D7.2 Final Cyber Security Assessment of the HONOR Flexibility Market

Zeeshan Afzal, Mathias Ekstedt, Per Eliasson, Joar Jacobsson, Roysten D'souza

Status

Date	Person	Task	Status
2022-10-15	Zeeshan Afzal	setup of document	Finished
2022-12-06	Zeeshan Afzal	first draft	Finished
2022-12-07	All	internal review	Finished
2023-02-03	All	external review	Finished

Contents

1 Introduction

1.1 Objective

The HONOR project focuses on the development, implementation, and evaluation of technologies to facilitate and realize an energy flexibility market (FM) mechanism. A crucial part of delivering a holistic and practical solution towards such a market is its cyber security assurance. Since the proposed market opens new interactions involving different stakeholders and a distributed information and communication technology (ICT) infrastructure, this potentially results in new vulnerabilities and threats, stressing the need to thoroughly analyze and assess the cyber security posture of the developed ICT infrastructure. Previously, we presented a preliminary cyber security risk assessment of the HONOR project. This report presents the results from the final cyber security analysis. Just like the first assessment, the goal with the analysis is to discover and reveal how attackers can target the FM proposed by the project and what kind of weaknesses they can exploit to reach their desired goals. The assessment is based on a threat modelling approach using automated attack simulations on a system model. The system model is based on the HONOR technical architecture which in turn is based on the ICT infrastructure and the relevant data streams in a FM.

1.2 Scope

The FM system targeted by the HONOR project consists of strong integration of cyber, physical, and market domains. On one hand this cross-domain integration sets the foundation for efficient deployment of flexibility assets, on the other hand it also introduces new vulnerabilities to all involved stakeholders and their systems. This is partly a consequence of the grid operation process becoming dependent on third-parties thanks to the application of end-user flexibility. At the same time, there is a higher incentive for cyber criminals to cause physical and financial damage. It is thus pivotal to assess the FM system proposed by the project from a cyber security point of view. Only then can the advantages of FMs be stressed and exploited and the confidence of all stakeholders increased.

This report is focused on the results from the final cyber security assessment of the market system developed by the project. The analysis and evaluation process is based on the HONOR technical architecture presented in D6.1 [1]. For the purpose of this report, the description of HONOR use cases is out of scope. For HONOR use cases, the reader is referred to D3.1 [2] and for the HONOR system architecture to D3.2 [3]. An overview of the requirements and benefits of FMs is provided in D2.1 [4]. The preliminary cyber security assessment report is available at [**?**].

1.3 Approach and structure

Threat modelling is used to measure the cyber security of the system proposed by the HONOR project. The HONOR technical architecture is transformed into models using the threat modeling language coreLang [5] of the attack simulation tool securiCAD [6]. Both, the coreLang and the securiCAD tool are developed and updated to ensure that they accurately represent the design, vulnerabilities, and available defense mechanisms of the HONOR ICT infrastructure. Once models are built, automated attack simulations are performed. The simulations focus on a subset of flexibility oriented attack scenarios where an attacker tries to subvert the normal operation of a FM. The attack simulations not only reveal the potential paths attackers may take to reach and compromise their desired systems, but also the attacker difficulty (probabilistic) calculated as time to compromise.

The report serves as deliverable D7.2. The rest of the report is structured as following. Section 2 presents the necessary background with a particular focus on FMs and cyber security assessment. Section 3 forms the core of this report detailing the reader on the cyber security analysis. The section starts by describing the model development process. Next, a number of relevant attack scenarios are explored and potential attack vectors are revealed as part of the analysis. Finally, the section ends with a discussion on the results from the attack simulations. Section 4 provides a conclusion.

2 Background

This section provides the necessary background to help understand the work presented in this report. We detail on the need for a cyber security analysis for a FM, the approach we have used to measure cyber security, the language and tools that are employed, and the HONOR reference technical architecture.

2.1 Flexibility Markets

Electricity generation and consumption must go hand in hand. This balance is becoming increasingly complex to maintain with the increase in renewable energy sources such as distributed energy resources (DERs) and an ever increasing consumption thanks to electrification of more and more industries and devices such as electric vehicles (EVs) and heat pumps (HPs). The drive towards a fully decarbonised energy system and sector coupling is further expected to increase the electricity consumption by more than three times [7]. The main challenge is to deal with the uncertainty as electricity from sources such as sun and wind is highly volatile because of its weather dependency. The requirements on distribution grids are also radically changing. Originally designed for centralized generation, distribution grids are increasingly used as carriers of volatile and often bi-directional power flows [8]. At the European level [9], one of the key solutions towards solving most of these challenges is flexibility. The flexibility of the overall energy system needs to be increased. For instance, flexibility is needed to balance the fluctuating generation of green electricity with the high amount of demand through utilization of demand response [10]. Concretely, in exchange for financial compensation, consumers agree to adapt their use of the electricity to the demands of the grid. By reducing equipment loading during peak hours, a distributed system operator (DSO) can utilize local flexibility to delay or avoid investments for reinforcement of transformers and power lines [11].

FMs are a widely discussed concept [12, 13, 14] for the integration of local flexibility. Such markets constitute of a competitive trading platform for electricity flexibility typically in a geographically restricted area such as neighborhoods or towns [15]. Already, there exist a variety of market designs while many new concepts are under development [12]. A typical setup of market consists of a DSO, a balance responsible party (BRP), several aggregators and a market operator [10]. Aggregators manage and gather multiple small residential flexibility assets. In this way, aggregators enable end users participation on the FM. Larger flexibility assets, such as industrial loads, can potentially also directly participate in the market. In a FM, DSOs and BRPs are typically flexibility buyers, while aggregators or private persons constitute flexibility sellers. DSOs procure flexibility for operational purposes such as congestion management or voltage control. BRPs buy flexibility for portfolio optimization. By adjusting the power demand of the aggregated residential flexibility assets, the aggregators earn profits according to a flexibility agreement. The owners of the flexibility assets earn profits by providing a DER, such as a HP or an EV, as a flexibility assets to the aggregator. The design of a FM consists of strong integration of cyber, physical and market domains. Such an integration allows for efficient deployment of flexibility assets but also introduces new vulnerabilities to all stakeholders and their systems [10]. By applying end user flexibility to avoid critical grid states, DSO grid operation process becomes dependent on third-parties. Moreover, the required implementation of ICT and the strong integration with the physical and market domain opens doors for cyber criminals. In addition, incorporating home devices of end users as flexibility assets also requires transmission, storage and processing of sensitive data for flexibility management.

2.2 Threat Modelling

While there exist a number of approaches (e.g., consult penetration testers, security auditing, etc) to assess and estimate the cyber security of large ICT infrastructures, they all have their limitations [16]. Threat modelling and attack simulations appear to be the most promising approach for this task as shown by previous research [17, 18].

2.2.1 Attack Trees, Graphs, & Language

Attack trees and graphs are key formalisms in the field of threat modeling. They were first elaborated in [19] over two decades ago, and further popularized by Schneier [20]. Later on, attack trees were formalized by Mauw & Oostdijk [21]. An important extension of attack trees was introduced by Kordy et al. [22] to also include defenses as a means to enable the analysis of the effectiveness of various countermeasure strategies. Overall, a large body of work in the area up until 2014 is neatly summarized in [23]. A fairly large sub group in the field works with probabilistic attacks graphs, oftentimes using Bayesian networks as the underlying formalism for analysis [24, 25, 26, 27, 28, 29].

Attack trees and graphs basically encode what attackers need to do as steps, combined in logic *AND* and *OR* gates, in order to compromise a certain target. This logic thus gives rise to several alternative attack vectors. In order to estimate their difficulty, the nodes are associated with some form of resilience metric such as attacker cost, capability, or time needed to succeed with each step. This metric is dependent both on properties of the attacker and the technical implementation of the attacked system (a highly capable attacker will be more successful in compromising the system, but a better protected system will be more difficult to compromise).

The main issue with using attack graphs for threat modelling is the cumbersome task of manually generating a new attack graph for each system. The Meta Attack Language (MAL) [30], that this work is based on, belongs to the group of probabilistic attack graphs. MAL attempts to ease the cumbersome task of manually generating a new attack graph for each system. It can be used to define domain-specific languages (DSLs) for different domains such as industrial control systems (ICSs), internet of things (IoTs), vehicles, etc. Conceptually, a MAL specification of a system consists of different assets (e.g., Host), attack steps on the assets (e.g., Host.Compromise), defenses on assets (e.g., Host.AntiMalware) and finally associations/relations between different assets. All those parts make up the MAL specification which is defined in a MAL file. Additionally, to encode attack graph logic, attack steps are connected to each other, which means that the successful compromise of one attack step can enable attempting another attack step. Attack steps can be of two types, OR or AND. An encoding that compromises of at least one of its parent attack steps is required to compromise this step (OR) or that compromise of all parent steps is required (AND). Moreover, defenses relate to attack steps, and if enabled, act as obstacles for the connected attack steps. To each attack step, a probability distribution called the local time to compromise (TTC) can be associated, representing the difficulty of succeeding with the attack step. Defense steps are probability distributions over boolean values representing if they are active or not.

2.2.2 coreLang

For the cyber security analysis of the HONOR system, we use a threat modeling language known as coreLang [5]. Although coreLang existed before this work, the HONOR project has contributed to an extensive developmental and quality assurance work to make the resulting analyses more accurate and representative of the real world. coreLang as the name hints is the core language comprising of predefined assets that appear in most environments and systems. Thus, it can serve both as a starting point to create more domain specific languages and be used to

model generic environments. For a detailed background and motivation behind coreLang, the interested reader is referred to [5].

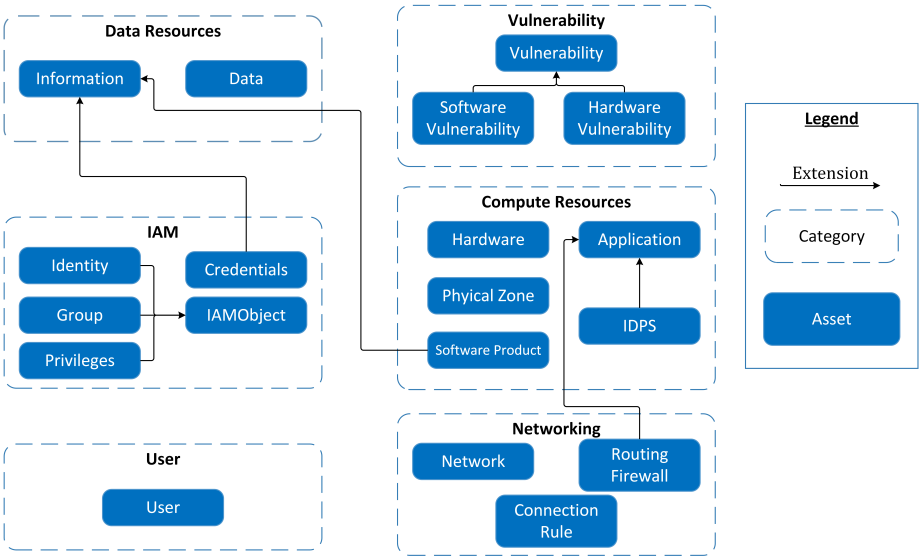

Figure 1: Overview of coreLang

Figure 1 presents the overall structure of coreLang. Assets in coreLang are grouped into six categories: `Compute Resources`, `Vulnerability`, `Data Resources`, `User`, `IAM (Identity and Access Management)`, and `Networking`. Below we briefly describe each of these six categories.

Compute Resources Software applications are the most common component of typical ICT infrastructure and, with exceedingly rare exceptions, cyber attacks target one or more of them as part of their operations. As such, the `Application` asset which represents any type of software running on a system is the most important asset in the language. It also contains a substantial number of attack steps to depict the various actions an attacker might take and many other assets interact with it.

Analogously, the `Hardware` asset specifies the hardware systems on which `Applications` can run. This asset is used to allow the attacker to obtain physical access to the hardware devices on which software applications are running.

`PhysicalZone` assets are used to group together `Hardware` and `Network` assets to represent that they are housed within the same area. If an attacker gains access physical access to a `PhysicalZone`, then they get physical access to all the `Hardware` and `Network` assets within it. Another asset introduced for the convenience of the modeler was the `SoftwareProduct` to specify that multiple `Applications` use the same software package, this can also be used by the attacker to launch supply chain attacks that compromise the source of the software being used in a particular environment. Various defensive measures used to protect software applications were coalesced into the `IDPS` (intrusion detection and prevention system) asset. An `IDPS` restricts many of the attackers actions on the `Applications` it protects. Because the `IDPS` asset extends `Application` it is also susceptible to the same of types of attacks normally targeting software applications, as such an attacker may be able to disable an `IDPS` in order to prevent it from protecting the `Applications` associated with it.

Vulnerability Vulnerabilities provide opportunities for an attacker to exploit flaws or weaknesses in software and hardware components in order to attain their goals. As the name implies the `Software Vulnerability`

asset is used to represent vulnerabilities in software components (i.e. Applications or SoftwareProducts). HardwareVulnerabilities function similarly, but they are used in association with hardware systems and are less configurable.

Data Resources In order to represent data that can be stored on Applications or Hardware or transmitted between Applications over Networks, we created the Data asset. An attacker gaining access to the data can then potentially read or alter it. Information, the other asset present it this category, is more conceptual asset than most of the other assets in the language. It represents any type of information and since information is immaterial, the Information asset always needs to be associated with Data containing it for it to be accessible for potential attacks. Data replication is also implemented by specifying that the same Information is backed up across multiple replicas.

User This category is quite straightforward, it consists of the User asset which acts as an attack surface for different social engineering attacks. The attacker can either extract credentials via phishing or trick the user into performing malicious actions (e.g. tricking the user into clicking on a malicious link). The security awareness of a user is accounted for in a defense that reduces the likelihood that attacks targeting the user would succeed.

IAM Identity and Access Management (IAM) plays an important role in cyber attacks where the adversary gains legitimate access to systems through authentication mechanisms by impersonating existing accounts and/or modifying the privileges associated with them. The first set of assets belonging to this category, Identity, Group, and Privileges, deal with this aspect. The Identity asset is used to specify the access privileges a particular role has, this includes authenticating on Applications and permissions on Data. Usually an Identity belongs to a User, and a User can have multiple Identities associated with it. Groups work similarly, but they can also be used to hierarchically organize Identities. The Privileges asset defines a collection of access control permissions that do not implicitly belong to a specific role and is typically used for more advanced models.

The other asset in this category is Credentials which can represent any type of token used in a wide variety of authentication mechanism, from physical ones, such as key cards or retina scans, to digital ones, like passwords and cryptographic keys. Due to its eclectic nature, the Credentials asset can be configured to match the required behaviour. In addition to serving as a means of authenticating accounts through an association with an Identity, Credentials can also be used for to encrypt or sign Data. Because Credentials extend Information they possess all of its attacks and defenses, as such an attacker that is able to reach Data that contain Credentials can use them to decrypt, spoof, or authenticate.

Networking Networking assets are the most typical assets used to extend an attacker's reach through the modeled environment. coreLang's approach to networking is to provide a generic protocol agnostic way of establishing connections. The Network asset abstractly covers all 7 layers of the OSI stack. It can be used to bridge the communications between multiple Applications and can carry Data that is in transit over it. Usually, an attacker that succeeds in gaining access to a Network is able to connect to the associated Applications and access the Data in transit over it. Applications communicating over the network can either have bidirectional access or specify that they are only receiving communications, not transmitting over the medium. This simplified use case is seldom employed in models, it is usually only applicable for small and basic internal LANs.

For more realistic scenarios, the `ConnectionRule` asset was introduced to represent network connections permitted by firewall rules. `ConnectionRules` are used to define allowed communications between `Appplication` and/or `Network` assets. A frequent pattern seen in models is having an `Application` reach a `Network` via a `ConnectionRule`. Directionality can also be specified for `ConnectionRules` and they cover more options, ingoing, outgoing, diode, and bidirectional options can be specified. The `RoutingFirewall` asset can be used to manage `ConnectionRules`, if it compromised[1] the attacker can bypass the restrictions on existing `ConnectionRules`.

The securiCAD tool As the goal of this work is to measure the cyber security of a large and complex infrastructure, it makes sense to employ a tool and perform automated assessment. Such a tool can also help perform a probabilistic analysis to cover for the missing details and consider different model variations. A number of tools are proposed and commercially available for the task of performing security analysis of cyber-physical systems [31, 32, 33, 6]. We decided to use securiCAD for this work as it is product of extensive research and is made available by the project partner foreseeti[2].

securiCAD [6] is a threat modeling tool that estimates the cyber security of systems-of-systems-level architectures. One advantage of using the securiCAD tool is that cyber security expertise is built-in, i.e. the configuration values regarding attacks pre-exist. Such values were collected from various studies [34, 35] and from public vulnerability databases such as US's National Vulnerability Database (NVD)[3]. Therefore, security expertise is not expected from the users. Instead, users model their system architecture using a DSL such as coreLang. From the modelled reference architecture, attack graphs are automatically derived and calculated. Next, given a user defined attacker starting point, the tool takes the local TTC values to calculate a global TTC of all attack steps in the attack graph (using Dial's approximate buckets shortest path algorithm [36]). As the TTC values are probabilistic, a Monte Carlo approach is used so the distributions are sampled and compiled in a cumulative distribution function. The shortest paths are also identified and combined into a critical path with the most traversed steps and edges. This analysis provides the modeller with valuable information on what the attacker can do, how they can do it, and how difficult it is expected for them to succeed with different attacks in the architecture. It should be noted that the analysis in securiCAD does not predict the attacker's behaviour. securiCAD comes in two variants; professional and enterprise. This work uses the enterprise version of securiCAD.

2.3 HONOR Technical Architecture

The HONOR system architecture presented in D3.2 [3] was oriented towards overall use cases of flexibility management and provided only few details on the actual system architecture and the relevant data streams. For the tasks of cyber security modelling and identification of relevant monitoring requirements, a detailed overview of data streams and systems within the HONOR system architecture was a prerequisite. Thus, the degree of detail of the system representation was increased and the various actors and communication paths were modeled in more detail, as presented in D6.1 [1]. A reference model of the underlying IT systems and network layer was also developed which for the rest of this report is referred to as the HONOR technical architecture. The HONOR

[1] The `RoutingFirewall` extends the `Application` asset, therefore it can be taken over by the attacker like any regular software application.

[2] https://foreseeti.com/

[3] https://nvd.nist.gov/

technical architecture provides the basis for cyber security modelling and assessment in the HONOR project. The architecture is designed such that is tailored to cyber security attack simulations and saves modelling time. Figure 2 shows an overview of the HONOR technical architecture. The architecture consists of a number of data streams and zones each occupied by actors playing an active role in the operation of a FM.

2.3.1 Overview of Zones and Actors

Here we briefly summarize and describe a few core actors and zones of the HONOR technical architecture based on [1]. For a full description of all actors and zones, the reader is referred to D6.1 [1].

Small Flexibility Asset Owner (FAO)

The FAO consists of a Home LAN which facilitates communication among devices and systems within a home. Smart meters are connected to Home LAN and energy consumption recordings are transferred to the meter data company on a regular basis. Smart devices such as network printers and mobile computers are also connected to the Home LAN. Flexibility assets such as electric vehicles and heating pumps are connected to the Home LAN via the Home Energy Management System (HEMS). The HEMS is responsible for controlling the smart devices of the household and thus for following a flexibility schedule to provide flexibility according to a contractual agreement. In some cases, the HEMS is capable of generating flexibility forecasts that can be send to the aggregator. If this is not the case measurements are transferred to the aggregator. The communication between the small FAO and the aggregator is conducted via an agent called FlexCom.

DSO SCADA Core Zone

The SCADA Core Zone is the central part of the architecture of the DSO. From the SCADA Core Zone operator commands are distributed to the process equipment such as the substations. The interaction of human operators with the SCADA system is conducted via the Human Machine Interface (HMI). Measurements, statuses, issued commands and other data are collected and stored in the Historian.

DSO Engineering Zone

Via the Element Manager of the Engineering Zone parameters of RTUs and IEDs are changed. Examples are allocation of signals to input board channels. The Vendor File Transfer Server collects software and firmware updates. From the Engineering Zones these updates are transferred to the SCADA Core Zone.

DSO Public DMZ and Office Zone

The public DMZ zone in the DSO is responsible for regular communication of the office with the public internet e.g. via a mail server. In the office zone, tasks that are not directly related to power system operation are located such as statistics and status information (e.g. outages). Staff (users) located in the office zone can access data from the replicated Historian and replicated SCADA server.

DSO Process Zone

The Process Zone is responsible for the communication between the SCADA Core Zone and the substations. By transferring data streams bidirectionally via the SCADA Front End, the Process Zone allows communication between the SCADA Core Zone and the Substations without a direct connection.

DSO SCADA DMZ Zone

The SCADA DMZ Zone is a network between the networks. It separates the OT or SCADA from less-trusted IT networks such as the Office Zone. Data from the SCADA Server and Historian are transferred to the replicated SCADA Server and replicated Historian, respectively, to allow the Office Zone access to the process data.

Aggregator Core Zone

The Aggregator Core Zone can be compared to the SCADA Core Zone of the DSO. Via the Core Zone the operator can enter commands and monitor the flexibility service activation via the HMI. The Flexibility Execution and Monitoring Module provides the control inputs for individual Flexibility Assets and monitors the flexibility service activation in real-time. The Aggregator Internal Database collects and stores process and contractual data such as flexibility asset measurements, control setpoints and market clearing results. The zone hosts service applications for the real-time operation and management of the flexibility portfolio.

2.4 Additions and Assumptions

The HONOR technical architecture provides only a base for the cyber security analysis. There is a need to be complement and refine it at modelling time by adding missing details and aspects. This added level of granularity on top of the technical architecture allows for a more accurate cyber security assessment. For instance, the architecture does not address details such as Identity and Access Management (IAM). The HONOR market involves different users and they need to be represented with dedicated user accounts in the model to accurately measure their impact. Similarly, defensive controls are not represented in the architecture except for security gateways. They were added afterwards by making additional assumptions. The modelled networks was protected with defenses to prevent eavesdropping, man-in-the-middle, and with access control. The software assets were protected with defenses such as `SupplyChainAuditing`. These are some of the examples of how hosts, clients and service represented by assets in securiCAD are protected. It should be noted that the defenses are configurable in securiCAD.

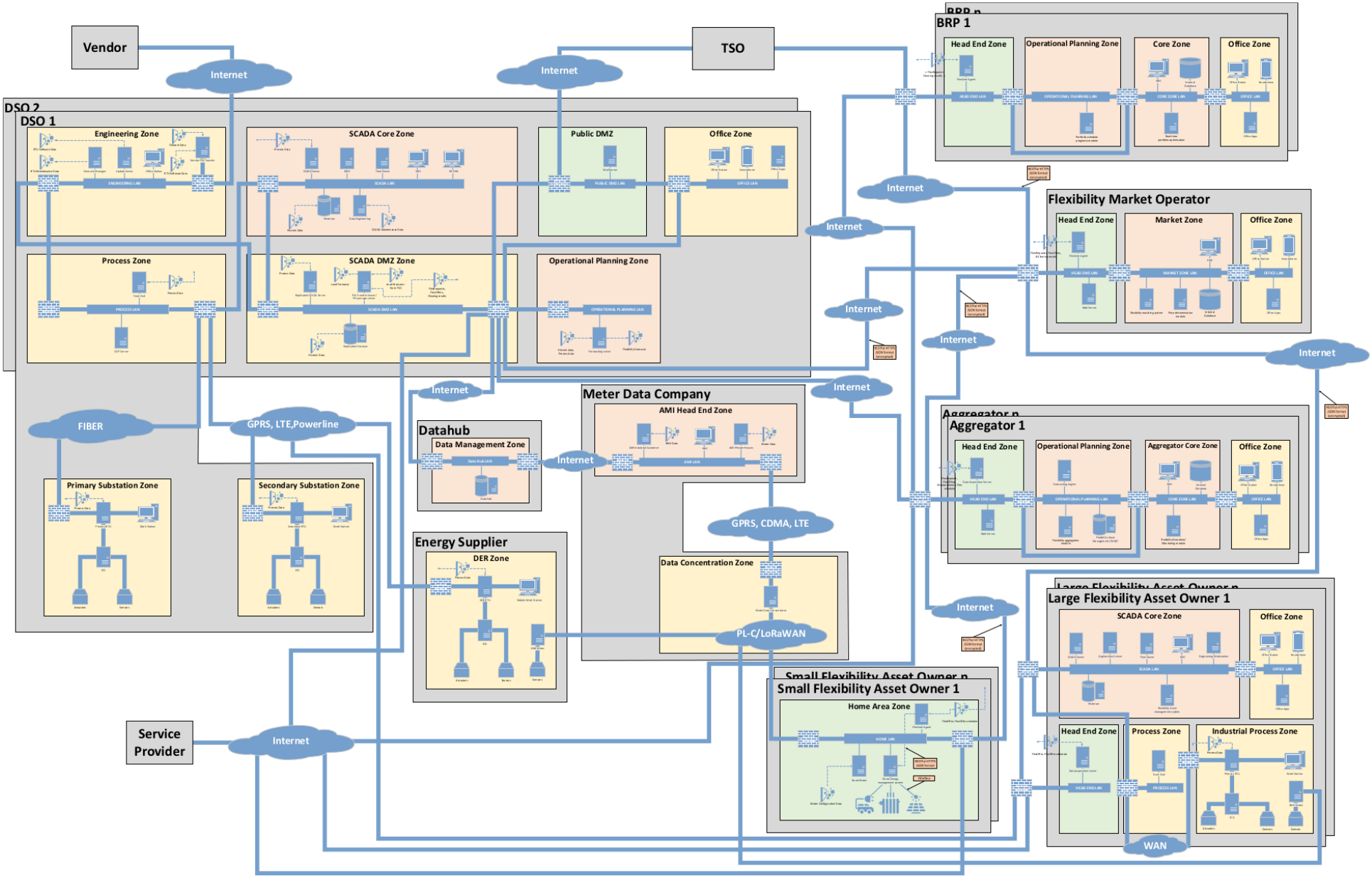

Figure 2: HONOR technical architecture [1].

3 Cyber Security Assessment

This section provides details of the final cyber security assessment of the HONOR technical architecture. The assessment consists of a comprehensive analysis covering most elements of the reference architecture. The focus of the analysis is on actors and data streams that are crucial and most interesting for the operation of a FM. The depicted scenarios are chosen carefully in order to form a good representation of the architecture's overall security status.

3.1 Model Building

This subsection details the process of building a model for the architecture and running attack simulations on it. The model is built in securiCAD enterprise edition and consists of 26 views where each view represents an actor in the reference architecture shown in Figure 2. Views are a way to organize the model so that related objects are presented together. However, all objects are part of the main model which means that their mutual impact, if any, is taken into account. These views are connected to each other using common assets such as networks. Overall, the model consists of a total of 303 assets and 367 associations between these assets. For the sake of readability, it is not possible to show all views of the model in this report. Instead we focus on showing the most interesting views of the model as we elaborate on different scenarios. The remaining views of the model are available at [37]. Each view of the model consists of coreLang objects inter-connected with each other to represent the different actors and systems of the technical architecture. As detailed earlier, to make the analysis more realistic, the technical architecture is complemented with a few more details during the modeling process. These include the addition of software vulnerabilities to the applications, hardware vulnerabilities to the hardware, and addition of users, data, identities, and credentials. Security gateways in the architecture are represented by a combination of connection rules and routing firewalls in the model.

3.2 Analysis

One of the advantages of an automated evaluation is the ability to explore different variations in the model. In terms of cyber security, two kinds of variations are of particular interest and value. First, the placement of certain security mechanisms and secondly their configuration to measure how well they perform. We have already shown in the first iteration of the security assessment that security controls make the architecture more secure by increasing the time to compromise for the attacker. In continuation, here we investigate the optimal security controls needed to protect the architecture from the attacks explored in the discussed scenarios. For each scenario in this analysis, we consider two configuration variations: As most of the assets in coreLang have defense mechanisms that are configurable, following configuration variants are considered.

1. A default and less secure configuration where defenses probabilities are set to 0 meaning that the defenses are disabled.

2. A more secure configuration where relevant asset defense probabilities are set to 1 meaning that there is 100% chance that a defense is active resulting in increased requirements to exploit a software vulnerability, network access control with stronger encryption, payload inspection, and users with better security awareness, among other things.

The idea with configuration (1) is to show the attack possibilities and the relevant attack paths. Then in (2), for each scenario, we identify and configure relevant defenses and show the most crucial defensive controls needed to thwart the attacker or make their job very difficult.

3.2.1 Attack Scenarios & Scope

The cyber security analysis is performed based on a number of attack scenarios, i.e. by defining attacker starting positions and assets with high value (e.g. a network) to protect. This allows for the calculation of the possible attack paths and to estimate the probability to succeed with the attack. For this work, the focus is on scenarios where an attacker tries to affect the normal operation of a flexibility market (offers, activation signals, etc) and thus the analysis mainly considers the attack scenarios identified in [10]. The following attacker starting positions are examined:

- At the smart meter in FAOs
- On the Internet
- At the vendor

Additionally, it was decided to measure the cyber security of the architecture by focusing on the following targets:

- Smart Meter Application
- Home LAN
- Core Zone LAN in Aggregator
- SCADA Core Zone LAN
- The RTUs in substations
- Energy Supplier's RTU

These attacker starting points and target assets form the scope of this analysis. Clearly, there are many other potential attacker starting points and target assets, but we believe the mentioned scenarios are good representatives of the architecture's cyber security status. The 3 attacker positions in combination with 6 different target assets result in a total of 18 threat scenarios. Table 2 summarizes the explored scenarios. The results of the security evaluation using securiCAD come in terms of a reachability map from the attacker's starting point and to the targets (i.e., all attack steps that are defined for each single entity present in the model). An attacker in securiCAD is considered to be a professional penetration tester who has all the public knowledge and tools available to them. The reachability of each attack step by the modelled attacker is represented by the distribution of time-to-compromise (TTC) across the population of professional penetration testers. A simulation may show multiple attack paths that lead to the activation of an attack step, i.e. the main attack path but also alternative paths that take a longer time to achieve but can still yield similar end result. It should also be noted that the attack simulations only estimate the attacker effort and do not say anything about what the attacker will ultimately decide to do. The goal of these simulations is not to predict the attacker's behaviour, but rather to measure the

Table 2: Table of explored scenarios in the analysis.

Scenario	Attacker Start	Target	Subsection
1	At the smart meter in FAOs	Smart Meter Application	3.2.2
2		Home LAN	3.2.2
3		Core Zone LAN in Aggregator	3.2.2
4		SCADA Core Zone LAN	3.2.2
5		The RTUs in substations	3.2.2
6		Energy Supplier's RTU	3.2.2
7	On the Internet	Smart Meter Application	3.2.3
8		Home LAN	3.2.3
9		Core Zone LAN in Aggregator	3.2.3
10		SCADA Core Zone LAN	3.2.3
11		The RTUs in substations	3.2.3
12		Energy Supplier's RTU	3.2.3
13	At the vendor	Smart Meter Application	3.2.4
14		Home LAN	3.2.4
15		Core Zone LAN in Aggregator	3.2.4
16		SCADA Core Zone LAN	3.2.4
17		The RTUs in substations	3.2.4
18		Energy Supplier's RTU	3.2.4

required effort for an attacker to move from their starting position to the targeted asset. Moreover, the TTC values of the targets are expressed in days. For practical reasons, number of samples in simulations were limited to 100 penetration tests, and the upper limit of TTC was set to 100 days. The following text presents the explored threat scenarios.

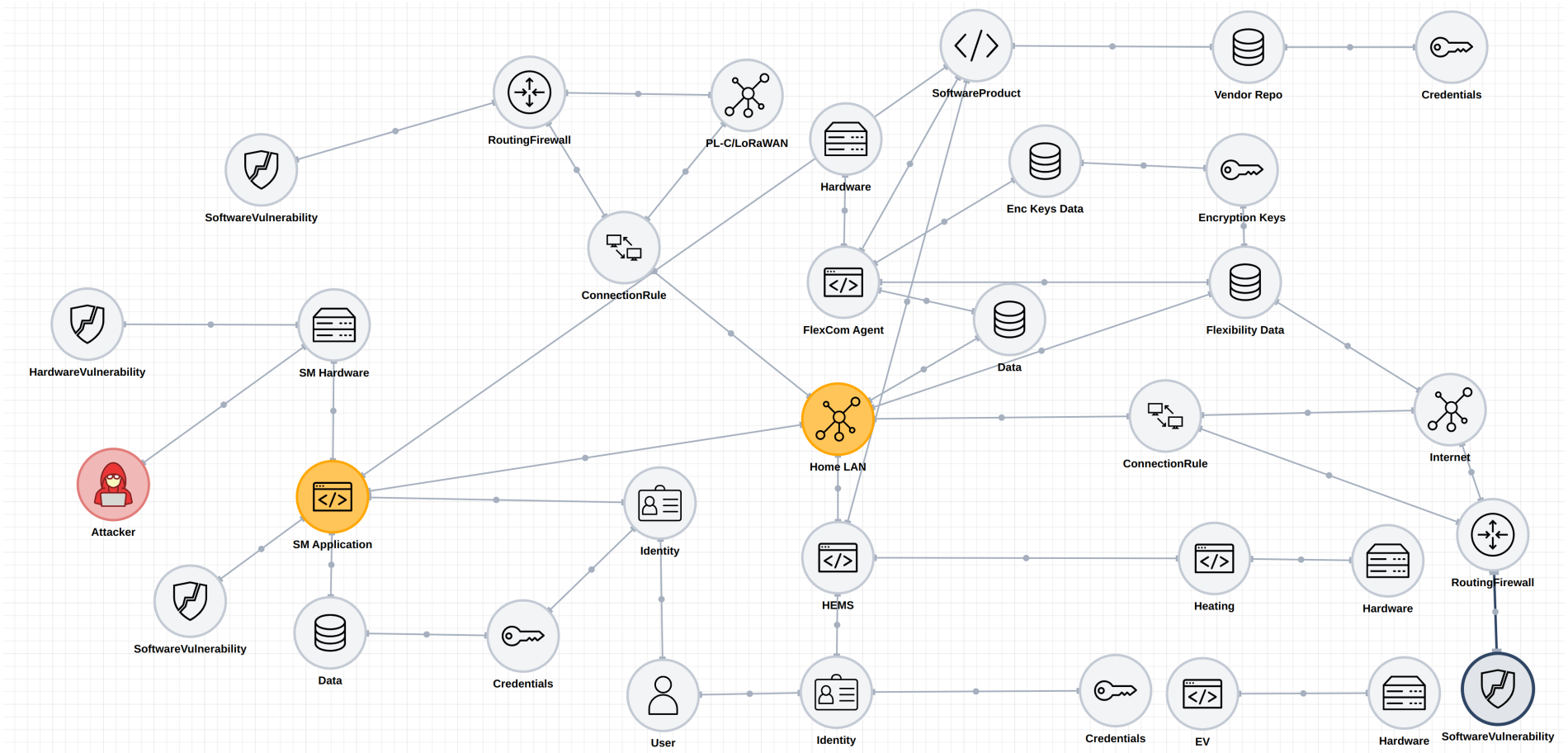

Figure 3: securiCAD model view for FAO.

3.2.2 At the smart meter in FAOs

Figure 3 depicts the system model showing the view for FAO actor. As smart meters are part of customer premises and the less protected FAOs, it is possible for an attacker to use them as a starting point to launch their attacks. Following we consider different scenarios that can result from an attacker connecting physically to smart meters in FAO.

Scenario 1: Full Access on Smart Meter Application This scenario has an attacker starting position set at the hardware of the smart meters in FAOs. The target asset for the attacker is the smart meter application and the contained sensitive data such as consumption, credentials (including keying material), and firmware information. Figure 3 shows the securiCAD model with FAO view. First we run attack simulations of the model for configuration A. Figure 4 shows the resulting attack path. As shown, once the attacker gains physical access to the smart meter hardware, the attacker can gain local connect to the smart meter application and then exploit a vulnerability in the application to modify it and gain full access on the smart meter application. The probability of this attack is 100% without any security controls. If the attacker is able to gain full access on the smart meter application, it can read/write any associated data e.g., they can read the smart meter credentials file. The attacker can further use these credentials to assume the identity of the home owner user and send wrong consumption data. In terms of FM, the impact of such an attack is that the asset owner could be fined for not fulfilling flexibility agreements and eventually be removed from the portfolio [10]. Moreover, smart meters deployed by a DSO often share the same vulnerabilities (e.g., a static encryption key [38]). Thus, if an attacker can control one smart meter, they can take control of multiple smart meters which may result in power outages for many customers and high social and financial cost.

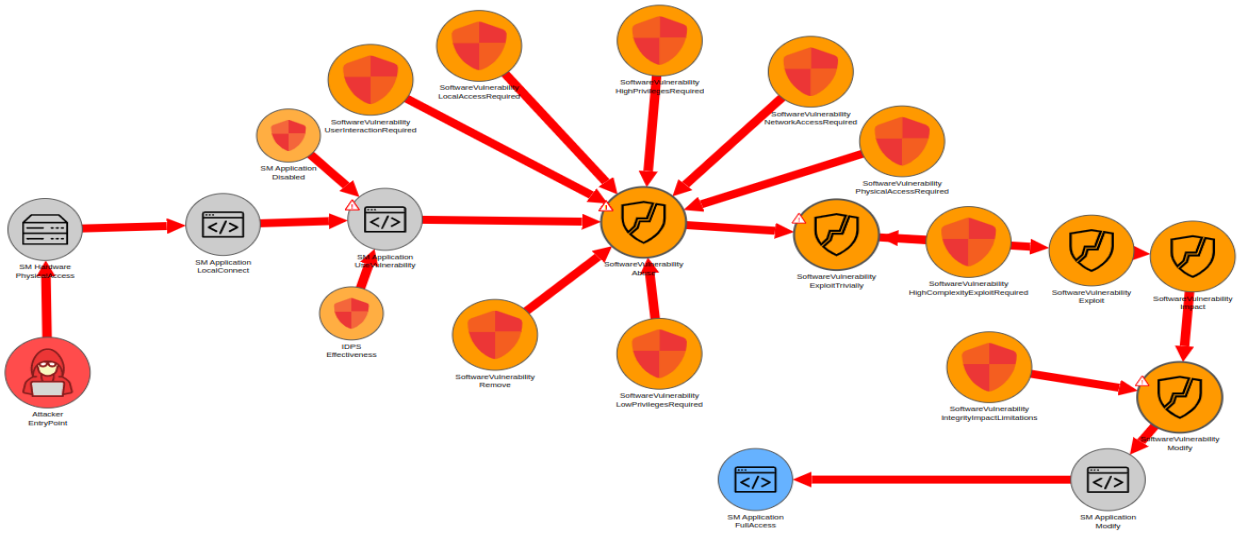

Figure 4: Attack Path for gaining full access on a smart meter application.

Now that we have shown the attack possibility and the probable attack path, let us now explore ways to defend against this attack. The most obvious solution in this case is to protect the smart meter application from being exploited. So either it can be ensured that no vulnerabilities exist in the smart meter software (which is hard) or alternatively we could protect the meter application with an `IDPS`. The idea with this IDPS is that it acts like an antivirus or antimalware to protect the smart meter application and thus deny any possibility of a

vulnerability being exploited. To test this security control, we simulate the scenario again with the newly added IDPS protecting the smart meter application with 100% effectiveness. Figure 5 shows the resulting attack path. Although, we are able to prevent the attacker from exploiting a software vulnerability, interestingly the attacker is still able to gain full access on the smart meter application through an alternative attack path. It can instead use some kind of hardware vulnerability to modify the meter hardware and gain full access on smart meter hardware and then its application.

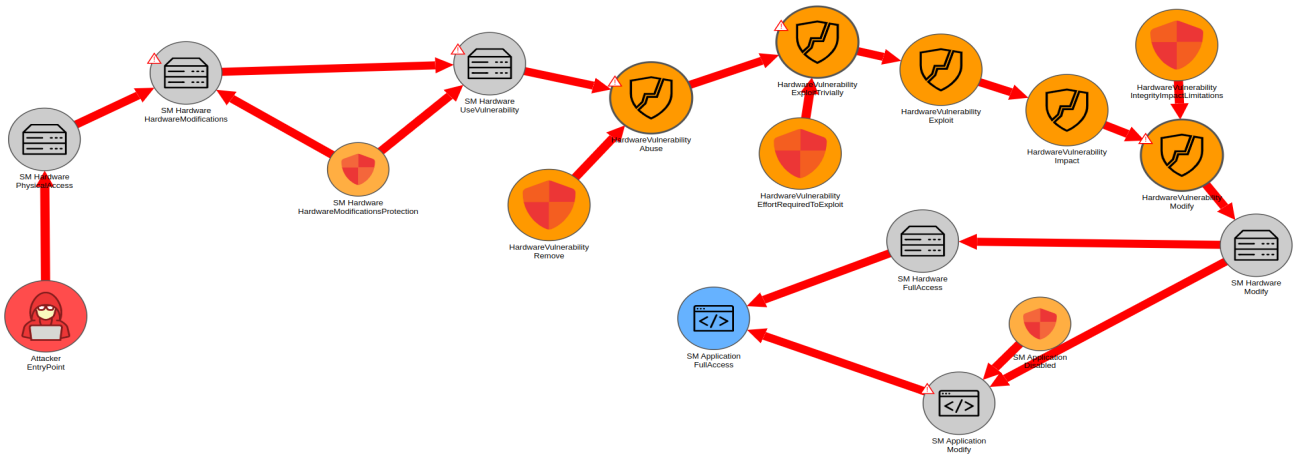

Figure 5: Attack Path with smart meter protected by an IDPS.

This implies that to be able to stop an attacker gaining full access on a smart meter application, it is not enough to protect just the application but we will also need to protect the meter hardware. This can be achieved by turning the hardware asset defense named `HardwareModificationProtection` on with 100% probability. Simulation results after the addition of latest defense show no possibility for the attacker to gain full access on the smart meter application.

Scenario 2: Man in the Middle (MitM) and Denial of Service (DoS) on Home LAN Figure 6 shows the attack path for an attacker connected at a smart meter with the intention to target the Home LAN and connected applications. The attack path shows that the attacker can abuse a vulnerability in a smart meter (as shown in the previous scenario) to be able to access the connected network HOME LAN and access its network data. Once the attacker can access the network data, it is able to modify any data transiting over the network. In a FM, HOME LAN is used by the FlexCom Agent to send and receive flexibility data. Thus the attacker is able to modify such data. Being able to gain a foothold on the HOME LAN can also lead to further attacks. For example, the attacker can connect to HEMS and they can exploit a software vulnerability such as weak password security or encryption to gain full access on the HEMS. With this access, the attacker can collect sensitive data and degrade flexibility assets, or increase costs by increasing consumption or mitigating flexibility activation, resulting in non-compliance with flexibility contracts [10]. The attacker could even introduce load peaks or oscillations resulting in customer disconnection by using access on HEMS to control multiple flexibility assets and switching them on or off. Another example is shown in Figure 7 where the attacker is able to launch a denial of service attack on HEMS to bring it down along with connected applications such as Heating and EV. The probability of both attacks (MITM and DoS) is 100% without any security controls.

To prevent the attack paths in this scenario, one possible defense is to encrypt all the flexibility data. This is shown in the model by associating the asset `Encryption Keys` with the `Flexibility Data`. Encryption

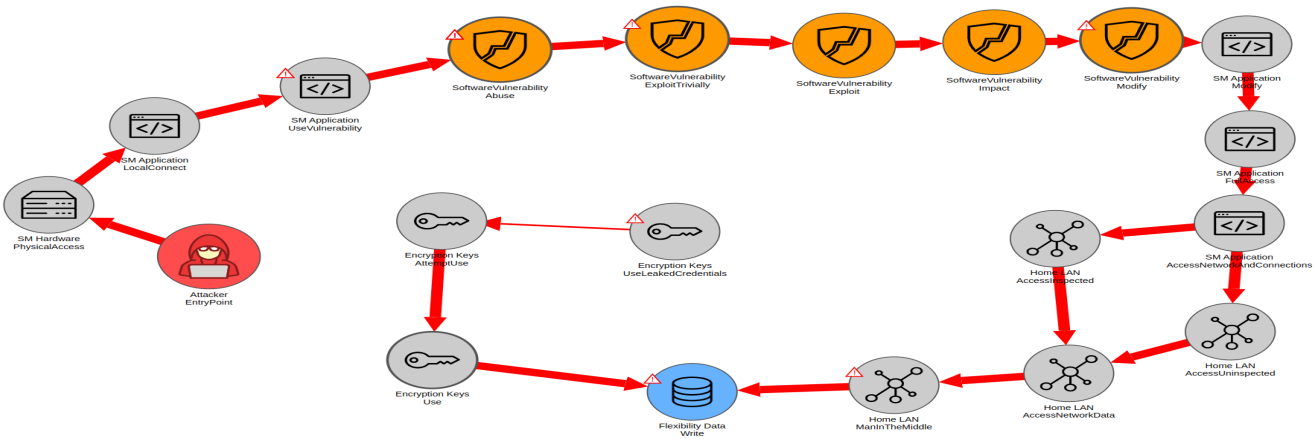

Figure 6: Attack Path for performing MITM on Home LAN.

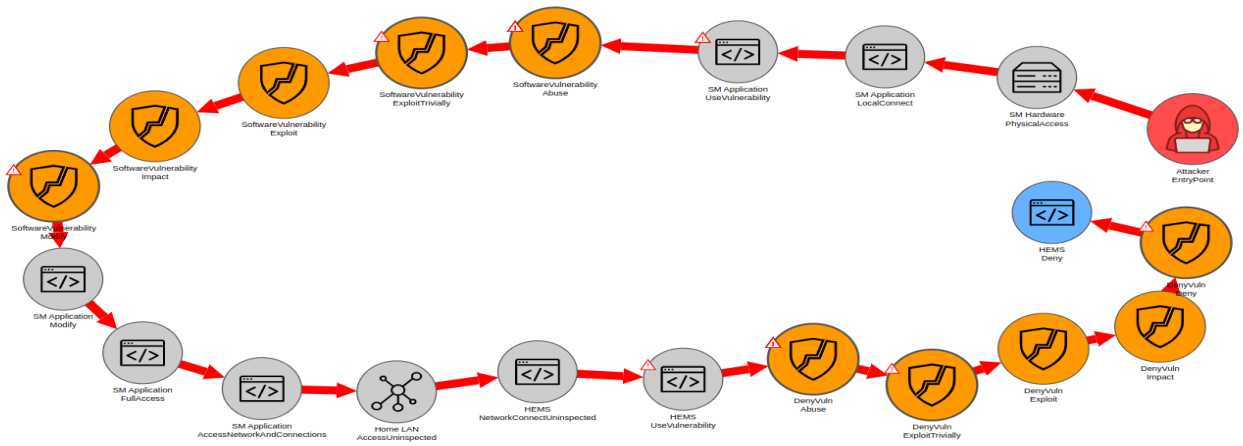

Figure 7: Attack Path for performing DoS on HEMS.

would make it impossible for the attacker to read and/or modify the flexibility data even if it has access to it. Additionally, the defense `NetworkAccessControl` on the HOME LAN asset can be used to prevent the attacker from launching denial of service attack while defenses `EavesDropDefense` and the `ManInTheMiddleDefense` can be used to stop the attacker from reading and modifying network data. Our simulations with these defenses turned on show that both attack path are not possible anymore.

Scenario 3: Man in the Middle on Core Zone LAN in Aggregator An attacker connected on a smart meter can also attempt to reach and access the LAN in the Aggregator Core Zone. Figure 8 shows the attack path from the point when the attacker has already gained full access on the smart meter application (for practical reasons) as shown in the previous scenarios. The path shows that the attacker can reach the Internet by using the allowed connections (connection rules), and forwarding from one network to another. From the Internet, the attacker again uses network forwarding and allowed connection rules to enter the aggregator and reach Head END LAN and eventually the Core Zone LAN to launch the attack. An attacker who has access to this network can tamper or disrupt flexibility activation signals or even disrupt or manipulate the flexibility measurements [10]. One way is the modification of flexibility portfolio recordings to disrupt the service verification process. The consequence for the aggregator for this attack could be milder in terms of fines for not fulfilling contractual agreements. In

severe cases, wrong flexibility activations may trigger grid protection, resulting in disconnection of customers and thus high social costs.

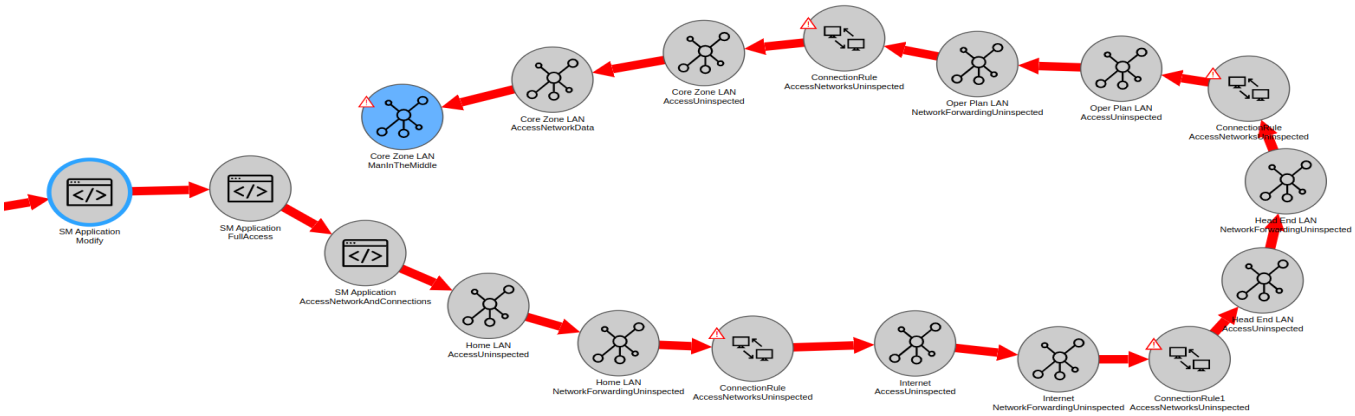

Figure 8: Attack Path for accessing Core Zone LAN in Aggregator.

This attack path can be stopped by protecting the security gateways (`connection rules` and `routing firewalls`) and the networks. If the attacker can not forward from one network to another and all networks impose strict access control, then this attack path can be stopped as per simulations. However, instead, the attacker will then rely on finding and exploiting vulnerabilities in the routing firewalls. The possible protection against this is discussed later.

Scenario 4: DoS on SCADA Core Zone LAN There is a possibility for an attacker connected at the smart meter in FAO to reach the SCADA Core Zone LAN through the Internet and launch attacks. As shown in Figure 9 (from the point where the attacker already has full access on the smart meter application), once the attacker reaches the Internet, the attacker can make use of a vulnerability in the security gateway in the Engineering Zone of the DSO and be able to modify it to enable access to the Engineering LAN. As Engineering LAN is typically allowed to connect to the SCADA Core LAN, the attacker can reach and access the SCADA Core LAN to launch a denial of service attack on the network or even target the SCADA server or Historian which stores the historical data. The consequence of an attack on the SCADA server can be devastating and impact millions of people. The historical data provides necessary information for flexibility planning, activation, and verification and are typically not checked for integrity after being stored. Thus, if attacker manages to impact the integrity of these data, all models based on the compromised data will be badly affected. This may also result in financial penalties due to imprecise flexibility planning and verification. In severe cases, power system monitoring techniques may fail, leaving critical grid conditions unresolved [10].

The most suitable place to start the process of defending against this attack is to strengthen the security gateway between the Internet and the Engineering LAN. If the attacker cannot exploit a vulnerability in the `routing firewall` then it can not enter the Engineering LAN even it is already present on the Internet. With the routing firewall properly protected, the attacker has to find alternate ways to reach the Engineering LAN and the current attack path will be thwarted. At the same time, both the Engineering LAN and the SCADA Core LAN should have all 3 network defenses (`NetworkAccessControl, EavesDropDefense, ManInTheMiddleDefense`) turned on for additional security. To test the mentioned defenses, we simulated this scenario again with the `Remove` defense of the software vulnerability associated with the routing firewall

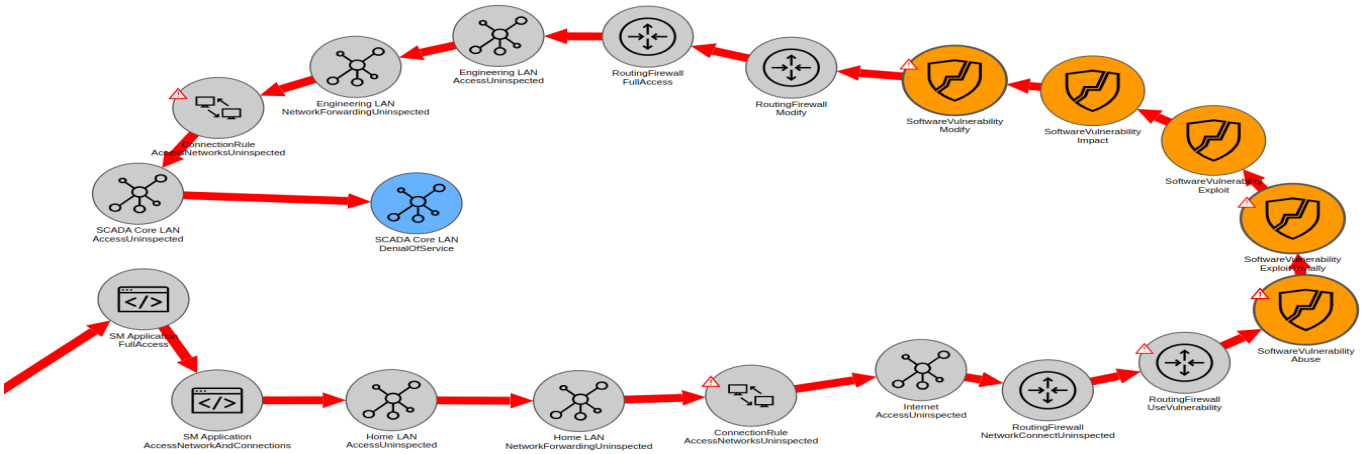

Figure 9: Attack Path for DoS attack on SCADA Core Zone LAN.

turned on along with the above mentioned network defenses turned on. Figure 10 shows the resulting attack path. Interestingly, now the attacker takes an alternative path to reach the Engineering Zone through the SCADA DMZ Zone. Similar to the earlier case, the attacker uses the vulnerabilities in the `routing firewall` to gain access. This emphasizes the importance of securing all possible entry points instead of just focusing on the obvious ones.

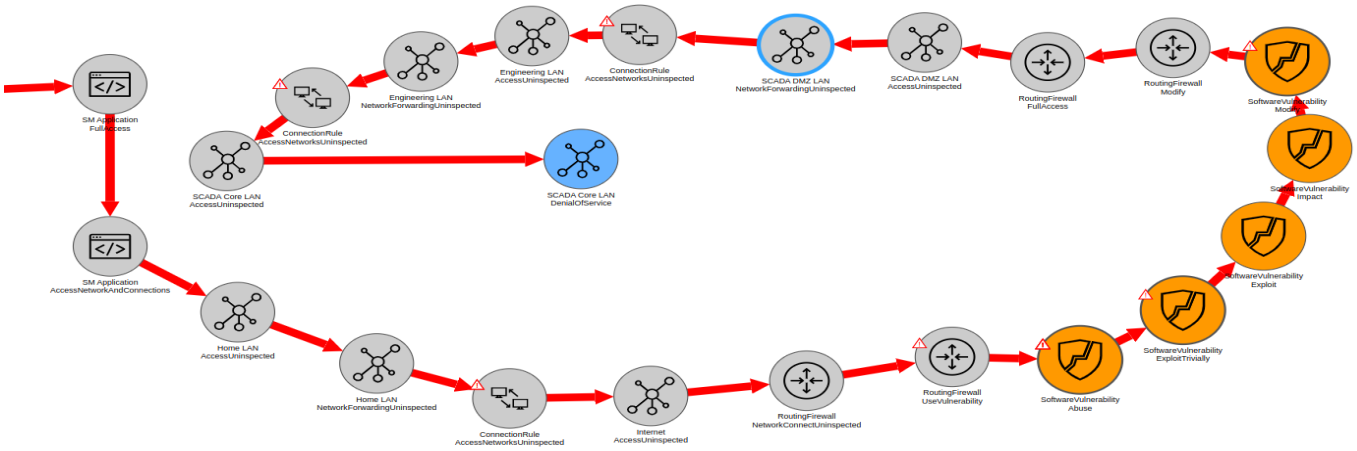

Figure 10: Alternate Attack Path for DoS attack on SCADA Core Zone LAN.

Scenario 5: Deny RTUs in substations For an attacker connected at the smart meter in FAO, it is also possible to reach the RTUs in either of the substations and deny their normal operation. There are two possible attack paths for this attack as per the simulations. The first attacker path is shown in Figure 11 and we again show it from the point when the attacker has already gained full access on the smart meter application as shown in the previous scenarios. The attacker can access and connect to the PL-C/LoRaWAN from the Home LAN using network forwarding and then exploit vulnerabilities in the KwH Meter to be able to reach and connect to the Energy Supplier Network. As the energy supplier uses a GPRS/LTE/Powerline network towards the Process LAN, this opens up the DSO network to the attacker. Once inside the DSO, the attacker can reach the substations from the Process LAN and be able to exploit vulnerabilities in the RTU to perform the attack. This attack path is made possible because the Process Zone hosts the front end which acts as a relay between the operators in

the SCADA Core Zone and the equipment in the substations. The consequence of this attack can be a blackout which is nothing short of a disaster depending on how long it takes for the grid operator to identify and rectify the problem.

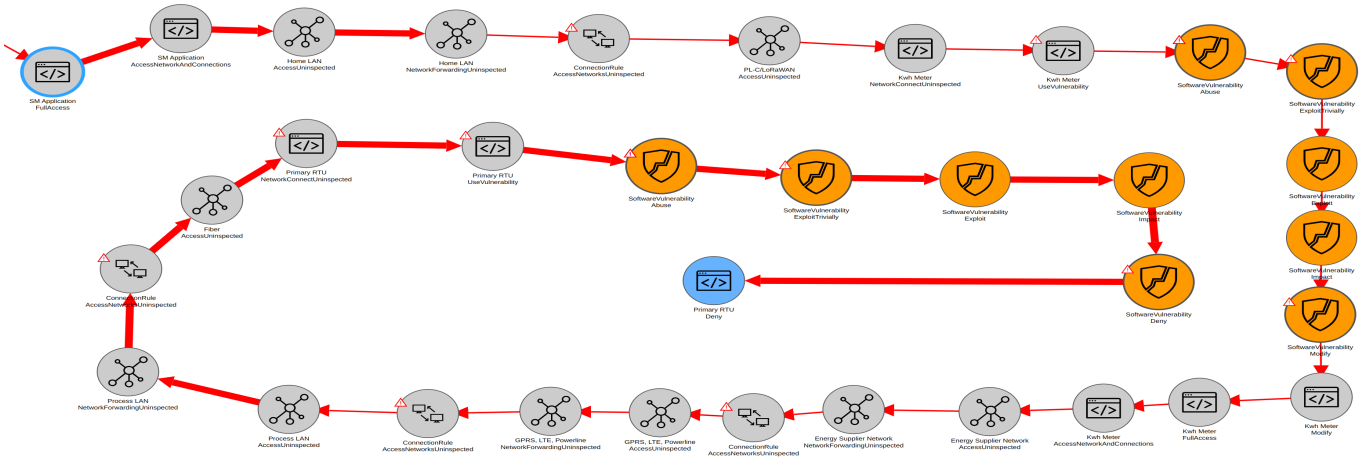

Figure 11: Attack Path for denying a RTU in a substation.

Alternatively, the attacker can also reach the RTUs through the Internet. This path is shown in Figure 12 and is slightly similar to the one shown in Scenario 4. Once the attacker gets access to the Internet from a smart meter, the attacker can enter the SCADA DMZ LAN through accessing the connected networks and be able to make its way to the Process LAN, from where the attack is similar to the above discussed attack path.

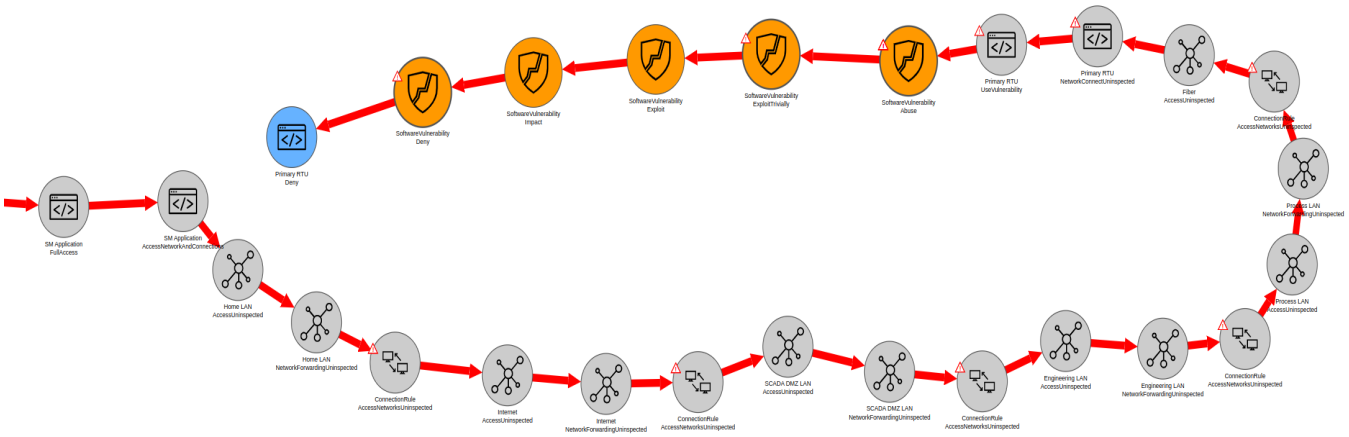

Figure 12: Attack Path for denying a RTU in a substation through the Internet.

For both attack paths, there are multiple possible defenses to stop them. First, it is crucial to stop the attacker at the perimeter of the DSO so the associated `connection rules` should have their defense `PayloadInspection` turned on. Similarly, all the networks should be using all three possible defenses available on the network asset as well as only allow forwarding for legitimate traffic. Finally, the RTUs themselves should use defenses both on the hardware and software level (just like smart meters) to be able to protect themselves for the case when the attacker already has remote access to the substations. The simulation results with the above mentioned defenses indeed show that the mentioned attack paths to the RTUs in substations are not possible anymore.

Scenario 6: Deny RTU in Energy Supplier Figure 13 shows the attack path for an attacker connected at a smart meter with the intention to target the RTU in the DER LAN. The path shows that after successful exploitation and control of the smart meter and the HOME LAN, the attacker can reach and connect to the PL-C/LoRaWAN network. Further, the attacker connects to the KwH Meter at the Energy Supplier and exploits a vulnerability to access the internal network of the Energy Supplier. Once the attacker has gained a foothold on this LAN, it can perform denial of service on the RTU.

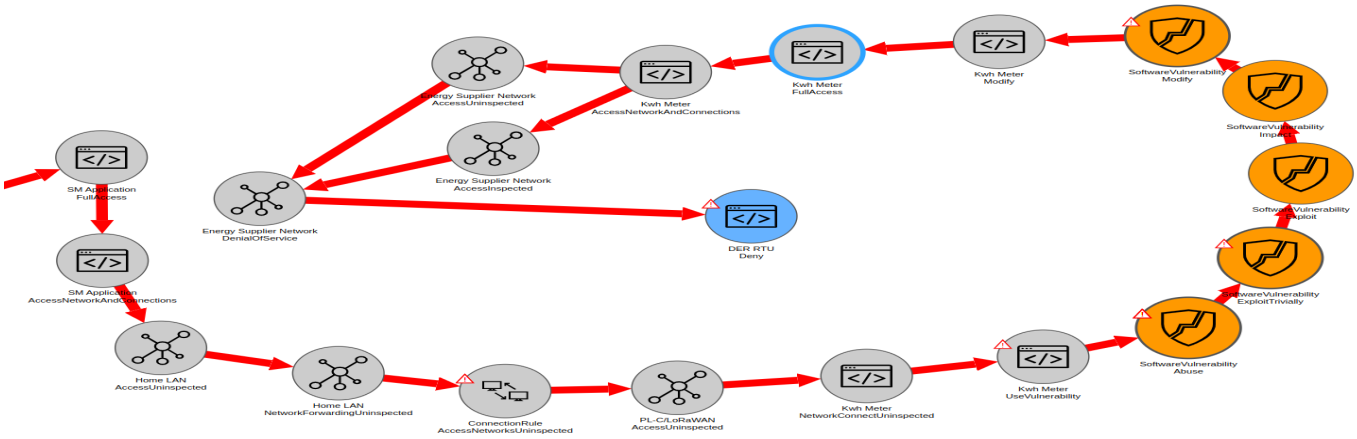

Figure 13: Attack Path for denying RTU in Energy Supplier.

The attack can be stopped by taking a number of steps. First the perimeter security between FAO, Data Concentration Zone, and the Energy Supplier should be enhanced. Secondly, the individual devices such as the KwH Meter can be protected by an `IDPS` asset. Additionally, the defense `NetworkAccessControl` on the Energy Supplier Network asset can be used to prevent the attacker from launching denial of service attack while defenses `EavesDropDefense` and the `ManInTheMiddleDefense` can be used to stop the attacker from reading and modifying network data. Our simulations with these defenses turned on show that the attack path is not possible anymore while the the probability of the attack is 100% without the above mentioned security controls.

3.2.3 Attacker on the Internet

The Internet being a public network allows anyone to connect to it and pose a threat. In the following, we consider scenarios where an attacker is present on the Internet.

Scenario 7: Full Access on Smart Meter Application An attacker connected on the Internet can access and compromise a smart meter application. There are two possible attack paths for this attack. First, as shown in Figure 14, the attacker can use the allowed connections rules of the security gateway to forward itself from the Internet to the Home LAN. This happens if the traffic is not inspected and filtered to detect and stop malicious communications and only allow legitimate communication. Without any payload inspection, the attacker can then easily access all associated networks without any restriction. Once on the Home LAN, the attacker can exploit a vulnerability in the smart meter application and gain full access on it.

Figure 15 shows the second possible attack path for this attack. In this case, the attacker can attempt to exploit a vulnerability in the `routing firewall` managing the connection rule between the Internet and the Home LAN to gain full access on it and modify it to gain access to the Home LAN. Once on HOME LAN,

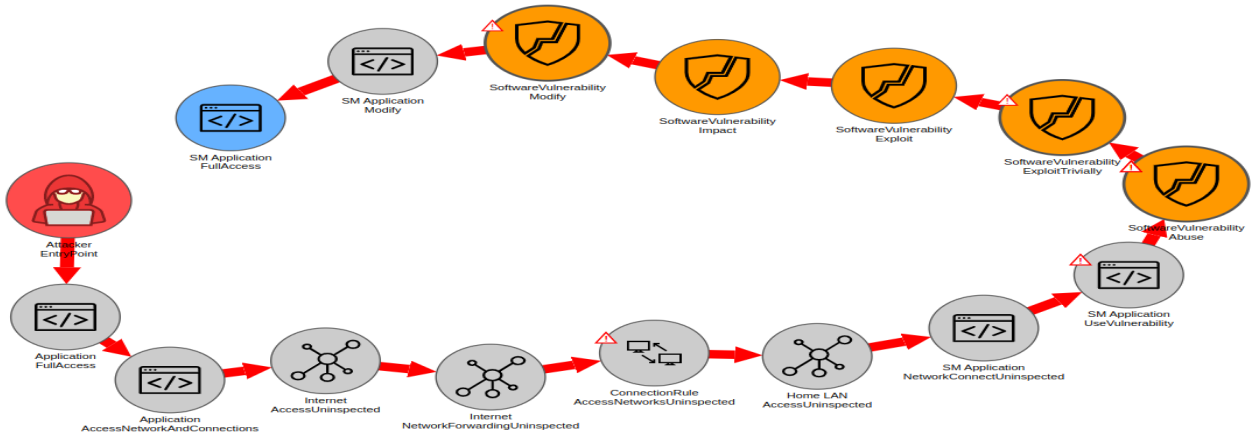

Figure 14: Attack Path for gaining full access on a smart meter application.

the attacker can then exploit a software vulnerability in the smart meter application and succeed in gaining full control over the smart meter.

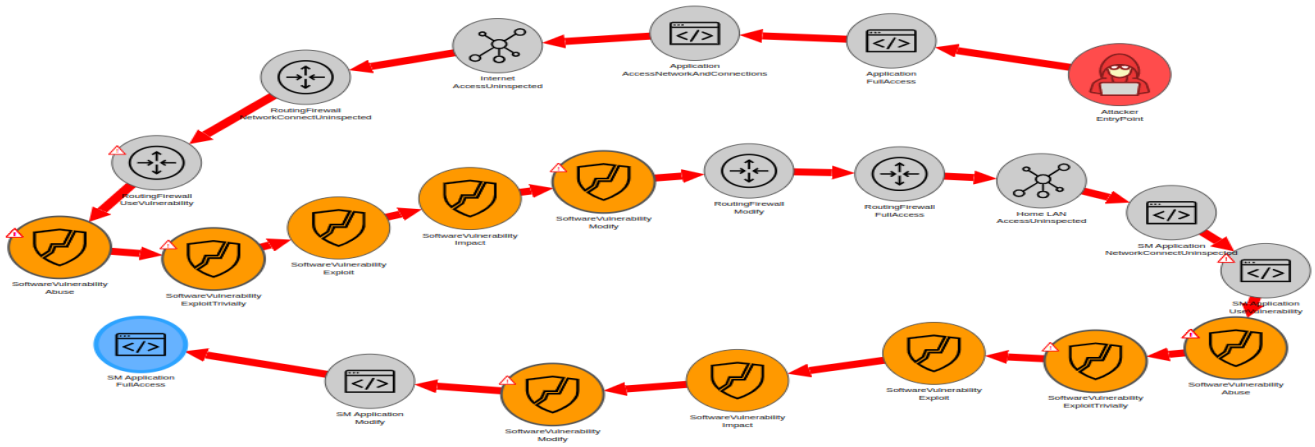

Figure 15: Alternate Attack Path for gaining full access on a smart meter application.

With some simple defenses these attack paths can be protected against. First the affected routing firewalls and the smart meter applications can be protected by an `IDPS`. Secondly, the security gateways (connection rules) have `PayloadInspection` defenses that should be turned on to perform traffic inspection and detect and block malicious traffic. The `IDPS` asset associated with systems can be seen as a host-IDS and the `PayloadInspection` parameter on connection rules can be seen as a network-IDS. This is especially crucial for the traffic coming in from the Internet. The simulations with the above recommended defenses showed that the above shown attack paths are not possible anymore, but the attacker is still able to reach the smart meter from an alternate path (Internet -> SCADA DMZ LAN -> Engineering LAN -> Process LAN -> GPRS, LTE, PowerLine Network -> Energy Supplier Network -> PL-C/LoRaWAN -> Home LAN). Although, it is unlikely that an attacker will take this attack path to reach a smart meter, this further signifies the importance of protecting all possible entry points and systems rather than focusing on the most obvious ones. Thus, to completely stop an attacker on the Internet from reaching the smart meter application, all security gateways need to be properly configured to

inspect traffic. Similarly, the intermediary networks and the target assets need to have their appropriate defensive controls properly configured and enabled.

Scenario 8: Man in the Middle on Home LAN Similar to the previous scenario, the attack paths for the scenario where an attacker on the Internet attempts to perform a man in the middle attack on the Home LAN are analogous. Figure 16 shows the path. As the Home LAN is directly connected to the Internet through a connection rule, the attacker can access the Home LAN using the methods discussed earlier to launch a man in the middle attack.

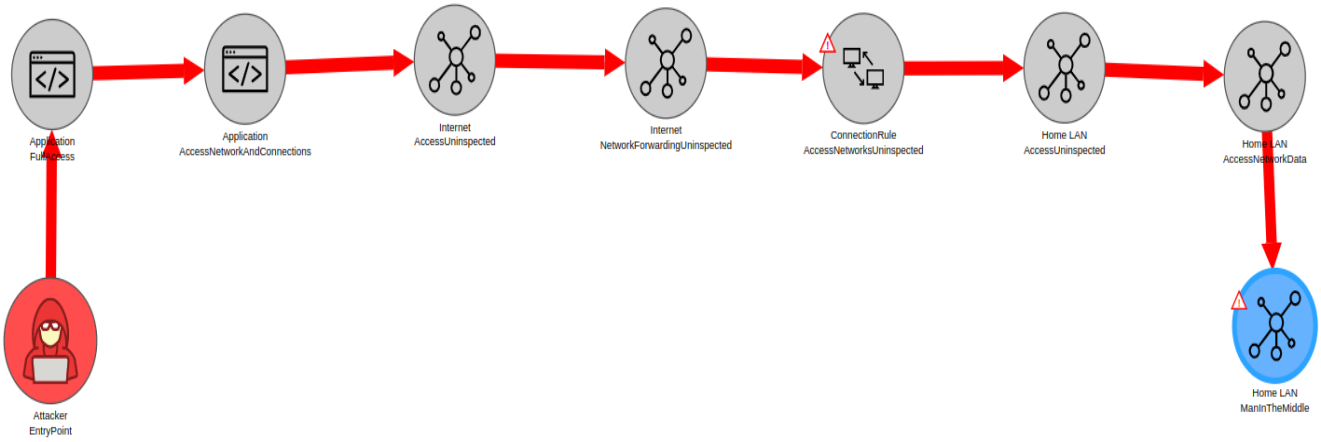

Figure 16: Attack Path for MitM on Home LAN.

The alternative attack path for this scenario is also similar to scenario 7 where the attacker instead focuses on exploiting a vulnerability in the security gateway. The eventual defenses to protect from these attack paths are also identical to Scenario 7. For example, Home LAN should have its three network defenses `(NetworkAccessControl, EavesDropDefense, ManInTheMiddleDefense)` turned on.

Scenario 9: Man in the Middle on Core Zone LAN in Aggregator An attacker on the Internet can easily attempt and reach the LAN in Aggregator Core Zone. Figure 17 shows the attack path. The attack path is similar to some earlier scenarios where the attacker uses the lack of inspection by the `security gateway` to go from one network to another and eventually reach its target asset and perform the man in the middle attack. The possible defenses to thwart this attack path are, again, enabling `payload inspection`, protecting intermediary networks using their defenses, and protecting the targeted assets.

Scenario 10: DoS on SCADA Core Zone LAN The usual attack paths for an attacker breaching the security through exploiting vulnerabilities in the security gateways or making use of the lack of payload inspection to use network forwarding to reach the targets still apply in this scenario. However, it can be assumed that DSOs are more security savvy and those attack paths are less likely to happen in reality. Therefore, in the interest of keeping the analysis interesting, we now focus on a different variation of attacks, one that involves the human factor.

Let us assume that there is an attacker on the Internet that targets social engineering attacks on a user in the Office Zone of the DSO actor. Figure 18 shows the resulting attack path when an attacker targets a user of Office Apps. The attacker attempts social engineering attack and either successfully assumes the identity of the user to

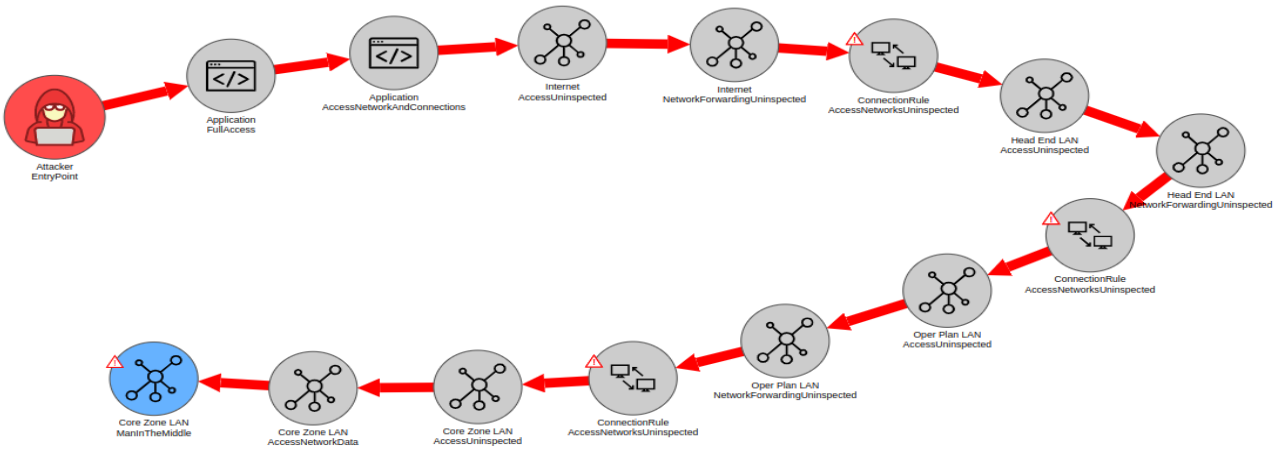

Figure 17: Attack Path for MITM on Core Zone LAN in Aggregator.

exploit the associated privileges and authenticate to the office application and gain specific access or relies on tricking the user with some probability into taking some unsafe action and exposing the office application to be able to gain specific access to it. Gaining specific access means the attacker is able to gain low-privilege access on the application which enables it to access the networks and connections associated with it. Once the attacker can access the connected networks, it can move to the DSO Office Zone LAN. Further lateral movement thanks to the lack of payload inspection between networks allows the attacker to reach the SCADA DMZ LAN and then the Engineering LAN. From the Engineering LAN, the attacker can reach and access the SCADA Core Zone and its LAN to launch the attack. The Engineering zone is allowed to send data to the SCADA Zone because it hosts services such as a vendor file transfer server that relies on collecting software and firmware updates from the Internet and transferring them to the SCADA Core Zone.

The above mentioned attack path is reminiscent to real world attacks such as the hack of Ukraine's Power Grid in 2015. According to experts [39], the attack on the power grid also began with a spear-phishing campaign targeting staff of multiple electricity distribution companies. Attackers sent emails with malicious Microsoft Word documents that when opened infected their machines and opened a backdoor for the hackers. This allowed the attackers access to the corporate networks. Once inside the corporate networks, the attackers gained access to the Windows Domain Controllers to gain access to VPN credentials used to remotely login to the SCADA network and perform further exploitations. Another alternative would have been to exploit vulnerabilities in the segregating firewalls or find alternative ways. This way the attackers were able to social engineer their way from people into the SCADA network.

Figure 19 shows the required attacker effort in terms of TTC values. It can be seen that the success rate is 23% after 100 days for a persistent attacker. Attacks exploiting users are hard to defend against in general. Possible defenses against this kind of attack include the `SecurityAwareness` defense of the user asset. The security awareness of the user makes it less likely that social engineering would be successful and reduces the likelihood that the user will engage in unsafe behaviour. If we assume that the user is fully security aware then the attacker is not able to perform this attack and the attack path is not possible anymore. The earlier discussed defenses for protecting the different assets leading to the target asset still also apply here.

Scenario 11: Deny RTU in substations The first possible attack path to this scenario resembles the attack path discussed earlier in Scenario 5. Although the attacker was connected on the smart meter then, it still used

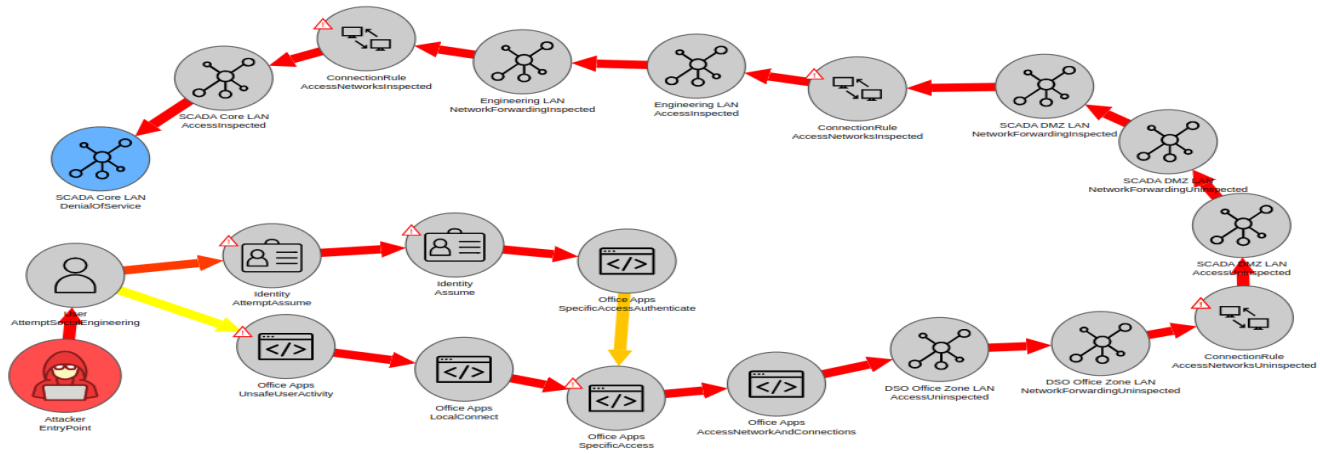

Figure 18: Social engineering attack targeting SCADA Core Zone.

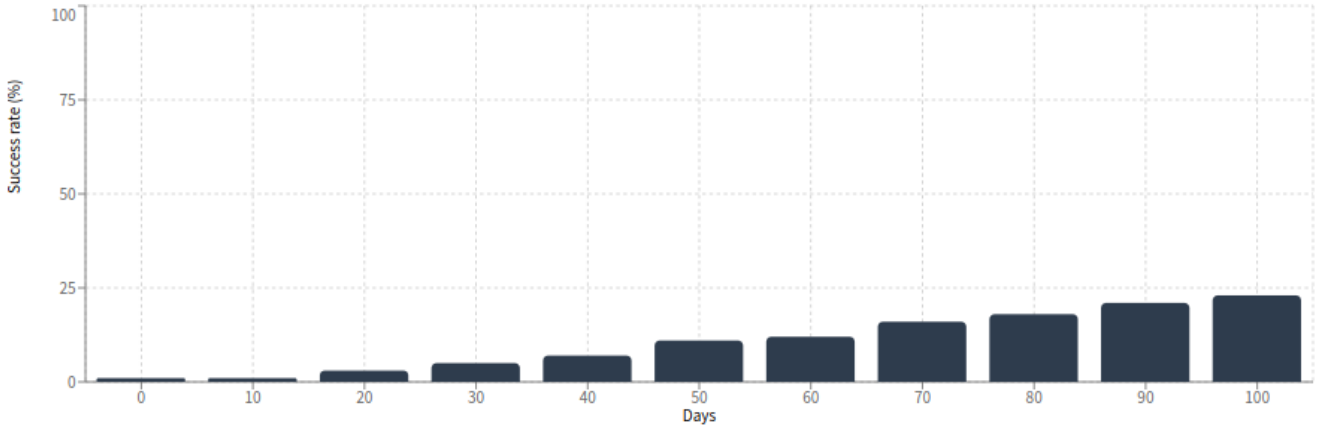

Figure 19: TTC for social engineering attack.

the Internet to approach the DSO and launch the attack. Instead of showing the similar attack path, we instead explore other possible ways for this attack to happen. Figure 20 shows how an attacker can use and exploit a human error or lack of security awareness to launch this attack. The attack path is similar to the last scenario except that once the attacker gains access to the Engineering Zone, it moves to the Process Zone and gains access on the Process LAN. From the process LAN, the attacker can connect to the intermediary network between substations and the process LAN and gain a foothold in a substation. If an RTU is vulnerable, it will then be exploited.

Figure 21 shows the required attacker effort in terms of TTC values. It can be seen that the success rate is 25% after 100 days for a persistent attacker. As mentioned before, this kind of attack can be prevented with a security aware user and earlier mentioned defenses enabled for all networks and targeted assets.

Scenario 12: Deny RTU in Energy Supplier We now show the possibility of for an attacker on the Internet to social engineer an operator in the SCADA Core Zone and target one of the RTUs in the Energy Supplier Network. Figure 22 shows the possible attack path. It has some resemblance to the previous scenarios as the attacker attempts social engineering attack to gain access to the HMI and SCADA Core Zone. From the SCADA Core Zone, the attacker moves to the Process LAN which is directly connected to the GPRS, LTE, PowerLine

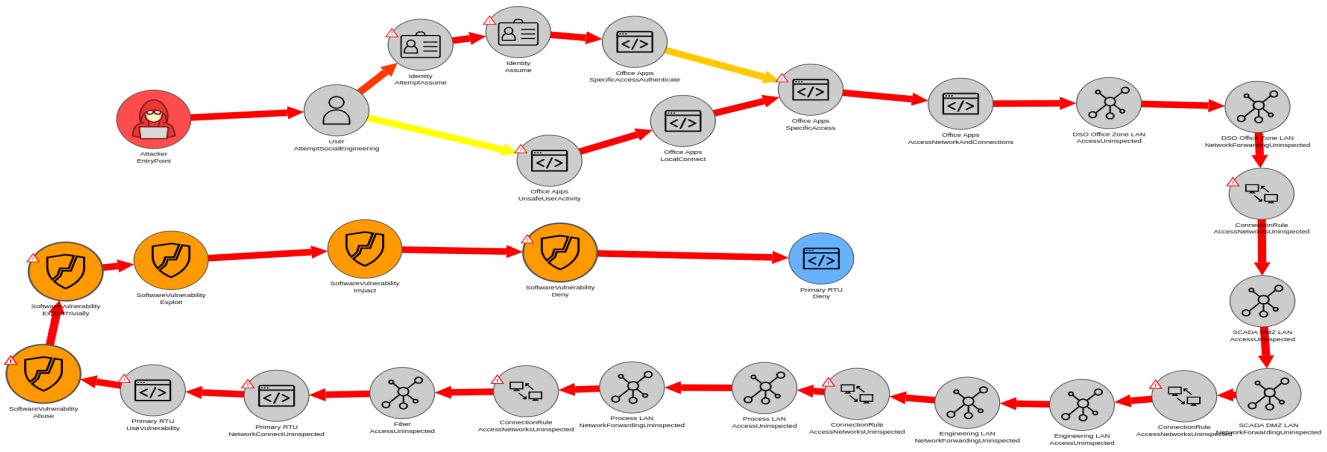

Figure 20: Attack Path for denying a RTU in a substation.

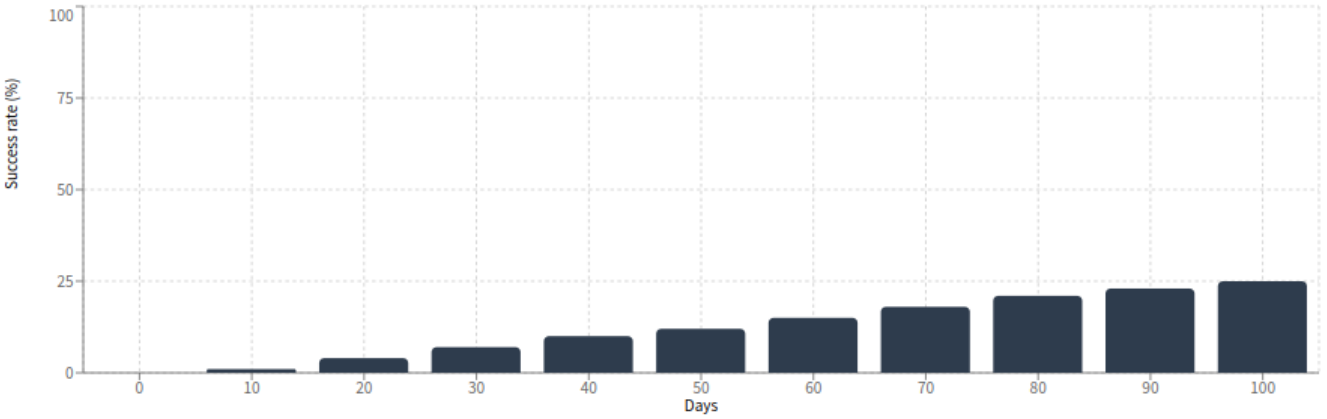

Figure 21: TTC for social engineering attack to deny RTU.

network. Then the attacker can gain a foothold in the Energy Supplier Network and launch a denial of service attack to bring the RTU down.

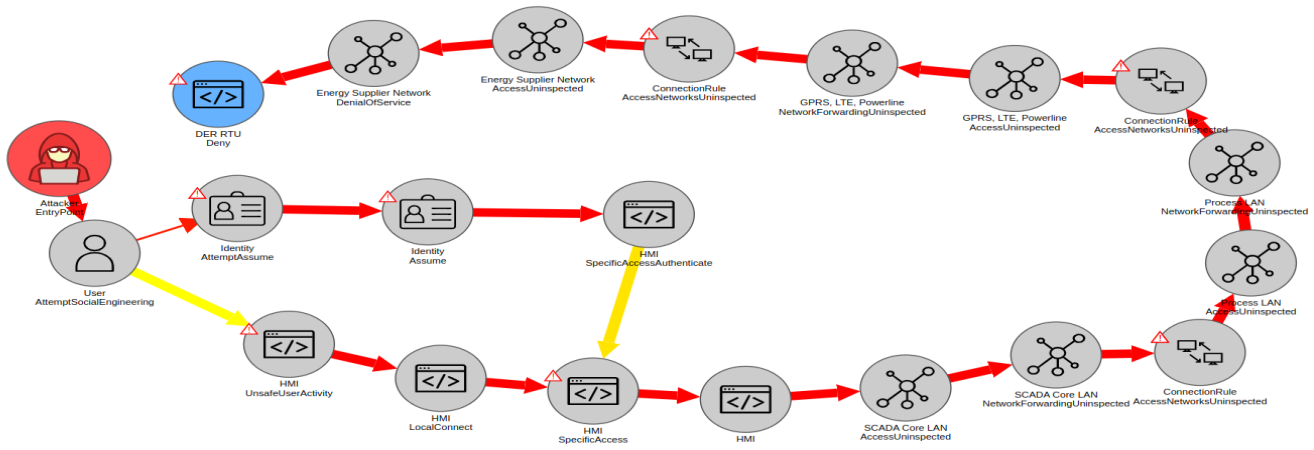

Figure 22: Attack Path to Denying RTU in Energy Supplier.

The success rate for this attack is estimated to be around 23% after 100 days for a persistent attacker. The attack can be prevented with a security aware user and earlier mentioned defenses enabled for all networks and targeted assets.

3.2.4 Attacker at the Vendor

All actors of a FM depend on services and equipment provided by external partners such as vendors. Traditionally, there exists an inherent trust between the vendors and the consumers which has increasingly been violated in the recent past. A real-world example of the severity of such a threat comes from the recent SolarWinds hack [40]. In a typical attack, at any point in the supply chain, an attacker installs malicious code in the provided hardware or software that is eventually used by a consumer. This could for example be malicious code in software or a backdoor in a smart meter hardware that is provided by a vendor. The attacker can later use them to launch attacks. The attack is very critical as multiple actors of a FM might be using the same equipment or the same vendor.

Scenario 13-14: Full Access on Smart Meter Application First we show the possibility for an attacker to attempt a hardware supply chain attack on the smart meter. Figure 23 shows the attack path. The attack path shows that an attacker can attempt a supply chain attack on the smart meter hardware to gain full access on the smart meter hardware and the application. The attack path is straight forward and the success rate for this attack is estimated to be around 31% after 100 days as shown in Figure 24.

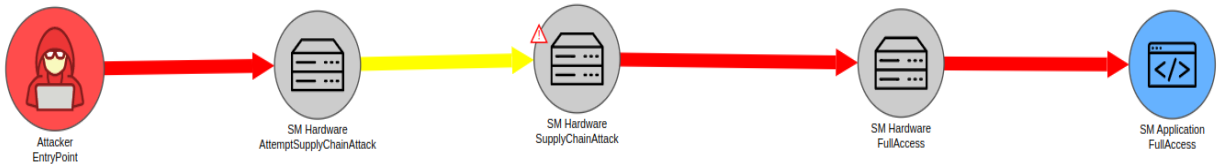

Figure 23: Attack Path for hardware supply chain attack on smart meter.

Once the attacker has full access on the smart meter application, it is trivial for it to access the connected network. Once an attacker is able to access the HOME_LAN network, they can perform man in the middle attacks on the network allowing the ability to read and write all associated data. This enables the attacker to disrupt the operation of a FM in multiple ways as detailed earlier. Figure 25 shows the attack path for a MitM attack on the HOME LAN and the attacker has a similar success rate of 31% after 100 days for this attack.

Hardware supply chain attacks are generally hard to protect against. One possible defense against these attacks is to perform `SupplyChainAuditing` on the hardware asset. In reality, the `SupplyChainAuditing` defense translates to testing newly acquired software and equipment in a sand-boxed fashion and inspect their behavior prior to installing them into production. Even with the defense in place, it is still possible for an attacker

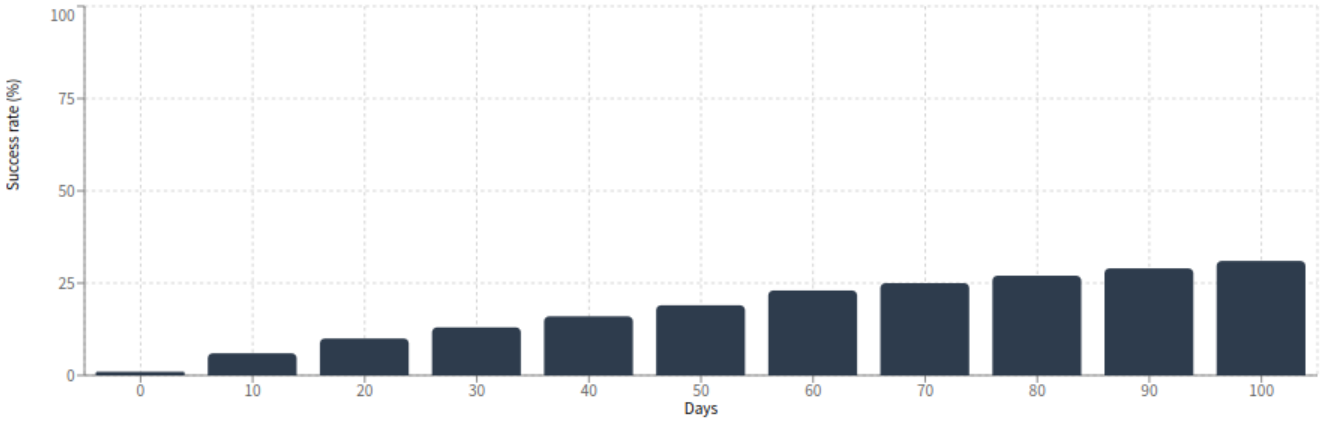

Figure 24: TTC for hardware supply chain attack on smart meter.

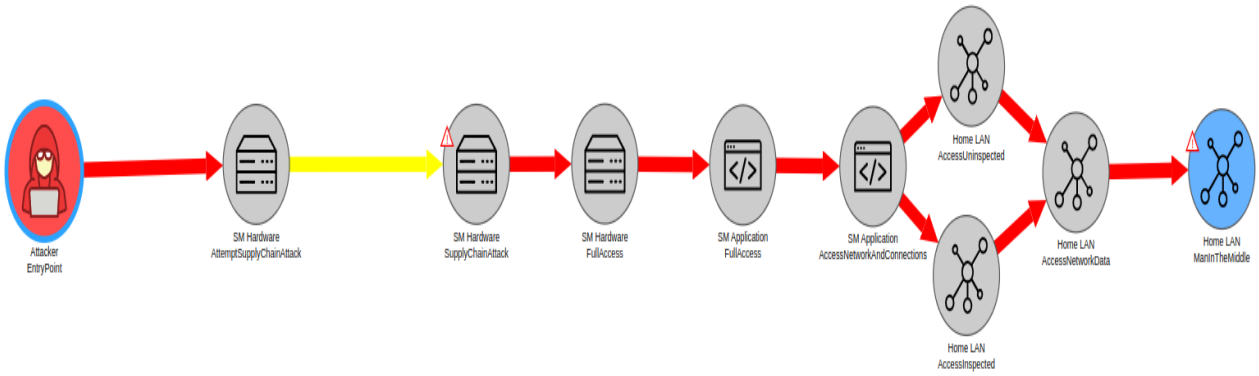

Figure 25: Attack Path for MitM on a smart meter using hardware supply chain attack.

to `bypass` the auditing process as shown in Figure 26. However, the probability of the original attack reduces significantly with the defense in place as shown in Figure 27 with the success rate now reduced to 7%. In the upcoming scenarios, we will discuss more possible defenses against these kind of attacks.

Scenario 15: Man in the Middle on Core Zone LAN in Aggregator Using a hardware supply chain attack on the smart meter hardware, an attacker can also target the Core Zone LAN in the Aggregator. The attack path for this attack is fairly obvious. Once the attacker has full access on the smart meter, it can reach the Home LAN as discussed earlier. From the Home LAN, the attacker can access the Internet which is connected to the Head End LAN in the Aggregator which in turn is connected to the Operational Planning LAN and the Core Zone LAN. Once the attacker can access the Core Zone LAN, it can launch the attack The success rate for this attack is similar to the above scenarios i.e., 31%. The possible defenses are also same.

Scenario 16: DoS on SCADA Core Zone For this scenario, we explore the possibility of a software supply chain attack. The Engineering Zone of the DSO relies on a vendor (just like any other actor in the FM) for

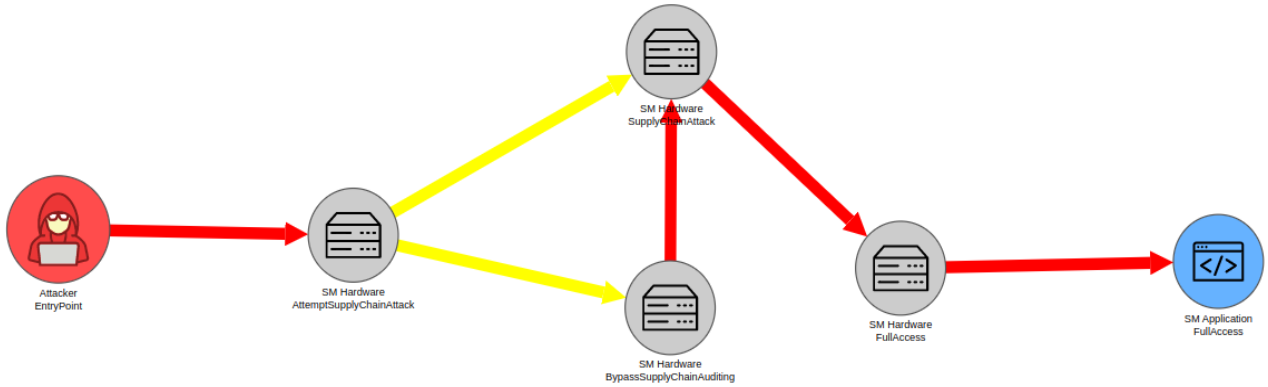

Figure 26: Attack Path for full access on a smart meter using bypass.

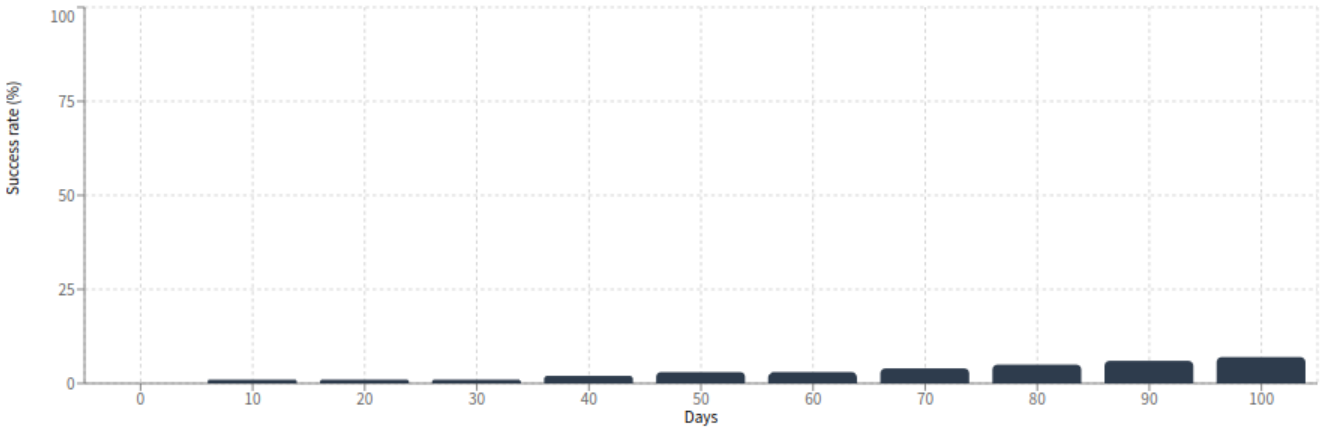

Figure 27: TTC for hardware supply chain attack on smart meter with supply chain auditing.

software and hardware updates. Figure 28 shows the securiCAD mode view for the DSO engineering zone. We assume that the Office Station connected to the Engineering LAN takes its updates from a vendor. To be specific, the Office Station takes updates/software packages from a vendor controlled software repository through the `SoftwareProduct` asset. If an attacker connects to the vendor system and gains full access, it can access and modify the data in the software repository and the `SoftwareProduct` used by the targeted application. This way the attacker is able to compromise the Office Station application to gain full access on it. Since the application is directly connected on the Engineering LAN which has direct access to the SCADA Core LAN, the attacker can reach and target the SCADA Core Zone with a denial of service attack. The full attack path is shown in Figure 29.

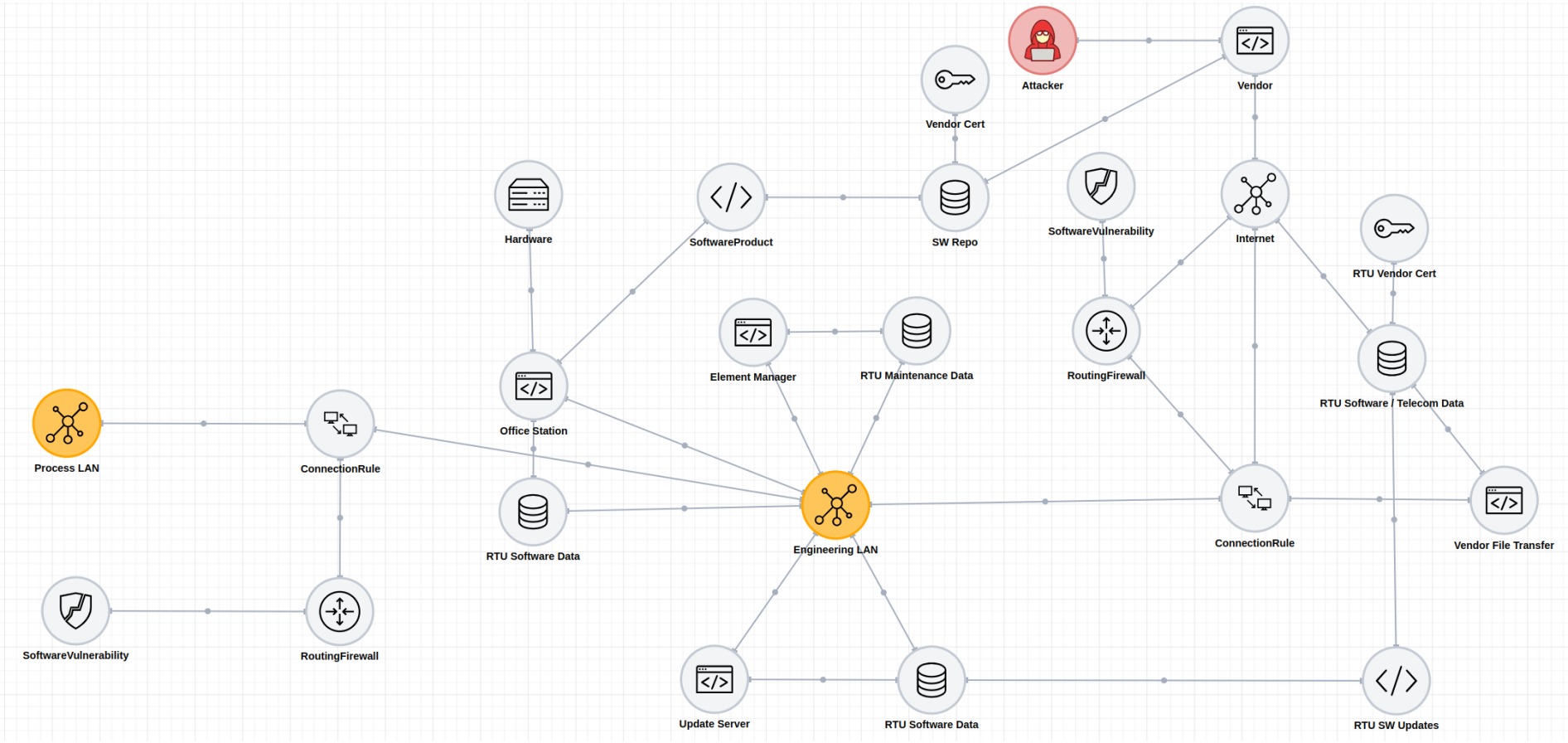

Figure 28: securiCAD model view for DSO Engineering Zone.

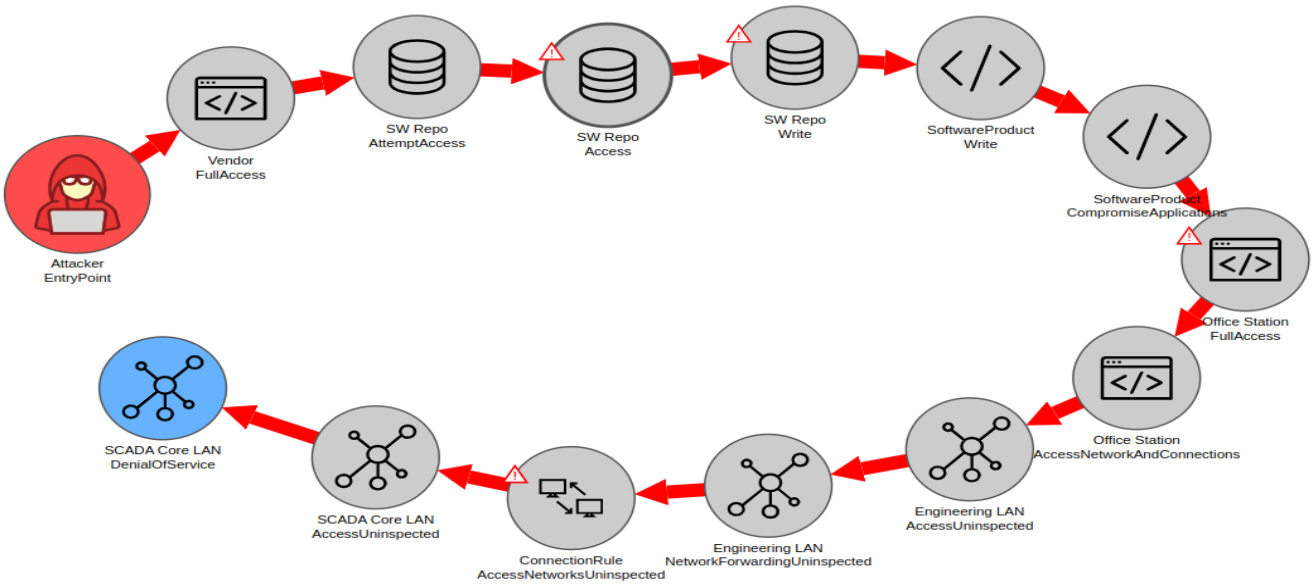

Figure 29: Attack Path for DoS on SCADA Core Zone.

The first possible defense against this attack is using `SupplyChainAuditing` defense of the Office Station asset, as discussed before. However, as mentioned earlier the attacker can still with small probability achieve its goal by bypassing the auditing defense. This is because the defense itself is not viewed as perfect. To further make the job of the attacker difficult, we now explore another possible security control to this attack. The model in Figure 28 shows an asset named `Vendor Certificate` connected to the `SW repository` asset. The idea is that the vendor can use this certificate to sign all software releases that are stored in the repository. If an attacker attempts to modify the stored software, this will then become detectable by the Office Station and the compromised updates/software is not installed. This shall completely thwart the shown attack path. Of course, the attacker can then target the certificate used by the vendor to sign, but its difficulty is significantly increased.

Scenario 17: Deny RTU in substations The last two, but not the least, scenarios in our considered scope is the possibility for an attacker at the vendor to target the RTUs in the substations and at the energy supplier. To show the attack possibilities, we again employ software supply chain attacks in the Engineering Zone of the DSO. The reason why Engineering Zone is chosen to show this attack possibility is because it hosts a number of critical systems. The Vendor File Transfer Server collects software and firmware updates from a vendor over the Internet. These updates are then transferred to the RTUs and the SCADA Core Zone. Assuming that an attacker can modify the vendor supplied RTU software update data, the attacker can perform a software supply chain attack to gain full access on all RTUs using the same RTU SW Updates product. The attack path is fairly straightforward and shown in Figure 30.

Similar to above, the possible defenses against this attack is to first enable `SupplyChainAuditing` on all relevant application assets. This will reduce the attack possibility to only bypasses assuming that the auditing is not 100% effective. As a next step, the vendor should also use a certificate to sign the RTU software update releases as shown in Figure 28. This will allow the consumer of the updates to establish if the update is compromised or not and prevent the attack from happening.

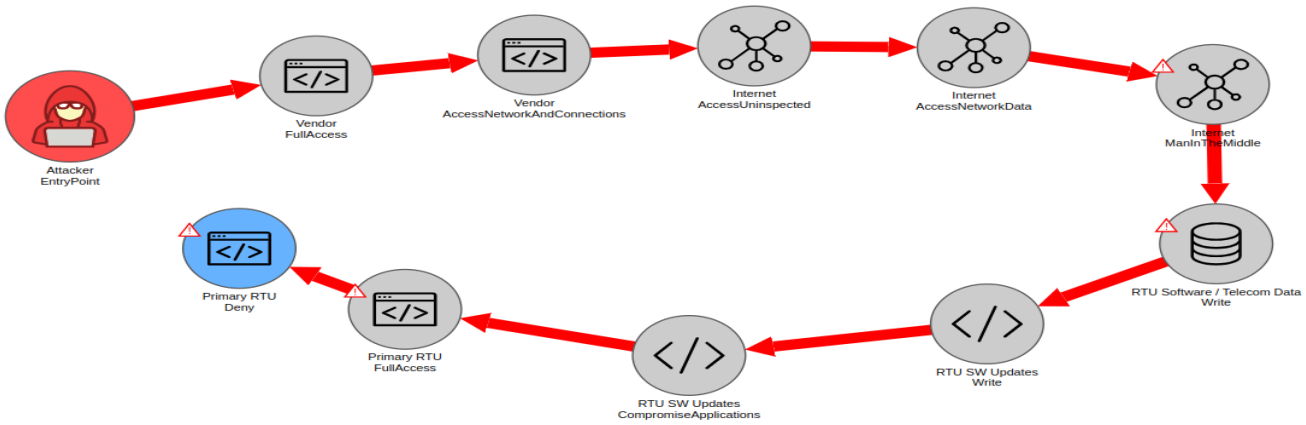

Figure 30: Attack Path for denying RTU in substations.

Scenario 18: Deny RTU in Energy Supplier The attack shown in this scenario works quite similarly to the last scenario. Once the attacker can reach the primary RTU through a software supply chain attack on the RTU software updates, it can access the connected FIBER network to reach the Process LAN which in turn is connected to the GPRS, LTE, Powerline network used by the Energy Supplier. Further accesses on this network allow the attacker to reach the Energy Supplier Network that hosts the RTU which is then possible to be targeted by the attacker. The attack path is shown in Figure 31 and the possible defenses to this attack are same as discussed in the last scenario.

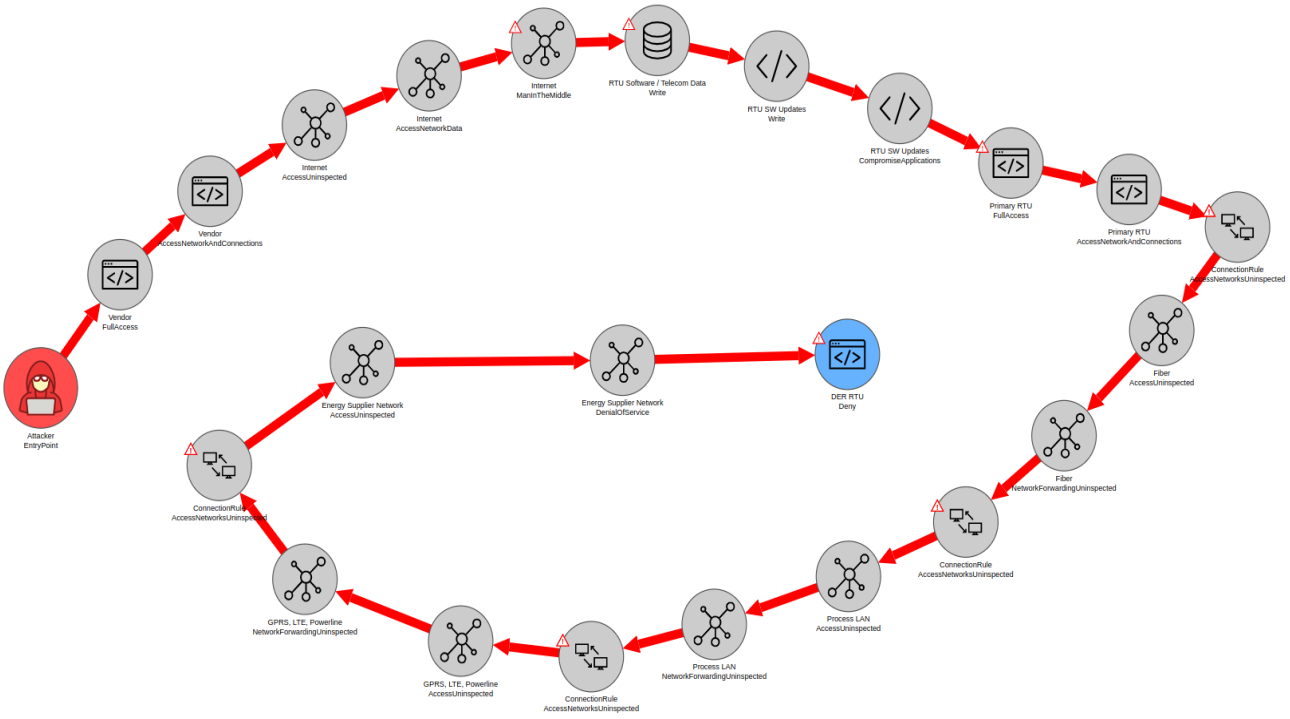

Figure 31: Attack Path for denying RTU in Energy Supplier.

3.3 Summary of Results

The presented analysis acts as a sort of mechanism to identify holes or flaws and understanding how the FM system is designed and where threats against the system may originate. This is usually the first step towards securing any architecture. The analysis focused on three attacker starting positions and six targets resulting in eighteen attack scenarios. The general takeaway from the analysis is that the attacker can reach their target assets in most scenarios. This is especially interesting to see in the scenarios involving the DSO, where the attacker was able to follow the allowed data flows and directions to go from one zone to another and succeed with the attacks. In some sense, this outcome was to be expected. OT networks such as SCADA were once isolated from other networks and physical access of the system was needed to realize an attack. With time, even these networks became connected to the Internet and thus physical access is no longer necessary for an attacker. This development also exposes these systems to both OT and traditional IT attacks. Good news is that the analysis has also shown that with properly configured defenses on the assets, it is possible to make the attacker's task difficult and in some scenarios completely stop the attack paths. It is also evident from the analysis that some security considerations were already made during the design process of the HONOR FM architecture.

Considering all eighteen scenarios, it is clear that the biggest area of concern is an attacker originating on the Internet. In most scenarios, the attacker used access to the Internet to reach different areas in the architecture e.g., majority of the scenarios with attacker starting on the Internet were quite similar to the scenarios where the attacker starts on the smart meter because the attacker anyway moves from the smart meter to the Internet. Worryingly, it is also much easier for an attacker to exist on the Internet compared to smart meters and vendors. Another important, but perhaps not novel, lesson from the analysis is that protecting the most obvious entry points into a network and to a high value asset is not enough. The attacker can, and will, find alternate paths to reach its target and it is thus imperative to monitor and protect all possible entry points.

When it comes to making recommendations to protect the FM not only against the explored scenarios in our analysis, but also against other similar threats, there are a few things that need to be considered. The most obvious apparent solution is to go back to the practice of air-gapping the systems. However, there is no silver bullet when it comes to cyber security. In practice, no system is actually isolated. Staff still needs to get data in and out of the system and to resolve problems. Such systems are also not practical for operators that require monitoring plants and RTUs from distant locations. Another problem is that if a functionality does not exist, then hackish workarounds are often improvised resulting in increased exposure to attacks. Therefore, we need to consider an inclusive/progressive approach that does not suggest on removing certain crucial functions when it comes to suggesting security controls for a FM.

Threat scenarios and security controls elaborated in the analysis point toward the following security policies. First, the networks should be segregated from each other using security gateways just like the way it is done in the analyzed FM reference architecture. Secondly, the number of entry points from the Internet should be limited as much as possible. Finally, remote access to critical infrastructure such as substations is crucial both as a function and for security. A Virtual Private Network (VPN) can be employed as an effective remote access solution, however, strict access control policy based on multi factor authentication should be used for authentication. Based on our simulations, we recommend at least 3 layers of defensive controls for a FM. First at the perimeter, the security gateways need to be securely configured and protected. There should be payload inspection for all traffic using some kind of networks based IDPS and the assets themselves should be kept free from vulnerabilities using frequent patching and updating. Secondly, all the networks need to employ defenses

such as eavesdrop, man in the middle, and network access control protections. Data should be encrypted to avoid eavesdropping. Finally, the assets should also follow the best end-point security practices in terms of defenses. Some suggestions that are discussed earlier in the scenarios include using an IDPS on hosts to detect and block malicious traffic and protection against hardware modifications. As mentioned before, there are no perfect solution for all security problems and the goal is mostly limited to make the required attacker effort so high that most attackers do not succeed with their attacks. Nevertheless, persistent attackers that are highly resourceful, given enough time and regardless of the available defenses, will eventually be successful. It should also be noted that all the simulations and the presented analysis are based on a number of assumptions that were made in the reference architecture and the model. The results (e.g., how to protect an asset) can be completely different if there was more specific information available about certain systems. Furthermore, in the analysis, the asset defenses are 100% (that they are always present and active) although they can be configured with any value between 0 and 100. The motivation behind this was to keep the analysis interesting as a 100% defense is always going to be better in terms of TTC than for example a 75% defense. Instead the analysis focused on finding the most effective defenses to stop the attack paths.

4 Conclusion

The HONOR FM system leads to new interactions involving stakeholders from completely different domains and a distributed ICT infrastructure. These factors potentially result in novel vulnerabilities and attack vectors. This work delivers the final cyber security risk assessment of the market system within the HONOR project. The aim is to discover and reveal how attackers can target different parts of the market, how long it will take for them to reach their targets, and what kind of weaknesses they can exploit. The assessment is based on a threat modelling approach using attack simulations on a system model in securiCAD. The system model is devised using coreLang and is based on the HONOR technical architecture. The biggest threat as revealed by the explored attack scenarios is from an attacker on the Internet. The cyber security assessment also makes a number of recommendations based on the simulated scenarios.

Acknowledgement

This document was created as part of the ERA-Net Smart Energy Systems project HONOR, funded from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 646039 (SG+) / no. 775970 (RegSys).

References

[1] Nils Müller, Kai Heussen, Zeeshan Afzal, Mathias Ekstedt, and Per Eliasson. D6.1 conceptual model of data streams, detection and verification requirements. Technical report, 04 2021. URL https://sp11321.hostedoffice.ag/Shared%20Documents/06_WP6_Cyber-physical_system_monitoring_verification_and_validation/03_Results/.

[2] Philip J. Douglass. D3.1 use cases. Technical report, 06 2021. URL https://sp11321.hostedoffice.ag/Shared%20Documents/03_WP3_System_Architecture_and_Evaluation_Scenarios/03_Results/.

[3] Oliver Kraft, Oliver Pohl, and Florian Rewald. D3.2 system architecture. Technical report, 06 2021. URL https://sp11321.hostedoffice.ag/Shared%20Documents/03_WP3_System_Architecture_and_Evaluation_Scenarios/03_Results/.

[4] Can Karatas, Gerhard Meindl, and Evyatar Littwitz. D2.1 requirements and expected benefits of flexibility markets. Technical report, 10 2021. URL https://sp11321.hostedoffice.ag/Shared%20Documents/02_WP2_Stakeholder_engagement_co-creation_and_replication/03_Results/.

[5] Sotirios Katsikeas, Simon Hacks, Pontus Johnson, Mathias Ekstedt, Robert Lagerström, Joar Jacobsson, Max Wällstedt, and Per Eliasson. An attack simulation language for the IT domain. In Harley Eades III and Olga Gadyatskaya, editors, *Graphical Models for Security - 7th International Workshop, GraMSec 2020, Boston, MA, USA, June 22, 2020 Revised Selected Papers*, volume 12419 of *Lecture Notes in Computer Science*, pages 67–86. Springer, 2020. doi: 10.1007/978-3-030-62230-5_4. URL https://doi.org/10.1007/978-3-030-62230-5_4.

[6] Mathias Ekstedt, Pontus Johnson, Robert Lagerström, Dan Gorton, Joakim Nydren, and Khurram Shahzad. Securi CAD by foreseeti: A CAD tool for enterprise cyber security management. In Jens Kolb, Barbara Weber, Sylvain Hallé, Wolfgang Mayer, Aditya K. Ghose, and Georg Grossmann, editors, *19th IEEE International Enterprise Distributed Object Computing Workshop, EDOC Workshops 2015, Adelaide, Australia, September 21-25, 2015*, pages 152–155. IEEE Computer Society, 2015. doi: 10.1109/EDOCW.2015.40. URL https://doi.org/10.1109/EDOCW.2015.40.

[7] Antti Alahäivälä. 4 questions on sector coupling. URL https://www.wartsila.com/insights/article/4-questions-on-sector-coupling. Accessed: 2021-11-10.

[8] Chun-Hao Lo and Nirwan Ansari. Decentralized controls and communications for autonomous distribution networks in smart grid. *IEEE Transactions on Smart Grid*, 4(1):66–77, 2013. doi: 10.1109/TSG.2012.2228282.

[9] European Commission. Proposal for a directive of the european parliament and the council on common rules for the internal market in electricity, February 2017. URL https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016PC0864R%2801%29.

[10] Nils Müller, Zeeshan Afzal, Per Eliasson, Mathias Ekstedt, and Kai Heussen. Threat scenarios and monitoring requirements for cyber-physical systems of energy flexibility markets. *arXiv preprint arXiv:2111.03300*, 2021.

[11] Konstantinos Spiliotis, Ariana Isabel Ramos Gutierrez, and Ronnie Belmans. Demand flexibility versus physical network expansions in distribution grids. *Applied Energy*, 182:613–624, 2016.

[12] Xiaolong Jin, Qiuwei Wu, and Hongjie Jia. Local flexibility markets: Literature review on concepts, models and clearing methods. *Applied Energy*, 261:114387, 2020.

[13] José Villar, Ricardo Bessa, and Manuel Matos. Flexibility products and markets: Literature review. *Electric Power Systems Research*, 154:329–340, 2018.

[14] Charalampos Ziras, Carsten Heinrich, and Henrik W Bindner. Why baselines are not suited for local flexibility markets. *Renewable and Sustainable Energy Reviews*, 135:110357, 2021.

[15] Pol Olivella-Rosell, Eduard Bullich-Massagué, Mònica Aragüés-Peñalba, Andreas Sumper, Stig Ødegaard Ottesen, Josep-Andreu Vidal-Clos, and Roberto Villafáfila-Robles. Optimization problem for meeting distribution system operator requests in local flexibility markets with distributed energy resources. *Applied energy*, 210:881–895, 2018.

[16] Alexandre Vernotte, Margus Välja, Matus Korman, Gunnar Björkman, Mathias Ekstedt, and Robert Lagerström. Load balancing of renewable energy: a cyber security analysis. *Energy Informatics*, 1(1):1–41, 2018.

[17] Teodor Sommestad, Mathias Ekstedt, and Pontus Johnson. Cyber security risks assessment with bayesian defense graphs and architectural models. In *42st Hawaii International International Conference on Systems Science (HICSS-42 2009), Proceedings (CD-ROM and online), 5-8 January 2009, Waikoloa, Big Island, HI, USA*, pages 1–10. IEEE Computer Society, 2009. doi: 10.1109/HICSS.2009.141. URL `https://doi.org/10.1109/HICSS.2009.141`.

[18] Hannes Holm, Khurram Shahzad, Markus Buschle, and Mathias Ekstedt. P^2cysemol: Predictive, probabilistic cyber security modeling language. *IEEE Trans. Dependable Secur. Comput.*, 12(6):626–639, 2015. doi: 10.1109/TDSC.2014.2382574. URL `https://doi.org/10.1109/TDSC.2014.2382574`.

[19] Cynthia A. Phillips and Laura Painton Swiler. A graph-based system for network-vulnerability analysis. In *Proceedings of the 1998 Workshop on New Security Paradigms, Charlottsville, VA, USA, September 22-25, 1998*, pages 71–79. ACM, 1998. doi: 10.1145/310889.310919.

[20] Bruce Schneier. Attack trees. *Dr. Dobb's journal*, 24(12):21–29, 1999.

[21] Sjouke Mauw and Martijn Oostdijk. Foundations of attack trees. In *Information Security and Cryptology - ICISC, 8th International Conference, Seoul, Korea, December 1-2, 2005*, volume 3935 of *Lecture Notes in Computer Science*, pages 186–198. Springer, 2005. doi: 10.1007/11734727_17.

[22] Barbara Kordy, Sjouke Mauw, Sasa Radomirovic, and Patrick Schweitzer. Foundations of attack-defense trees. In *Formal Aspects of Security and Trust - 7th International Workshop, FAST, Pisa, Italy, September 16-17, 2010.*, volume 6561 of *LNCS*, pages 80–95. Springer, 2010.

[23] Barbara Kordy, Ludovic Piètre-Cambacédès, and Patrick Schweitzer. DAG-based attack and defense modeling: Don't miss the forest for the attack trees. *Comput. Sci. Rev.*, 13-14:1–38, 2014. doi: 10.1016/j.cosrev.2014.07.001.

[24] R Dantu, K Loper, and P Kolan. Risk management using behavior based attack graphs. In *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004*, volume 1, pages 445–449 Vol.1. IEEE, 2004. ISBN 0769521088.

[25] Elena Doynikova and Igor V. Kotenko. Enhancement of probabilistic attack graphs for accurate cyber security monitoring. In *IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation, 2017*, pages 1–6, 2017.

[26] Pengwen Lin and Yonghong Chen. Dynamic network security situation prediction based on bayesian attack graph and big data. In *2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC)*, pages 992–998. IEEE, 2018. ISBN 9781538653739.

[27] Yu Liu and Hong Man. Network vulnerability assessment using bayesian networks. In *Proc. SPIE*, volume spie-5812, pages 61–71, 2005. ISBN 0819457973.

[28] N Poolsappasit, R Dewri, and I Ray. Dynamic security risk management using bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1):61–74, 2012. ISSN 1545-5971.

[29] Cui Yimin, Li Junmei, Zhao Wei, and Luan Cheng. Research on network security quantitative model based on probabilistic attack graph. *ITM Web of Conferences*, 24:02003, 2019. ISSN ITM Web of Conferences.

[30] Pontus Johnson, Robert Lagerström, and Mathias Ekstedt. A meta language for threat modeling and attack simulations. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ARES 2018, New York, NY, USA, 2018. ISBN 9781450364485. doi: 10.1145/3230833.3232799.

[31] An Hoa Vu, Nils Ole Tippenhauer, Binbin Chen, David M. Nicol, and Zbigniew Kalbarczyk. Cybersage: A tool for automatic security assessment of cyber-physical systems. In Gethin Norman and William H. Sanders, editors, *Quantitative Evaluation of Systems - 11th International Conference, QEST 2014, Florence, Italy, September 8-10, 2014. Proceedings*, volume 8657 of *Lecture Notes in Computer Science*, pages 384–387. Springer, 2014. doi: 10.1007/978-3-319-10696-0_29. URL `https://doi.org/10.1007/978-3-319-10696-0_29`.

[32] Skybox Security. Risk analytics for cyber security. URL `https://www.skyboxsecurity.com/`. Accessed: 2022-12-02.

[33] RedSEAL Systems. Redseal cloud cybersecurity solution. URL `https://www.redseal.net/`. Accessed: 2022-12-02.

[34] Hannes Holm. A large-scale study of the time required to compromise a computer system. *IEEE Trans. Dependable Secur. Comput.*, 11(1):2–15, 2014. doi: 10.1109/TDSC.2013.21. URL `https://doi.org/10.1109/TDSC.2013.21`.

[35] Erland Jonsson and Tomas Olovsson. A quantitative model of the security intrusion process based on attacker behavior. *IEEE Trans. Software Eng.*, 23(4):235–245, 1997. doi: 10.1109/32.588541. URL https://doi.org/10.1109/32.588541.

[36] Edsger W. Dijkstra. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1: 269–271, 1959. doi: 10.1007/BF01386390. URL https://doi.org/10.1007/BF01386390.

[37] Zeeshan Afzal, Mathias Ekstedt, Per Eliasson, Joar Jacobsson, and Roysten D'souza. D7.2 Final Cyber Security Assessment of the HONOR Flexibility Market. Technical report, 12 2022. URL https://sp11321.hostedoffice.ag/Shared%20Documents/07_WP7_Cyber-security_modeling_of_SCADA_and_control_system_solution/03_Results/Threat%20Model%20Views.

[38] Mihai Costache and Valentin Tudor. Security aspects in the advanced metering infrastructure. M.Sc. Thesis, Chalmers University of Technology, Department of Civil and Environment, Gothenburg, Sweden, 2011.

[39] Kim Zetter. Inside the cunning, unprecedented hack of ukraine's power grid. URL https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. Accessed: 2022-12-02.

[40] Sean Peisert, Bruce Schneier, Hamed Okhravi, Fabio Massacci, Terry Benzel, Carl Landwehr, Mohammad Mannan, Jelena Mirkovic, Atul Prakash, and James Bret Michael. Perspectives on the solarwinds incident. *IEEE Security & Privacy*, 19(02):7–13, 2021.