http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RÉSEAUX ÉLECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2013 Colloquium
November 13-15, 2013
Mysore – KARNATAKA - INDIA

D2-02_11

APPLICATION OF A CYBER SECURITY ASSESSMENT FRAMEWORK TO SMART GRID ARCHITECTURES

by

M. EKSTEDT*, M. KORMAN, R. TERRUGGIA, G. DONDOSSOLA

KTH, KTH, RSE, RSE

(SE, SE, IT, IT)

SUMMARY

This paper focuses on the cyber security in smart applications for energy grid topologies characterised by high penetration of distributed energy resources (DER) with renewable generation, storage devices and controllable loads, and the involvement of multiple active actors across the smart grid domains.

To illustrate this, a representative use case dealing with the Voltage Control (VC) of active Medium Voltage (MV) distribution grids will be considered. The role of the VC function is to adjust the voltage profile on the MV grid to optimise technical and economic objectives, sending set points to distributed energy resources and to the distribution grid devices.

The aim of the work is to demonstrate techniques for deriving justifiable estimations of the difficulty of succeeding with different kinds of cyber attacks to VC related communication services within the substation automation system.

Following the attack modelling activity ongoing within the Cigré working group D2.31 on “Security architecture principles for digital systems in Electric Power Utilities (EPUs)” [1], this paper evaluates the capabilities of CySeMoL (Cyber Security Modelling Language).
The CySeMoL methodology is applied to describe the grid ICT architecture (networks, operating systems, services, protocols, data flows), the security measures and the source and the target of the attack. The CySeMoL modelling approach is based on the attack graph formalism and provides justifiable quantitative estimates on the likelihood that different attack paths will be successful. In this paper CySeMoL will be used for estimating the likelihood of certain attack processes affecting the VC functions, including attacks caused by the remote maintenance procedures on the VC devices.

Starting with the description of a Voltage Control function architecture as a representative use case of future smart grids, the paper focusses on the application of CySeMoL to the sample case aimed at the evaluation of the adequacy of the tool to the smart grid sector.

KEYWORDS

Smart grid applications, cyber security analysis, graphical attack modelling

* Industrial Information and Control Systems, KTH Royal Institute of Technology, SE10044, Stockholm, Sweden, Fax: +46 8 790 6839, E-mail: mathias.ekstedt@ics.kth.se

http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RÉSEAUX ÉLECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2013 Colloquium
November 13-15, 2013
Mysore – KARNATAKA - INDIA

1. VOLTAGE CONTROL FUNCTION

The operation of active distribution grids with high penetration of DER, connected to MV bars and feeders, requires the implementation of a new VC function (cf. Use Case WGSP-0200 in [2]). In MV feeders including distributed generation, the power injected by DERs can lead the voltage beyond the limits in some parts of the grid, mainly due to uncontrollable generation from renewable sources. Control actions limited to the OLTC (On Line Tap Changers) of the substation transformers and compensation measures, as usually operated in passive grids, may be not sufficient to meet the supply requirements established by the norm EN 50160. Voltage profiles in the MV grids may be adjusted acting also on DERs connected to the MV feeders and substation devices as capacitor banks and storage devices.

Figure 1 presents the main components of the grid control architecture involved in the VC function. By focusing on the HV/MV substation, the figure highlights the need of a new VC function performed by a station level control system (called Substation SCADA). The main control loop of the VC function is based on substation – centre, intra-substation and substation-DER communications. Given the grid topology, field measurements, market prices and resource operation costs, the VC function optimises the voltage profile computing and sending appropriate set points to the third party distributed energy resources (generators, flexible loads and storages) and distributor's devices (i.e. capacitor banks and OLTCs). The algorithm is based on an AC Optimal Power Flow where grid losses and integral constraints are taken into account. The status of the grid, required by the control algorithm, is computed by a State Estimator function, based on actual measurements and grid topology.

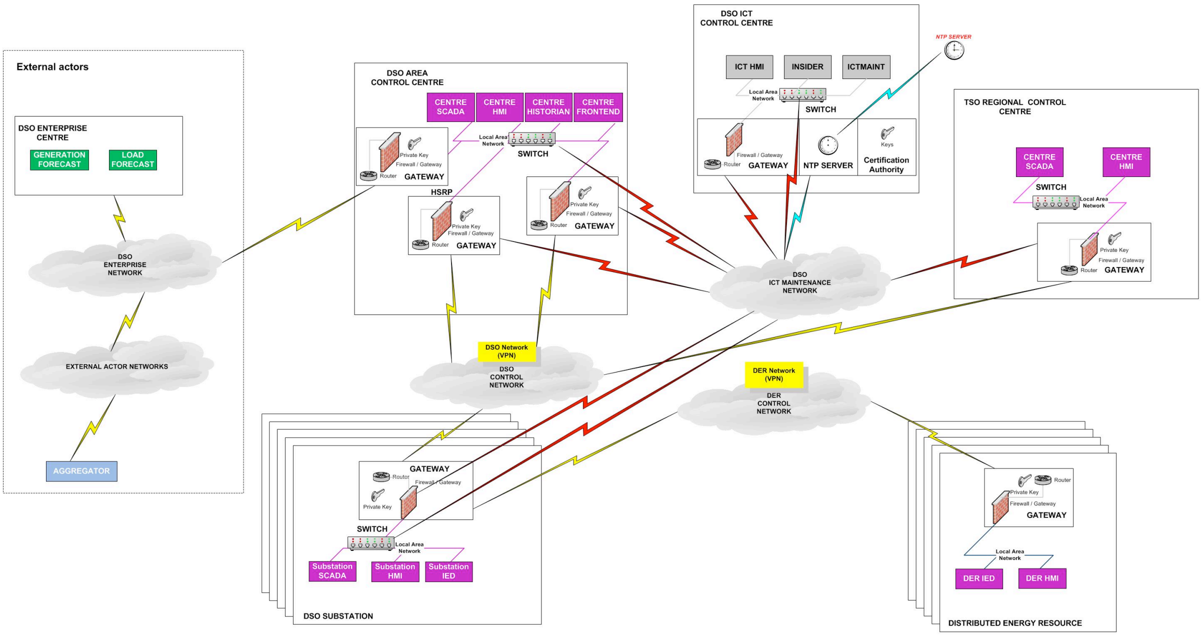

Figure 1: ICT architecture

The management and the security administration of the centre and substation ICT components and networks are performed by the DSO ICT Control Centre. It has direct access to network and control components, except substation IED elements and DER components. The data flows for the remote management of communication and control devices are based on secure operations using, e.g. HTTPS and SSH protocols.

According to the architectural layout in Figure 1, the supply chain of the VC function depends on several communication links involving remote accesses from systems outside the perimeter of the DSO organisation. In particular the VC application in the substation has communication links with third party DERs, possibly deploying heterogeneous communication technologies available in different geographical areas. From the operation stand point, the optimization function has to receive voltage regulation requests by the TSO (Transmission System Operator) whenever a transmission grid contingency needs to apply preventive measure to voltage collapse. Load and generation forecasts are used to optimize the operation of distributed devices, while the economic optimization is based on market prices and DER operation costs.

The information exchanges of the VC function would map onto the IEC 60870-5-104 protocol (for centre-substation communications) and the MMS profile of the IEC 61850 standard (for the intra-substation and substation-DER communications).

By focusing on the core of the MV regulation scheme, it results evident that the correct elaboration of the optimal set points depends on the provision of correct operation and economic data from the above communication channels [3]. A malicious attack to one of the above communication links may cause the loss of generation forecasts, economic data from the market, TSO requests, topological changes, operational data from the DMS, the introduction of faked generation forecasts, economic data from the market, TSO requests, topological changes, operational data from the DMS, monitoring data or set points. The effects of communication attacks may lead the regulation function either to diverge from optimum set points or, even worse, to produce inadequate set points with cascading effects on connected generators. The objective of the security countermeasures integrated in the architecture is to meet the VC availability and integrity communication requirements, i.e. to undo data losses and to avoid injection of spurious messages.

In order to reduce the scope of the analysis, this paper covers the DSO Area Control Centre, DSO Substation, DER and DSO ICT Control Centre, together with their interconnections and related information flows. As for the security measures, the capability of firewalls in interconnecting gateways, gateway-to-gateway network layer VPN and end-to-end transport layer security, as prescribed by the Part 3 of the IEC 62351 standard [4], are comparatively evaluated by means of CySeMoL runs.

Regarding the attack scenarios, this paper focuses on attack processes exploiting vulnerabilities in the remote ICT maintenance accesses to the substation SCADA and targeting the generation of faked set points. The tool will evaluate the success probability of the possible attacks sorting them by decreasing probability. The vulnerabilities/actions exploited/performed by the attack process getting the highest scores will be then considered for further protection of residual risks.

2. THE CYBER SECURITY MODELLING LANGUAGE

Before describing the specifics of our ICT architecture, a brief introduction to CySeMoL is needed. CySeMoL is a domain specific language, a meta-model, which allows modelling of ICT architectures. From the architecture models CySeMoL specifies what potential attack processes that exist through the system architecture. In addition, every attack step in the attack process is acquainted with a probability measure indicating how difficult it would be to succeed with it (given the countermeasures relevant to the attack step specified in the model). All the individual attack step probabilities are based on a combination of knowledge elicited from domain experts and previously published academic research studies (where such exist). The attacker is assumed to be a professional penetration tester with one week of preparation. The main concepts modelled in CySeMoL are the following: First, each local area network (e.g., DSO area control centre) is modelled as a network zone, assuming full reachability between arbitrary hosts (e.g., services, applications or operating systems) located within the network zone. Network zones are interconnected through gateways, with which firewalls and intrusion detection systems can be associated. Second, within each of the network zones and across them, there are services, applications and operating systems (i.e., software installations), each corresponding to a software product. Third, services, applications and other software installations can connect to and communicate with each other. This is modelled by data flows and protocols, while data possession is modelled by data stores. Fourth, there are human users having access to systems, which can be protected through authentication – access control points, authentication mechanisms and user accounts. Finally, network zones can be associated with physical zones and zone management processes. For a more elaborate description of CySeMoL, cf. [5]. CySeMoL with its related software tool can be downloaded[1] online.

3. VOLTAGE CONTROL ARCHITECTURE IN CYSEMOL

The ICT architecture under evaluation is separated into four logical zones: DSO ICT control centre; DSO area control centre; DSO substations; and DERs (see Figure 2). Each of these logical zones corresponds to a network zone (local area network) and a physical zone in CySeMoL.

We model and evaluate three variants of implementing substation communication briefly depicted in Figure 2. In all of the variants, there is a single gateway in each substation, which connects the substation's local area network (LAN) with all other immediate networks. The variants differ by use of different configuration of virtual private networks (VPN) for protection of communication. They are described in the next section.

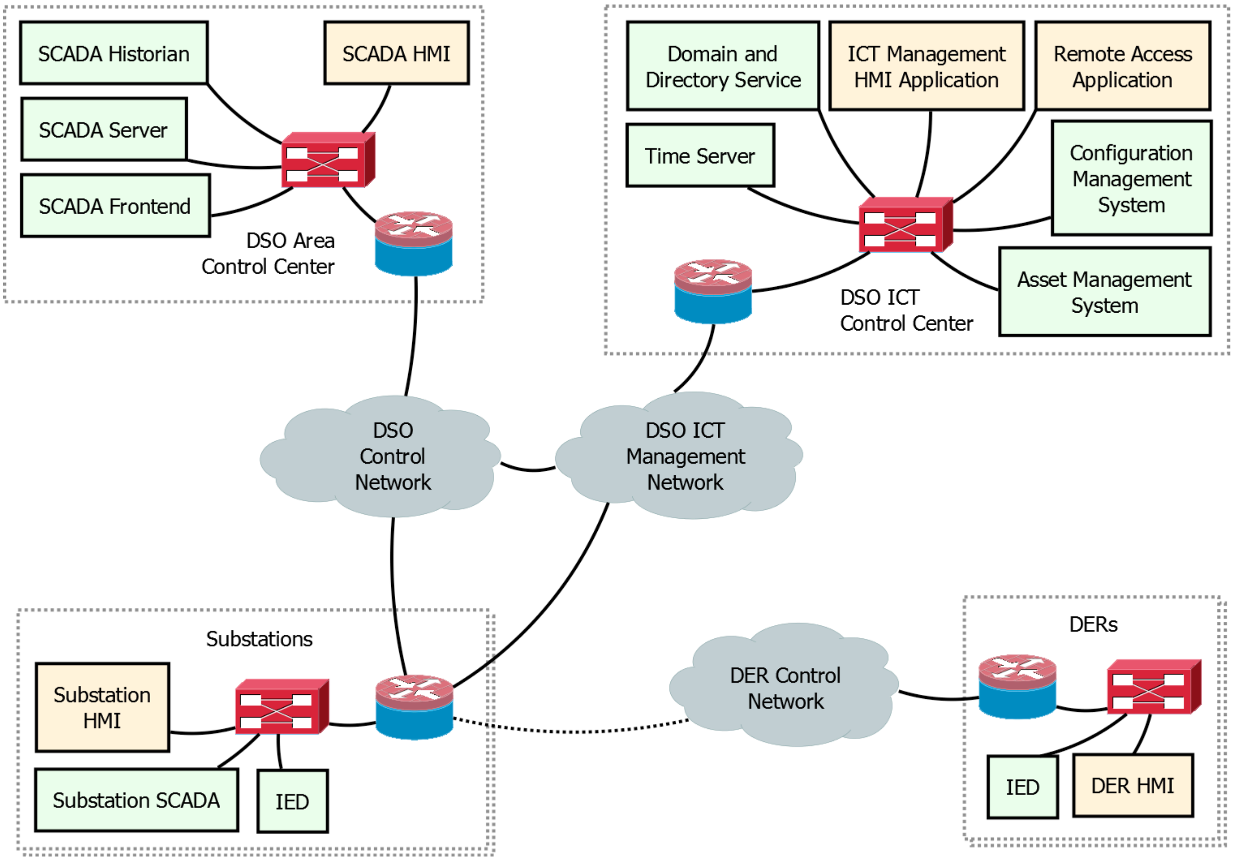

Figure 2: Services and applications in the ICT architecture

From the DSO ICT control centre, ICT technicians maintain the ICT infrastructure of the DSO. The centre also hosts a few services that support the ICT infrastructure and maintenance activities. We therefore assume that the centre hosts the following systems: (1) asset management system; (2) time server; (3) domain directory service; and (4) update and configuration management server. In addition, applications for remote access and maintenance are used from the centre. The DSO area control centre, from which the power grid is supervised and controlled, hosts SCADA system and its components: SCADA server; historian; front end; and a human-machine interface (HMI). At each of the substations, there is a local SCADA service, intelligent electronic devices (IEDs), and a local HMI (for maintenance purposes). At each of the DERs there is an IED and a local HMI, too. Each of the centres connects to their respective outside networks through a gateway with firewall. Figure 2 provides an overview of the ICT architecture with regards to services and applications run in/from their respective networks. Each of the systems is modelled as consisting of a service or an application client, and an operating system, on which it runs. These are connected to their respective network zones.

[1] http://www.kth.se/en/ees/omskolan/organisation/avdelningar/ics/research/sa/p/eaat/downloads-1.387300

The systems mentioned above interconnect and interoperate, even across their respective network zones. We therefore model data flows and corresponding protocols as follows. Time synchronization is done using the network time protocol (NTP). All of the operating systems used within DSO synchronize with the time server placed in the DSO ICT control centre. The time server, as well as the operating systems in DERs, synchronizes directly with an Internet source. Directory services are used for hostname resolution and access control within the DSO domain. Interconnected applications, services, and their underlying operating systems use directory services from all of DSO's networks (thus excluding DERs). The protocol suite used is X.500. Process automation happens between the substations and the DERs (DER IED vs. substation SCADA), within the substations (substation IED vs. substation SCADA), between the substations and the DSO area control centre (substation SCADA vs. control centre SCADA frontend), and within the DSO area control centre (SCADA server vs. SCADA frontend, historian and HMI). Intra-substation communications and those between substations and DERs use the IEC 61850 standard (MMS and Goose profiles). The central SCADA system interoperates with the substation-level SCADA using the IEC 60870-5-104 protocol. Process maintenance at substations is performed by operators from the DSO area control centre, as well as technicians directly at the substations. The former happens through the central SCADA, and uses the IEC 60870-5-104 protocol. The latter happens through the substation HMI, which communicates with the substation SCADA. ICT maintenance is done by ICT administrators at the DSO ICT control centre. The administrators can log in to arbitrary operating system equipped with a remote access service. Remote access takes place using the SSH protocol and SSH-tunnelled VNC protocol. Update operations are performed through the update and configuration management server, to which most of DSO's operating systems connect. Although some systems are configured to update automatically (e.g., workstations, and some ICT management servers) while others need administrative intervention (e.g., servers hosting process-sensitive services), all of the systems download update lists and updates from the update server using either Microsoft Windows Update (MS-WUSP protocol), or HTTPS based access to update lists and update packages (Linux systems). Finally, the SCADA HMIs both at the DSO area control centre and the substations interoperate with the asset management system located in the DSO ICT control centre, to seamlessly provide product information to operators and technicians upon need. This interoperation uses web services based on the HTTPS protocol.

Regarding access and authentication, we have assumed that there are three users – an operator (at the DSO area control centre), a technician (at substation level), and an ICT administrator (at the DSO ICT control centre). The account details and access credentials of these are stored in the domain directory service, as well as locally at the computers they use, where the authentication usually takes place.

All of the above described parts of the ICT architecture were modelled in CySeMoL. Altogether this becomes a fairly large model, to extensive to include in this paper. An excerpt of a part of the total CySeMoL model is provided in Figure 3.

To model the configuration and properties of the ICT architecture, we made numerous assumptions and choices in attempt to reflect typical configurations of networks, protocols and systems. For most of the modelled entities mentioned above (e.g., services, operating systems, gateways, zone management processes, etc.) there are a number of parameters, based on which CySeMoL also evaluates cyber-security dispositions. Our assumptions are briefly described in table 1.

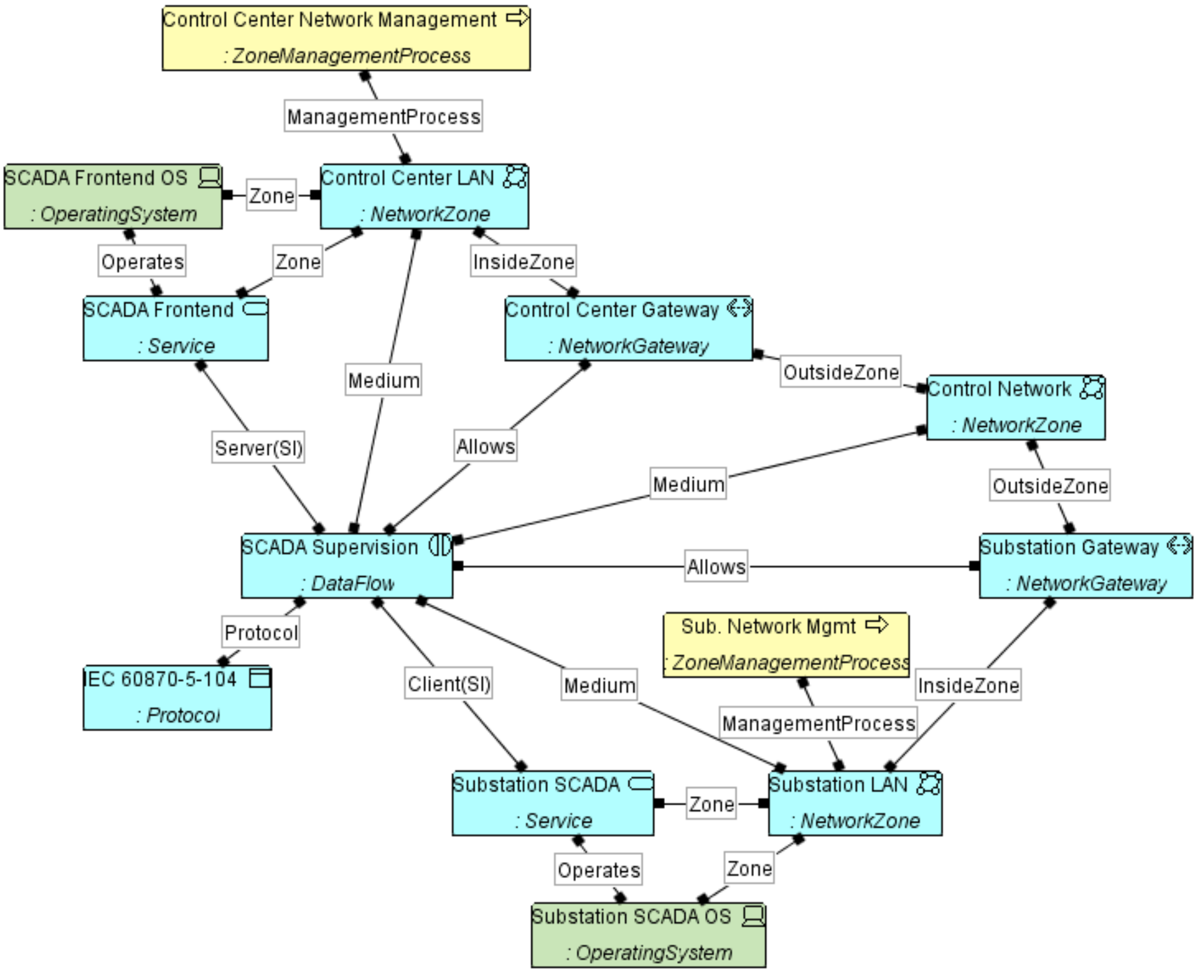

Figure 3: Supervision data flow between the SCADA frontend in the control centre and a substation-level SCADA (together with a few surrounding entities) as modelled in CySeMoL

Table 1: Brief description of assumptions made for the CySeMoL model

Subject	*Assumptions*
Both workstation and server operating systems	On many systems (but not all) a host firewall is present and functioning. In particular substations and DERs devices could not be equipped with a well configured firewall
Workstation operating systems	In centre domain they are generally up to date, and use recent operating systems (i.e., Windows 7 as compared to Windows XP or older). Although workstation systems are proprietary (as opposed to open-source), binaries are obtainable by antagonists, since the systems are well known and widely used (e.g., Windows). Substations and DERs components could not be updated
Server operating systems	Systems are usually well patched and use recent operating systems (usually Linux based, thus open-source). Systems sensitive for control of the electrical process (including those at substations) are an exception, since frequent regular updating of systems sensitive for process control poses high verification demands and stability/compatibility risks, based on which such updates are seldom performed.
Switches and gateways (network infrastructure)	In the control centres, gateways use static ARP tables and switches use port security, which disallows unknown network interface units to connect.

Remote access client applications	They are generally up to date (having recent patches applied).
Enterprise-level systems (e.g., asset management system) and SCADA systems.	They are proprietary, and thus source code is not available to the attacker.
Infrastructure systems (e.g., NTP server, remote access services)	They are open-source, as well as using on open-source protocol implementations (e.g., SSH).
Services and applications	Applications and services such as those for remote access, similarly to operating systems, have undergone considerable cyber security scrutiny and improvements within their development life cycle. This is not the case for process control services and applications, which are heavily verified regarding baseline functional correctness and process-robustness, rather than cyber security.
Network management	Network management is generally working according to best practice in the DSO ICT control centre. Somewhat less so in the DSO area control centre, where regular updating is not present for all systems, and regular security audits also are uncertain. On the substation level, regular log reviews do not take place, in addition.
Security awareness program	Security awareness program takes place for ICT maintenance personnel and the control operators. For technicians working on substation level, it is uncertain.
Communication protocols	Remote access protocols and protocols based on SSH, TLS or SSL, such as HTTPS, are both encrypted and cryptographically authenticated, as well as freshness indicated. Process control protocols are neither encrypted nor cryptographically authenticated. Network time synchronization protocol does not use any cryptographic techniques. Domain services (X.500) and Windows Update (MS-WUSP) use cryptographic authentication, but not obfuscation (communication encryption). Process control communication protocols are neither encrypted nor cryptographically authenticated.

We hereby present the evaluation of three variants of the ICT architecture presented above, as summarized in table 2.

Table 2: Description of the evaluated variants of the ICT architecture

Variant	*Configuration specifics*
Variant 1	An IPsec based network-to-network VPN protection is handled by gateways, and only covers communication flowing through the intermediary networks.
Variant 2	As in variant 1, except that the VPN only covers DSO control network and DSO ICT management network, not the DER control network.
Variant 3	A TLS-based VPN is following a host-to-host scheme, and so protects communication flowing through the intermediary networks, as well as the local networks.

4. SECURITY EVALUATION USING CYSEMOL

For each variant of the ICT architecture we analysed seven attack targets. The targets were chosen according to their assumed sensitiveness to the potential of cyber-sabotaging the electrical process in the smart grid. The attack targets are listed in table 3. There are two types of attack sources. First, we modelled outsider attacks. The outsider-attacker was modelled as someone equipped with a computer and able to access in a malicious manner to an intermediary network (i.e., DSO control network, DSO ICT management network, and DER control network). Second, we modelled insider attacks. The insider-attacker was modelled as someone able impersonating an ICT administrator, who had access to the remote access application and a respective workstation operating system in the DSO ICT maintenance network.

For every single pair of source and target of the attack there exist a large number of potential paths. For every scenario we are only considering the most likely attack (the easiest attack according to CySeMoL). In figure 4 one such attack scenario is visualized. In this particular example the starting point of the attack is assumed to be the DSO Control Network (framed with a yellow rectangle), where the attacker has gained access. The target is the DSO Control Center SCADA Front End (red rectangle). According to the calculations the most probable path in would be that there first is a poorly configured firewall in the DSO Area Control Centre (which assumes that we don't have full understanding of its actual state) (step 8 – there is a 35% chance that this attack step is reached). After that it is assumed to be able to connect to the SCADA front end without any problem (steps 9 and 10 – still a 35% chance to succeed). Next, there is a chance that there exists a high severity vulnerability (according to the CVSS[2] [6]) in the Front End service to which it also exists an exploit readily available that the attacker gets hold of (steps 11 through 14 – there is a 32% chance that the attacker has such an exploit). (Again this assumes that we do not have the exact knowledge about such vulnerability and exploits exist for the Front End.) Finally, the attacker launches an arbitrary code execution attack and by doing this achieves full control over the operating system hosting the Front End (steps 15 through 17 – the final probability of reaching this state is 5%. It is assumed that if the arbitrary code attack is successful, which in itself is quite low probability, it also gets full access to the operating system.)

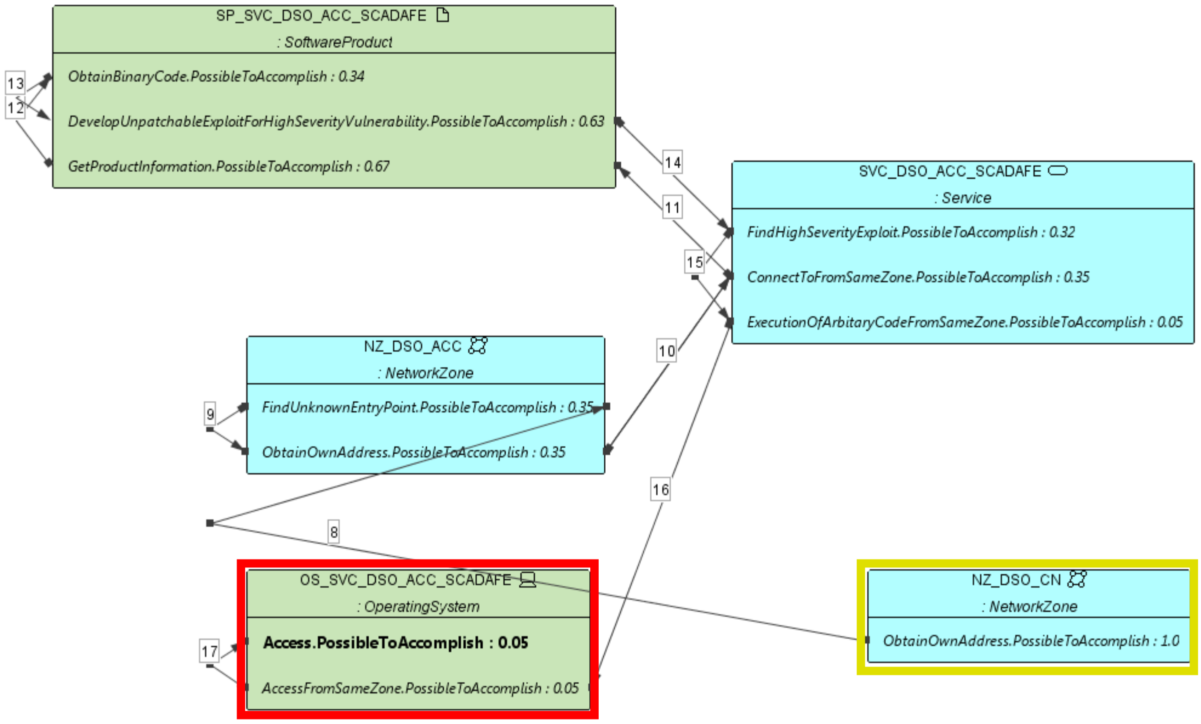
SP_SVC_DSO_ACC_SCADAFE
: SoftwareProduct
ObtainBinaryCode.PossibleToAccomplish : 0.34
DevelopUnpatchableExploitForHighSeverityVulnerability.PossibleToAccomplish : 0.63
GetProductInformation.PossibleToAccomplish : 0.67
13
12
14
11
SVC_DSO_ACC_SCADAFE
: Service
FindHighSeverityExploit.PossibleToAccomplish : 0.32
ConnectToFromSameZone.PossibleToAccomplish : 0.35
ExecutionOfArbitaryCodeFromSameZone.PossibleToAccomplish : 0.05
15
10
NZ_DSO_ACC
: NetworkZone
FindUnknownEntryPoint.PossibleToAccomplish : 0.35
ObtainOwnAddress.PossibleToAccomplish : 0.35
9
16
8
OS_SVC_DSO_ACC_SCADAFE
: OperatingSystem
Access.PossibleToAccomplish : 0.05
AccessFromSameZone.PossibleToAccomplish : 0.05
17
NZ_DSO_CN
: NetworkZone
ObtainOwnAddress.PossibleToAccomplish : 1.0

Figure 4: An example of an attack path visualized in CySeMoL. Attack steps are ordered according to numbers on the arrows and the cumulative likelihood of succeeding the attack is visualized after the attack step (attack steps 1-7 have been omitted for the sake of clarity)

In table 3 the end results (attack probabilities) for all scenarios are displayed – both for outsider and insider attacks (in parentheses). For clarity, they are also plotted in figure 5. We explain the results below.

[2] http://www.first.org/cvss/cvss-guide.pdf

Table 3: Results of the CySeMoL evaluation

	Probability of the conditional success of the attack for outsider (insider) in:		
Attack target	*variant 1*	*variant 2*	*variant 3*
SCADA HMI in the DSO area control centre	.15 (.4)	.41 (.4)	.08 (.4)
SCADA frontend in the DSO area control centre	.05 (.4)	.47 (.4)	.09 (.4)
Substation-level SCADA	.11 (.38)	.13 (.38)	.11 (.38)
Substation gateway	.17 (.19)	.21 (.19)	.21 (.19)
Control communications between the area control centre and substations	.33 (.38)	.99 (.38)	.17 (.05)
Control communications within substations	.32 (.37)	.98 (.37)	0.0 (.05)
Control communications between substations and DERs	.32 (.37)	1.0 (.37)	0.0 (.05)

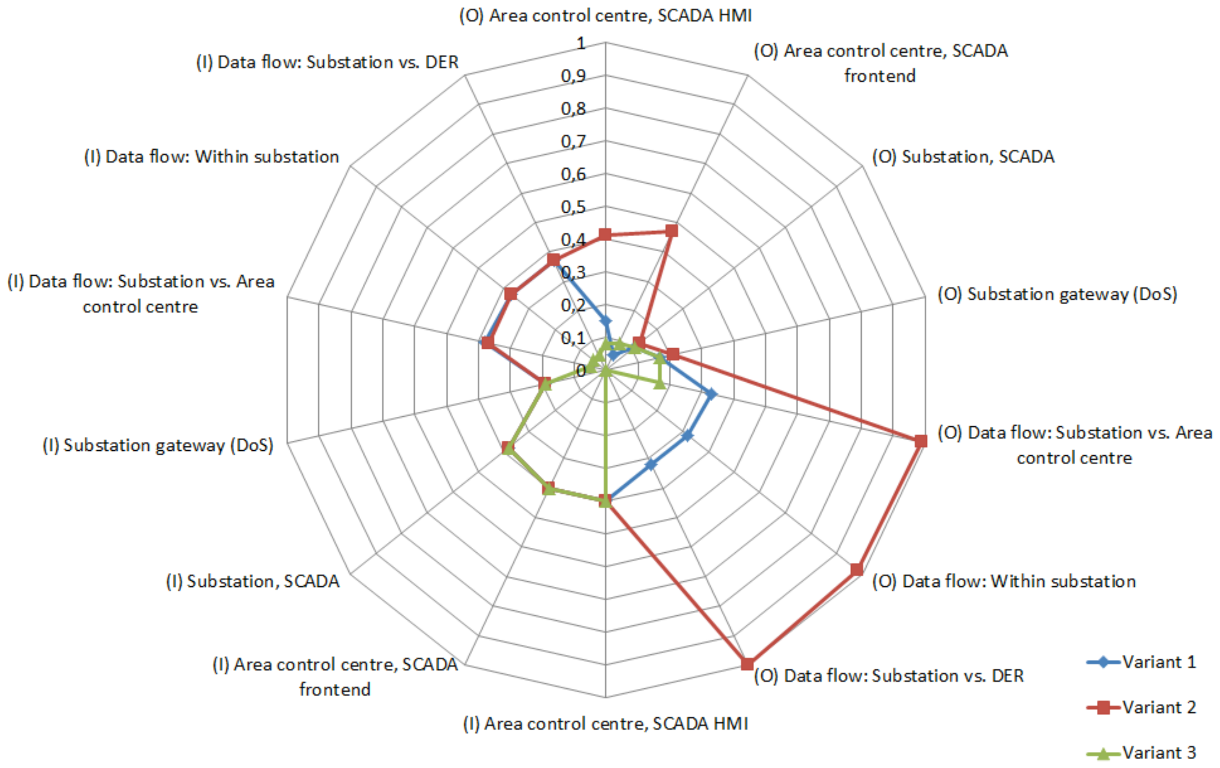

Figure 5: Plotted summary of results of the CySeMoL evaluation

The results show that variant 2, which does not use a VPN protection for communication across the DER control network (i.e., between substations and DERs), appears by far least secure. As the outsider attack initially propagates through the process control data flows, the process communications appear highly exposed, resulting in almost certainty of being compromised (if an attack is attempted). Consequently, the SCADA frontend and the SCADA HMI at the DSO area control centre become notably easier targets. The substation-level SCADA also appears more exposed. The second worst scoring variant is variant 1, which on the other hand appears considerably more secure than variant 2 – thanks to no major shortcoming such as a missing communication protection on an untrusted network. Realizing the VPN protection in a host-to-host fashion (as is the case for TLS VPN), which normally protects the communication anywhere outside the source, the destination host and the VPN concentrator (gateway), appears to lead to the attacker's inability to compromise such data flows from positions other than the two hosts themselves. All in all, the evaluations show that VPN protection is an important countermeasure in such architecture, and that the protection of TLS VPN is superior to that of IPsec VPN, since it protects larger parts of the communication.

5. REMARKS

Cyber security analysis of ICT architectures is becoming more and more relevant in future smart grid applications, characterised by multiple and heterogeneous communication links for critical grid control systems. The application of modelling and evaluation tools supporting security analysis allows managing the complexity of correlating component configurations with attack steps and security controls. Based on the assumption that architecture configurations are the cornerstone of smart grid cyber security, this paper explores the application of an attack graph formalism, CySeMoL, to the security analysis of architecture variants for the Voltage Control in active distribution grids connecting DER.

In this paper we have represented the VC architecture using the CySeMoL meta-model and we have estimated the probability of attack successful comparing three configuration variants. CySeMoL evaluation has shown a few differences among the configuration variants of the examined ICT architecture. However having a real and more detailed architecture at hand, more certain results could have been obtained from the evaluation. Moreover, CySeMoL is a simplified although comprehensive meta-model, which integrates a number of different topics within the domain of cyber security. As such it can be a powerful tool for an IT architect, who considers or develops different alternatives of a Smart Grid securement, and who might appreciate guidance with roots in established models of cyber security, research experiments and knowledge elicited from experts in the domain of cyber security.

From these preliminary evaluations we can conclude that the confidence in the output probability values increases with the adequacy of the architecture and attack models captured by the tool knowledge base, while decreases with the uncertainty in architecture configurations that is reflected by the amount of assumptions used in the evaluation. The application of the current CySeMoL version to the Voltage Control architecture variants has allowed identifying specific aspects that are not covered by the current version of CySeMoL, e.g. details on communication protocols and security measures. The further application of CySeMoL to smart grid architectures will provide results about the adequacy of this formalism to the smart grid sector.

BIBLIOGRAPHY

[1] G. Dondossola, L. Pietre-Cambacedes, J. McDonald, M. Ekstedt, A. Torkilseng, 2011, “Modelling of cyber attacks for assessing smart grid security”, Proceedings Cigré D2 2011 Colloquium, Buenos Aires 19-20 October 2011

[2] CEN/CENELEC/ETSI “Use Case Management Process — Use Case Collection, Management, Repository, Analysis and Harmonization”, Draft Report of the Working Group Sustainable Processes to the Smart Grid Coordination Group - Mandate M/490, November 2012

[3] G. Dondossola, F. Garrone, G. Proserpio, C. Tornelli, 2012, “Impact of DER integration on the cyber security of SCADA systems – the Medium Voltage regulation case study”. CIRED 2012 Lisbon (PT), 29-30 May 2012

[4] IEC/TS 62351-3 ed1.0 Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCP/IP, 22 June 2007

[5] T. Sommestad, M. Ekstedt, H. Holm, 2012, “The Cyber Security Modeling Language: A Tool for Assessing the Vulnerability of Enterprise System Architectures”. IEEE Systems Journal, 2012

[6] P. Mell, K. Scarfone, S. Romanosky, 2007, ”A complete guide to the common vulnerability scoring system version 2.0”. Forum of Incident Response and Security Teams (FIRST), 2007