SINTEF

SINTEF Digital
Postal address:
Postboks 4760 Torgarden
7465 Trondheim, Norway

Switchboard: +47 40005100

info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

Smart Grid Threat Modelling Tool Documentation

VERSION 1.05	**DATE** 29-June-2023
AUTHOR(S) Lars Halvdan Flå	
CLIENT(S) Lnett	**CLIENT'S REFERENCE** Siri T. Ravndal
PROJECT NO. 102021132	**NO. OF PAGES/APPENDICES:** 21+ Appendices

Abstract

This memo describes the setup and use of the Smart Grid Threat Modeling Tool. This includes installation of the tool, steps for how to perform the threat modelling exercise, and how to further develop the tool. In addition, it gives an overview of the threat modelling theory behind the tool, and a detailed overview of all threats included in the tool.

PREPARED BY Lars Halvdan Flå	SIGNATURE Lars Halvdan Flå
APPROVED BY Oddbjørn Gjerde	SIGNATURE Oddbjørn Gjerde
PROJECT MEMO NO. 102021132-1	**CLASSIFICATION** Unrestricted

Document history

VERSION	DATE	Version description
0.05	2023-05-10	Draft distributed to project partners for comments.
1.00	2023-06-22	Addressed comments from partners
1.05	2023-06-29	Addressed comments from project quality assurer

Table of contents

1 Introduction

This document describes the setup and use of the Smart Grid Threat Modeling Tool (which in turn consists of the Microsoft Threat Modeling Tool and the Smart Grid Threat Modeling Template). It is intended to offer new users hands-on guidance on how to create a new model of a smart grid use case and how to perform the threat modelling process. Furthermore, it provides guidance on how the Smart Grid Threat Modelling Tool can be changed and extended in the future, if needed.

The Smart Grid Threat Modelling Tool was originally developed in the CINELDI project [1], [2] and has been used and further developed in the InterSecure project [3]. Additional material on the Microsoft Threat Modeling Tool can be found here online.[1] The guidance and instructions in this document are written for version 7.3.21108.2 of the tool. Please note that future versions of the tool may deviate in terms of functionality and user interface.

The Smart Grid Threat Modelling Tool is meant to be used together with the other deliverables from the InterSecure project. An overview of the project activities is shown in Figure 1. Within InterSecure, the Smart Grid Threat Modelling Tool has been developed in WP 2.

WP 3 has developed a SCADA simulation model. From the perspective of the Smart Grid Threat Modelling Tool, the simulation model can be used to explore selected threats in more detail. As an example, the simulation model can investigate the effects of a Denial-of-Service attack.

WP 4 has developed a method for vulnerability assessment of cyber-physical power grids, based on the bow-tie model. We believe that the Smart Grid Threat Modelling Tool and the vulnerability assessment method can complement each other, since they approach security of the power grid from different directions. The Smart grid threat modelling tool studies the data flow between elements and the threats to them, while the vulnerability assessment method focuses on one element. However, for this element, the method studies the chains of event leading up to an attacks, and the chains of actions which can be performed after an attack.

WP 5 has developed an overall method for risk management. The smart grid threat modelling tool can be used to support specific parts of this process, more specifically the process of risk identification. Once threats have been identified and evaluated, selected threats can be exported back to the risk management method.

[1] https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

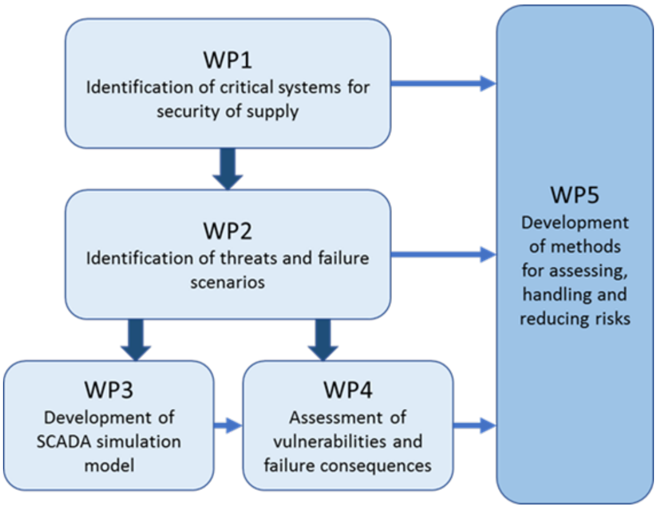

WP1
Identification of critical systems for security of supply
WP2
Identification of threats and failure scenarios
WP3
Development of SCADA simulation model
WP4
Assessment of vulnerabilities and failure consequences
WP5
Development of methods for assessing, handling and reducing risks

Figure 1: Overview of project activities and work packages.

The Smart Grid Threat Modelling Tool can be used both in the design phase and in the operations phase. The tool is intended for those concerned with cyber security in the smart grid, for example cyber security professionals in power grid companies, cyber security consultants or cyber security researchers.

2 Terminology

Analysis instance: A tuple of (source, flow, target)-stencils, considered together when the Microsoft Threat Modeling Tool generates threats.

DFD: Data Flow Diagram. Model for describing the flow of data in a system, used as basis for the analysis in the Microsoft Threat Modeling Tool.

Microsoft Threat Modeling Tool: Software created by Microsoft used both to create models and performing threat modeling, and for creating custom templates.

Model: A representation of the system of interest, created by combining stencils.

Smart Grid Threat Modeling Template: A template created for the smart grid domain.

Smart Grid Threat Modelling Tool: This term is used to refer to joint use and combination of the Microsoft Threat Modelling Tool and the Smart Grid Threat Modelling Template.

Stencil: Stencils are the elements used to create a model. These elements include components such as processes, data flows and trust boundaries, as explained further in section 4. A stencil may contain a set of attributes, to which values can be assigned during the threat modelling process.

STRIDE: Threat modeling method originating from the software security domain. STRIDE is a mnemonic for Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.

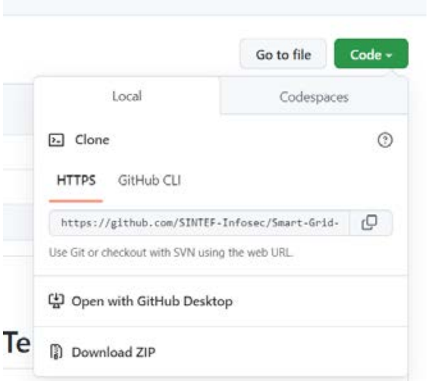
Template: A set of stencils, stencil attributes, threats logic, and threat descriptions. The information contained in a template determines what stencils are available when building the model, how threats are generated, and how threats are described. Templates are often created with a specific domain in mind.

3 Installation and setup

1. The threat modeling is done using the Microsoft Threat Modeling Tool, which is freely accessible and can be downloaded from Microsoft.[2]
   Run the downloaded executable (TMT7.application) and the tool should start automatically once installed.

2. In addition to the Microsoft Threat Modeling Tool, the Smart Grid Threat Modeling Template must be downloaded from github[3].

   Press "Code", download, and extract the zip file. See Figure 2.



https://github.com/SINTEF-Infosec/Smart-Grid-

Use Git or checkout with SVN using the web URL.

Figure 2: How to download the Smart Grid Threat Modelling Template from GitHub.

3. In the Microsoft Threat Modeling Tool, under "Template for New Models", click browse, navigate to the newly extracted folder, and select the "Smart_Grid" file.

4. You can now create a new model, open an existing model, or open a template.

[2] https://aka.ms/threatmodelingtool
[3] https://github.com/SINTEF-Infosec/Smart-Grid-Threat-Modeling-Template

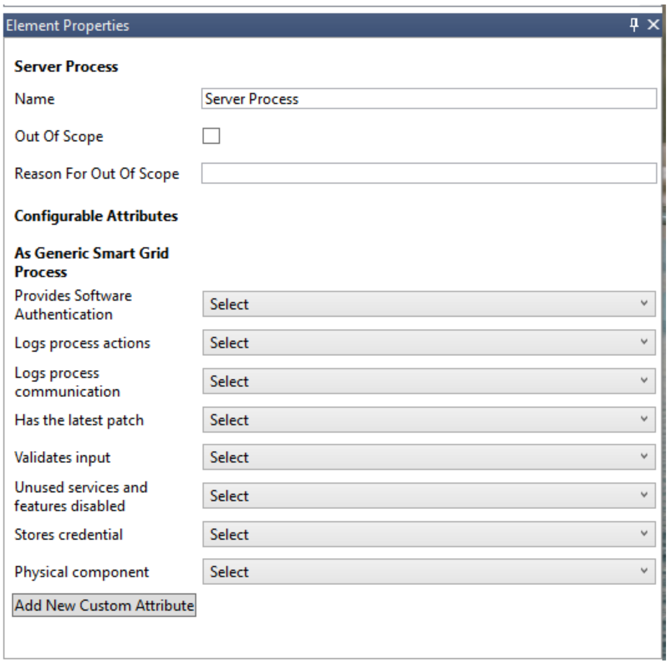
4 Create new model or open an existing model

1. Start by either creating a new model (make sure the "Smart Grid" template is selected from the dropdown menu) or open an existing model.

2. A model is created (or edited) by drag and drop from the "Stencils" menu to the right. Similarly, stencils are connected by dragging and dropping the data flow stencil. The Smart Grid template has 5 main stencil categories:
   - **Generic Smart Grid Process**: Includes the components/processes found in the smart grid.
   - **Generic Trust Border/Line Boundary:** The trust border/line are identical, apart from the shape. They are used to indicate that the communication crossing the line is not trusted, and that threats should therefore be generated for the affected stencils. For more information on the logic of threat generation, see section The theory behind the tool.
   - **Generic External Interactor:** Includes the components that interact with the smart grid assets of a grid company, but which are not under the control of the company (e.g. external networks, vendor organizations).
   - **Generic Data Store:** Includes databases, but smaller amounts of storage (device memory, device storage) are assumed to be included in the process stencils.
   - **Generic Data Flow:** Used to describe the communication between processes.
   - **Human Input:** Human input could have been a derived stencil of the Generic data flow but was for threat logic convenience included as a top-level stencil.
   - **GPS Signal:** Like the case for "Human Input", GPS Signal was included as a top-level stencil for threat logic convenience.

3. Once the model is built, click on each of the stencils to configure them in the "Element Properties" window (see Figure 3). The most important configuration is to assign values to the different attributes for the stencil in the dropdown menus. This is because these attributes have a direct effect on the threats included in the analysis.

4. Once all desired stencils (including Trust Boundaries) are included, connected, and configured, the threat modeling process can start. Due to the potentially high number of threats generated, it may be beneficial to split complex systems into several threat modelling sessions and for instance threat model one use case at a time.



Element Properties

Server Process

Name	Server Process
Out Of Scope	□
Reason For Out Of Scope	

Configurable Attributes

As Generic Smart Grid Process

Provides Software Authentication	Select
Logs process actions	Select
Logs process communication	Select
Has the latest patch	Select
Validates input	Select
Unused services and features disabled	Select
Stores credential	Select
Physical component	Select

Add New Custom Attribute

Figure 3: Element properties window.

5 Performing the threat modeling exercise

By threat modeling exercise, we refer to the stage where the tool is used to generate and evaluate threats based on a model.

1. Build or open an existing model as described in section Create new model or open existing model.

2. Press the magnifying glass symbol in the top bar to go into analysis view and generate the threats, see Figure 4:

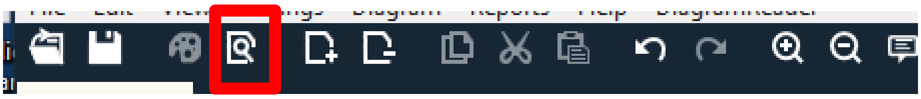


Figure 4: How to generate threats in the Microsoft Threat Modeling Tool.

Press the Palette-symbol directly to the left of the magnifying glass to go back to design view.

3. A threat list should emerge at the bottom of the window, listing all identified threats. The threat modeling exercise is conducted by going through this list of threats, and for each threat input information on:

a. Status: This should be set to "Needs investigation" for all threats not mitigated or out of scope.

b. Justification: This line should provide an explanation for the other values selected, along with other remarks on the threat.

c. Priority: Should be used to help prioritize which threats to address first. (e.g., all threats with the potential to cause a blackout affecting more than one substation should be given a high priority)

d. Impact: Optional. If used, a definition for "High", "Medium", and "Low" should be established before starting the threat modeling exercise.

e. Probability: Optional. See Impact.

f. Possible mitigations: This field can be used to suggest mitigations.

For each threat, there is a description of the threat, meant to be relevant for all types of stencils. In the case that there are aspects particularly relevant to specific stencils, this is included in the fields named "Considerations for [host device] / [IED] / [network device] / [sensor/actuator]". The information in these fields can be considered if either the source and/or target stencil is either a host device, IED, network device or sensor/actuator. These stencils are meant to reflect the types of component typically found in the smart grid, and are children of the "Generic Smart Grid Process".

Many of the fields contain references on the form (T*xyz*). These refer to Techniques in the MITRE ATT&CK for ICS framework.[4] The team performing the threat modelling can consult these for further information and support.

For more information on the logic of threat generation, see section The theory behind the tool.

4. The threat modeling is complete when all threats have been evaluated. The result of the threat modelling exercise can be exported in different ways, see section 5.2.

5.1 Some tips for the threat modeling exercise.

1. The threat modeling should be performed in a team which has both cyber security and power grid competence. The greatest value of the tool lies in the discussions it facilitates.

2. Clearly define scope and values/criteria for "High", "Medium", and "Low" used by the "Priority", "Impact", and "Probability" categories.

5.2 Exporting the threat modelling results

The results of the threat modelling exercise can primarily be exported in two different ways, either as an HTML report or as a list of Comma Separated Values (CSV).

[4] https://attack.mitre.org/techniques/ics/

HTML report

An HTML report of the evaluated threats can be created by clicking "Reports" > "Create Full Report" in the toolbar at the top of the window.

CSV

While in the analysis view, the list of threats can be exported by clicking the "Export Csv"-button at the bottom left of the list of generated threats.

6 Making modifications to the threat modeling tool

This section is intended for those who are already familiar with the Smart Grid Threat Modeling Tool and wish to modify it.

1. Start the Microsoft Threat Modeling Tool and select "Open Template" and open the Smart-Grid template.

2. You now have the option to add new stencils, modify existing stencils, change threat properties or add/change threats.
   a. **Add new stencil**: You can either add a stencil or add a derived stencil. A derived stencil will inherit the properties of its parent stencil. After creating a stencil, you can define what properties it should have and the values these properties can take.
   b. **Modify existing stencil**: clicking on the stencil of interest allows you to change or add properties.
   c. **Change threat properties**: By clicking on "Threat Properties" in the bottom bar, you have the option of adding or changing threat properties.
   d. **Add/change threats**: By clicking on "Threat Types" in the bottom bar, you have the option of changing, adding or removing threats. For each threat, there are two input fields, "Include" and "Exclude", used for threat generation. For more information on the logic of threat generation, see section The theory behind the tool.

6.1 Further functionality

- Two templates may be merged by clicking "File" > "Merge Template to this".

7 The theory behind the tool

This section introduces the threat modeling theory used in the Smart Grid Threat Modeling Tool.

The Microsoft Threat Modeling Tool uses Data Flow Diagrams (DFD) to build a representation of the system of interest. As the name suggests, data flow diagrams visualize how data is transmitted between different elements (stencils). DFDs have originally been used for threat modeling of software, which is also reflected in the type of DFD elements which make up DFDs. The DFD elements are process, data store, data flow, and external interactor. For the purpose of threat modeling, a fifth element, the trust boundary, is normally included. The stencils defined in the Smart Grid Threat Modeling Tool share large similarities with the DFD elements, but there are also some differences.

STRIDE-per-Interaction: Once the model is created and configured, the Microsoft Threat Modeling Tool generates threats according to a STRIDE-per-Interaction approach. This approach means that every instance of a source, a flow, and a target stencil is analyzed for threats. This is illustrated in Figure 5. In this figure, the Sensor Process is the source, the Sensor data is the flow, and the SCADA Server Process is the target, and together they constitute an "analysis instance". If we add another data flow going from the SCADA Server Process to the Sensor Process, the roles would be reversed. The SCADA Server Process would be the source and the Sensor process the target. In this case we would have two "Analysis instances", and the Microsoft Threat Modeling Tool would analyze both independently for threats.

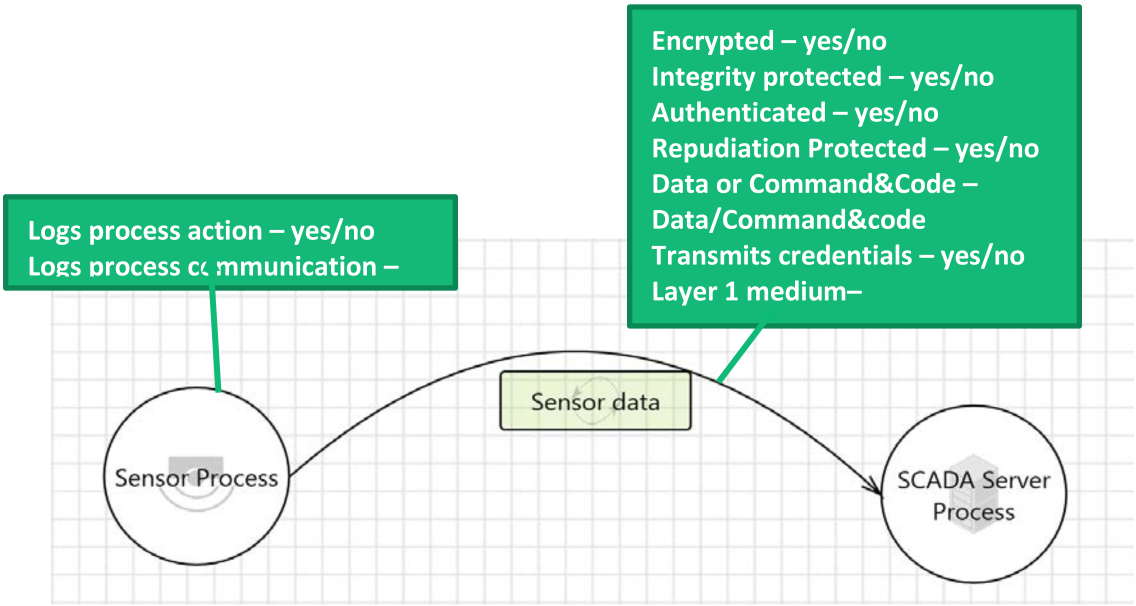

Encrypted – yes/no
Integrity protected – yes/no
Authenticated – yes/no
Repudiation Protected – yes/no
Data or Command&Code – Data/Command&code
Transmits credentials – yes/no
Layer 1 medium–
Logs process action – yes/no
Logs process communication –
Sensor data
Sensor Process
SCADA Server Process

Figure 5: Example of source, flow, and target stencils, with associated attributes.

To determine what threats to generate for each "analysis instance", the Microsoft Threat Modeling Tool checks each instance against a list of threats defined in the Smart Grid Threat Modeling Template. Each threat definition has two input fields, "Include" and "Exclude". A threat is generated (included in the analysis) based on Boolean logic. If the expression in the "Include" field evaluates to true and the expression in the "Exclude" field evaluates to false (or is empty), the threat is included in the analysis. Otherwise, it is excluded. The Boolean threat logic is based on stencil category and stencil attributes (shown in blue boxes above). An example is shown in Figure 6.

Include:
(flow is [Generic data flow]) **and** (flow crosses [Generic Trust Border Boundary] **or** flow crosses [Generic Trust Line Boundary])
Exclude:
flow.[Encrypted] is 'Yes' **or** flow is [BGP advertisement]

Figure 6: Example of Boolean logic for threat generation.

8 References

[1] L. H. Flå, R. Borgaonkar, I. A. Tøndel, and M. G. Jaatun, “Tool-assisted threat modeling for smart grid cyber security,” presented at the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland: IEEE, Jun. 2021.

[2] L. H. Flå, “Threat modeling framework for smart grids,” NTNU, 2021. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2781029

[3] F. Holik, L. H. Flå, M. Gilje Jaatun, S. Yildirim Yayilgan, and J. Foros, “Threat modeling of a smart grid secondary substation,” *Electronics*, vol. 11, no. 6, Mar. 2022.

Appendix A: Detailed documentation of threats included in the Smart Grid Threat Modelling Tool

Spoofing Threats

Spoofing of device	
Description	An attacker may attempt to send messages appearing to come from {source.Name}. This may lead to unauthorized access to the {target.Name} or incorrect data delivered to the {target.Name}. Spoofing can for instance be performed through a man in the middle attack, replaying captured messages or forging new messages.
Logic	**Include:** (source is [Generic Smart Grid Device] or source is [Generic Data Store] or source is [Generic External Interactor]) and (target is [Generic Smart Grid Device] or target is [Generic Data Store]) and (flow is [Generic data flow]) and (flow crosses [Generic Trust Line Boundary]) **Exclude:** flow.[Authenticated] is 'Yes'
Considerations for host device	An attacker can attempt to perform spear phishing (T0865) if the device allows for connections to email servers, or otherwise fool the user to install a malicious application (T0863). An attacker already present on the network may try to spoof status/measurement messages from the process to deceive the operator (T0856), possibly causing an operator to perform harmful actions. A way of performing this attack include to set up a rouge device or setting up a man-in-the-middle attack to spoof communication to other host devices or IEDs (T0848).
Considerations for IED	An attacker may attempt to send unauthorized command messages from higher up in the control hierarchy (T0855) or send a false measurement value from a sensor. Serial protocols may lack security features, and an attacker may exploit this to act as a device on the serial network.
Considerations for network device	Spoofing the administrator login to a network device may be attractive, as it can allow for denial-of-service attacks on process measurement/commands.
Considerations for sensor/actuator	Serial protocols may lack security features, and an attacker may exploit this to act as a device on the serial network.

Tampering Threats

Tampering of transmitted data	
Description	An attacker may attempt to tamper with the communication between the {source.Name} and the {target.Name}. This can for instance happen through a man-in-the-middle attack (T0830).
Logic	**Include:** (flow is [Generic data flow]) and (flow crosses [Generic Trust Line Boundary]) **Exclude:** flow.[Authenticated] is 'Yes' or flow.[Integrity Protected] is 'Yes'

Considerations for host device	IP based protocols may be vulnerable to ARP spoofing.
Considerations for IED	IP based protocols may be vulnerable to ARP spoofing.
Considerations for network device	Tampering routing tables and rules can be a prerequisite for tampering of transmitted data.
Considerations for sensor/actuator	Sensor data may be attractive to tamper to manipulate the state perceived by the operator. Tampering actuator commands may be the end goal of an attack to cause a blackout.

Tampering of data store	
Description	An attacker may attempt to tamper values stored on the {target.Name} database. This can happen if the communication from {source.Name} is not authenticated, the database does not check the received value before adding it to the database, or if default, hardcoded or easily guessable credentials are used.
Logic	**Include:** (target is [Generic Data Store]) and (flow crosses [Generic Trust Line Boundary]) **Exclude:** target.[Sanitize input] is 'Yes' or flow.[Authenticated] is 'Yes'
Considerations for host device	-
Considerations for IED	-
Considerations for network device	-
Considerations for sensor/actuator	-

Tampering of device	
Description	An attacker may attempt to tamper the information contained in the {target.Name}, for instance configurations or memory locations relevant for the correct operation of the {target.Name} (or other dependant devices). Possible methods can be to compromise the supply chain of the devices to make the devices behave in malicious ways (T0862), or exploit interfaces exposed by the device, for instance a command line interface (T0807).
Logic	**Include:** (source is [Generic Smart Grid Device] and flow is [Generic data flow]) and (flow crosses [Generic Trust Line Boundary]) **Exclude:** -
Considerations for host device	An attacker may attempt to modify device parameters (T0836), for instance alarm settings (T0838), and misuse the HMI (T0823) to control the device. One approach is to change I/O values (T0806), either randomly or more deliberately. An attacker without access to interact with the device application directly, may attempt to hook APIs (T0874),

	for instance Windows APIs. An attacker may also try to infect project files (T0873).
Considerations for IED	An attacker may seek to change the operating mode of the controller (T0858) and download malicious programs (T0843). Another approach may be to install malicious firmware (T0839), potentially though a remote update function(T0857). An attacker with a presence on the IED may attempt to manipulate the I/O tables (T0835) (T0806), modify alarms (T0838), execute their own programs (T0821) (T0889), exploit APIs (T0871) (T0834), modify process parameters (T0836), modify software process tasking (T0821).
Considerations for network device	An attacker may attempt to target the configuration interfaces of the network device to redirect traffic or disable security features (e.g., VPNs, firewalls).
Considerations for sensor/actuator	An attacker may attempt to install malicious firmware (T0839), potentially though a remote update function(T0857).

Repudiation Threats

Repudiation of performed actions	
Description	An attacker may deny having performed an action on the {target.Name} if the device does not log actions. This might in turn hinder restoration and forensic efforts. To evade detection by logs, an attacker may masquerade malicious files as legitimate application (T0849), otherwise target exploits to evade detection (T0820), or remove indicators of their presence from the host (T0872).
Logic	**Include:** (target is [Generic Smart Grid Device] or target is [Generic Data Store]) and (flow is [Generic data flow] and flow.[Data or Command&Code] is 'Command&Code') and (flow crosses [Generic Trust Line Boundary]) **Exclude:** target.[Logs device actions] is 'Yes'
Considerations for host device	-
Considerations for IED	Devices at lower levels in the control hierarchy may have limited capacity for logging.
Considerations for network device	-
Considerations for sensor/actuator	Devices at lower levels in the control hierarchy may have limited capacity for logging.

Repudiation of customer data	
Description	An owner of transmitted data may deny association to it if the communication is not signed, which in turn may have financial implications.
Logic	**Include:** (target is [Host Device] and source is [Sensor Device]) and (flow.[Customer data] is 'Yes') and (flow is [Generic data flow] and (flow crosses [Generic Trust Line Boundary])) **Exclude:** flow.[Repudiation Protected] is 'Yes'
Considerations for host device	-
Considerations for IED	-
Considerations for network device	-
Considerations for sensor/actuator	-

Information Disclosure Threats

Disclosure of transmitted information	
Description	An attacker may attempt to learn the content of the information transmitted between the {source.Name} and the {target.Name}. This can for instance be accomplished by setting up a man-in-the-middle-attack (T0830), an attack that is particularly critical if credentials are transmitted in an insecure way. An attacker may also seek to enumerate network devices (T0840), systems (T0846, T0888) and to sniff network traffic (T0842).
Logic	**Include:** (flow is [Generic data flow]) and (flow crosses [Generic Trust Line Boundary]) **Exclude:** flow.[Encrypted] is 'Yes'
Considerations for host device	-
Considerations for IED	Devices configurable via insecure protocols (for instance HTTP or telnet) may reveal credentials to an attacker.
Considerations for network device	An attacker may fill the ARP table of a switch to cause it to act as a hub.
Considerations for sensor/actuator	-

Disclosure of device information	
Description	An attacker may attempt to extract information from the {target.Name}.
Logic	**Include:** target is [Generic Smart Grid Device] **Exclude:** target is [Network Device]

Considerations for host device	An attacker may attempt to collect industrial environment information (T0802, T0811, T0852), including information on the physical process state (T0801) and equipment tags (T0861).
Considerations for IED	An attacker may attempt to collect industrial environment information (T0802, T0811, T0852), detect IED operating modes (T0861), extract programs from IEDs (T0845) and collect I/O table values (T0877) to understand the logic.
Considerations for network device	-
Considerations for sensor/actuator	-

Denial of Service Threats

External distributed denial of service attack	
Description	An attacker with a presence in an external network may attempt to flood the {target.Name} with network traffic, in an attempt to make it unavailable.
Logic	**Include:** (source is [External Network] and target is [Generic Smart Grid Device]) and (flow crosses [Generic Trust Line Boundary]) **Exclude:** -
Considerations for host device	-
Considerations for IED	-
Considerations for network device	-
Considerations for sensor/actuator	-

Denial of transmitted information	
Description	An attacker may attempt to deny the arrival of transmitted information, for instance by dropping packets after setting up a man-in-the-middle attack (T0830).
Logic	**Include:** flow crosses [Generic Trust Line Boundary] **Exclude: -**
Considerations for host device	-
Considerations for IED	An attacker may attempt to block commands and reporting messages (T0803, T0804, T0805) from reaching their target. Wireless IEDs can be vulnerable to signal jamming.
Considerations for network device	An attacker may attempt to target a network device to reroute, drop or otherwise bock the arrival of transmitted information.

Considerations for sensor/actuator	Wireless sensors/actuators can be vulnerable to signal jamming.

Denial of service of device	
Description	An attacker may attempt to generate large volumes of data, send specially crafted packet, or otherwise attempt to make the {target.Name} unavailable. Such attacks may exploit different protocols (ARP, IP, UDP, TCP) or happen at the application level. An attacker can also compromise the supply chain of devices or applications to make them malfunction (T0862, T0800).
Logic	**Include:** (source is [Generic Smart Grid Device]) and (target is [Generic Smart Grid Device]) and (flow is [Generic data flow]) and (flow crosses [Generic Trust Line Boundary])
Considerations for host device	Attackers may deny the service internet-facing applications and devices by overwhelming it with traffic. An attacker may attempt to deny the correct functioning of alarms by modify alarm setting (T0838) or cause other types of DoS by destroying data (T0809).
Considerations for IED	An attacker may exploit built-in mechanisms for shutdown/restart (T0816), stop certain service (T0881), cause a DoS through manipulating I/O tables (T0835), exploit functionality for remote firmware update (T0857), destroy data (T0809), or otherwise perform a Denial of Service (T0814). Without causing the whole device or process to stop, an attacker may also attempt to modify alarm settings (T0857) or supress alarms (T0878).
Considerations for network device	-
Considerations for sensor/actuator	-

Signal jamming	
Description	An attacker may attempt to jam the signal from the {source.Name} leaving it unable to communicate with the {target.Name}.
Logic	**Include:** (flow.[Layer 1 medium] is 'Wireless' or flow is [GPS signal]) and (flow crosses [Generic Trust Line Boundary]) **Exclude:** -
Considerations for host device	-
Considerations for IED	-
Considerations for network device	-

Considerations for sensor/actuator	-

Denial of service of data store	
Description	An attacker may attempt to prevents access to the {target.Name}.
Logic	**Include:** (target is [Generic Data Store]) and (flow crosses [Generic Trust Line Boundary])
Considerations for host device	-
Considerations for IED	-
Considerations for network device	-
Considerations for sensor/actuator	-

Unauthorized Access Threats

Unauthorized access to device	
Description	An attacker may attempt to get access to the {target.Name} and potentially use the rights to perform tampering, information disclosure and denial of service attacks. An attacker may obtain access by for instance compromising the supply chain, exploiting disclosed or unknown vulnerabilities, remote update functionality, misconfiguration, unused services or features that have not been disabled, lack of input validation (for instance buffer overflow), weak or easily guessable password, or otherwise weak authentication mechanisms.
Logic	**Include:** (target is [Generic Smart Grid Device] or target is [Generic Data Store]) and (flow is [Generic data flow]) and (flow crosses [Generic Trust Line Boundary]) **Exclude:** -
Considerations for host device	An attacker can use a compromised web page to get initial access to a device (T0817), spear phishing (T0865), or exploit service exposed by the device (T0819, T0833). These can be services exposed to the local network (T0866), for instance Server Message Block, or externally exposed services (T0822), for instance VPN. An attacker can also obtain access through infected removable media (T0847), transient cyber assets (for instance maintenance computers) (T0864), hardcoded (T0891), default (T0812) or stolen (T0859) credentials or rely on user interaction to obtain a presence (T0863). Once established, the attacker can set up command and control over application protocols such as HTTP(S), OPC,

	RDP, telnet, DNP3 (T0869), or in some other way using common port (T0885).
Considerations for IED	An attacker can attempt to get access to an IED through an infected removable media (T0847), through hardcoded (T0891), default (T0812) or stolen (T0859) credentials, or through any services exposed by the IED.
Considerations for network device	-
Considerations for sensor/actuator	-

Unauthorized access through vendor	
Description	An attacker may attempt to obtain access to the {target.Name} by compromising the vendor organization.
Logic	**Include:** source is [Vendor organization] and (flow crosses [Generic Trust Line Boundary]) **Exclude:** -
Considerations for host device	-
Considerations for IED	-
Considerations for network device	-
Considerations for sensor/actuator	-

Insider Threats

Insider threat	
Description	{source.Name} may attempt to install and execute malware, issue harmful commands or configure the {target.Name} in a harmful way.
Logic	**Include:** (source is [Human Operator]) and (flow is [Human Input]) and (flow crosses [Generic Trust Line Boundary]) **Exclude:** -
Considerations for host device	-
Considerations for IED	Insiders with access to IEDs may upload malicious programs or place them in vulnerable states (for instance by setting program modes to allow for updates).
Considerations for network device	-
Considerations for sensor/actuator	-