionality, local FLISR solutions will require manual reconfiguration; this implies that such solutions will be less dynamic.

B. Centralised Self-healing

A centralised FLISR solution where the intelligence resides in the DMS, requires the DMS to be able to actively manipulate breakers in the SCADA network, as illustrated by the top right arrow (in red) in Fig. 10.

C. Decentralized Self-healing

A decentralized FLISR solution relies on a central analysis function residing in DMS or dedicated system assisting the logic in a local FLISR domain in order to complete all steps in FLISR.

If the central analysis function is residing in the DMS it will introduce the same security issues as with centralized FLISR solutions, and from a security point of view, there is thus no difference between the decentralized and the centralized solutions.

IV. Security Considerations

Currently, good practice at Norwegian DSOs dictates that it should not be possible to control the SCADA network from the DMS. This is because, as illustrated in Fig. 2, the DMS generally is connected to the Internet (albeit via one or more firewalls), and thus conceivably could be compromised by an outside attacker. Thus, most DSOs currently require a human-in-the loop when performing system restoration operations, as illustrated in Fig. 11.

A. Lessons from Ukraine

Vulnerabilities in the control system network can be exploited by an attacker that wants to obtain unauthorized access to cause a blackout, this can for instance be achieved by

- Sending commands directly to the SCADA equipment
- Remote access to the Human Machine Interface (HMI)
- Changing the GIS/NIS database
- Man-in-the-middle attacks on protocols
- Spoofing sensor input to FLISR

In the Ukraine incident (Section II-B), the attackers misused legitimate commands similar to what an insider or “rogue operator” would be able to. When facing such threats autonomous FLISR and other automated safety features could actually also act as a security mechanism, preventing the opening of too many breakers, as long as manual overrides are not readily available to the insider attacker.

Another security and safety aspect when introducing FLISR and other automation tools in smart grids is how the dependency on automated control affects the restoration time in case there is an outage. In the Ukraine case, the Remote Terminal Units (RTUs) that were bricked by malicious firmware needed to be replaced, and in the mean time it was crucial that the operator was able to get the network up and running by switching to manual control.

SCADA protocols have traditionally had poor security [17], and even where more secure alternatives are available, the slow update and replacement pace in the industry ensures that SCADA systems remain vulnerable. The prevalent SCADA security approach has thus been deploying a firewall as a “crunchy shell around a soft, chewy center” [18]. The problem with a firewall is that it is generally necessary to punch holes in it in order to get work done.

B. Communication between SCADA and DMS

In the typical case today, a one-way connection initiated from the SCADA network to the DMS is used to

regularly update information on breaker settings. Since a DMS-based FLISR is doing the analysis based on the up-to-date GIS/NIS database reflecting the distribution network, the GIS/NIS database is normally maintained and used in a security zone below the SCADA zone, which introduces the problem with how to do a daily import of the up-to-date topology that can be trusted. Importing a manipulated GIS/NIS database into the DMS can have dramatic impact on erroneous breaker operation and outage if manipulation is not detected and changes are executed in the SCADA system. Manipulation could be detected by operator inspection of the day-to-day evolution of the topological changes, by a human-in-the-loop as in today's manual self-healing illustrated in Fig. 11. Automatic detection of manipulation is also a possibility, for instance with intrusion detection systems based on machine learning algorithms. Importing manipulated data can also be automatically prevented by whitelisting or rate limiting the number of allowed changes.

Breaker and sensor data for FLISR analysis will normally be received by SCADA and forwarded to the DMS/FLISR. Even though end-to-end security, signatures and certificates can protect against man-in-the-middle-attack [17], physical tampering at the location and spoofing analogue lines interfacing RTUs cannot be detected and remains as a problem. Cyber security must be based on that proper physical shield protection is in place.

The DMS is a likely candidate for aggregating new types of data such as power quality, environmental sensor and other sensor data from smart meters and network components. By integrating more and more data into the DMS, it is evident that ensuring the integrity of data being imported will be critical. This type of DMS integration also contradicts a security policy that no data should enter the DMS/SCADA security zone.

One way to organize the DMS would be to establish a reduced functionality DMS as a proxy between the lower security zone and the DMS/SCADA zone. The proxy DMS would be stripped for FLISR operations. Another way would be to run two versions of DMS, one with FLISR functionality and to-way communication with the SCADA, and the other stripped for FLISR and only importing breaker status from the SCADA through a read-only channel. The SCADA would interconnect the two DMS FLISR and DMS.

C. Organizational Aspects

In general, it is not possible to achieve 100% security from a technical perspective, and it is therefore necessary to ensure that the DSO is capable of handling cyber security incidents when (not if) they occur [2]. It is important that different categories of employees receive appropriate training through exercises, and that organizational silos are avoided – cyber security should be everyone's concern!

V. Further work

From a practical point of view, the centralised FLISR solution is clearly preferred. We there need to formalize protection measures that can handle the potential threat of tainted NIS/GIS information from affecting the SCADA network.

VI. Conclusions

Local and Centralized FLISR address the same class of problems, but differ in capability, flexibility and performance. It is reasonable to expect to see more of both in operations.

Centralized FLISR solutions depending on daily import of updated NIS data clearly introduce a critical point regarding vulnerability and integrity of data. Object filter mechanisms should be in place between DMS and SCADA, filtering which breakers should be allowed to be operated on from FLISR/DMS. Alternatively, critical breakers in SCADA in the HV network should be protected with access lists, preventing DMS to operate on breakers outside the defined FLISR domains, typically the MV network.

Cyber security intrusion in Local FLISR solutions are less likely to spread to the entire SCADA domain due to local tampering or control of FLISR components, due to the fact that SCADA only receives state messages from the local FLISR domain.

All FLISR solutions should have in place strict validation procedures executed by SCADA Quality Assurance personnel to track changes in the NIS and the validation of these changes before they are activated for operation in DMS/SCADA.

There is thus a case for both local and centralized FLISR solutions, depending on the context. For mission-critical situations where speed is of the essence and where cyber security incidents can have far-reaching consequences, we would still advise sticking to a local, autonomous FLISR solution. However, in more widely distributed systems the added flexibility of a centralized FLISR solution may outweigh the security concerns. In any case, technical mechanisms must inevitably be bolstered by state-of-the-art organizational procedures in order to be able to handle cyber security incidents when they occur.

Acknowledgements

The research reported in this paper is supported by the Norwegian Research Council's ENERGIX program through the Flexnett project (project number 245412).

References

[1] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in smart grids," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Dec 2011, pp. 1–8.

[2] M. G. Jaatun, M. Bartnes, and I. A. Tøndel, *Zebras and Lions: Better Incident Handling Through Improved Cooperation.* Cham: Springer International Publishing, 2016, pp. 129–139. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-49466-1_9

[3] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukrainian power grid, defense use case," SANS ICS and E-ISAC white paper, 2016. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[4] N. Falliere, L. O. Murchu, and E. Chien. (2011) W32.Stuxnet Dossier. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
[5] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Computers & Security*, vol. 25, no. 7, pp. 498 – 506, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404806000514
[6] M. G. Jaatun, E. Albrechtsen, M. B. Line, I. A. Tøndel, and O. H. Longva, "A Framework for Incident Response Management in the Petroleum Industry," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 1–2, pp. 26–37, 2009.
[7] M. Line, O. Nordland, L. Røstad, and I. A. Tøndel, "Safety vs. Security?" in *Proceedings from Probabilistic Safety Assessment and Management (PSAM)*, 2006.
[8] H. Chivers and J. Hird, "Security blind spots in the atm safety culture," in *2013 International Conference on Availability, Reliability and Security*, Sept 2013, pp. 774–779.
[9] L. Pietre-Cambacedes, M. Tritschler, and G. N. Ericsson, "Cybersecurity myths on power control systems: 21 misconceptions and false beliefs," *IEEE Transactions on Power Delivery*, vol. 26, no. 1, pp. 161–172, Jan 2011.
[10] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare," *Computers & Security*, vol. 31, no. 4, pp. 418 – 436, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404812000429
[11] M. B. Line, A. Zand, G. Stringhini, and R. Kemmerer, "Targeted Attacks Against Industrial Control Systems: Is the Power Industry Prepared?" in *Proceedings of the 2Nd Workshop on Smart Energy Grid Security*, ser. SEGS '14. New York, NY, USA: ACM, 2014, pp. 13–22. [Online]. Available: http://doi.acm.org/10.1145/2667190.2667192
[12] I. A. Tøndel, M. G. Jaatun, and M. B. Line, "Threat Modeling of AMI," in *"Proceedings of the 7th International Conference on Critical Information Infrastructures Security (CRITIS 2012)"*, 2012.
[13] A. Cherepanov and R. Lipovsky. (2017) Industroyer: Biggest threat to industrial control systems since stuxnet. WeLiveSecurity by eset. [Online]. Available: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-\-stuxnet/
[14] Dragos Inc. (2017) CRASHOVERRIDE – Analysis of the Threat to Electric Grid Operations. [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf
[15] Symantec Security Response. (2014) Dragonfly: Cyberespionage attacks against energy suppliers. [Online]. Available: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf
[16] "Fault location, isolation, and service restoration technologies reduce outage impact and duration," U.S. Department of Energy, 2014. [Online]. Available: https://www.smartgrid.gov/document/fault_location_isolation_and_service_restoration_technologies_reduce_outage_impact_and.html
[17] P. E. Nordbø, "Cyber security in smart grid stations," in *22nd International Conference and Exhibition on Electricity Distribution (CIRED 2013)*, 2013, pp. 1–4.
[18] B. Cheswick, "The design of a secure internet gateway," in *USENIX Summer Conference Proceedings*, 1990. [Online]. Available: http://csrc.nist.gov/publications/secpubs/gateway.pdf