1128

CIGRE South East European Regional Council Conference 2020 in Vienna, Austria

The topic: Cross Border Cooperation – Cyber Security

Cooperation through Automation: Applying Automated Cyber Risk Assessment for the Smart Grid

D. CAMPARA
KDM Analytics
Canada
djenana@kdmanalytics.com

A. HRUSTEMOVIC
JP Elektroprivreda BiH
Bosnia and Herzegovina

M.Sc. A. AHMETHODZIC
JP Elektroprivreda
Bosnia and Herzegovina

Dr. N. MANSOUROV
KDM Analytics
Canada

M.Sc. E. HADZOVIC
JP Elektroprivreda BiH
Bosnia and Herzegovina

Dr. M. VELEDAR
BH K CIGRE
Bosnia and Herzegovina

SUMMARY

To be effective during operations energy sector organizations need to be agile, mobile, secure, and robust while allowing efficient interoperability between numerous systems. Delivering this need means relying heavily on Internet Services Technology (IT), Industrial Control Systems (ICS), processes and people, working together to enable automated end-to-end information exchanges with minimal human intervention. This digital transformation in the sector enables large-scale energy production from renewable sources and dynamic, wide-ranging operations associated to electrical grid. Also, with this digital transformation we are building a new kind of global infrastructure where physical borders and their security do not automatically map onto cyber space.

Due to these threats, cybersecurity of next-generation power system (referred to as the Smart Grid) cannot be afterthought and requires new approach that is based on cross-border collaboration and information exchange.

The European energy infrastructure historically was structured around each country's regulations and polices. The assessment and mitigation of the cyber risks of those systems are disparate causing lack of confidence in their security. Security assessments cannot be about checklists, simple pass-fail results, or generating paperwork to pass inspections or

audits. Rather, they should provide concrete evidence that the implementers and operators of Power Grid information systems are meeting their stated security goals and objectives.

Currently, understanding, assessing and managing the risks to Power Grid systems in cyberspace is a very costly and challenging task that requires the expertise of well-trained and seasoned security professionals - a scarce commodity. Furthermore, risk analysis and risk mitigation of interdependent elements of these systems are too often done in isolation (within borders or cross-borders), making these systems vulnerable to multi-stage cyber-attacks, with the potential to wreak havoc in governments, industrial, commercial and private domains regionally, nationally and globally.

To achieve cross-border harmonized risk and mitigation assessment of Power Grid systems we need stakeholders to agree on risk assessment methods accompanied by set of specifications/standards and supported by advanced technologies that are able to identify, acquire, correlate, analyse, and display cyber and physical security-related data from all levels of the energy delivery systems architecture (device, system, and network) and across the cyber physical domains. This approach would enable automated solutions in support of decision-making process and prioritizing activities to guide the risk management responsibilities.

Automated model-based risk assessment is a game-changing approach that is capable of understanding intricate attack options that involve multiple access points, characterizing vulnerabilities, understanding their operational impact and providing adequate data to risk management process suggesting effective controls and countermeasures. It builds upon several best practices and standards such as Risk Management Framework, System Assurance Process and Model Based System Engineering (MBSE).

This paper describes a case study performed by 2 organizations: cybersecurity organization from Canada and the largest power utility company from Bosnia and Herzegovina to evaluate the usefulness of this approach. This case study strongly demonstrates the importance of standardization in the field, which also enables utilization of automated model-based risk assessment approach – together providing objectivity, repeatability and cost-effectiveness while being systematic and comprehensive.

KEYWORDS

Risk – Cybersecurity – Threats – Attacks - Risk Mitigation - Security Controls

INTRODUCTION

Over many years the industry and the defense organizations have been developing in-house and 3rd party approaches to evaluate and measure security posture of systems. Although significant progress has been made in understanding and documenting "what" needs to be evaluated together with expected results, the lack of efficient approaches that address the "how" component made these evaluation methods underutilized. In addition, most of energy organizations view cybersecurity as an IT cost and therefore are influenced by a key driver "Fewer is Better": The fewer the security requirements to implement and evaluate, the faster and less costly will the experience be. [1] They are constantly making a trade-off between accepting the benefits of a system versus the mishap risk it presents. While achieving 100% security of all systems against all threats is not realistic economically, identifying and prioritizing all risks followed by calculating the residual risk and implementing appropriate security countermeasures to maintain order and control is absolutely necessity. For example, while the trust side of the security equation has received a great deal of attention in the world of security, this growing reliance on Web and Internet Services raise security issues that cannot be mitigated by traditional authentication processes. Although it remains important to know whether to trust information, it is becoming imperative to verify that there is no threat-related activity associated with this information. This is not achievable with subjective and costly manual risk assessments [4]. The need for highly automated solutions is recognized, however for successful acceptance and wide deployment of such solutions across the energy sector many challenges need to be addressed by the energy sector community – these challenges are centred around establishing a culture of security, assessing and monitoring risk, developing and implementing protective measures to reduce risk, managing incidents, and providing resources necessary to continuously sustain security improvements as new threats emerge and operating environments advance [10]. In other words, the community needs to establish a set of standards in this field that organizations could utilize and certify their systems' compliance against [5]. This mutually agreed security requirements would ensure consistent approach to confidence level measures for power systems of different origin/pedigree (e.g. organization, countries …) enabling utilities to quickly understand where to focus cyber-risk mitigation resources. To address this necessity, international CIGRE formed a new group in January 2020: TOR WG D2.50 ELECTRIC POWER UTILITIES CYBERSECURITY FOR CONTIGENCY OPERATION.

SCIENTIFIC NOVELTY OF THE APPROACH

The key to the success of the automated risk identification is a systematic risk assessment methodology that builds upon several of the existing approaches to risk assessment, focusing at the use of discernible concepts, and a sequence of steps that maximizes assurance. This approach should be based on solid engineering practices where the elements of the architecture and the corresponding elements of risk are managed together. This allows combining a risk assessment methodology with the concepts of evidence-driven system assurance, referred to as Fact-Oriented Repeatable Security Assurance (FORSA) approach [1], is aimed at maximizing the assurance confidence and is guided by a built-in assurance case for risk assessment which answers the question "How do we know that all possible risks have been identified" [1,9]

In addition to integration of risk assessment methodology with system assurance process, scientific novelty in our approach is separation of concerns between two inputs provided to the automated solution through its technological framework: 1. System & operational architecture information in the form of the model vs. 2. cybersecurity knowledge containing information related to threats, undesired events, attacks & vulnerability patterns, security controls, e.t.c. [Figure 1]. This separation of concerns enables experts in each field to focus and contribute to the respective knowledge areas and also provides an opportunity for development of standards/specifications in support of a best-of-breed solutions related to cybersecurity for energy sector. The central part of the automated risk assessment is where the two inputs are integrated to enable risk analytics [9].

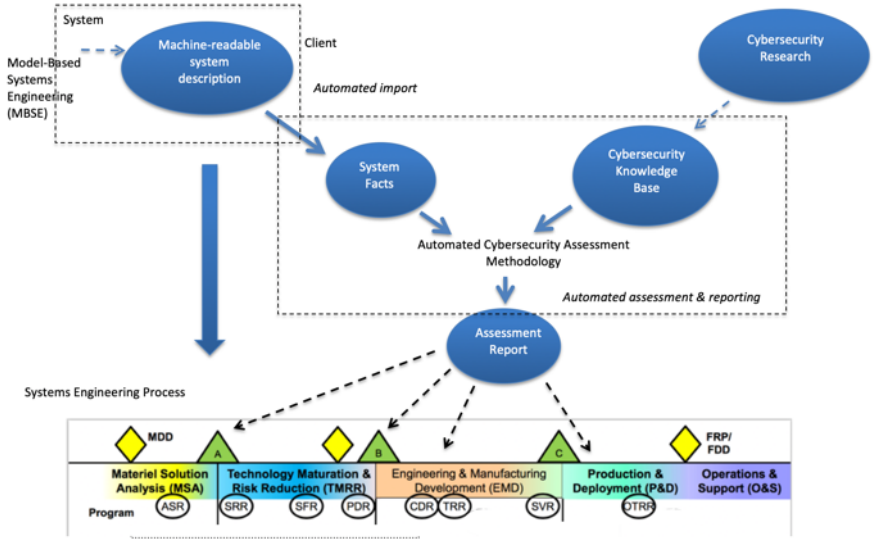

Figure 1:Separation of concerns – System vs. Cybersecurity knowledge as inputs to automated risk assessment

The goal of the FORSA approach supported by technological framework is to automatically assess the system and to recommend controls and countermeasures that can enhance its resilience to cyber threats and ensure operational success. The key step in the assessment is automated construction of an attack tree. The system's operational architecture is analyzed to determine the relative operational importance of hosts and applications. The system data is combined with rules describing attack techniques to compute all possible attack paths (given the rules and data such as attack targets, vectors, entry points and entry point sources) in the system. The potential attacks are chained together with aim to compute possible attack paths and stored in a tree data structure giving the pre-conditions and post-conditions for each attack step. Attack steps in the path depend on attack goals and attack methods chosen by attacker. One can view the approach as fully automated Cyber FME(C)A - Failure Mode, Effects and Criticality Analysis.

Furthermore, the FORSA approach with technical framework brings together evidence-driven assurance capabilities and automated risk assessment solution to provide justified confidence that the operational and system architecture views adequately represent the system and provide a solid basis for selecting optimal controls to remediate security issues. Within this approach, the risk analytics repository contains the connected elements of the risk model that represent the evidence to the risk claims [1,7,9].

As mentioned above (Figure 1), data for risk analysis comes from 2 sources: User provided system information and tool-incorporated cybersecurity knowledge base composed of information obtained from decades of research. The system information provided by user needs to be in machine readable form. Some industries, like defence and automotive industry apply Model Based System Engineering (MBSE) during system development lifecycle. MBSE is an emerging discipline where a formal machine-readable model of the system is used as a means of communication between various participants of the systems life cycle where each group has a viewpoint into the common model. In other words, the model is used to facilitate system requirements, design, analysis, verification, and validation activities, and can be applied in different stages of the process from the conceptual design phase throughout development and later life cycle phases. It can be applied to any System or System-of-Systems. More on this subject is published in our upcoming CIGRE-Paris paper (12).
The input model needs to be able to tell "cause-and-effect" story for system under analysis in order to provide high confidence in the risk assessment outcome. To that end, as a part of our solution we implemented the following:

- internal pivotal system model that is based on risk-relevant views of Unified Architecture Framework (UAF) standard from Object Management Group (standard aligned with ISO 42010 (Architecture Description) [7]
- "fit-for-purpose" analysis of the developed MBSE model to determine level of confidence in the outcomes of risk assessment (e.g. Correctness, Completeness, Consistency) [7].

By implementing internal pivotal model, we were able to work and seamlessly integrate with different MBSE approaches where tool's system information import capability can be adopted to any format and mapped to internal pivotal model for "fit-for-purpose" analysis and risk-assessment operations.
However, as we discovered by working with different organizations, one of the biggest challenges to the use of the automated risk assessment remains the availability of high-fidelity models of the control system as not many utility companies are using MBSE [3]. To lower the barrier to entry into repeatable and objective risk assessments using the automated capability, we developed a light-weight approach to modelling control systems in Word documents with several key tables among others, describing:

- the Performers (physical or logical devices) with the sub systems that are considered as being relevant to the context of the system ("inside" the boundary) or as being influential on the system ("outside" of the boundary),
- interfaces between Performers, classified as internal vs. external information exchanges
- the data types with their security classifications and impacts (Confidentiality, Integrity and Availability) and the data flows describing system activities/scenarios
- system capabilities as they relate to defined activities and persons/operators involved with devices (ensuring insider attacks are considered: malicious, clueless or carless)

These tables are imported, mapped to our internal pivotal system model and interpreted in the context of the selected knowledge base to build the risk model [11,12].

CASE STUDY

The case study performed by 2 organizations: cybersecurity organization from Canada and the largest power utility company from Bosnia and Herzegovina, to evaluate the usefulness of this approach is discussed in upcoming CIGRE-Paris paper (12). The Case Study in this

paper focuses on importance of standardization and automation of assessment to determine effective compliance with standard. The Case Study uses an example of standardization of Security Controls (SC), SC-related baseline (the minimum set of SCs to satisfy particular security level of the system) and SC-related strength (level of effectiveness of each SC). We started with high-level description of a Supervisory Control and Data Acquisition (SCADA) system for energy production management that was used by the cybersecurity department to discuss their current activities. Production Level of EP BiH SCADA implementation and its overview is captured in Figure 1 while detail information describing/modelling the system is captured using number of template tables in MS Word. Some of the key information captured in the tables are as follows: SCADA Nodes/Components and their Links (which are referred as Targets in the Risk Assessment Process), External Systems that SCADA interacts, Data Types and their Sensitivity Levels, Internal and External Information Exchanges, System data Flows, Persons, Capabilities. A Word document template was given then to the cybersecurity team to enter the information about the SCADA system. Once completed, the document was used as the input into the automated risk assessment tool, which acted as a virtual team member, trying to interpret the model and provide feedback. The reported gaps in the model were straightforward for the SCADA experts to fix. As the result of about a 3-day effort, the model was showing meaningful risks. The tool has identified over 1200 attacks by 30 attacker categories including external attackers (nation state, hacker, terrorist, etc.) and internal attackers (careless, clueless or malicious operators), supply chain and maintenance. As the result, 40 risks have been identified and estimated. Identification of the riskiest components was intuitive when reviewed by the cybersecurity team.

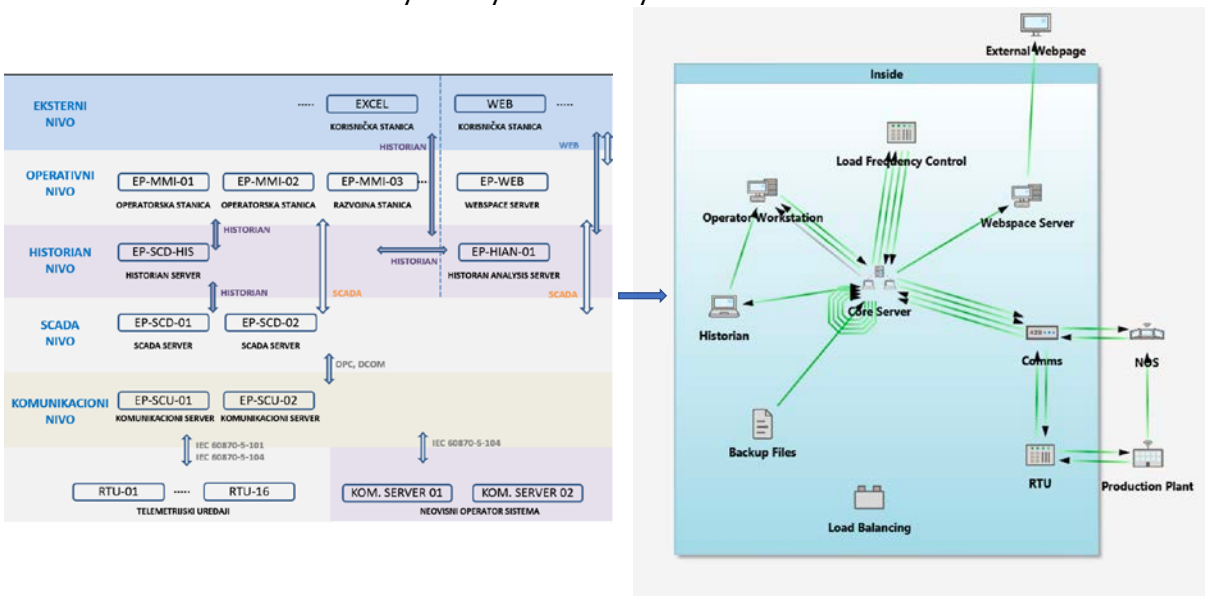

Figure 2 : EP BiH SCADA implementation and automatically synthesized graphical model based on Word tables' information

It is important to note that:

1. only the model is assessed and not real system,
2. SCADA "model" is very high level,
3. The BRM tool was used out-of-box, meaning no SCADA tailoring was introduced, such as Security Controls (we used the NIST 800-53 catalogue), threats and attacks (all were considered, without any adjustments and implemented controls).

4. For this Case Study, external components (Production Plant, NOS and External Webpage) were treated as possible attack vectors influencing Risk to operations of SCADA (SCADA operations are referenced as Inside boundary container in Figure 1).

The initial risk result is captured in the risk metrics table below followed by tables describing the distribution of the risk:

- The overall risk of SCADA DC on production level is Very High with the score of 2018.3
- Risk distribution: 1 Very High, 5 High, 25 Moderate, 5 Low, and 4 Very Low.

Table I : Initial Risk Metrics by Risk Group Count

LI / IMPACT	I1 -Negligible	I2 - Minor	I3 - Moderate	I4 - Major	I5 - Catastrophic
L5 - Near Certainty	R1 - 0	R2 - 0	R3 - 0	R4 - 0	R5 - 0
L4 - Probable	R1 - 1	R2 - 2	R3 – 2	R4 - 3	R5 - 1
L3 - Occasional	R1 - 0	R2 – 0	R3 – 5	R3 -18	R4 - 2
L2 - Remote	R1 - 0	R2 – 1	R2 – 2	R2 - 0	R3 - 0
L1 - Improbable	R1 - 0	R1 – 0	R1 – 3	R2 - 0	R2 - 0

Table II : Top 6 Risks

Identified Risk	Category (Risk to)	Impact Level	Likelihood level	Risk Level	Risk %
Corruption of Process Data information	information	Catastrophic	Probable	Very High	40.7
Loss of Process Data information	information	Catastrophic	Occasional	High	13.4
Loss of Request Data information	information	Major	Probable	High	4.6
Loss of Calculated Items information	Information	Major	Probable	High	4.6
Loss of Regulation Items information	Information	Major	Probable	High	4.2
Denial of System Control capability	capability	Catastrophic	Occasional	High	3.5

Table III : Attack Performer/Node risk percentage distribution

Performer	Category	Risk Percent	Risk Rank
Load Frequency Control	EMS	16.6	1
Core Server	EPBIH DC | HMI	14.6	2
Operator Workstation	EPBIH DC | SCADA Server	14.5	3
Comms	EPBIH DC | Data Acquisition	13.3	4
Historian	EPBIH DC | Data Management	11.5	5
RTU	EPBIH DC | Data Acquisition	10.2	6
Webspace Server	EPBIH DC | HMI	8.3	7
Backup Files	EPBIH DC | SCADA Server	1.6	8
Load Balancing	EMS	0.0	9

Next step is to mitigate all risks. For this Case Study we used the NIST 800-53 catalogue of Security Controls and its defined baseline levels: low, moderate and high impact category. The chosen impact level makes the determination what type and how many Security Controls will be considered when deciding which Security Controls are the most effective to mitigate vulnerabilities and associated attacks. This step is referred to as “Determining the Impact Level Baseline Security Controls”. In this Case Study we performed “what if scenarios” by completing the following steps and examining the results:

1. We set the baseline to Low and apply a set of SCs that are intended for systems categorized as Low impact followed by auto-mitigation of all vulnerabilities contributing to risks. This would be optimal and most effective mitigation. After risks are mitigated,

the risk is re-calculated and the resulting changes are summarized as follows and also presented in the table 4 below:

- The overall risk of SCADA DC on production level is Low with the score of 5.8
- Risk distribution: 24 Low, 16 Very Low.

It needs to be mentioned that side effect of auto-mitigation is that some other risks that share the portions of the same attacks and vulnerabilities would be mitigated as well.

Table IV ; Mitigated risk metrics

LI / IMPACT	I1 -Negligible	I2 - Minor	I3 - Moderate	I4 - Major	I5 - Catastrophic
L5 - Near Certainty	R1 - 0	R2 - 0	R3 - 0	R4 - 0	R5 - 0
L4 - Probable	R1 – 0 ↓	R2 – 0 ↓	R3 – 0 ↓	R4 – 0 ↓	R5 – 0 ↓
L3 - Occasional	R1 - 0	R2 - 0	R3 – 0 ↓	R3 – 0 ↓	R4 – 0 ↓
L2 - Remote	R1 - 0	R2 – 0 ↓	R2 - 0	R2 – 0	R3 - 0
L1 - Improbable	R1 – 1 ↑	R1 – 3 ↑	R1 – 12 ↑	R2 – 21 ↑	R2 – 3 ↑

2. We changed the baseline for the system to Moderate Impact and rerun risk calculation without changing the set of SCs already applied to the system intended for Low Impact category. In other words, we performed risk assessment of the system categorized and mitigated as Low Impact in the context of Moderate Impact. The results are presented in Table 5 and summarized as follows:
   - The overall risk of SCADA DC on production level is High with the score of 328.7
   - Risk distribution: 2 High, 19 Moderate, 15 Low, and 4 Very Low.

   This shows that systems need to be properly security-categorized for an environment that will be operating in and assigned corresponding SCs.

Table V : Risk metrics result : the system with SCs for Low Impact assessed in the context of Moderate Impact category

LI / IMPACT	I1 -Negligible	I2 - Minor	I3 - Moderate	I4 - Major	I5 - Catastrophic
L5 - Near Certainty	R1 - 0	R2 - 0	R3 - 0	R4 - 0	R5 - 0
L4 - Probable	R1 – 0	R2 - 0	R3 - 0	R4 - 0	R5 - 0
L3 - Occasional	R1 – 1 ↑	R2 – 1 ↑	R3 – 5 ↑	R3 – 13 ↑	R4 – 2 ↑
L2 - Remote	R1 - 0	R2 – 2 ↑	R2 – 4 ↑	R2 – 8 ↑	R3 – 1 ↑
L1 - Improbable	R1 – 0 ↓	R1 – 0 ↓	R1 – 3 ↓	R2 – 0 ↓	R2 – 0 ↓

3. In the next scenario we will illustrate importance of assigning the strengths to each SC, which determines the most effective SC within identified set. In this scenario Assessment1 had all SCs at the same strength level while Assessment2 had SCs assigned different strength levels: policy related SCs are assigned strength level 1 and 2, procedures range between 2 and 4 and mechanisms range between 4 and 5.
   Our starting point was calculated initial risk as it is presented in Table 1; The Baseline is set to Moderate Impact and top risk “Corruption of Process Data information” presented in the red cell of the matrix table is mitigated in the following way: remote access control mechanism-related SCs [AC17[2], AC17[3] and AC18[1]] are replaced with Remote access control policy and procedures [AC1] in Core Server and Operation Workstation.
   Assessment1 and Assessment2 are performed and results shows the following:

- Assessment1: the top risk is mitigated and reduced to the Low level (table 6) and risk score calculated at 238.3
- Assessment2: top risk is not entirely mitigated, it is reduced to the Moderate level (table 7) and risk score calculated at 241.2

Table VI : Risk metrics result from Assessment1

LI / IMPACT	I1 -Negligible	I2 - Minor	I3 - Moderate	I4 - Major	I5 - Catastrophic
L5 - Near Certainty	R1 - 0	R2 - 0	R3 - 0	R4 - 0	R5 - 0
L4 - Probable	R1 – 1 ●	R2 – 1 ↓	R3 – 0 ↓	R4 – 3 ●	R5 – 0 ↓
L3 - Occasional	R1 – 0	R2 – 1 ↑	R3 – 4 ↓	R3 – 16 ↓	R4 – 2 ●
L2 - Remote	R1 - 0	R2 – 0 ↓	R2 – 3 ↑	R2 – 0	R3 – 0
L1 - Improbable	R1 - 0	R1 – 1 ↑	R1 – 5 ↑	R2 – 2 ↑	R2 – 1 ↑

Table VII : Risk metrics result from Assessment2

LI / IMPACT	I1 -Negligible	I2 - Minor	I3 - Moderate	I4 - Major	I5 - Catastrophic
L5 - Near Certainty	R1 - 0	R2 - 0	R3 - 0	R4 - 0	R5 - 0
L4 - Probable	R1 – 1 ●	R2 – 1 ↓	R3 – 0 ↓	R4 – 3 ●	R5 – 0 ↓
L3 - Occasional	R1 – 0	R2 – 1 ↑	R3 – 4 ↓	R3 – 16 ↓	R4 – 2 ●
L2 - Remote	R1 - 0	R2 – 0 ↓	R2 – 3 ↑	R2 – 0	R3 – 1 ↑
L1 - Improbable	R1 - 0	R1 – 1 ↑	R1 – 5 ↑	R2 – 2 ↑	R2 - 0

The scenario described above (bullet 3) illustrates that in this particular case, policy related control enforcements are considered not as effective as mechanisms. This demonstrates importance of assigning SC strength/effectives for each SC.

CONCLUSION

Evaluating the risk posture of complex SCADA systems requires knowledge of the factors internal to the system, such as the system boundaries, components, access points, safeguards, assets, impact, policy, design, etc., as well as the factors that are external, such as threats, hazards, capability and motivations of the threat agents, etc., making this process costly due to the amount of manual effort involved [4]. There is a growing concern that the current security certification practices are antiquated and unable to scale with the amount of software being deployed. Manual certification process is mostly ad-hoc and subjective. Also, produced results is difficult to compare between systems and organizations [2]. Power Utility organizations could benefit from new automated risk assessment technologies that are systematic, comprehensive, objective, timely and cost-efficient nature [6,7]. However, the new techniques require better management of the engineering description of systems as automation is often possible in the context of managed descriptions of systems as machine-consumable input. Once an organization affords an upgrade in its cyber capabilities, the benefits are overwhelming, as an automated solution can be used continuously in near real time and provide reliable guidance regarding the cyber security posture. This paper demonstrates the new environment where an automated solution makes security planning measurable through a multitude of new metrics obtained from an automatically constructed risk model in an objective and repeatable way. The new metrics can be easily communicated

to the executive management in the terms of the cost of risks and priorities of implementing security controls to mitigate risks.

Automated model-based risk assessments allow objective comparison of risks and facilitate reuse of templates and best practices that can be immediately picked up and implemented into the automated solution [8]. To build upon these powerful technologies some effort needs to be made across the community of equipment suppliers, utilities, transmission operators and regulators on the following:

- Standard set of Information and the corresponding templates documenting the system including OT and IT components,
- Common approach to impact characterization of the system
- Catalogue of Security Controls to choose from based on system-impact characterization and their individual effectives/strength

CIGRE community is uniquely positioned to be an ideal platform to facilitate standardization efforts leading to adoption of game changing technologies for model-based risk assessment.

BIBLIOGRAPHY

[1] Dr. N. Mansourov, D. Campara, “System Assurance: Beyond Detecting Vulnerabilities” [Morgan Kaufmann Publishers, De. 2010]

[2] Congressional Research Service (CRS) US Government, “Electric Grid Cybersecurity” [Sep. 2018]

[3] Joint INCOSE WG Project (Power&Energy/CIPR/OOSEM), “Applying MBSE to Develop a Microgrid Reference Model” [EnergyTech and Expo, Cleveland, OH USA, Nov. 2017]

[4] D. Campara, “System Assurance - Discipline of Building Confidence that System is Trustworthy” [Object Management Group Cybersecurity Special Event, Ottawa, ON, Canada, Sep. 2018]

[5] D. Campara, “Reducing Cyber Risk Exposure when designing Cyber-Physical systems” [OCM Manufacturing Event, Ottawa, ON, Canada, Apr. 2017]

[6] Dr. N. Mansourov, “IoT and Risk Analytics”, Object Management Group IoT Conference [Reston, VA USA, Mar. 2018]

[7] Dr. N. Mansourov, “Automated Model-Based Risk Assessment”, MBSE Cyber Experience Symposium [Allen, TX, USA, May 2019]

[8] Dr. N. Mansourov, “UAF-based Risk Analytics” [Object Management Group UAF Special Event, Amsterdam, Netherlands, Jun. 2019]

[9] D. Campara, “Threat Modeling and Automated Risk Analysis” [Cybersecurity Workshop, Coronado, CA USA, Dec. 2016]

[10] US Department of Energy, “Electricity Subsector Cybersecurity Capability Maturity Model Version 1.1”, [Washington, DC, USA, Feb. 2014

[11] Dr. N. Mansourov, D. Campara, A. Hrustemovic, MSc. A. Ahmethodzic, E. Hadzovic, Dr. M. Veledar, “Understanding and mitigating cyber risk in Smart Grid” [BH K CIGRE, Neum, Bosnia and Herzegovina, Oct. 2019]

[12] D.campara, Dr. N. Mansourov, A. Hrustemovic, MSc. A. Ahmethodzic, E. Hadzovic, Dr. M. Veledar, “Applying Automated Cyber Risk Assessment for the Smart Grid” [CIGRE-Paris 2020 abstract accepted, full paper submitted]