CIGRE *Centennial* 2021

Revised Paper
D2-204

Applying Automated Cyber Risk Assessment for the Smart Grid

D. CAMPARA*
BH K CIGRE
Bosnia and Herzegovina

A. HRUSTEMOVIC
JP Elektroprivreda BiH
Bosnia and Herzegovina

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

Dr. M. VELEDAR
BH K CIGRE
Bosnia and Herzegovina

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

Dr. N. MANSOUROV
KDM Analytics
Canada

SUMMARY

Daily cyber-attacks have the potential to wreak havoc in the industrial, commercial, government and private domains on a world-wide basis. Global and critical infrastructure is facing multi-millions cyber-attack incidents each day, making the systems that are part of or dependent on it extremely vulnerable. One of such a system is the next-generation power system, referred to as a Smart Grid, where the ability of energy production, transmission and distribution systems to provide timely, accurate information to system operators is highly dependent on information and communication technologies (ICT). Also, to achieve flexibility and large-scale energy production from renewable sources, operations associated to electrical grid need to be agile, mobile, secure, and at the same time robust while allowing efficient interoperability between numerous systems. Delivering this need means relying heavily upon automated end-to-end information exchanges with minimal human intervention.

The cyber-attacks against Smart Grid systems can originate simultaneously from thousands of computers located thousands of miles away, geographically distributed across multiple jurisdictions, and can penetrate interconnected computer systems within milliseconds jeopardizing energy delivery operations. Addressing these cyber-threats requires cyber technical capabilities and a workforce capable of understanding intricate hostile attack options to facilitate decision-making that enables sustained operational system performance.

Currently, the assessment processes for Smart Grid systems are seldom automatable and are laborious, costly and challenging tasks. As a result, assessments are often not systematic and comprehensive, leaving the systems vulnerable to multi-stage cyber-attacks.

The best course forward for stakeholders is to deploy risk-based methods in support of decision-making process and prioritizing activities to guide the risk management responsibilities. The risk-based methods need to be 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 requires automated solution that is capable of understanding intricate attack options that involve multiple access points,

djenana@kdmanalytics.com

characterizing vulnerabilities, understanding their operational impact and providing adequate data to risk management process suggesting effective controls and countermeasures.

Automated model-based risk assessment is a game-changing approach that can deliver these objectives. However, one of the 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 Model-Based System Engineering [MBSE]. To lower the barrier to entry, we developed a light-weight approach to modelling control systems in Word documents with several tables describing the physical devices, their interfaces, the data types and the data flows of the system under assessment. These tables are interpreted in the context of the selected knowledge base to build the model of the system under assessment.

This paper describes a case study performed by KDM Analytics and JP Elektroprivreda BiH, the biggest power utility company in Bosnia and Herzegovina to evaluate the usefulness of this approach. This case study strongly demonstrates the feasibility of the model-based risk assessment approach, its objectivity, repeatability and cost-effectiveness while being systematic and comprehensive.

KEYWORDS

risk, cybersecurity, threats, attacks, risk mitigation, security controls

INTRODUCTION

Achieving 100% security of all systems against all threats is not realistic economically. Many iterations are needed to understand the system as the target of cyberattacks and to go through multiple “what if” scenarios to address every stakeholder’s burning question: where I should focus my cyber-risk mitigation efforts, budgets, and resources [1]. 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 and importance 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.
More specifically, the methods and metrics used across the sector continue to vary, lack of consistent criteria or metrics, benchmarking and comparing Smart Grid systems risk and evaluating the impact of mitigation efforts is problematic. Quantifying risk is also problematic when the energy sector faces rapidly changing threats that are difficult to predict and have consequences that are hard to demonstrate [10]. This is especially amplified by increasing complexity of systems and their interconnections with other systems from different infrastructure sectors which can introduce new vulnerabilities [2]. One of the trends is that those systems are not physically separated like they used to be in the past and are dependable on existing IT infrastructure. To address this gap several things are needed [1,5]:

1. understanding the abuse scenarios of the control systems. This requires structural methods and availability of high-fidelity models of the control systems in a such way that “cause-and-effect” analysis of the system could be rigorously examined;
2. measuring the risk by taking into account both threats and mitigation controls and applying structural methods to understand the residual vulnerabilities and their impact;

typically this process involves 4 risk phases: initial (risk identification), mitigated, compliance and residual risk (after controls have been applied).
3. correlating potential incidents with the impact;
4. making this whole process repeatable, so that "what-if" scenarios can be evaluated by considering changes to the threats, the operational infrastructure, or the mitigation controls; This step provides continuous improvement.
5. automating the process so that the evaluation can be done repeatedly, which will allow integrating risk assessment directly into the workflow at the business level (changes in the business model), design (alternative designs), policy level (changes to security policy) and operational level (scoring individual operations). This step provides continuous improvement.

Our approach to automated model-based risk assessment is a game-changing approach that addresses these gaps. It builds upon several best practices to populate a computer-based risk analytics infrastructure and systematically identify the assets, attack surface and attack paths that are allowed by the system under assessment and their impact on the capabilities and the mission of the system.
Although the paper briefly touches on all aspects of automated model-based risk assessment, the focus is on the approach to overcome the lack of high-fidelity models of the control system, addressing bullet 1 in the above list.

AUTOMATED RISK ASSESSMENT

The key to the success of the automated risk identification is a systematic 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 [1,4,9]. Combining a risk assessment methodology with the concepts of system assurance allowed to achieve full automation. The strategy behind the steps of a risk assessment methodology 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 abuse scenarios have been identified” [4]. Within this approach, the risk analytics repository contains the connected elements of the risk model that represents the evidence to the risk claims [1,7,9].

As a central part of the approach to systematically understand the abuse scenarios of a system, its input model is interpreted, a threat model is automatically constructed by matching known attackers to the system according to their motivation and tactics, then a comprehensive walk-through is performed to systematically identify entry points, attacks (direct and multistage), and related vulnerabilities and provide fully quantifiable risk calculation over the risk model. Vulnerabilities as well as security characterization and selected standard guide automated assignment of Security/Mitigation Controls in order to eliminate the possibility of adding non-effective Controls and/or adding Controls in wrong places. This is a key to successfully identifying mitigated, compliance and residual risk. Also, a single unified risk score for the system under assessment allows the risk to be presented in the form of distributions per various risk factors, such as attack targets, attacker types, attack tactics, the types of impact. This approach facilitates prioritization of risks and allows comparison of mitigation options.
This approach allows repeated push-button assessment, unlike some other approaches where

- risks assessment is based on the checklist. For example, CSET tool developed by US Department of Homeland Security (DHS), takes a system information/network map in the form of nodes and interfaces and guides the user in answering automatically

formed questions regarding presence of mitigation controls from selected standard and identified security characteristics.

- risk assessment is based on manually constructed threat model. For example, TRACE tool developed by MITRE, takes as input network map, manually created attack tree and specified vulnerabilities to perform simulation performs Monte Carlo analysis and outputs Likelihood and Impact to mission.

MBSE Approach

Originally, automated risk assessment solution has been developed in the context of the Model-Based Systems Engineering (MBSE) approach [3,7,8]. MBSE is an emerging discipline where a formal machine-readable model of the system is used as the 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. Currently, we support a particular MBSE approach known as Unified Architecture Framework (UAF) published by Object Management Group (OMG) International Standard Organization were the language architecture is in terms of UML profiling mechanism. UAF is aligned with ISO 42010 (Architecture Description), is flexible to support all domains and supports model of models by enabling development of integrated model layers.

The input UAF 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 UAF risk-relevant models/views
- "fit-for-purpose" analysis of the developed UAF models/views to determine level of confidence in the outcomes of risk assessment, e.g. **Correctness**, **Completeness**, **Consistency, Causality** and **Correlation**.

By implementing internal pivotal model, we were able to work and seamlessly integrate with other MBSE approaches where our 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.

MS Word-based Template Approach

As we discovered by working with client 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, specifically classified as internal vs. external information exchanges
- the data types with their security classifications (e.g. Classified/Unclassified, Secret, ..) and impacts (Confidentiality, Integrity and Availability)
- the data flows of the system under assessment describing system activities/scenarios
- system capabilities as they relate to defined activities
- Persons/operators involved with devices (this is to ensure that insider attacks are considered: e.g. malicious, clueless or carless operator)

These tables are imported, mapped to our internal pivotal system model and interpreted in the context of the selected knowledge base to build the model of the system under assessment.

There are other Word document-based templates for describing systems, one of them is IEC 62559-2, Use case methodology with focus on defining requirements for the system. Although the IEC 62559-2 Use case Word document-based template consists of some key information needed for risk assessment, it has some gaps. However, it can be utilized in current automated risk assessment solutions in a couple of ways:

- Utilize current IEC 62559-2 Use case template and manually enter additional system information needed to perform risk assessment (internal pivotal system model helps to assess gaps and provide the guidance for additional information)
- Extend current IEC 62559-2 template to capture additional information necessary for risk assessment

Also, information captured in the template needs to reflect system throughout its lifecycle (become living document), ensuring that system information provided in the template accurately reflects system as implemented and not its assumptions.

CASE STUDY

This paper describes a case study performed by KDM Analytics and JP Elektroprivreda BiH, the biggest power utility company in Bosnia and Herzegovina to evaluate the usefulness of this approach. We started a 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. A Word document template was given then to the cybersecurity team to enter the information about the SCADA system. 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.

As the result of this quick initial effort, we felt that the cybersecurity team has jump-started their automated risk assessment environment: they had established an easy to modify template in the form of a Word document and used the automated tool to reassess the model in a matter of seconds [11].
This case study strongly demonstrates the feasibility of the model-based risk assessment approach. The automated risk assessment capability is objective, systematic, repeatable and cheap to use iteratively, and it can be used as a communication tool which can explain to the executive management the cost of risks and priorities of implementing security controls to mitigate risks.
Description of the system through Word document is not ideal, but reasonably quick. For example, more high-fidelity facts can be obtained directly from the System Configuration Utility (SCU) files but requires an upfront development of the importer and some tuning until the first results can be obtained. The use of easy to understand tables in the context of a Word document makes it easy to spot inconsistencies and re-run analysis. This approach facilitates a quick start into risk assessment by starting with a simplified model to frame the

top risks and then evolving the model by introducing additional detail to increase the confidence of the assessment.

The Case Study is 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.

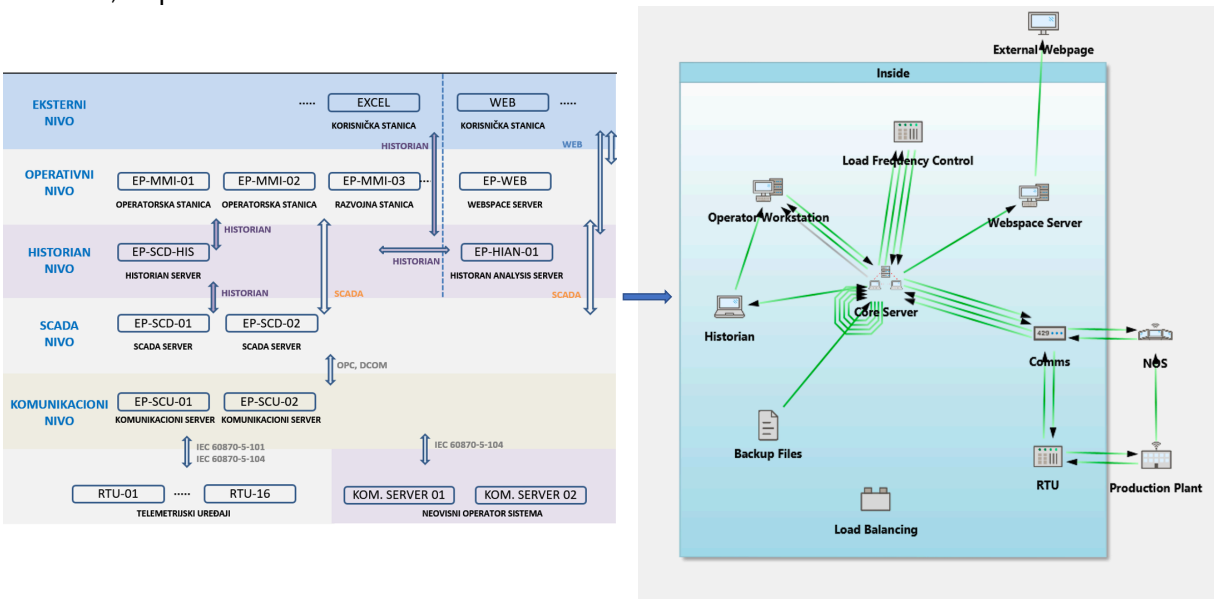

Figure 1: EP BiH SCADA implementation and automatically synthesized graphical model based on Word tables' information

It is important to mention that modelling the system takes several iterations, in this Case Study we did couple of iterations to ensure correctness of this high-level model.
Provided SCADA information is imported into automated risk assessment solution, Blade Risk Manager (BRM) for the analysis. It is important to note that:

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

Results of the Case Study

The first step was to assess the initial risk of the system, meaning that we are not considering any security controls that system might have implemented - initial phase. This step is important in order to understand:

1. considered threats and associated attacks (including multi-stage attacks) and adjust them to reflect better understanding of threat environment for given system,
2. prioritized row risks and their distribution in order to prioritize mitigation options – balancing system's security with our budget and resources.

The Overall Results from this first step are summarized as follows:

- The overall risk of SCADA at production level (SCADA DC) is Very High
- 40 risks were identified: 1 of them Very High, 5 of them High, 25 Moderate, 5 Low, and 4 Very Low (Refer to Table 1; NIST 5X5 Risk Metrics). Risk levels are based on the NIST

800-30 Risk assessment DoD Risk Management Guide and are computed based on the risk group's likelihood and impact.

- 161 threat events were considered, covering all key performers. From this analysis, 28 different attackers are identified.
- The undesired events corresponding to security risks were identified, and full fault trees constructed, linking them to threat events. This produced 1327 attacks

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 1: Overall Risk Metrics by Risk Group Count

Table 2 below captures the top 6 risks for SCADA DC. For each risk, the values of likelihood and impact levels are noted as the computational input for each risk level. The risk percent denotes this risk group's contribution to the overall risk (100%).

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 2: Top 6 risks

Furthermore, there are 6 key tables describing risk distribution, below we present 3 of them (Table 3 through 5) - each showing how risk is distributed among the components. This is important information influencing decision making process.

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

Table 3: Attack Performer/Node risk percentage distribution

Attacker	Category	Risk %	Risk Rank
Malicious Supervisory Control and Data Acquisition on production level (SCADA DC) Supplier	Human Malicious Internal	17.5	1
Nation state	Human Malicious External	12.6	2
Malicious Supervisory Control and Data Acquisition on production level (SCADA DC) Operator	Human Careless Internal	8.2	3
Careless Supervisory Control and Data Acquisition on production level (SCADA DC) Operator	Human Malicious Internal	7.8	4
Clueless Supervisory Control and Data Acquisition on production level (SCADA DC) Operator	Human Careless Internal	7.5	5
Careless Administrator	Human Careless Internal	6.8	6
Malicious Administrator	Human Malicious Internal	5.7	7

Careless Operator	Human Careless Internal	5.4	8

Table 4: Attacker risk percent distribution

Sensitive Asset	Category	Risk Percent	Risk Rank
Process Data information	Information	54.7	1
Request Data information	Information	7.7	2
Calculated Items information	Information	7.7	3
Regulation Items information	Information	7.3	4
System control capability	Capability	3.5	5

Table 5: Sensitive assets percent distribution

Also, attack/fault tree is automatically generated for the review of particular attack/fault paths (Figure 2).

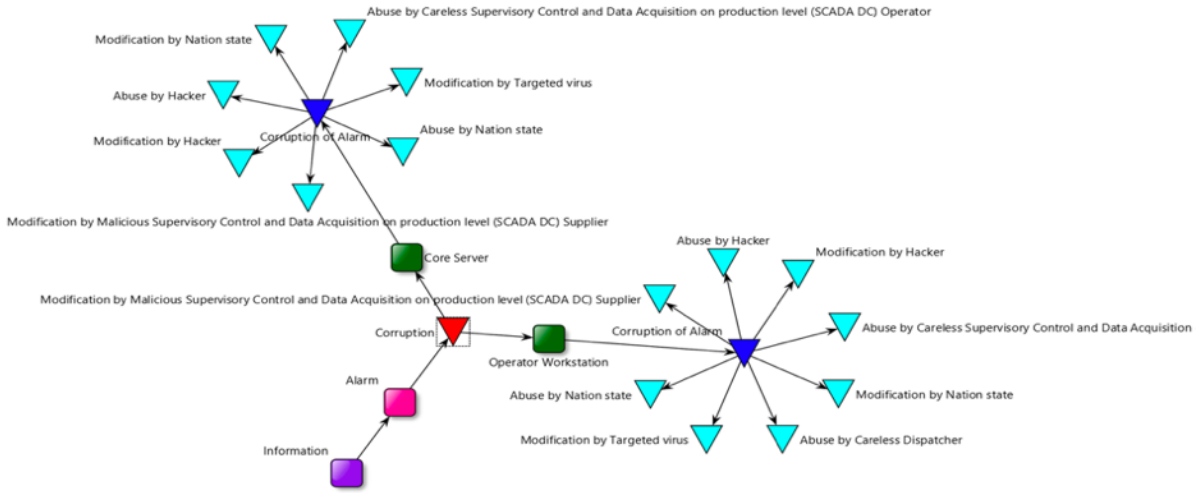

Figure 2: Visual representation of part of Attack Tree related to Corruption of Alarm Information

Based on this information, our next step would be to mitigate top 6 risks and reduce the overall risk level at least to moderate. To do this step, we first need to determine impact level of SCADA DC – this would mean if SCADA DC is successfully attacked, what would be an impact on overall operation and how critical that operation is. Not every and each system should be protected equally, impact levels are deferent based on security criteria assigned for industry. That criteria should examine number of parameters such as: any life lost, how many regions/people are affected, do we have back-up solutions, … etc.
For this Case Study, we chose NIST 800-53 Low Impact Level. The chosen impact level makes the determination what type and how many Security Controls will be pulled-in and made available to tool to choose from 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”.
Once Baseline is defined, we can start mitigating top risks. It was done by invoking the attack and vulnerability list for top 1 risk, choosing all listed vulnerabilities and invoking auto-mitigate command. This was repeated for 5 other top risks. 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. This would be optimal and most effective mitigation. After top 6 risks are mitigated, the risk is recalculated, and the resulting changes are summarized as follows:

- The overall risk of SCADA DC on production level is Low

- 40 risks were identified: 0 of them Very High, 0 of them High, 1 Moderate, 30 Low, and 9 Very Low. Risk levels are based on the NIST 800-30 Risk Assessment DoD Risk Management Guide and are computed based on the risk group's likelihood and impact.

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 - 0	R5 - 0
L3 - Occasional	R1 - 0	R2 - 1	R3 - 1	R3 - 0	R4 - 0
L2 - Remote	R1 - 0	R2 - 0	R2 - 4	R2 - 2	R3 - 0
L1 - Improbable	R1 - 0	R1 - 1	R1 - 7	R2 - 19	R2 - 3

Table 6: Mitigated risk metrics

As a final product at this level we were able to automatically generate security requirements in the following terms:

1. List of Security Controls per target (nodes and links) with implementation guidance – all exported in spreadsheet for easy management (the sample presented in Table 7).
2. Software related vulnerabilities that needs to be checked against source code either through penetration testing, static code analysis, using automated application security testing tools and identification of known vulnerabilities. The list is exported in the spreadsheet for easy management (the sample presented in Table 8).

Control Id	Control Name	Target Name	Target Element	Effective?	In 'Very Low Impact Controls' baseline?	Guidance
AC-19	Access Control for Mobile Devices	Core Server	Performer	Yes	Yes	The organization: a. Establishes usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices
AC-18	Wireless Access	Core Server	Performer	Yes	Yes	The organization: a. Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access b. Authorizes wireless access to the information system prior to allowing such connections.
AC-17	Remote Access	Core Server	Performer	Yes	Yes	The organization: a. Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and b. Authorizes remote access to the information system prior to allowing such connections.

Table 7: The sample of exported Security Controls list that reduce risk to Low when implemented as per guidance

Target	Element	Vulnerability Level	SFP Id	CWE Id	CWE Name
Core Server	Performer	V5 - Very High	SFP-04	CWE-431	Missing Handler
Core Server	Performer	V5 - Very High	SFP-04	CWE-248	Uncaught Exception
Core Server	Performer	V5 - Very High	SFP-04	CWE-600	Failure to Catch All Exceptions in Servlet
Core Server	Performer	V5 - Very High	SFP-04	CWE-252	Unchecked Return Value
Core Server	Performer	V5 - Very High	SFP-04	CWE-253	Incorrect Check of Function Return Value
Core Server	Performer	V5 - Very High	SFP-04	CWE-478	Missing Default Case in Switch Statement
Core Server	Performer	V5 - Very High	SFP-19	CWE-609	Double-Checked Locking
Core Server	Performer	V1 - Negligible	SFP-36	CWE-272	Least Privilege Violation
Core Server	Performer	V1 - Negligible	SFP-16	CWE-022	Path Traversal
Core Server	Performer	V1 - Negligible	SFP-16	CWE-023	Relative Path Traversal

Table 8: The sample of exported vulnerability list – vulnerabilities categorized as very high need to be eliminated

UPDATE TO ORIGINAL PAPER

In this short update to our original paper, we elaborate further on importance of attack tree and quantifiable risk calculation – addressing some of received questions.

Our methodology involves a unique 14-tier attack tree (Mission-Asset-Subsystem-Target-Threat Event-AttackSurface-AttackKind-EntryPoint-AccessPoint-AttackVector-AttackPath-Tactic-AttackMechanism-Attacker). The catalogue of elements for each tier has been accumulated over the last 10+ years of research and risk assessments. Each tier is tailored to the system under assessment, based on the systematic evaluation of its design. The attack tree is supplemented with a built-in assurance case: an argument that actively ingests available evidence to maximize confidence that all possible attacks have been accounted for. Completeness of an argument is essential for automatically constructing effective defence-in-depth options for the given budget. This methodology is crucial when determining and mitigating attacks driving the risk to its level, thus focusing resources and efforts where it matters. We demonstrate this in the Case Study by choosing a risk presented in Figure 2 "Corruption of Alarm Information" (marked as Moderate Risk in yellow) and producing a Risk Assessment Report (RAR). RAR identified driving set of attacks, among all attacks contributing to the risk. Figure 3 below is generated RAR with distilled information describing drivers of the risk level to Moderate (Corruption of Alarm by Malicious Supervisory Control and Data Acquisition on production level (SCADA DC) Supplier & Corruption of Alarm by Careless Dispatcher) and suggested Security Controls (SCs) to be applied reducing the risk to Very Low Level.

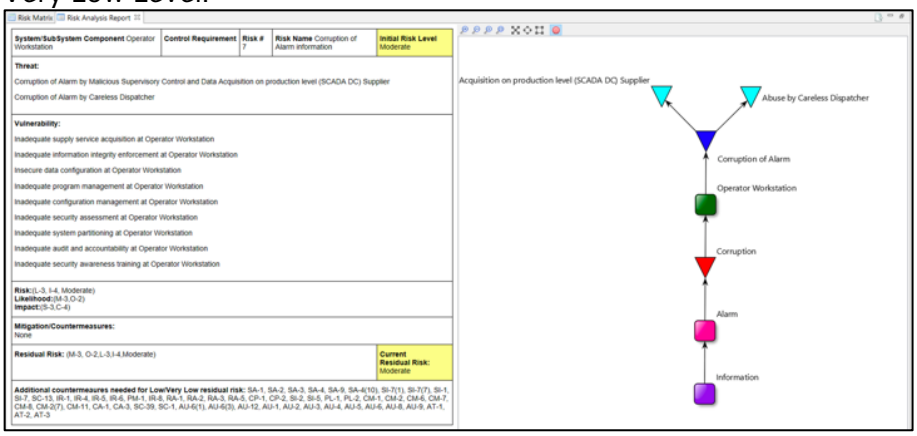

Figure 3: Distilled information focusing on driving forces of the Corruption of Alarm Information risk level to Moderate

As next step we choose and apply a set of SCs that would reduce the risk to Low vs. Very Low Level and regenerate report. The new RAR is presented in the Figure 4 outlining the risk level reduction: Low level (green), rank 27, applied SCs, suggested SCs to further reduce risk level.

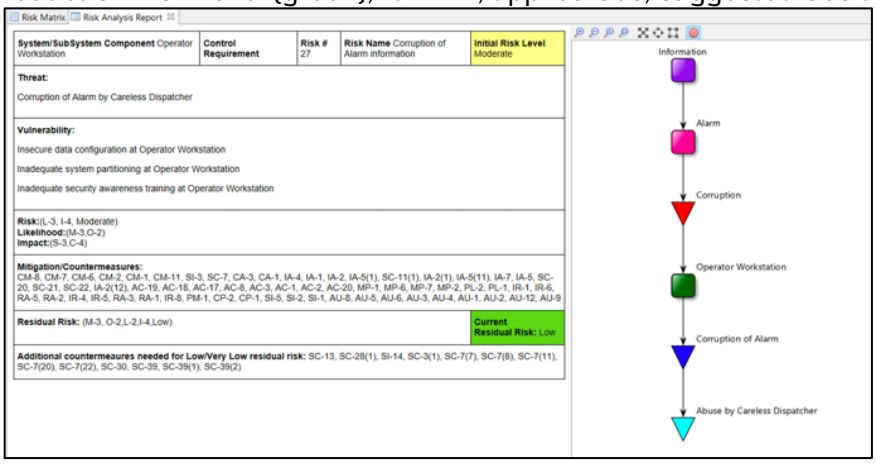

Figure 4: Updated distilled information of the risk after mitigations applied to reduce risk level to Low

CONCLUSION

Understanding, assessing, and managing risk for today's complex SCADA systems can be costly and laborious. Often the process is ad-hoc and subjective, making results difficult to compare between systems and organizations, depending on the risk assessment professional [2]. Power Utility organizations could benefit from model-based risk assessment approach and existing automated risk assessment technologies due to its systematic, comprehensive, objective, timely and cost-efficient nature [6,7]. It can be used as a communication tool which can explain to the executive management 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.

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]