Wide-area Cyber-security Analytics Solution for Critical Infrastructures

Padraic McKeever
Institute for Automation of Complex Power Systems
RWTH Aachen University
Aachen, Germany
pmckeever@eonerc.rwth-aachen.de

Manuel Allhof
P3 Energy & Storage GmbH
Aachen, Germany
Manuel.Allhof@p3-group.com

Antonello Corsi
Ingegneria Informatica Spa
Rome, Italy
acorsi@eng.it

Igor Sowa
Institute for Automation of Complex Power Systems
RWTH Aachen University
Aachen, Germany
isowa@eonerc.rwth-aachen.de

Antonello Monti
Institute for Automation of Complex Power Systems
RWTH Aachen University
Aachen, Germany
amonti@eonerc.rwth-aachen.de

***Abstract*—On-line sharing of cyber-security information is necessary to effectively counter cyber-attacks. An online cyber-security analytics system for detecting and mitigating cyber-attacks and sharing information between Critical Infrastructure operators and regional and national authorities and also internationally is presented. The system contains one part which acts as a Security Operations Centre at Critical Infrastructure-level, with the capability to automatically mitigate attacks, and a part on meta- Critical Infrastructure level which, on a pan-European scale, gathers and analyses cyber-security information provided by the Critical Infrastructure operators and provides the results of the wide-area cyber-security analytics to authorities and back to the Critical Infrastructure operators. A use case of the system detecting and mitigating an attack is presented.**

Keywords—Critical Infrastructure, Security Operations Centre, cyber-security, data analytics

I. INTRODUCTION

Cybersecurity is a serious and ongoing challenge to the security and reliability of Critical Infrastructures (CIs), such as the electricity, gas and water production and distribution systems [1]. The different CIs are not stand-alone systems but are dependent on one another so that cyber-attacks on one CI can cascade to cause collateral damage to other CIs. The system architectures of the CIs are similar, consisting of a hardware infrastructure being monitored and controlled by ICT systems which increasingly base on common technologies, which contributes to making CIs threatened by the same type of cyber-attacks. Cyber threats to CIs can impact national security, public safety, and the national economy. Securing CIs against cyber threats is a shared responsibility of both the public and private sectors. Seeking to secure the individual CIs is not enough; security is needed between CIs and on regional, national and international level. Achieving this cyber-security requires that stakeholders such as CI operators and authorities co-operate in sharing data to support cyber-security activities, including attack detection and mitigation [2]. The motivation of CI operators to participate in such co-operative information sharing is that they benefit by receiving security incident information, thus enhancing their own cyber-security [3]. A common vision and a framework for achieving cyber-security on CI- and meta-CI-levels in needed which can be flexibly applied to the different types of CIs and different national organisational structures.

II. SUCCESS SECURITY SOLUTION (SUSS)

This paper presents the architecture of the SUCCESS Security Solution (SUSS), developed in the SUCCESS project [4]. SUSS is an online system addressing cyber-security both inside individual CIs and on a meta-CI level, i.e. enabling the individual CIs to share cyber-security information bilaterally with a network which spans regional, national and international levels [5], based on a wide-area security analytics and information sharing approach. SUSS monitors data in the CI for detecting and mitigating cyber-attacks. It enables co-operation by allowing CI operators to share information on attacks, mitigation measures and operational data. The information thus shared by various CIs is analysed on the pan-European meta-CI-level (which to detect attacks which might be undetectable at the CI-level and the information thus won shared with authorities across the continent and back to the individual CI operators. SUSS thus performs wide-area cyber-security information sharing and analytics, spanning from the level of the individual CI to regional, national and international levels. The system is generally applicable to different types of utility CIs but exemplified in this paper by the electrical distribution grid. SUSS supports implementation of the European Commission's 2016 Network and Information Systems (NIS) Directive [6], which identifies a need for closer international cooperation to improve security standards and information exchange and complements existing initiatives for trust-based cyber-security data and information sharing exist in the electricity sector, such as E-ISAC (Electricity Information Sharing and Analysis Centre) in the USA [7], EE-ISAC (European Energy ISAC, launched 2015) in Europe [8] and JE-ISAC (Japan Electric ISAC, launched 2017) in Japan [9].

To address the global nature of the cyber-attack threat, SUSS, as shown in Figure 1, is an on-line cyber-security monitoring, analytics and attack mitigation solution for CIs, which operates both at CI-level and meta-CI-level (through the CI Security Analytics Network (CI-SAN). As implemented in SUCCESS for the electrical distribution grid, SUSS is the first solution that obtains data from various DSOs/TSOs across Europe to combine them to form a holistic view of the security status. Operating on a networked, wide-area basis, allows analysing of data from multiple dispersed sources and detection of cybersecurity incidents which could not be detected by examining data on a smaller scale.

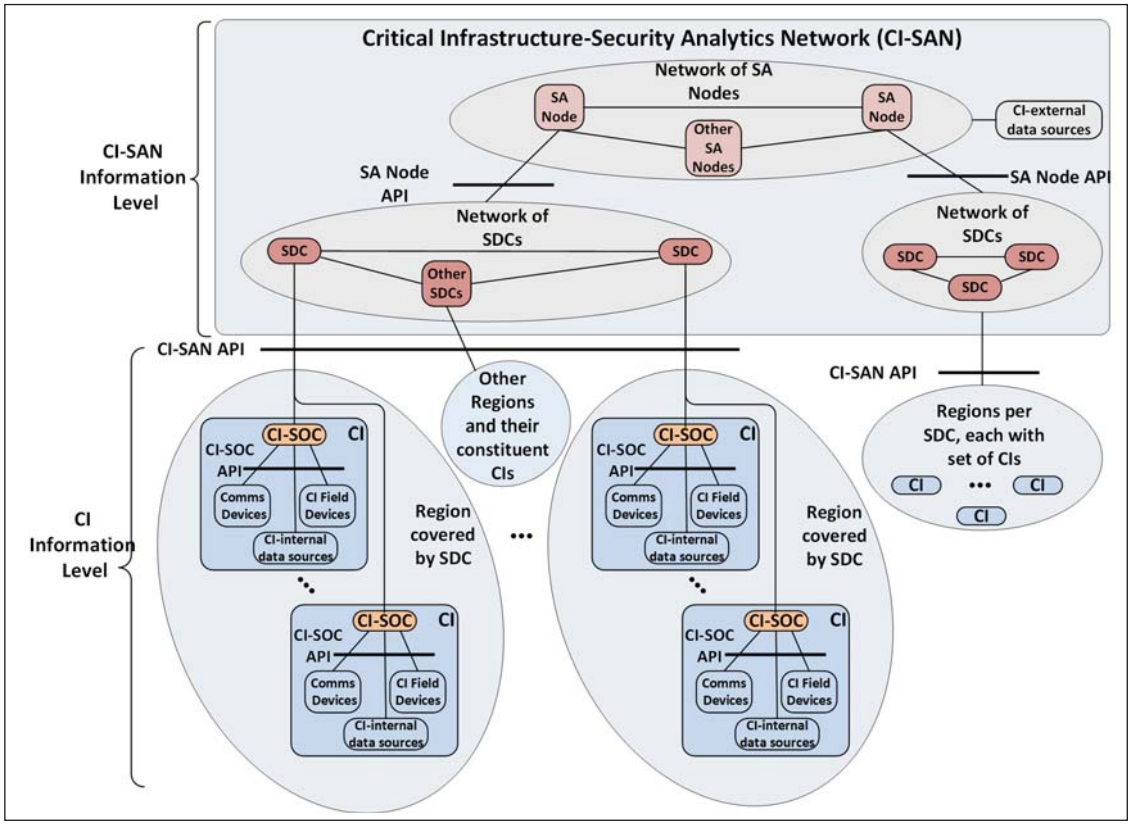

Figure 1: SUCCESS Security Solution (SUSS): Security Analytics on wide-area level (CI-SAN) and Critical Infrastructure level (CI-SOC)

Critical Infrastructure Security Operations Centre (CI-SOC): CI-SOC is part of the CI's IT system. It is a cloud application to detect cyber-physical attacks and itself directly implement a set of countermeasures to mitigate detected security incidents. It gathers dynamic (e.g. voltage, frequency or power measurements in electrical grids) and static (e.g. CI topology) operational data, log files from IT and OT systems and communications systems in individual CIs, as well as information from channels external to the CI (such as social media or weather) and performs cyber-security analytics and autonomous mitigation at CI-level of threats detected on CI-level. CI-SOC has the capability to manage a given number of risks as reported in ENISA taxonomy [10], link the risks to attack trees to provide a threat modelling, analysis of new threats and countermeasure extraction. Countermeasure extraction is based on a countermeasure historical knowledgebase that is fed with the detected threat and applied countermeasure. Additionally, the CI-SOC passes monitored data and information about detected incidents and countermeasures to the CI-SAN level of SUSS, which forms a pan-European network, called the Critical Infrastructure Security Analytics Network (CI-SAN), for sharing information about security incidents and countermeasures.

Critical Infrastructure Security Analytics Network (CI-SAN): CI-SAN is conceived as a network of Security Analytics (SA) Nodes, each of which is responsible for a region or a country, and which share cybersecurity information with each other. Gathering of information from, and sharing of information with, the CIs is performed by a network of Security Data Concentrators (SDC) instances, which aggregate operational data coming from CI-SOCs. Each SDC interfaces a set of CI-SOCs. The SA Node API defines the information exchange between SDCs and SA Nodes. The reason for defining CI-SAN in this way with two hierarchical levels is to allow it to provide wide-area coverage, scalability and flexibility to account for local, regional and national circumstances. SA Node is designed as a scalable, highly available Big Data platform, receiving and processing massive amounts of data in almost real time from SDCs, storing information about the attacks in a data lake for downstream analysis, sharing this information in CI-SAN (so that the network of SA Node instances thus form an international network for sharing information about cyber-attacks) and also alerting CI-SOCs, who thus obtain information that cannot be derived locally. Wide-area data analytics leverages real-time processing of the received data streams to detect cyber-attacks and anomalies which are undetectable on the micro-scale. CI-SAN develops a comprehensive wide-area (continent-wide) view of the security status of critical infrastructures, rather than just national scope as in [11]. Moreover, it shares information about identified cyber-attack incidents inside CI-SAN and with CI operators automatically and in real-time, which increases the chance of containing an attack. In addition, SUSS (in particular CI-SOC and SA Node) are able to learn and adapt to new attacks.

SUSS APIs: In order to encourage and promote sharing of cybersecurity information by the owners of the information (primarily the CI operators), it is paramount that a network of trust exists between the CI-operators and the entities with which they share their data. In SUSS, information is shared over defined APIs between information domains, so that the data being shared and the entities with which it is being shared are exactly defined and controlled.

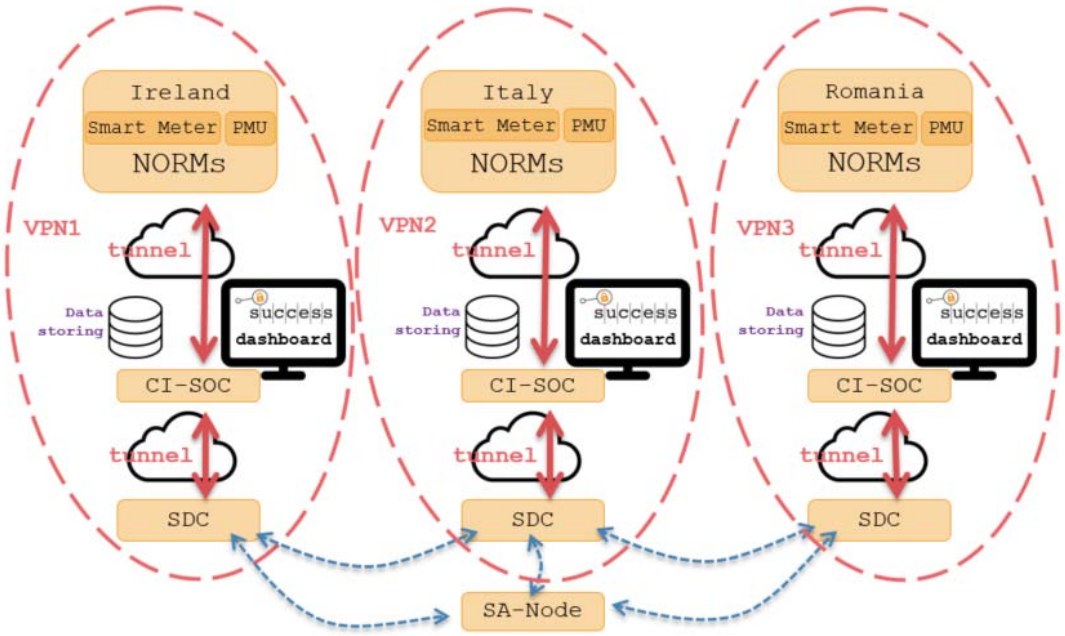

Figure 2: SUSS infrastructure in SUCCESS Field Trials

The CI-SAN API defines the interwork between the CI-SOC (which is part of the information domain of the CI) and the CI-SAN, which is a separate information domain. It supports passing information about security incidents, triggering and advising of countermeasures and CI-related data, e.g. grid status information or aggregated voltage or power readings. The API uses the Incident Object Description and Exchange Format (IODEF) [12], which is open, vendor-neutral and flexible [3], to represent information of the incident report message and Intrusion Detection Message Exchange Format (IDMEF) [13] to represent alert messages.

The CI-SOC API defines the interwork between the CI-SOC the CI-internal data sources, i.e. the IT and OT systems such as smart meters, smart meter gateways, communications equipment, SCADA systems firewalls etc. Having a defined API for this purpose facilitates information gathering in a standardised way inside the CI. The API supports different CI types (e.g. electrical grids, water grids, gas grids etc.), through a modular approach. In SUCCESS [4], it is supported by the Next-generation Open Real time smart Meter (NORM) [14], which is a secure Smart Meter Gateway from which services can be offered securely to the customer and by the Breakout Gateway (BR-GW), which implements mobile core network functionality on an edge cloud system located at the eNodeB (the radio base station of 5G mobile systems) and additionally can implement real-time countermeasures to cyber-attacks.

SUSS Scalability: An important factor upon which the feasibility of such a large data-sharing network as SUSS depends is its scalability. On CI level, each CI is its own information domain with its own CI-SOC, so that adding more CIs has no effect on SUSS's scalability except by producing additional data which must be handled by CI-SAN. CI-SAN's division into networks of SDCs means that additional SDCs or SDC networks can be added to deal with additional CIs and additional SA Nodes can be added or their capacity increased as needed to cope with the amount of data to be analysed. From an architectural standpoint, therefore, SUSS may be considered to be scalable.

Data Volumes in SUSS: to obtain a basic understanding, we perform here a calculation based on the German electricity distribution grid, which has about 890 electricity DSOs [15] serving around 50.5 million households [16]. Assuming the houses are evenly divided over the DSOs, that the data rate per house is 2,048 bits per second, that CI-SOC reduces the data rate by a factor of 10, that there is a 1:1 relation of CI-SOC to SDC; that the amount of data that CI-SOC gathers data from internal utility-related sources other than smart meters (e.g. IDS, antivirus) is 10% of that from smart meters; that SA Node covering 100 DSOs, i.e. there are about 9 SA Nodes in Germany; then the expected average data rates between the SUSS components, based on the above assumptions, is summarised in Table 1 in Mbps. In practise, the amount of data to be handled by the SA Node depends on the number of SDCs it handles, so there is a design tradeoff between the SA Node's capacity, its cost and the CI-SAN topology.

from household	from SDC	to SA Node
0.002048	12.78	1278

TABLE I. TABLE 1: OVERVIEW OF SAMPLE EXPECTED AVERAGE DATA RATES IN SUSS (MBPS)

III. DEMONSTRATION OF SUSS IN SUCCESS PROJECT

In the SUCCESS project [4], the current cyber-security threats to energy infrastructures have been categorised following the taxonomy described by ENISA [10] and modelled with attack trees based on those of NESCOR [17]. In addition, potential mitigation actions have been identified. A number of the cyber-attacks and mitigations have been tested by using SUSS in field trials in electricity distribution grids in Ireland, Italy and Romania. As shown in Figure 2, grid measurements were taken using low-cost Phasor Measurement Units connected to NORMs and sent to CI-SOC instances performing security analytics for the concerned grid. Each CI-SOC was associated with a corresponding SDC

instance. A single SA Node performed security analytics on the data received from all three distribution grids. VPN networks were implemented for the three distribution grids, connecting the NORMs to the CI-SOC and SDC.

Detection of False EV Charging Interrupt Command from TSO: an exemplary demonstration of the use of SUSS in the Irish grid was to detect falsification of a command from the TSO to the distribution grid operator to disconnect all EVs in a scenario with a large-scale deployment of smart EV chargers, which can be connected and disconnected by the DSO. When doing this, grid conditions should be considered by the DSO. A sudden mass disconnection of the chargers could cause grid instability due to the sudden imbalance between generation and loads. However, in case of a grid emergency, the TSO could issue an order to the DSO to perform just such a mass disconnection. The attack considered is where a false mass EV charger disconnect command is issued to the DSO by someone impersonating the TSO. When this type of command, regardless if genuine or not, are issued the DSO must react to it instantaneously, there is no time for human interaction but the response must be automated. The countermeasure to this type of attack is for the DSO to verify that the grid indeed is in a state that the received commands are warranted. As shown in Figure 3, this is done checking whether an estimate of the rate of change of frequency (RoCoF) made by the CI-SOC was greater than a threshold value of z=1 mHz/s. This simple method could give rise to anomalous values in certain circumstances and a better definition would be needed for larger scale deployment. The information to support the decision must be provided by routing multiple real time data streams across the VPN.

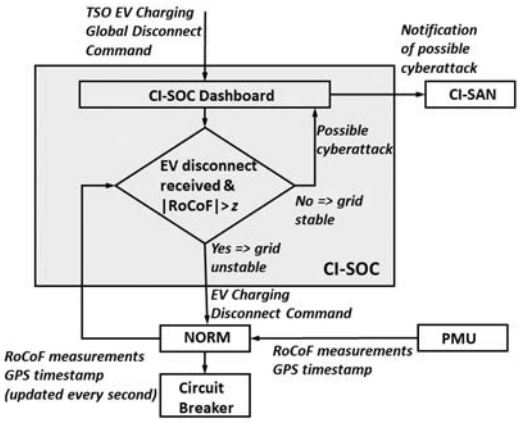

Figure 3: Grid Stability Logic

In field tests in the Irish grid, 5 EV chargers were connected via NORMs and BR-GWs to SUSS. As tested, the number of EVs did not threaten grid stability but was sufficient to show the principle of attack detection and mitigation. Measurements in the Irish grid resulted in RoCoF variations indicative of instability which enabled the Irish CI-SOC to mitigate the TSO impersonation attack by rejecting the mass EV charger disconnect command and inform CI-SAN (and thereby the other CI-SOCs) of the incident.

IV. CONCLUSION

The effectivity of cyber-security analytics in Critical Infrastructures can be improved by sharing data and analysing data coming from a wide-area covering other CIs, regions and countries. SUSS supports both analytics locally inside the CI and analytics on a wider-scale, based on data sharing. Detection and mitigation of exemplary cyber-attacks has been tested in trials in the real electrical grids.

ACKNOWLEDGMENT

This work was supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 700416.

REFERENCES

[1] Onyeji, I.; Bazilian, M.; Bronk, C . Cyber Security and Critical Energy Infrastructure. *The Electricity Journal* 2014, Volume 27, Issue 2, Pages 52-60. doi: 10.1016/j.tej.2014.01.011

[2] ENISA (European Union Agency for Network and Information Security). Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches, 2015. Available online: https://www.enisa.europa.eu/publications/cybersecurity-information-sharing

[3] ENISA (European Union Agency for Network and Information Security. Detect, SHARE, Protect – Solutions for Improving Threat and Data Exchange among CERTs, 2013. Available online: https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs

[4] SUCCESS: Securing Energy Critical Infrastructures. Available online: www.success-energy.eu

[5] ETSI TR 103 644 DTR/CYBER-0037 V1.1.1 (2019-08), *Increasing smart meter security*

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[7] E-ISAC Electricity Information Sharing and Analysis Center. Available online: https://www.eisac.com/

[8] EE-ISAC European Energy - Information Sharing and Analysis Centre. Available online: https://www.ee-isac.eu/

[9] JE-ISAC Japan Electricity Information Sharing and Analysis Center. Available online: https://www.je-isac.jp/english/

[10] ENISA (European Union Agency for Network and Information Security). Threat Taxonomy. Available online: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view,

[11] Kaufmann, H.; Hutter, R.; Skopik, F.; Mantere, M. A structural design for a pan-European early warning system for critical infrastructures, *Elektrotechnik und Informationstechnik*, 2015, Vol. 2/2015, doi 10.1007/s00502-015-0286-5

[12] Danyliw, R., Meijer, J. and Demchenko Y.: The Incident Object Description Exchange Format, 2007. Available online: https://www.ietf.org/rfc/rfc5070.txt

[13] Steinberger, J.; Sperotto, A.; Golling, M.; Baier, H. How to exchange security events? Overview and evaluation of formats and protocols, *2015, IFIP/IEEE International Symposium on Integrated Network Management (IM)*, Ottawa, ON, pp. 261-269. doi: 10.1109/INM.2015.7140300

[14] Sanduleac, M.; Lipari, G.; Monti, A.; Voulkidis, A.; Zanneto, G.; Corsi, A.; Toma, L.; Fiorentino, G.; Federenciuc, D. Next Generation Real-Time Smart Meters for ICT Based Assessment of Grid Data Inconsistencies, *Energies* 2017, 10(7), 857, doi 10.3390/en10070857

[15] Anzahl der Stromnetzbetreiber in Deutschland in den Jahren 2008 bis 2018. Available online: https://de.statista.com/statistik/daten/studie/152937/umfrage/anzahl-der-stromnetzbetreiber-in-deutschland-seit-2006/

[16] Anzahl der Zählpunkte von Letztverbrauchern im deutschen Stromnetz in den Jahren 2011 bis 2017. Available online: https://de.statista.com/statistik/daten/studie/618001/umfrage/zaehlpunkte-von-letzverbrauchern-im-deutschen-stromnetz/

[17] National Electric Sector Cybersecurity Organization Resource (NESCOR). Available online: http://smartgrid.epri.com/NESCOR.aspx