2024 Paris Session

10770

D2 Information Systems, Telecommunications and Cybersecurity

PS2 cybersecurity in emerging application domains and technologies for securing energy organisations

Performing Risk Assessments of EV Charging System

Djenana CAMPARA*

BH K CIGRE

BiH

djenana@kdmanalytics.com

Dr. Nikolai MANSOUROV	Adnan BOSOVIC	Svetlana MISUT	Adnan AHMETHODZIC	Dr. Meludin VELEDAR
KDM Analytics	JP Elektroprivreda	JP Elektroprivreda	JP Elektroprivreda	BH K CIGRE
Canada	BiH d.d. - Sarajevo	BiH d.d. - Sarajevo	BiH d.d. - Sarajevo	BiH
nick@kdmanalytic.com	a.bosovic@epbih.ba	s.misut@epbih.ba	a.ahmethodzic@epbih.ba	meludin.veledar@gmail.com

SUMMARY

As Electric Vehicles (EVs) become more available and the long-term policies to phase out gasoline-powered vehicles are being adopted there is a growing demand for EV Charging Station (EVCS). EVCS system described in the section below ("**Description of the EVCS System"**) is connected to the power grid to deliver power to the EV. To be effective, EVCS system depends on several critical infrastructure sectors and require interoperability between numerous systems. Internet Services technology enables automated end-to-end information exchanges with minimal human intervention to authorize charging, orchestrate the charging process, and manage a load. However, these enhanced information exchange capabilities raise a growing concern over cybersecurity-related risks including security supply chain components.

Control systems utilized in EVCS are often referred to as Operational Technology (OT). Such systems involve a central controller configured to receive an ancillary service order from a power grid and distribute it to one or more local controllers periodically, which in turn are configured to control a multitude of electric vehicle supply devices based on the distributed ancillary service order in real time. Over the years, these control systems have evolved from air-gapped, independent OT systems towards interconnected and interdependent conglomerates embracing IT-enabled networks, systems, and infrastructure. As a result of IT/OT integration, EVCS components become exposed to the outside world, which has a rather complex geopolitical and regulatory structure, with impacts on the security of these systems. The attack surface has expanded due to the possibility of cyber threats coming from multiple new directions: direct attacks aimed at the EVCS system or indirect attacks through other critical infrastructure or supply chains that could impact the operations or security of the EVCS system. The opportunities to corrupt, compromise, and disable networks and systems have grown exponentially, resulting in new and highly automated malicious mechanisms. In their effort to protect systems

against these highly automated malicious mechanisms, federal regulators are hardening their requirements for cybersecurity protection and are emphasizing the need to demonstrate systems' compliance and effectiveness of its protection mechanisms. Consequently, this situation requires more advanced ways to analyze and certify such systems.

Within this landscape, traditional risk assessment is a manual, long, costly, and laborious process that relies on subject matter experts to keep up with changes, constantly advancing their own knowledge related to new threats and/or regulations. This is both costly and time-consuming. The community must come to the realization that risk assessment is a big data exercise that includes not just risk assessment of complex systems and risk prioritization but also selecting optimal mitigation solutions and calculating their effectiveness. We need to question ourselves: in the digital era, should we be manually performing big data analysis to protect our systems, operations, and organizational reputation?

The objective of this paper is to cover the benefits of applying an agile risk assessment process to EVCS to comply with today's government cybersecurity requirements for protecting related infrastructure sectors. As a part of this objective, KDM Analytics partnered with JP Elektroprivreda BiH d.d. - Sarajevo (EPBiH), the biggest power utility company in Bosnia and Herzegovina, to perform an agile risk assessment of an EVCS deployed and supervised by EPBiH to

1. systematically and comprehensively identify cybersecurity-related risks in EVCS
2. automatically identify the current EVCS cybersecurity posture and recommended mitigations
3. quantify the benefits of the agile, model-based risk assessment approach.

KEYWORDS

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

INTRODUCTION

As the landscape of both threats and regulations is rapidly changing, time is of essence; therefore, there is a need for systematic and comprehensive risk assessments of EVCS in near real-time, resulting in a proposed course of action to harden the protection of the system to ensure a secure supply chain, protection of sensitive information, and readiness to mitigate cyber-attacks. These requirements demand agility and scalability in the risk assessment process.

The amount of evidence required to determine EVCS conformance to certification can be overwhelming, resulting in superficial, incomplete, and/or unacceptably long evaluation cycles. The main factor preventing increased scalability of risk assessment and certification practices is the widespread use of human evaluators. The consequences of using manual effort in risk assessment are significant: the cost of each assessment is high and dependent on the size of the system; the number of assessments conducted at any given point in time is limited; skills are hard to transfer; and lessons learned during one assessment are difficult to apply to other systems.

Cybersecurity Risk Assessment tools are facing challenges in supporting diverse cybersecurity frameworks, catalogs (e.g., threat catalog, security control catalog), standards, requirements, attack mechanisms, etc.; however, few of them (if any) are expressed in machine-consumable content. Over the last several years, the industry has found ways to overcome some of these challenges and deploy automated model-based risk assessment within defense industry. In our previous paper, we showed how this automated solution has also been extended to Smart Grid systems [4].

PROJECT STRUCTURE

The goal of this project was to identify possible risks associated with Electric Vehicle Charging Stations (EVCS) currently deployed by EPBiH within country. Deployment consists of 12 EVCSs.

In this project, our approach has the following considerations:

- **EVCS System Information**: The risk assessment of the EVCS system is based solely on its architecture (operational, logical, and physical), and proposed risk mitigations are expressed in terms of Security Controls
- **Agile Risk Assessment Solution**: We utilized the commercially available Automated Cyber Risk Assessment Solution (CRAS)This solution is applicable within a broad spectrum of mission- critical requirements, such as aeronautics, defense, public security, healthcare, and the Internet of Things. It ties foundational risk assessment (correlating attacks and controls that mitigate attacks) to security requirements expressed in broad terms (such as the NIST Risk Management Framework (RMF)), overlays controls with frameworks of users' choice, and provides full traceability of risk mitigations to a system's security requirements.

Why Agile Risk Management?

While security practices in engineering became more mainstream (security is often built-in rather than bolted-on); however, as the system gets larger and more complex, its design erodes, which hinders system comprehension, compromises architectural integrity, and decreases maintenance productivity. This creates several problems moving forward. Very often quick fixes are introduced with many shortcuts and only a partial investigation for the obvious "weak links". New functionality is usually "shoehorned" into the pre-existing architecture in response to yet another security panic that further compromises the security of the system.
This situation is more aggravated by frequent changes in threat environment and/or regulatory Policies in response to the accelerated frequency and severity of cyber threats and attacks.

Within this landscape, traditionally, the manually driven risk assessment process is a long, costly, and laborious process that relies on subject matter experts to keep up with changes, constantly advancing their own knowledge related to new threats and/or regulations. This is costly and requires time, – both

of which are limited resources. Obviously, this type of analysis is a big data analysis that includes not just risk assessment of complex systems and risk prioritization but also selecting optimal mitigation solutions and calculating their effectiveness [5]. This traditional risk assessment/management process does not produce the timely results necessary to address immediate threats and very often produces a false sense of security due to lack of systematic and comprehensive methods. Agile Risk Assessment Solution promises to overcome these shortcomings because it is automated and easily adaptable to changes in all areas, such as the system's architecture, threat environment and regulatory policies. It enables a quick, detailed, and assured risk assessment process with a timely response and optimal results. We will utilize this solution to perform a risk assessment of an EVCS system currently deployed by EPBiH and suggest optimal mitigations. We'll establish the infrastructure for risk management of the EVCS system to rapidly respond to changes related to the system's growth (e.g., new capabilities, expansion in the number of charging stations), threat environment and regulatory policies.

Setting up Agile Risk Management Solution

The key to the success of 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, aimed at maximizing assurance confidence, and is guided by a built-in assurance case for risk assessment that answers the question "How do we know that all possible risks have been identified?" [2, 3].

There are 2 sources of data for risk analysis performed by utilizing CRAS: 1) User-provided system information; and 2) CRAS-incorporated cybersecurity, threat, and regulatory context information.

System Information

The system information provided by the user needed to be in machine-readable form. Some industries, like the defence and automotive industries apply Model Based System Engineering (MBSE) during the 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 in 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 was published in the CIGRE-Paris paper [3].

The system model needs to be able to tell a "cause-and-effect" story for the system under analysis in order to provide high confidence in the risk assessment outcome. Therefore, an automated solution (such as one we used) needs to be able to perform "fit-for-purpose" analysis of the developed model (e.g. Correctness, Completeness, Consistency) [1] and generate a report. CRAS is also capable of importing models created by different MBSE tools. However, 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 [3,4]. To lower the barrier to entry into repeatable and objective risk assessments using the automated capability, the CRAS import capability was extended to understand system models created utilizing information captured in MS Word Tables, a light-weight approach to modelling OT (control) and IT systems. Information from tables is parsed and analyzed for "fit-for-purpose." At the end, a graphical model representing the system/system of systems is created automatically, ready for users review and any corrections, if needed.

CRAS-incorporated Cybersecurity, Threat, and Regulatory Context Information

Risk assessment revels how system fails when attacked, and helps prepare the system (and its defenders) for real attacks by building defences, planning, and training. The system "goes into battle" with the best defences, plans and training – as recommended by the risk assessment. The objective of the ***agile*** risk assessment is to automatically assess the system (as described by a formal model), so that when the situation changes, the defenses can adequately change as well – as often as needed and as quickly as

needed. Example of changes are new functionality of the system, new regulations, new ways of conducting business, and/or new threats. Quick re-assessment of the updated model is not possible when manual practices are involved. Since it usually takes some time to implement the new defence plans and mechanisms, agile risk assessment allows organizations to become truly proactive by simulating new threats prior to actually experiencing them in real-time.

The key step in the agile risk assessment is the automated construction of the attack tree directly from the system information [2]. The system's operational architecture is analyzed to determine the relative operational importance of hosts and applications. The system data is combined with cybersecurity 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 the aim of computing 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 this approach as a fully automated Cyber FME(C)A - Failure Mode, Effects, and Criticality Analysis [2, 4].

ELECTRIC VEHACLE CHARGING STATION (EVCS) PROJECT

Description of the EVCS System

The EVCS system information was obtained through a series of technical stakeholder interviews and documentation reviews. The information was captured in an evolving Architecture Analysis Report (AAR) document utilizing MS Word tables (machine-readable content described in the above section, "System Information") augmented with narrative text describing the high-level architecture and functions of the EVCS system. This AAR document formed basis for the EVCS architecture model used in Risk Assessment.

The high-level architecture and functions of the EVCS system are described as follows:
The e-mobility system consists of charging stations and a back-end system for monitoring and managing these stations. The charging stations have integrated controllers that control charging, authenticate users via RFID cards, record sessions, and perform several basic functions that enable the autonomous operation of the charging station. The controllers also support the Open Charge Point Protocol (OCPP) protocol for communication with the Charging Point Management System (CPMS) system and connecting the charging station via the IP network. The charging stations are connected to the CPMS system, currently used by EPBiH, via the Internet and the OCPP protocol. Currently, the system uses a mix of version 1.5 of the OCPP protocol (using the http protocol, although htpps is also supported) and version 1.6.

A cloud-based CPMS software is exclusively intended for the field of e-mobility. EPBiH uses this system as a SaaS type service, with access via the Internet and the https protocol, with the use of appropriate user credentials. The system provides all the functions necessary for the functioning of the electromobility system. EPBiH currently uses only a part of the functions that are needed at the moment, namely: Monitoring the status of filling stations, Recording and display of charging sessions, Registration and working with clients, Reporting on events, Defining users and their permissions.
The system also provides several functions, that are currently being tested and certified for deployment: Billing and payment functions, Roaming functions, Interface to the Front-end system for mobile users.
In addition to its own users, EPBiH provides access and limited capabilities for the use of certain functions to partner EVCS systems (charging stations owned by partners).
Charging stations at EPBiH locations are connected to the CPMS system via the Internet, as follows:

- Charging stations at EPBiH locations are connected through the optical WAN network of EPBiH, with access to the Internet through the corporate firewall.
- DC charging station of EPBiH is connected via mobile network and corporate access service (private AP); an external router is installed at the location of the charging station, which enables connection in the mobile network.
- Charging stations owned by third parties are connected via LAN networks and Internet connections at the locations of the charging stations.

The basic use cases involve:

- User registration and authentication: The system registers RFID cards for user identification, which can be used in the system. Upon receipt of a request from the user, the users are registered in the system (manually specified user data is entered), and a specific RFID is attached to them, which is given to the user for charging.
- Monitoring the status of charging stations: The operator uses a dashboard display to monitor the connectivity and status of the charging stations connected in the system; in addition, defined users receive reports in case of the occurrence of relevant events in the system.
- Session data: Session data that is archived in the system is used as needed for various analyses. Detailed data on sessions are available in the system (user, charging station, connector, method of identification, duration, consumed energy, maximum power, beginning and end of the session, etc.).

Producing the AAR document was an iterative process since CRAS flagged several gaps and inconsistences in the informal description that needed to be addressed. Once the System Diagram was produced by CRAS and reviewed by the EPBiH team several corrections were made.

Internal Components	External Components
1. **EP Charging Station (EP-EVSE)** 1. **System Charging Station Controller** 1. **System Controller** 2. **EVSE Data Storage** 2. **CPO-EVSE Communication Servers** 1. **EVSE WebServer** 2. **EVSE AppServer** 3. **HMI** 4. **Maintenance Terminal (MT)** 5. **Supply Equipment Communication Controller (SECC)** 6. **Power Module Control** 7. **Heat Controller** 8. **Charger Meter** 2. **CPMS** 1. **CPMS Communication Servers** 1. **CPMS AppServer** 2. **CPMS WebServer** 2. **EV Charging Stations Control and Monitoring (EVSE-CM)** 3. **CRM** 1. **CRM Database (CRM-DB)** 2. **CRM Helpdesk** 4. **Support and Maintenance Service Subsystem** 1. **Maintenance** 2. **CPMS Data Storage** 5. **Usage Service Subsystem (Usage)** 6. **Authentication Service Subsystem (Authentication)** 7. **Billing Service Subsystem (Billing)** 3. **Charge Point Operator (CPO)** 1. **CPMS Operator Dashboard (CPMS-CPO)** 2. **EVSE WebClient (EVSE-WebCPO)** 3. **EVSE AppClient (EVSE-AppCPO)**	**1. Vehicle (EV)** **1.1. EV Communication Controller (EVCC)** **1.2. Battery Management System (BMS)** **1.3. Electronic Control Unit (ECU)** **1.4. Telemetric Control Unit (TCU)** **1.5. On-Board Diagnostic Unit (OBDU)** **1.6. Gateway** **1.7. Head Unit** **1.8. EV-HMI** **2. Client Subsystem** **2.1. Client HMI** **2.2. Client Browser** **2.3. Client Mobile** **2.4. EV Client** **3. EV Original Equipment Manufacturer (EV-OEM)** **4. EVSE OEM** **5. Partner Charging Station (PCS)** **5.1. Partner EVSE (P-EVSE)** **5.2. Partner CPO** **5.2.1. Sub CPO Dashboard (SubCPO-D)** **6. DSO** **7. Roaming Platform (RP)**

Figure 1: Internal and External EVCS components

The final EVCS System Diagram (graphical model) can be viewed at several levels of detail: aggregated and leaf levels (refer to Figure 2: Formal EVCS System Diagrams):

- Nodes (physical or logical devices) - their acronyms used in the CRAS Generated System Diagram are introduced in Figure 1: Internal and External EVCS components
  - Nodes could be leaf nodes (components) or aggregated nodes (e.g., subsystems, segments).
  - Nodes relevant to System Under Assessment (nodes being relevant to the context of the system) are placed "inside" the boundary, while nodes communicating with System Under Assessment (nodes being influential on the system) are placed "outside" of the boundary.
- Lines between nodes represent Exchanges (interfaces between nodes)
  - Exchanges are classified as internal or external information exchanges
  - Exchanges carrying data of the specific Data Type (e.g. SmartChargingInformation, AdjustUpgrade Capacity, Billing Info). Dashed lines indicate multiple Exchanges carrying data

of different Data Types. The data types are assigned sensitivity related to their security classifications and impacts (Confidentiality, Integrity, and Availability). Colors of lines outline security classification of data types (Blue indicates For Official Use Only, Green indicates Unclassified). Classification of data types plays role in risk assessment.

- ➢ Exchanges are grouped into scenarios referred to as data flows which describe systems' activities necessary to perform a particular capability.

❖ System's capabilities, relate activities and persons/operators involved with devices (ensuring insider attacks are considered: malicious, clueless, or carless) are defined in the model.

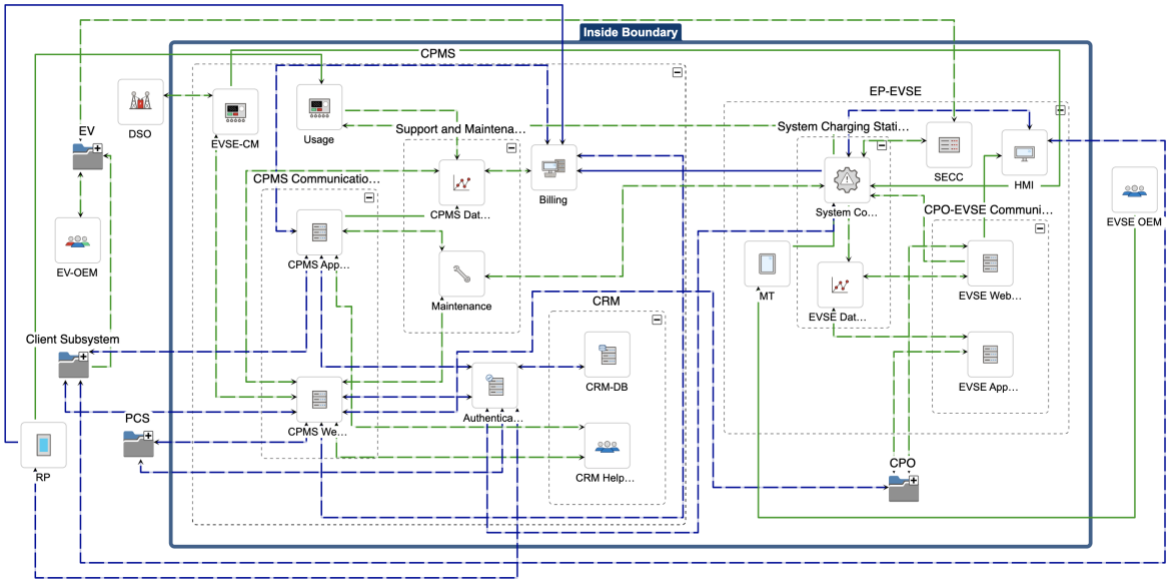

Figure 2: Formal EVCS System Diagrams (for a full name of components refer to Figure 1)

Tailoring Cybersecurity, Threat, and Regulatory Content

The next step consists of tailoring Cybersecurity, Threat, and Regulatory content. This is performed in the following way:

❖ Cybersecurity Rules: preconfigured for OT/IT systems

- ➢ CRAS provides a couple hundred rules covering cyber-attack space. Each rule composed of a valid combination from a set of 5 parameters (Threat Event Category & Pattern, Attack Tactic, Asset, and Attacker Category) is assigned a Means and Opportunity (likelihood of attack to happen and likelihood of attack to succeed when it happened) used to calculate the likelihood for that attack rule. Rules are extracted from various risk assessment standards, in particular NIST 800-30, Canadian HTRA and French EBIOS.. CRAS provides a second rule set describing Impact Severity and Criticality covering failure mode types. Once likelihood of all attacks and impact of all failure modes are determined risks are calculated and results presented in 5 by 5 risk metrics (refer to Figure 3: Risk Calculation and 5 by 5 Risk Metrics)
- ➢ It was determined that the EVCS System could use existing cyber-attack rules without major tailoring of its Means and Opportunities, while Impact Severity and Criticality of the failure modes were determined by the tailored sensitivity statements of the data types (captured in the AAR document).
- ➢ We further tailored the operational mission of the EVCS System, referred to as the Enabling to Recharge Electrical Vehicle mission, categorizing the availability and integrity of the mission as Very High and the Confidentiality of the mission as Moderate.

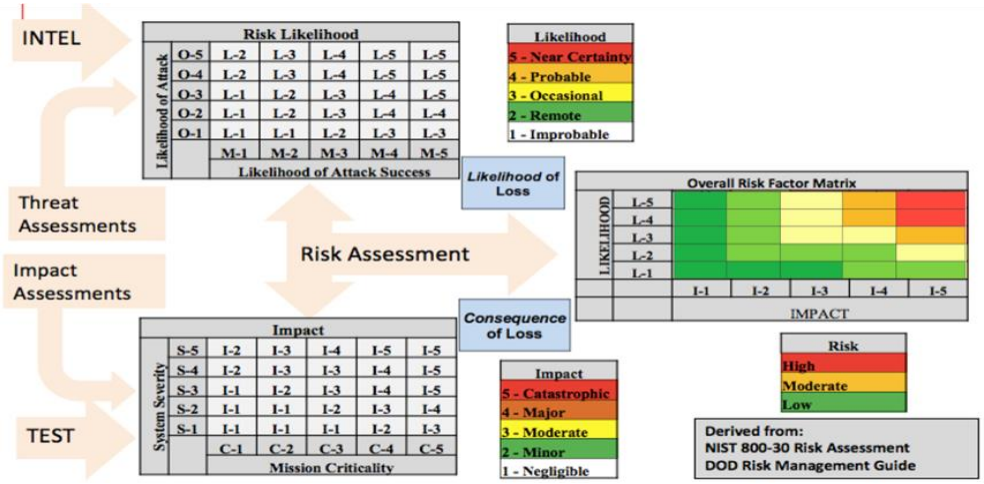

Figure 3: Risk Calculation and 5 by 5 Risk Metrics

- Threat Model: automatically generated for the EVCS System
  - Attacker Category (such as External, Maintenance, Internal, Malicious and others) are applied to all viable prospects and generated a set of viable attackers. The Internal attacker category has further decomposition into Clueless, Carless, and Malicious. Each attacker has a unique Means and Opportunities that are considered when calculating the resulting likelihood of an attack (which involves an attack type and a specific attacker).
  - For the purposes of this case study, EP Operators are highly trusted and knowledgeable personnel. This is due to a couple of reasons: the EVCS system is currently a small system (consists of 12 charging stations deployed), and EVCS Subject Matter Experts are selected to perform the EP Operator's role. This consideration warranted a reduction in likelihood (Means and Opportunities) for EP Operator Clueless, Carless, and Malicious attacker categories.
- Regulatory Content is determined by the system categorization for given regulatory policies. For the EVCS System, we applied the National Institute for Standards and Technology (NIST) Risk Management Framework (RMF) described in NIST SP 800-37 and NIST SP 800-53 Security Controls and identified an applicable baseline.
  - We determined that the current EVCS System is categorized at a Moderate level and should use a tailored NIST Moderate Baseline. In the course of the assessment, we recommended additional Security Controls to the NIST Moderate baseline (NIST Moderate Plus) to be able to mitigate top risks.

Once the EVCS System evolves and becomes a part of the nation's critical infrastructure, current tailoring will need to be adjusted to reflect the new reality related to the extended system and threat environment. However, all other parameters should stay the same; therefore, risk assessment could be performed systematically and comprehensively within hours rather than months.

EVCS Risk Assessment Results

Each identified EVCS risk is assigned a percent of the total risk and score (based on a harmonized scoring system where the initial risk score is the maximum available risk for the system while the mitigated risk score reflects the efficiency of applied mitigations in terms of Security Controls). The distribution of risks is presented in the form of a NIST 5X5 (refer to Figure 3: Risk Calculation and 5 by 5 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 - 9	R3 - 66	R3 - 4	R4 - 0
L2 - Remote	R1 - 0	R2 - 3	R2 - 5	R2 - 15	R3 - 1
L1 - Improbable	R1 - 4	R1 - 0	R1 - 0	R2 - 0	R2 - 0

Figure 4: Risk Distribution Metrics Prior Mitigations

Details of Assessment

- CRAS identified 107 risks with a maximum risk score of 269.5, characterizing system risk at a moderate level (assessment shows no High or Very High risks). The risk distribution for the current EVCS System is presented by risk metrics (refer to Figure 4: Risk Distribution Metrics Prior Mitigations).
- The undesired events corresponding to security risks were identified and integrated into the full attack tree, linking them to risks. A Criticality analysis of the nodes and operational exchanges was performed and prioritized based on their contribution to the overall risk.
- 1624 individual threat events were identified and integrated into full attack trees constructed for EVCS, linking them to the undesired events (and further to risks).
- The threat events were further expanded into 8335 attacks (a combination of an attack type and a specific attacker) and integrated into the full attack tree, resulting in a full correlation between risks and attacks.
- Each element of the resulting risk model was automatically given a structured English statement.

Risk levels are determined by the means and opportunities of the attackers (tailored as part of the selected threat environment; see above). Mitigations (security controls) are meant to make certain attacks more difficult and therefore, their impact less likely. CRAS calculates the "raw" risk score (based on the threat environment without considering any controls) and the "mitigated" risk score for a set of controls. The mitigated scores are calculated fully automatically from the same model, allowing the analyst to consider multiple mitigation variants as needed.

The top 5 risks were marked as risks that need to be mitigated:

- **Risk 1 & 2 - Deception and Failure of the operational mission: Enabling to Recharge Electrical Vehicle** are identified as the top two risks related to the EVCS mission which is Enabling to Recharge Electrical Vehicle. This is due to the mission's possible integrity and availability impacts caused by the attacks. CRAS has identified 186 possible attacks related to top 2 risks, of which 10 are prioritized as attacks that need to be mitigated. These 10 attacks are related to 2 categories, each impacting the same 5 software components: CPMS WebServer, EVSE Control and Monitoring, Authentication, CRM, and System Controller. These attack categories and their impacts are as follows:
  - **Multi-stage attacks** with targeted viruses (e.g. via phishing tactic) directed at identified software components. In this case, attacker installs and executes malicious code (e.g., rootkit, ransomware, spyware) in an effort to achieve a negative technical impact that enables them to deceive mission, causing the takeover control of the EVCS System:
  - **Impact 1:**. - Granting attackers great freedom to do whatever they want with consequence of financial loss for EPBiH (e.g. changing charging rates, can control start/end charging session) or
  - **Impact 2:** stealing credentials to impersonate an authorized client in an effort to steal power/payment with consequences for EPBiH such as loss of nonrepudiation and negative impact on EPBiH brand reputation.
  - **Attacks causing software failure** (e.g. via exploitation of known vulnerabilities) at identified software components. In this case, an attacker obstructs the interactions between system components. By interrupting or disabling these interactions, an attacker can often force the system into a degraded state or even to fail.
  - **Impact:** The consequence is the denial of charging service – EV not charged when needed leading to loss of clients' confidence. If attacks are coordinated cross multiple EVCSs (number of stations cross the country is small), no charging station might be available.
- **Risk 3 - Corruption of Smart Charging Information**: Smart Charging Information is sent by DSO to CPMS. CRAS has identified 16 possible attacks related to this risk, where 1 of them is prioritized as the attack that needs to be mitigated. This attack targets communication messages

between DSO and EVSE Controlling and Monitoring components containing information such as Cable Capacity Forecast (maximum forecast value, remaining value, start and end time of the block) and Heartbeat that include intervals. Category of attack and its impact is as follows:

- **A spoofing (Injection) attack** with the aim of corrupting the Smart Charging Information. There are many ways to perform this attack, e.g., through (1) Parameter Injection, where an attacker manipulates the content of request parameters for the purpose of undermining the security of the target; (2) Input Data Manipulation, where an attacker exploits a weakness in input validation by controlling the format, structure, and composition of data to an input-processing interface. By supplying input in a non-standard or unexpected form, an attacker can adversely impact the security of the target; (3) Traffic Injection, where an attacker injects traffic into the target's network connection. The attacker is therefore able to degrade or disrupt the connection and potentially modify the content.
- **Impact:** This attack, if successful, enables an attacker to tamper with power delivery and furthermore, tamper with chargers to introduce electrical conditions such as electrical short. Consequences are harm to the EVCS System and safety concerns for EV Driver (people could be injured while utilizing an EVSE).

- **Risk 4 - Corruption of Problem Report**: Problem report message is originated by the client and sent to the CPMS system. CRAS has identified 56 possible attacks related to this risk, of which 2 are prioritized as attacks that need to be mitigated. Category of attacks and their impact are:
  - **Both attacks are related to injection attack** targeting Problem Report message between (1) Mobile Client and CPMS AppServer, and (2) Web Client and CPMS WebServer. The intent is to corrupt the Problem Report message. The ways to perform this attack are described in the previous corruption risk above. Internally, this message is passed as an Alarm message requiring immediate consideration for an investigation or fix, e.g. upgrade the firmware.
  - **Impact:** If this Problem Reporting message is corrupted, consequences could result in multiple failures of the EVCS, including Denial of Service, effecting Charging Station availability when most needed. Also, if attacker crafted a malicious payload for firmware and previously successfully performed multistage attack as described above under Risk 1 & 2, the malicious firmware payload will be successfully delivered through legitimate update. If such attacks are coordinated cross multiple EVCSs (creating a botnet of compromised chargers), attacker can activate particular logic that can be used to target the power grid stability. It needs to be noted that currently country doesn't have enough EVCS systems and EVs to mount such an attack, however the growth in the EV numbers in the near feature would provide a large enough surface to make it possible.
- **Risk 5 - Disclosure of Payment**: This risk is related to the client's payment information, including but not limited to credit card information, that could be leveraged by a malicious actor (e.g., steal funds for their own purpose). CRAS has identified 39 possible attacks related to this risk, of which 15 are prioritized as attacks that need to be mitigated. These 15 attacks are related to 3 attack tactics: abuse, modification, and Information Gathering, and targeting 3 components: CPMS AppServer, the CPMS WebServer and Billing. Attack tactics and their impact are as follows:
  - **Abuse attack** can happen through attacks such as API Manipulation, Authentication Abuse, Authentication Bypass, Privilege Abuse, Buffer Manipulation, Exploitation of Trusted Credentials, Privilege Escalation and more.
  - **Modification attack** can happen through attacks such as Content or Action Spoofing, or Code Inclusion.
  - **Information Gathering attack** can happen through "excavation", where an attacker actively probes the target in a manner that is designed to solicit information that could be leveraged for malicious purposes.
  - **Impact:** These attacks, if successful, enable attackers to obtain client information that can be sold. Consequence is loss of clients' information and negative impact on EPBiH reputation.

Recommended Mitigations

To mitigate the top 5 risks using the NIST Moderate Plus baseline (provides a list of Security Controls to be used as a course of action to mitigate identified risks), the suggestions are to apply 218 Security Controls (mix of technical and organizational) to mitigate the list of vulnerability conditions that enable identified attacks involved in the top 5 risks.

- The following is a list of vulnerability conditions affecting 7 software components (CPMS WebServer, CPMS AppServer, Authentication, Billing, CRM, System Controller and EVSE Control and Monitoring) and proposed mitigations
  - Vulnerability conditions are Inadequate: program management, access control, supply service acquisition, identification and authorization, boundary protection and system partitioning
  - Suggested mitigations are:
    - Organizational: policy and procedures in area of security and contingence planning, access control, supply chain management, identification and authorization, system and service acquisition, and system and communication protection; acquisition process, develop security engineering principals, develop testing and evaluation
    - Technical: cryptographic module authentication, device id and authorization identifier management, identity proofing, boundary protection (e.g. network separations, deny by default - allow by exception), information input validation, memory protection from unauthorized code, separation of system and user functionality, route traffic to authenticated proxy servers,
- The following is a list of vulnerability conditions affecting 3 software components (CPMS WebServer, CPMS AppServer, and Billing) and proposed mitigations
  - Vulnerability conditions are Inadequate configuration management & security assessment, and Insecure failure & data configuration
  - Suggested mitigations are
    - Organizational: policy, procedures and plans in area of configuration management, assessment, authorization, user-installed software and software usage restriction; develop Plan of Action and Milestones, Assign a senior official as the authorizing official for the system, develop continuous monitoring strategy, configuration setting, system component inventory, software usage restriction and access restriction for change
    - Technical: predictable failure prevention, fail secure, Cryptographic protection of data/information, vulnerability analysis, prevent unauthorized and unintended information transfer via shared system resources;
- And one vulnerability condition effecting Data Flow for Payment information is Inadequate security monitoring. Suggested mitigations are system monitoring of system-generated alerts, inbound and outbound communications traffic, and deployment of automated tools and mechanisms for real-time analysis
- All Security Controls and their locations within the EVCS System are presented to the EPBiH in a spreadsheet format known as Security Control Traceability Metrics.

After proposed mitigations were applied, a new risk metrics in Figure 5: Risk Distribution Metrics When recommended Mitigations Applied showed the following risk distribution.

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 - 9	R3 - 65	R3 - 0	R4 - 0
L2 - Remote	R1 - 0	R2 - 3	R2 - 5	R2 - 18	R3 - 0
L1 - Improbable	R1 - 4	R1 - 0	R1 - 1	R2 - 1	R2 - 1

Figure 5: Risk Distribution Metrics When recommended Mitigations Applied

Managing a secure system involves a complex argument that must be supported by serious big data analytics. This security argument involves an enumeration of the attackable targets, assets, and

capabilities of the system (that are impacted by attacks and failures of the nodes and information exchanges) and also the enumeration of all possible attacks.

When CRAS systematically considered possible attacks on all targets (as they were described in the input AAR document), it was managing over 8000 attacks. The likelihood measure for each attack is derived from the tailored threat environment. It is important to emphasize that such measures must be managed outside of the specific assessment; only this approach removes subjectivity and allows assessment results to be transferrable and comparable from one assessment to the next.

Security countermeasures (referred to as security controls) constitute a completely separate dimension of the assessment since they address security concerns in a certain threat environment. For the same system, different threat environments may require different security controls, either because of the capabilities and motivations of the attackers or because of a different categorization. Note that each countermeasure is an application of a certain type of security control to a certain target in the system.

The main challenge here is to construct the entire attack tree fully automatically from the system data. Once the attack tree is constructed, the use of a human analyst changes dramatically to review the full model with full prioritization based on measurements, focusing on the outliers, top risks, and high-watermark attacks, and vulnerability conditions.

CONCLUSION

This project helped identify potential inherent risks of the EVCS system as it is deployed by EPBiH. The risk assessment was performed based on the given operational EVCS system architecture without consideration of any existing security controls. This enabled us to focus on the identification of inherent risks as the system is deployed and utilized by EPBiH and their clients. Also, it gave us an opportunity to recommend what set of mitigations (in the form of Security Controls) should be applied and what components those mitigations should protect the most. The recommendation could be compared with current protections to identify any possible gaps.

This project also underscored the need for an agile risk assessment approach. The agility of this approach, as illustrated by the EVCS case study, involves iterations on the input system information, applying different/modified threat environment contexts, and applying different security controls. After each modification, the CRAS solution simply re-builds the attack tree and re-applies the measurements, presenting the risk analyst with the views and data distributions that reflect the changes. Going forward, the EPBiH EVCS System will undergo expansion, and the threat environment will change. As the risk assessment process will need to be repeated, the infrastructure is in the place for a quick turnaround result (taking only hours vs. months).

BIBLIOGRAPHY

[1] Dr. N. Mansourov, D. Campara, A. Hrustemovic, MSc. A. Ahmethodzic, E. Hadzovic, Dr. M. Veledar, “Role of Digital Engineering and Digital Twin Technology in Cybersecurity of Electrical Grid” [CIGRE Paris 2022]

[2] 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]

[3] 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]

[4] D. Campara, Dr. N. Mansourov, A. Hrustemovic, MSc. A. Ahmethodzic, E. Hadzovic, Dr. M. Veledar “Cooperation through Automation: Applying Automated Cyber Risk Assessment for the Smart Grid” [CIGRE South East European Regional Council, 2020 Vienna, Austria]

[5] Djenana Campara, Steve Seiden, Leighton Johnson, “Automated Risk Assessment Process for Government Agencies & Industry Leaders: Cybersecurity Protection for Operational Technology” Autotestcon, August 2023 in National Harbor, MD, USA]