PSS TRA –

Threat and Risk Analysis

Product and Solution Security (PSS)

Threat and Risk Analysis Method Description

SIEMENS

1 | Introduction

1.1 Purpose of this document

This document describes a method and provides guidance how to prepare and conduct a Product and Solution Security (PSS) Threat and Risk Analysis (hereafter referred to as "TRA"). Relevant method steps are explained and, where relevant, reference on helpful documentation, tools and further information is provided.

The described method is aligned with international standards on information security and ICS risk management, including ISO/IEC 27005:2018 [1], and IEC 62443 [4], [4], [5]. It can be understood as an implementation of the requirements for cybersecurity threat and risk assessment stated in these standards. The referenced international standards do not provide such implementation on their own.

The method can be applied to several target areas, as described in section 1.3. The method description branches into profiles for different target areas, i.e. specific guidance is provided per target area.

IEC 62443-4-1 matches the target area 'Development of a component'. The method profiled for that target area satisfies the requirements of IEC 62443-4-1 for threat modelling, as detailed in the Appendix. IEC 62443-2-4 matches the target area 'Design and deployment of a system'. The method profiled for that target area satisfies the requirements of IEC 62443-2-4 for security risk assessment, also detailed in the Appendix.

Note that this document does not cover security risk treatment and security risk acceptance. The presented method is a pre-requisite, and the Appendix contains a mapping that shows how the method contributes to fulfilling ISO/IEC 27005:2018.

Each organizational unit fulfils the Siemens-wide requirements for PSS risk management by defining a PSS risk management strategy and establishing processes for PSS risk treatment and PSS risk acceptance. These processes are integrated in the development lifecycle (PLM) process and the project execution (PM) process of an organizational unit and define the responsibilities for security risk treatment and acceptance. With respect to the latter, the PM process includes the customer, i.e. the asset owner or intermediates like engineering companies.

Primary target group of this document are persons responsible for conducting (e.g. within projects or as part of their job function) or contributing to TRAs, as well as persons interested in understanding or evaluating the method specified by this document. The roles responsible for security risk treatment and acceptance need to understand the results of a TRA and are hence also a target group.

Disclaimer

- This document is designed to describe the method applied by Siemens to conduct a PSS TRA also to customers and authorities.
- Every reasonable effort has been taken to ensure that the information contained in this document is accurate. However, Siemens assumes no liability whatsoever with respect to the accuracy and completeness of the information, or with respect to data and references contained in this document.
- The information contained in this document does not, and is not intended to, constitute legal advice; instead, all information contained in this document is for general informational purposes only. Any liability with respect to actions taken or not taken based on the contents of this document is hereby expressly disclaimed.
- This document contains links to other third-party websites. Such links are only for the convenience of the reader; Siemens does not recommend or endorse the contents of the third-party sites.
- Nothing in this document shall be construed as a guarantee or warranty of specific properties of any Siemens product, solution or service. Siemens assumes no liability whatsoever with respect to the content of this document. Thus, this document does not extend the contractual and/or statutory liability of Siemens vis-à-vis customers and authorities.

1.2 Method Scope

TRA is a Siemens-wide standardized security risk analysis method to be used for product, solution, and service business, during product development, engineering (solution design and project delivery), or service projects.

The TRA method provides the basis for PSS risk management in the following way:

- In the TRA, **security threats** in terms of possible attacks exploiting security weaknesses of a product, solution, or service are **identified**.
- In the TRA, the **security risk level of threats is analyzed**, leading to a prioritization of threats.
- Based on documented threats, **security measures** that reduce the security risk level are selected and implemented (risk-based approach).
- Documented risk levels provide transparency about security risks, as a basis for making decisions on **risk acceptance** on management level.
- Linking security measures to threats allows to **trace and track security risk treatment**.
- Performing a TRA raises security know-how in the project team.

The TRA method supports the systematic analysis and evaluation of threats in a workshop. During the preparation and planning the following factors should be addressed:

- The complexity of the system.

- The depth to which the system is analysed.
- The available time for the TRA.
- Knowledge and experience of the participants regarding the TRA method and the system.

The TRA focuses on the identification and analysis of security threats and risks. The method includes the documentation of threats but does not specify procedures for specifying security measures to mitigate the risks. The development lifecycle (PLM) process and the project execution (PM) process of an organizational unit contains a TRA as a key step and describes how to use the output of a TRA for other security activities such as security requirements engineering, secure design, and security testing.

1.3 TRA Target Areas

A TRA can be applied in different target areas. Siemens distinguishes between three different target areas, as presented in Figure 1. The terminology of the target areas helps to identify and document the target of analysis of a TRA.

- **Development of a component:** This target area is used in a development project of a component. Two main types of components are developed by Siemens organizational units:
    - **Software application:** Examples are desktop applications for process control operation and engineering, software applications to process medical images, and in general Web applications. A software application typically includes several modules and could comprise protocol implementations.
    - **Embedded devices and network devices** Examples are PLCs, protection relays, computer tomographs, firewall and switch devices, and include the firmware of such devices.

  The security aspects that typically need to be addressed during development include authentication, authorization, input validation, use of cryptographic methods, and logging.

  The next target area provides the *intended technical environment* of components, i.e. the network and the hosts onto which the components are deployed.

- **Design and deployment of a system** This target area is used or provides the basis in an engineering project where a system is designed based on specifically configured Siemens and 3rd party components. Examples are industrial automation and control systems, and centralized traffic control. System-level security aspects include hardening, secure configuration, network security, malware protection, logging, and monitoring.

  A system consists of the following:

    - **Configured hosts and devices:**
        - **Host,** i.e. a computer with an operating system on which software applications are installed.
        - **Embedded devices**

  - **Design the network:** This includes the design of network zones and technical implementation in terms of configuration of network devices and network protocols. The components are connected to the network and are configured to communicate according to the communication matrix.

  The system that is target of a TRA can itself be a subsystem of an overall system and can be connected to other systems. The overall system and the systems connected to it form the technical environment.

  The next target area provides the *intended organizational environment* of a system, i.e., the physical characteristics and the organizational processes that apply when a system is operated by an organisation (the asset owner) at a physical site.

- **Management of a system:** This target area is applied when setting up or improving a management system to securely set-up, operate, maintain and use the system. Examples of security aspects in this scope are asset management, user identity and access rights management, physical access, personnel-related security, security patch management processes as well as security monitoring.

While the TRA method presented in this document in principle fits all three target areas, the description branches into profiles for the two target areas of components and systems. No details are provided on how to apply the method to the third target area.

In product development, the technical environment provided by the systems where software applications or other components will be installed is often not fully known in advance, and likewise for the organizational environment. Instead, assumptions on the environment are stated and documented during development.

In case of a solution project for a customer, the technical environment, e.g., connection other systems, needs to be clarified with the customer, i.e., the asset owner or his/her/its intermediates, and documented as part of the design specification. Assumptions on the organizational environment should also be clarified with the customer and are documented in operation manuals.

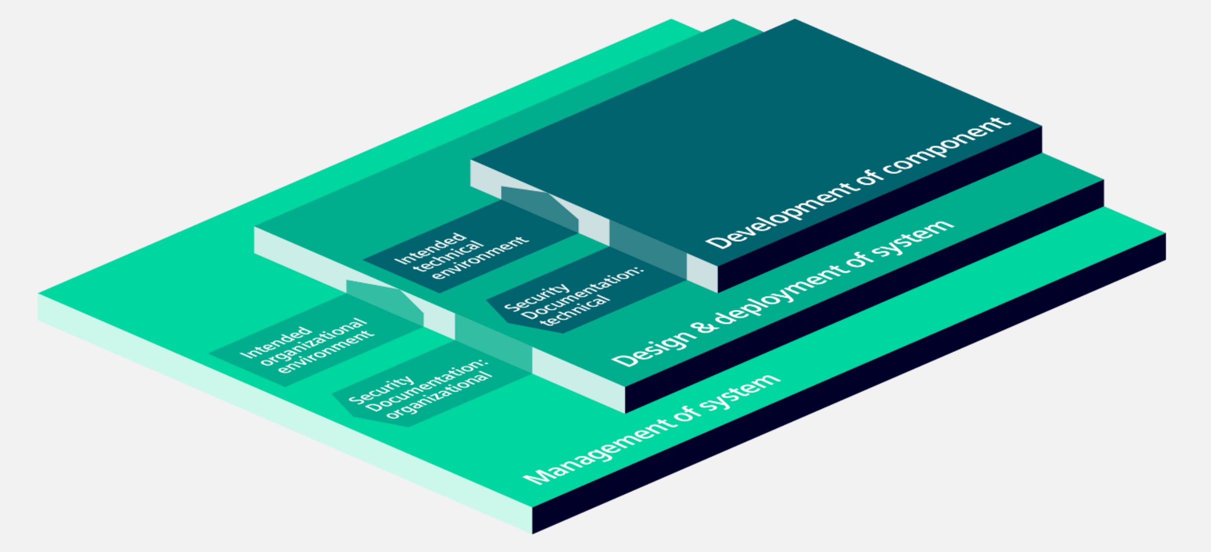

Development of component
Intended technical environment
Security Documentation: technical
Design & deployment of system
Intended organizational environment
Security Documentation: organizational
Management of system

Figure 1: TRA target areas

1.4 Essential Terms and Concepts

This section provides an overview about the terms and concepts used in the TRA context.

A *security risk level* is determined by rating the *likelihood* of a security threat's occurrence and its harmful *impact*, as depicted in Figure 2. A security risk originates from and is rated per *security threat.* A security threat is directed against a target and is the potential for violation of security of the target that has harmful impact on organizations or individuals related to the target.

The method described in this document focuses on security threats against a system in its technical and operational environment. Depending on the target of analysis, security threats against a specific component or against a part of the system are considered in a TRA. The part of the system that is not the target of the analysis forms the *intended operational environment*.

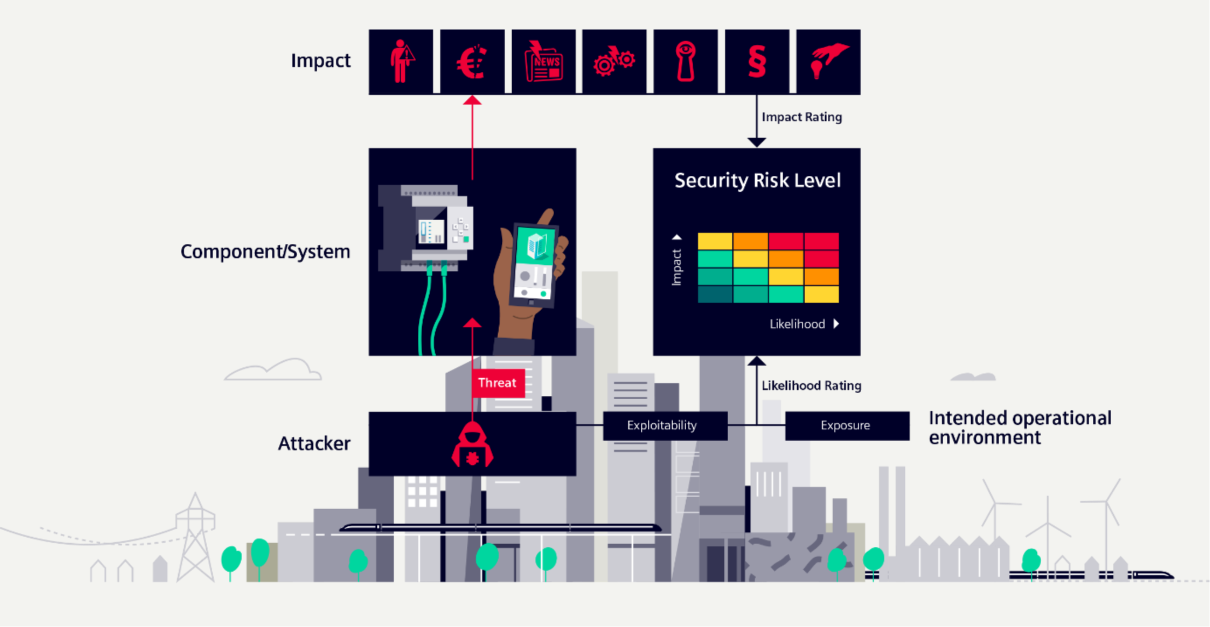


Figure 2: Illustration of security risk rating terminology

A security threat is structured into different aspects, called a *threat scenario*. As shown in Figure 3, a threat scenario consists of an *attack action* that exploits a *weakness* of the target such that a protection goal gets violated. The attack action is performed by an *attacker* of a certain type, characterized by skills and level of access.

The *protection goals* are specified in terms of confidentiality, integrity or availability of data or services of the target. If a protection goal is violated in an attack, this might have a harmful impact on organizations like the owner or the vendor, or on individuals like users, employees, or the public, in one or several impact categories.

The likelihood of a threat scenario rated in terms of two factors: The first is *exposure*, i.e., how easy it is for an attacker to obtain the level of access that is required to perform the attack action. The second factor is *exploitability,* i.e., how easy it is for an attacker to perform the attack action.

The result of a TRA is a list of rated security threat scenarios against the target of analysis.

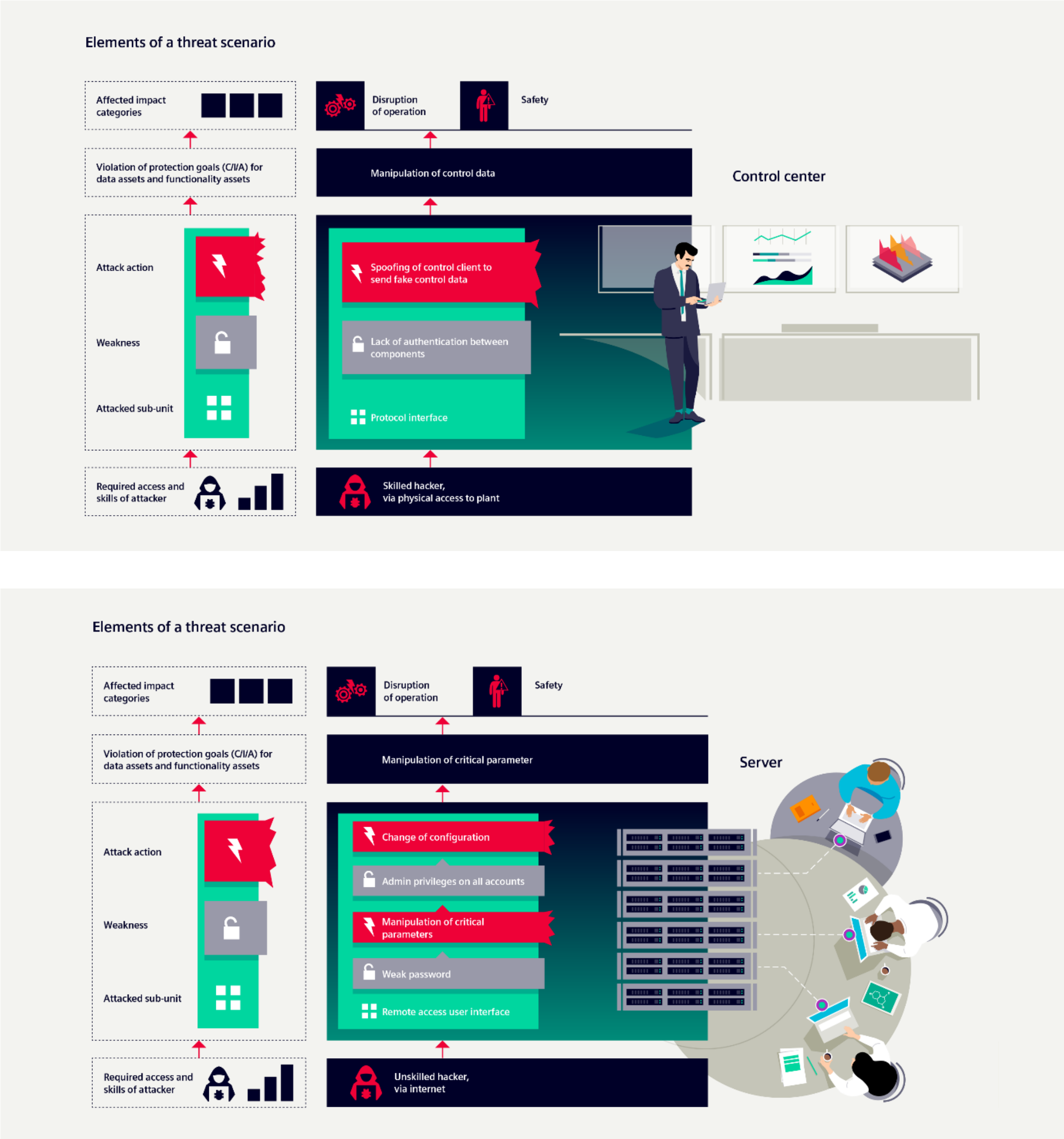

Elements of a threat scenario
Affected impact categories
Disruption of operation
Safety
Violation of protection goals (C/I/A) for data assets and functionality assets
Manipulation of control data
Control center
Attack action
Spoofing of control client to send fake control data
Weakness
Lack of authentication between components
Attacked sub-unit
Protocol interface
Required access and skills of attacker
Skilled hacker, via physical access to plant
Elements of a threat scenario
Affected impact categories
Disruption of operation
Safety
Violation of protection goals (C/I/A) for data assets and functionality assets
Manipulation of critical parameter
Server
Attack action
Change of configuration
Admin privileges on all accounts
Weakness
Manipulation of critical parameters
Weak password
Attacked sub-unit
Remote access user interface
Required access and skills of attacker
Unskilled hacker, via internet

Figure 3: Threat scenario terminology and examples

Figure 3 provides two exemplary threat scenarios: In the first, a skilled hacker with physical access to the plant sends fake data to a control center by spoofing the client (attack action). This is possible because the control center does not sufficiently authenticate the client (weakness). This means that the control center receives manipulated control data, and hence the protection goal ‘Integrity of control data’ is violated. As a result, the control center will trigger some control actions that could disrupt the operation or even harm people working in the plant (impact category 'Safety').

In the second exemplary threat scenario, an unskilled hacker obtains access to the server via the Internet by guessing a password (attack action) to access the server. The first weakness of the system is a weak authentication mechanism, more precisely weak password quality enforcement and missing time delay functionality after the several unsuccessful log-on attempt. The second weakness of this threat scenario is the disregard of the "least privilege principle", as all user accounts within the system have admin privileges.
After performing the attack actions, the attacker can violate the protection goal 'Integrity of critical system parameters'. The manipulation leads to malfunction or complete outage of the system, an impact of the category is 'Disruption of operation'. As further impact, the attack could gain media attention, resulting in impact in the category "Loss of reputation".

The terminology presented in this section has been derived from [1], [2], [7] and [6]. As these standards use different terms, the terminology presented in this section has been established for common use within Siemens. Appendix B contains further explanations on the terminology.

1.5 References

[1] ISO/IEC 27005:2018 "Information technology – Security techniques – Information security risk management".

[2] ISO/IEC 27000:2018 "Information technology — Security techniques — Information security management systems — Overview and vocabulary".

[3] IEC 62443-2-4:2015. "Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers".

[4] IEC 62443-3-2:2020. "Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design".

[5] IEC 62443-4-1:2018. "Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements".

[6] IEC TS 62443-1-1:2009 "Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models".

[7] NIST SP 800-30 Rev. 1 "Guide for Conducting Risk Assessments". 2012.

2 | Method Description

This section defines the steps of the TRA method and describes the necessary preparation activities to conduct a TRA. The method description is independent of actual tooling.

2.1 TRA Method Overview

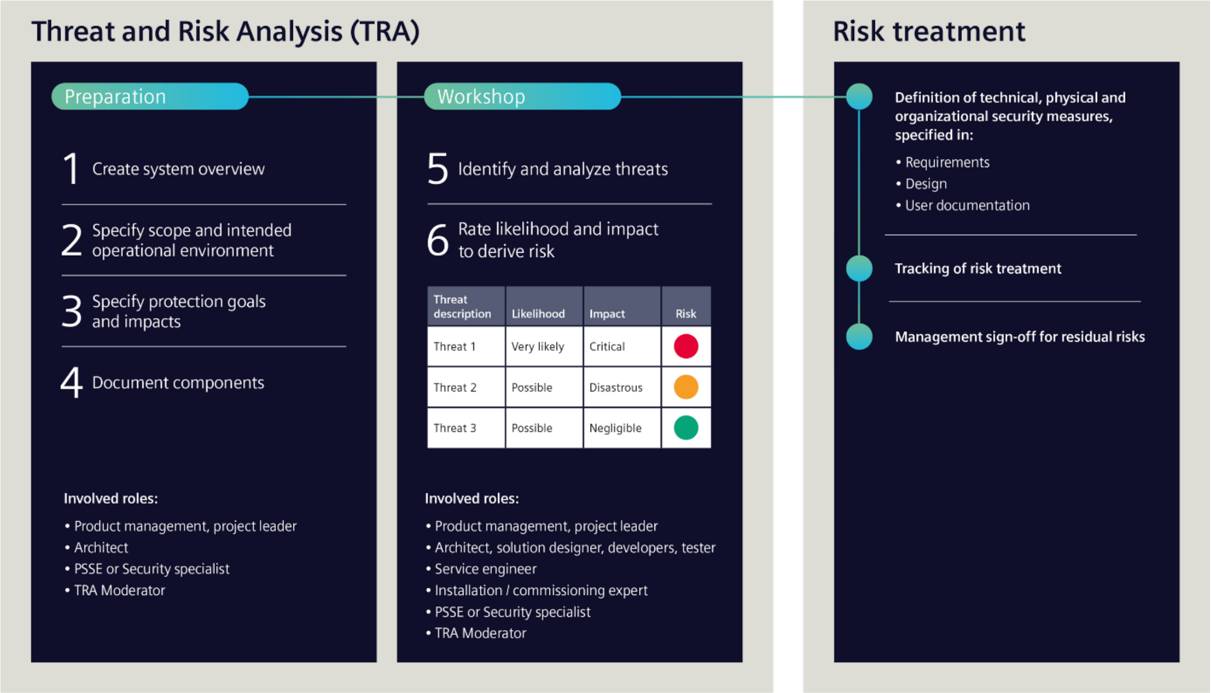
In Figure 4, the steps of the TRA method are shown. The first four steps are done in the preparation phase, whereas the steps 5 and 6 are performed in a workshop. Subsequent steps in PSS risk management are also shown in the figure. The preparation phase is explained in section 0 and the TRA workshop is detailed in section 2.3.

The TRA can only provide meaningful results if the required roles are involved (see Figure 4). There are two roles that require TRA-specific expertise:

- TRA moderator
  leads through the steps of the TRA methodology.
- Security specialist
  knows typical attacks and security weaknesses and supports to identify whether these apply for the target of analysis.

Besides the TRA-specific roles, the key roles for the target of the analysis need to take part in the TRA. Both the business role (the owner such as product manager or project leader) and the person responsible for the architecture and design are required.

Details on the responsibilities and expected experience of the different roles are listed in section 2.4.



Threat and Risk Analysis (TRA)

Preparation

1 Create system overview

2 Specify scope and intended operational environment

3 Specify protection goals and impacts

4 Document components

Involved roles:

- Product management, project leader
- Architect
- PSSE or Security specialist
- TRA Moderator

Workshop

5 Identify and analyze threats

6 Rate likelihood and impact to derive risk

Threat description	Likelihood	Impact	Risk
Threat 1	Very likely	Critical	🔴
Threat 2	Possible	Disastrous	🟠
Threat 3	Possible	Negligible	🟢

Involved roles:

- Product management, project leader
- Architect, solution designer, developers, tester
- Service engineer
- Installation / commissioning expert
- PSSE or Security specialist
- TRA Moderator

Risk treatment

Definition of technical, physical and organizational security measures, specified in:

- Requirements
- Design
- User documentation

Tracking of risk treatment

Management sign-off for residual risks

Figure 4: Overview of the TRA method steps

The output of all steps of the TRA shall be properly documented with adequate TRA tooling.

The results of the TRA are input to security risk treatment, where mitigations for the identified risks are defined. In the case mitigation is done by technical security measures, these are specified, implemented and documented in the development or engineering project. Physical and operational security measures need to be included in the documentation that is handed over to the customer.

The PSS risk management process of the organizational unit ensures that an appropriate management level decides on acceptance of residual risks. It also defines how security risk treatment tracking and tracing are integrated into the established processes of the organization.

2.2 Preparing the Threat and Risk Analysis

A proper preparation of a TRA workshop is essential to increase the quality and efficiency of the workshop. Insufficient preparation can lead to avoidable discussions and uncertainties during the workshop about the analyzed system and the related system overview.

2.2.1 Step 1: Creating System Overview

2.2.1.1 Goals

The first step of the preparation of a TRA is to create a system overview. A system overview is the graphical representation of the target of analysis in its technical environment. As explained in section 1.3, the technical environment of a component is a system, so a system overview is required for all target areas. The system overview shall be on a consistent level of detail in order to ensure during the TRA workshop:

- Creating a common understanding of the target of analysis, especially regarding scope, boundaries, functionality, and data.
- Ensuring that the workshop participants use the same terminology for all parts of the system.
- Providing a basis for the identification and analysis of threats.
- Identifying existing controls that are taken into account during the security risk rating.

Care shall be taken to ensure that the system overview that is used for the TRA is consistent with the existing system or design specifications of the project. In case of changes to the system, an update to the TRA is necessary.

2.2.1.2 Approach

System overview for target area “Development of component”

A proven way to create system overviews for software applications and embedded devices is the use of data flow diagrams. A system overview shall contain the following elements

- SW-services with their interfaces, e.g. APIs or user interfaces.
  [In a data flow diagram, these are displayed as circle.]
- Data stores, e.g., file shares, database and shared memory, with their interfaces.
  [In a data flow diagram, these are displayed with two parallel lines.]

- Data flows between the interfaces of services and data stores as well as external systems. Examples are API calls, data base queries, and HTTP communication with Web applications. The protocol used in the data flow should be annotated.

  [In a data flow diagram, data flows are displayed as arrows. The arrows can indicate which part initiates the communication (client-server relationship) or direction of data flow. The latter is important for understanding how data move through the system, while for identifying threats, it is important to know which is the server, as this is 'listening' to requests, and is hence exposed to attacks.]
- Physical interfaces of a device or host, e.g., USB ports, ports for memory cards, and debug ports. This includes circuit board connections like JTAG.
  [Not shown in a classical data flow. The data flow diagram should be extended with boxes to show physical devices. The physical devices should be drawn on the boundary of the boxes.]
- External systems that are connected through data flows.

  [In a data flow diagram, external systems can be displayed as rectangle.]
- Actors e.g., user, administrator, customer, service engineer, who access via the user interfaces.

  [In a data flow diagram, these can be displayed by matchstick figures.]
- Security zones of the technical environment and trust boundaries between the zones.

  [In a data flow diagram, trust diagrams are displayed with dotted lines.]

System overview for target area "Design and Deployment of a System"

Systems in their technical environment are typically represented in terms of network topology diagrams. In addition, the data flows have to be documented and the system overview shall contain the following aspects:

- Components, including:
  - Hosts with software applications (both 3rd party and Siemens applications) and data stores.
  - Embedded devices
  - Third party components like storage devices or tablets.
- Remote access components, service tools and interfaces.
- Data flows between the components, resp. the applications and data stores on the components. The interface of a component that handles the data flow should be indicated if space allows. Such interfaces are described further in Step 4, as described in Section 2.2.4
- Network topology in terms of network segments and network devices.
- External (i.e., not included in the target of analysis) components or systems that are connected through data flows.
- Security-relevant components or features, e.g. user management, patch management server, firewalls.
- Actors e.g. operator, administrator, service engineer.

- Security zones and trust boundaries.
  Note that security zones are more abstract than network segments. A security zone might comprise several network segments that serve the same purpose and a have a similar level of security and trust. A network segment could also be split into several security zones with different physical access characteristics, e.g., different rooms.

2.2.2 Step 2: Specifying Scope and Intended Operational Environment

2.2.2.1 Goals

As the system overview shows the target of the analysis in its technical environment, a scope statement is required to clarify the target of the analysis. Furthermore, target of analysis could be split and handled in several TRAs, and this is also part of the scope statements.

The *intended operational environment* is what is outside the target of analysis, i.e., the technical and organizational environment as explained in section 1.3.

The security characteristics of the intended operational environment might influence the security risk levels. Those characteristics that decrease a risk level have to be carefully documented as part of the TRA as *assumptions*.

Assumptions often refer to the existence of security measures and processes. This means that those security measures that are not part of the target of the analysis are documented in this step.

2.2.2.2 Approach

Scope Statements

The scope of the TRA shall be clearly stated, including the following aspects:

- Clarify the target of analysis and provide details about the target of analysis as far as necessary to resolve potential ambiguities. State the responsible group of the organization.
- In case the target of analysis is split and handled in several TRAs: List the parts or layers that are covered in the present TRA. Include references to existing related TRAs, and responsible groups.
  For example, different groups could be responsible for the network design and the configuration of hosts respectively. A software application could be covered by several TRAs for its modules.
- List the third-party parts, and state whether a TRA or security documentation exists for each.

Assumptions on the Intended Operational Environment

The documentation of the intended operational environment shall include measures expected to be provided by the technical or organizational environment, including:

- Network: Technical network security measures (controls) include network separation, protection of network access, and access control for network devices. If the system contains several network segments, the assumptions should be described separately for each network segment.

- Physical and operational: Controls for physical access restrictions, e.g., for sites, rooms or cabinets where the system components are located. Security training of employees, security monitoring etc.
- Hosts: Security measures on the level of operating systems, including hardening, access restrictions, and regular patching. In each area, the existence and quality of operational processes to maintain the security measures (e.g., the user accounts, or the configuration of the firewall) during operations, installation and commissioning, is also part of the intended operational environment.

The assumptions on the intended operational environment are an integral part of the TRA, and any change requires an update of the TRA.

Assumptions shall be referenced during the risk rating. Typically, assumptions decrease the exposure of a threat, and consequently the risk from that threat.[1] Often additional assumptions are identified during the risk rating of threats. For example, the rating of a threat could depend on whether a server is directly accessible from the Internet, which would imply a high exposure. The assumptions that that the server is located behind a firewall would decrease the exposure rating. In such cases, the new assumptions shall be added to the list of assumptions.

The assumptions on the intended operational environment shall be included in the installation and operation manuals and the customer security documentation.

2.2.3 Step 3: Specifying Protection Goals and Impacts

2.2.3.1 Goals

A clear statement of the protection goals for the target of analysis and potential impacts in case the protection goals get violated is essential for an impact rating that reflects the business view.

The TRA method uses the term *protection goal* in the following way: A protection goal falls into one of the three main protection goal categories in security: confidentiality, integrity, and availability. For a definition, see ISO 27000:2018 [2].

A protection goal for the target of analysis states the need to protect the confidentiality, integrity or availability of specific data or functionalities that are handled or provided by the target of analysis. The latter are called data assets and functionality assets. An example of a protection goal for a control system is: Integrity of controller code.

For each protection goal for the target of analysis, the role that has business responsibility for the system shall rate the impact in case the protection goal is violated. As explained in section 1.4, a protection goal is part of a threat scenario. The impact rating for violation of the protection goals is used as impact factor in the risk level. As business provides the impact rating, it is ensured that business, as owner of security risks, understands the risk from a threat scenario.

[1] Please note that more details on the risk rating are provided in section 2.3.2.

2.2.3.2 Approach

Data assets and functionality assets

The first step in formulating protection goals is to identify the data and functionalities of the target of analysis that need protection. These are called *data assets* and *functionality assets*.[2] Data assets and functionality assets shall be identified in the following way:

- Data assets: In this context, data is used in a broad sense, and includes commands, process data, log data, binaries, source code, and configuration. Such data is a data asset if the following is the case:
  When the integrity, confidentiality or availability of the data is violated, i.e., when that data has been disclosed or manipulated, or deleted, there is a harmful impact.
- Functionality assets: The purpose of a system or component can be broken down into the functionalities (or services) it provides. For example, a controller provides input/output functionality, while a Web application provides responses according to its business logic. In a less granular view, a control system provides control of (for example) a chemical process. Such a functionality is a functionality asset if the following holds:
  When the availability, integrity or confidentiality of the functionality is violated i.e., access to the service is impeded for some time, or the functionality has been manipulated and behaves differently from the intended way, or data handled by the functionality is disclosed, there is a harmful impact.

The granularity of data assets and functionality assets can depend on the target area of the TRA: For development of components, the list of data assets could be more detailed than for design of systems.

Impact rating

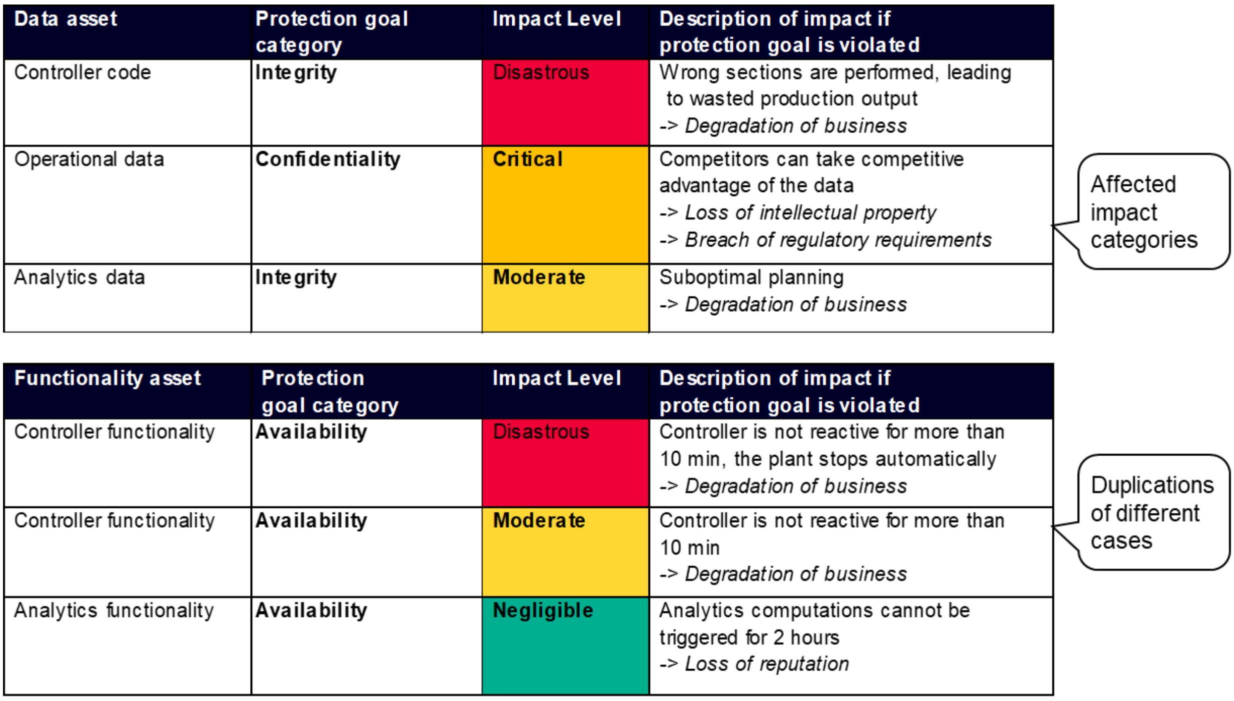
In the next step, for each protection goal the level of impact in case of violation shall be rated. The levels and impact categories for the rating are defined in the impact rating scheme shown in Figure 6, and are explained in the next section.

The level of impact is determined by the business purpose of the system in operation, and by the domain in which it is used. For example, for a system used in critical infrastructure, the manipulation of the controller code can lead to physical damage or even affect safety of people. Hence in that case, integrity of the controller code is a protection goal, and the impact of its violation is rated with the highest level, i.e., *Disastrous*.

The reason for the rating shall be indicated by providing an explanation of the operational or business consequences of a violation of the protection goal and by the affected impact categories. See Figure 5 for examples.

Often the impact can be better rated after differentiation between cases of violation. For example, for availability of a functionality the duration of unavailability matters for the impact rating. See again Figure 5 for examples.

[2] Note: Annex B of [1] proposes to differentiate between primary and secondary assets. Primary assets are data and functionality assets in the sense of this method description. Secondary assets comprise the components, which can include hardware, software, subsystems, or network components.



Data asset	Protection goal category	Impact Level	Description of impact if protection goal is violated
Controller code	**Integrity**	Disastrous	Wrong sections are performed, leading to wasted production output -> *Degradation of business*
Operational data	**Confidentiality**	**Critical**	Competitors can take competitive advantage of the data -> *Loss of intellectual property* -> *Breach of regulatory requirements*
Analytics data	**Integrity**	**Moderate**	Suboptimal planning -> *Degradation of business*

Affected impact categories

Functionality asset	Protection goal category	Impact Level	Description of impact if protection goal is violated
Controller functionality	**Availability**	Disastrous	Controller is not reactive for more than 10 min, the plant stops automatically -> *Degradation of business*
Controller functionality	**Availability**	**Moderate**	Controller is not reactive for more than 10 min -> *Degradation of business*
Analytics functionality	**Availability**	**Negligible**	Analytics computations cannot be triggered for 2 hours -> *Loss of reputation*

Duplications of different cases

Figure 5: Example for impact ratings for the violation of protection goals

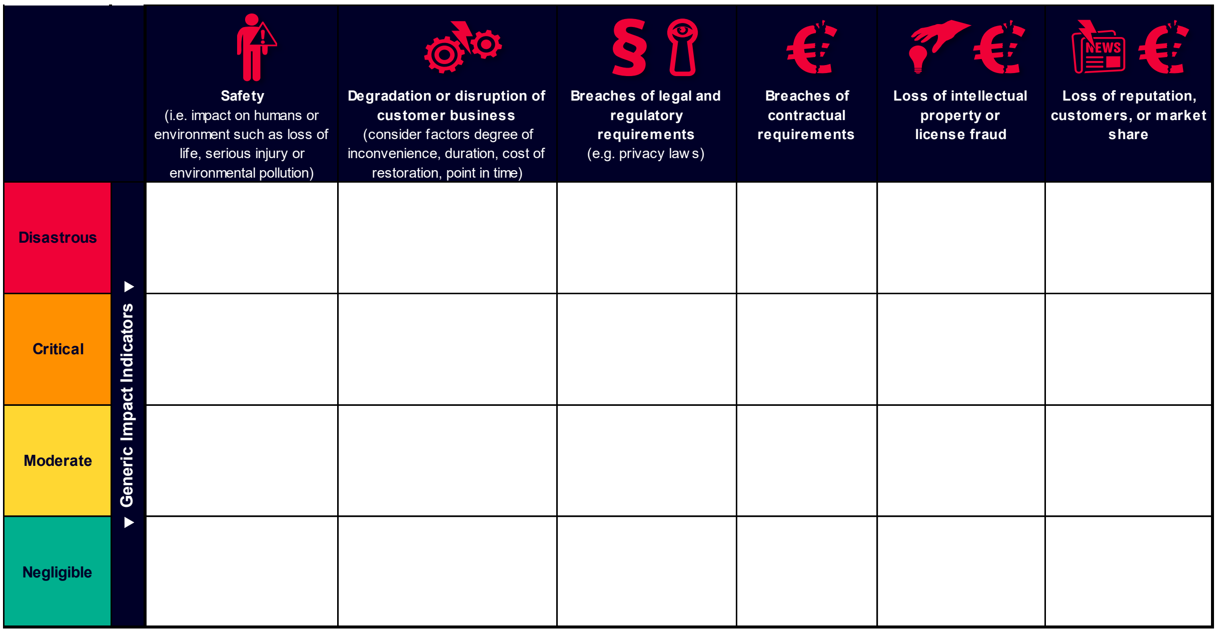
Impact Rating Scheme

Figure 6 shows the impact rating scheme that supports determination of the level of impact. It consists of six impact categories:

- Safety,
- Degradation or disruption of customer business,
- Breach of legal and regulatory requirements,
- Breach of contractual requirements,
- Loss of intellectual property or license fraud, and
- Loss of reputation, customers or market share.

There are four impact levels: *Negligible, Moderate, Critical* and *Disastrous*. The impact rating scheme in Figure 6 is filled with indicators that help to choose the matching impact level by an organizational unit. For example, relevant privacy laws and related fines could be listed in the category ‘Breaches of legal and regulatory requirements.

For determining the impact rating of a threat, the highest applicable rating in any of the impact categories has to be chosen.



		Safety (i.e. impact on humans or environment such as loss of life, serious injury or environmental pollution)	**Degradation or disruption of customer business** (consider factors degree of inconvenience, duration, cost of restoration, point in time)	**Breaches of legal and regulatory requirements** (e.g. privacy laws)	**Breaches of contractual requirements**	**Loss of intellectual property or license fraud**	**Loss of reputation, customers, or market share**
Disastrous	Generic Impact Indicators						
Critical							
Moderate							
Negligible							

Figure 6: Impact rating scheme

2.2.4 Step 4: Document Sub-Units

2.2.4.1 Goals

In this step, the system overview is augmented with a description of sub-units. The goal is to document aspects of a sub-unit that are relevant for the identification and analysis of threat scenarios.

In this context, sub-units are the elements displayed in the system overview, as listed in Section 0. So, the notion of sub-unit depends on the target area. For the target area 'Development of a Component', the sub-units include SW-services, data stores and interfaces, while in the target area 'Design and Deployment of a System', the sub-units are the components, typically structured into different zones and sub-systems.

The following questions indicate typical security-relevant aspects of a sub-unit.

- How does the sub-unit store, process or provide data assets or functionality assets? Documenting the relation of the assets to the sub-unit helps to understand how attacks on the sub-unit can lead to the violation of protection goals for these assets.
- How does the sub-unit interact with other sub-units to provide the overall system functionality? This can be relevant in order to understand how an attack against the sub-unit could affect the overall functionality.
- Does the sub-unit have security weaknesses? This helps to identify threats later on.

2.2.4.2 Approach

Topic Areas for Sub-Unit Documentation

All sub-units, as displayed and named in the system overview, shall be listed. For each sub-unit, a description shall be provided, including the following topics:

- Main functionality (which functions are provided by the sub-unit in the overall system context), and corresponding data assets and functionality assets.
- Interfaces of the sub-unit, as these form the attack surface.
  - User interfaces
  - Component-to-component interfaces and the underlying network interfaces and protocols
  - Physical interfaces that are used, e.g., USB or local diagnostic interfaces.
- Third-party status: If the sub-unit is supplied by a third party, references to the security-relevant information available from the supplier is referenced.
- Existing and missing security measures and related weaknesses. For example, authentication at the interfaces with an insecure storage of passwords.[3] Also can include operational aspects like hardening and security patching.
- Network segment and physical location, if not clearly identifiable from the system overview or the description of the intended operational environment.

Impact Rating on the Level of Sub-Units (Optional)

This section describes an optional step, in which violation of confidentiality, integrity and availability is considered and rated per sub-unit.

Impact rating on the level of sub-units is an extension of step 3 described in section 2.2.3, and there are different approaches to do so. In the following, three approaches are discussed.

1) Replacing step 3: Apply step 3 per sub-unit, i.e., iterate per sub-unit, considering the data assets and functionality assets handled by that sub-unit. This approach can be used in the target area "Design and deployment of System" for systems with many components for which it is difficult to identify the relevant data and functionalities in a top-down fashion.
2) Prioritization of sub-units: The results of step 3 are used to determine an impact level for confidentiality, integrity and availability for each sub-unit. This can be used to prioritize sub-units with high impact levels during the identification of threats.
   More precisely, this approach consists of first selecting for each sub-unit the data and functionality assets from step 3 that are handled by this sub-unit. Then the maximum impact level for of the protection goals for these assets is determined, in each of the protection goal categories confidentiality, integrity and availability.
3) Summarize threats per sub-unit:
   In the step 'Identify and analyze threats', the threat scenarios contain the information against which sub-unit the attack action is performed. Hence threat scenarios can be associated with sub-units.
   In this approach, the threat scenario with the highest impact rating that violates a

[3] Note: Annex B of [1] proposes to differentiate between primary and secondary assets. Data that can be used in attacks, e.g. passwords, can be considered to be secondary assets.

protection goal in the category of confidentiality is selected and referenced. Accordingly for integrity and availability.

2.3 TRA Workshop

2.3.1 Step 5: Identifying and Analyzing Threat Scenarios

As explained in section 1.4, a threat scenario consists of an attack action, performed by an attacker, that exploits a weakness such that a protection goal of the system gets violated. In this method step, threat scenarios for the system shall be identified and analysed, based on the information gathered in the preparation phase described in section 0.

There are three main approaches for the systematic identification and analysis of threat scenarios. These approaches complement each other:

1) **Analyze all interfaces of the sub-units for possible attack actions at that interface.** E.g., a network user interface could be subject to malicious input like XSS or SQL injection. Brute-forcing or guessing passwords would be other relevant attack actions. The operating system could also be an entry path, e.g., through malware that is executed by a negligent user. Typically, an attack action is possible due to a security weakness.

   The next step is to analyze which protection goals might get violated. This is not necessarily straightforward, i.e., some more steps, involving different sub-units, could be necessary to violate the protection goal. All steps of the attack from the entry point to the violation of the protection goal have to be documented.
   If there is no matching protection goal, but the attack action can cause harm, a corresponding new protection goal has to be added.

2) **Consider possible security weaknesses.**
   The sub-unit descriptions might contain indications about security weakness. For such a security weakness, the attack actions that could exploit the weakness are analyzed. Given an attack action and weakness, full threat scenarios are obtained and documented as in step 1).

3) **Analyze for all protection goals with impact level *Disastrous* or *Critical* how these could get violated in an attack.**
   In this approach, the outcome of the threat scenario is the starting point, and it is analyzed with which attack actions the protection goal could get violated. This approach complements the first two approaches and helps to check whether relevant attack actions have been overlooked.

The three approaches shall be applied in a 'round robin' way, to prioritize the identification of threat scenarios based on their risk level.

The systematic identification of threat scenarios can be supported by taxonomies or catalogs.

- Taxonomies of attack actions or threats, see STRIDE[4] or an approach described by Siemens[5], help to cover the different types of attack.

[4] Adam Shostack. "Threat modeling – Designing for security". Wiley Publishing, 2014.

[5] Maidl, Münz, Seltzsam, Wagner, Wirtz and Heisel: „Model-Based Threat Modeling for Cyber-Physical Systems: A Computer-Aided Approach", https://link.springer.com/chapter/10.1007/978-3-030-

- Catalogs that list common attack actions in detail can be used as knowledge repositories, see e.g., ATT@CK by Mitre[6], the TOP 10 Threats and Countermeasures by BSI[7], or CAPEC[8].
- Lists of typical security weaknesses are available, e.g., the OWASP Top Ten[9] or ISO 27005 Annex D.1 in [1] . A gap analysis with respect to security requirements lists like IEC 62443-3-3 or the SANS CIS Controls[10] is proven way to detect security weaknesses.

It is important to document all threat scenarios that are discussed, even if their risk level is rated low. In that way it can later be demonstrated that the threat from a particular attack action or weakness has been considered.

2.3.2 Step 6: Rating Likelihood and Impact to Derive Risk

For each threat scenario the risk level shall be evaluated by rating the likelihood and the impact.

2.3.2.1 Rating the Likelihood of a Threat Scenario

The likelihood rating is determined by two factors *exposure* and *exploitability (simplicity)*.

- ***Exposure***

  The *exposure* rating relates to the likelihood that an attack is attempted, which depends on how difficult it is for an attacker to obtain the level of access needed for the attack. For example, an attack that is possible over the Internet gets a high exposure rating. For some environments, physical access could also be easy.

  On the other hand, if the attacker risks to get caught, e.g. due to extensive logging or physical surveillance measures, the likelihood of attack attempt decreases. See Figure 7 for the rating scheme with the two categories *'Level of Access Needed'* and '*Risk of Getting Caught'*. For determining the exposure rating, the two categories have to be weighed against each other. For example, for an attacker who has regular access during operation or maintenance, it is easy to get the level of access needed for the attack. On the other hand, if all events are logged and can be traced back to users, the risk of getting caught is high, and on balance the exposure is rated to be medium. The rating of both two categories typically depends on the intended operational environment. For example, an attack that requires access to a network segment, the exposure rating depends on how secure that network is. If the exposure is rated medium or low, it has to be checked whether the rating is based on an assumption that has not yet been stated. In that case, the assumption has to be added to the list of assumptions.

83007-6_8, 2021

[6] https://attack.mitre.org/

[7] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.html;jsessionid=1CBA3DF2F6EB642DBD6A31A02CBD6924.internet081?nn=448734#download=1

[8] https://capec.mitre.org/data/definitions/1000.html

[9] https://owasp.org/www-project-top-ten/

[10] https://www.sans.org/blog/cis-controls-v8/

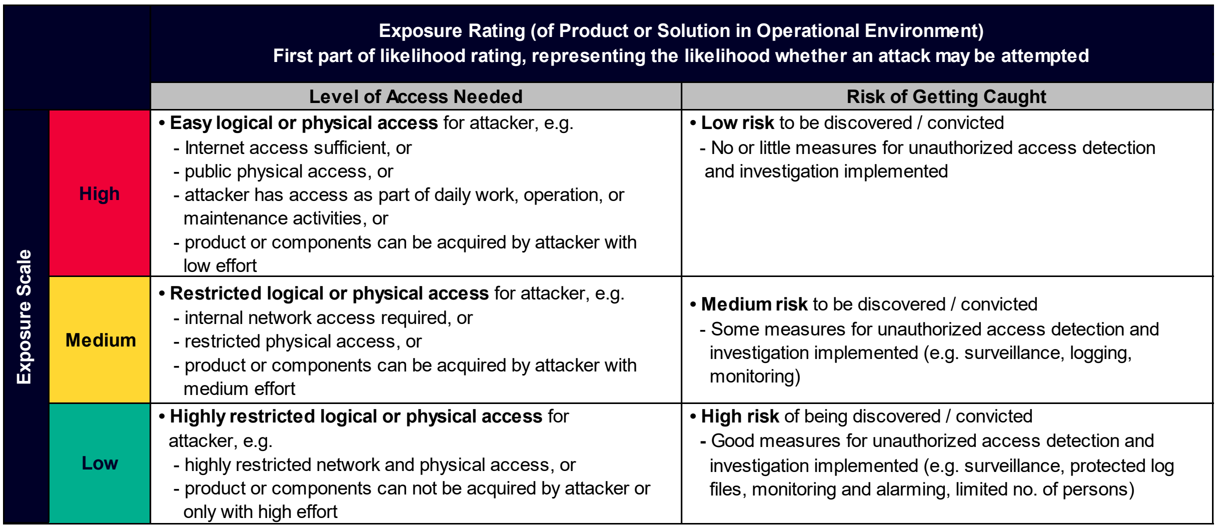
The rating of exposure requires an understanding of the level of access required for an attack action.

- ***Exploitability (simplicity)***

  The *exploitability* rating relates to the likelihood that an attempted attack succeeds, which depends on the simplicity of the attack, or how easily a security weakness can be exploited. Thus, indicators are for example the level of security know-how required for the attack, the strength of countermeasures and the effort required to perform the attack. See Figure 8 for the rating scheme.

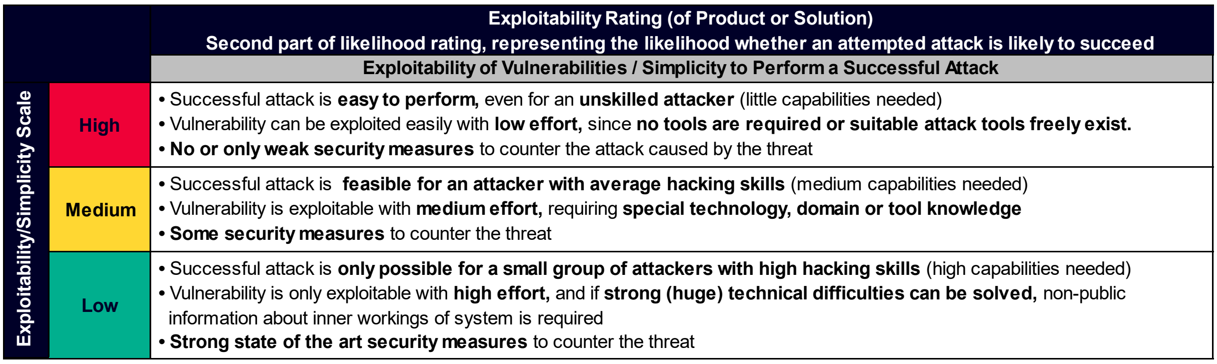
  The exploitability rating typically depends on the quality and strength of the security measures of the system. Strong security measures, such as 2-factor authentication, lower the exploitability rating.

  The rating of exploitability requires an understanding of common attack actions, available hacking tools, and how difficult it is to overcome certain security measures.



		Exposure Rating (of Product or Solution in Operational Environment) **First part of likelihood rating, representing the likelihood whether an attack may be attempted**	
		Level of Access Needed	**Risk of Getting Caught**
Exposure Scale	**High**	• **Easy logical or physical access** for attacker, e.g. - Internet access sufficient, or - public physical access, or - attacker has access as part of daily work, operation, or maintenance activities, or - product or components can be acquired by attacker with low effort	• **Low risk** to be discovered / convicted - No or little measures for unauthorized access detection and investigation implemented
	Medium	• **Restricted logical or physical access** for attacker, e.g. - internal network access required, or - restricted physical access, or - product or components can be acquired by attacker with medium effort	• **Medium risk** to be discovered / convicted - Some measures for unauthorized access detection and investigation implemented (e.g. surveillance, logging, monitoring)
	Low	• **Highly restricted logical or physical access** for attacker, e.g. - highly restricted network and physical access, or - product or components can not be acquired by attacker or only with high effort	• **High risk** of being discovered / convicted - Good measures for unauthorized access detection and investigation implemented (e.g. surveillance, protected log files, monitoring and alarming, limited no. of persons)

Figure 7: Exposure Rating Scheme



		Exploitability Rating (of Product or Solution) **Second part of likelihood rating, representing the likelihood whether an attempted attack is likely to succeed**
		Exploitability of Vulnerabilities / Simplicity to Perform a Successful Attack
Exploitability/Simplicity Scale	**High**	• Successful attack is **easy to perform,** even for an **unskilled attacker** (little capabilities needed) • Vulnerability can be exploited easily with **low effort,** since **no tools are required or suitable attack tools freely exist.** • **No or only weak security measures** to counter the attack caused by the threat
	Medium	• Successful attack is **feasible for an attacker with average hacking skills** (medium capabilities needed) • Vulnerability is exploitable with **medium effort,** requiring **special technology, domain or tool knowledge** • **Some security measures** to counter the threat
	Low	• Successful attack is **only possible for a small group of attackers with high hacking skills** (high capabilities needed) • Vulnerability is only exploitable with **high effort,** and if **strong (huge) technical difficulties can be solved,** non-public information about inner workings of system is required • **Strong state of the art security measures** to counter the threat

Figure 8: Exploitability/Simplicity Rating Scheme

The likelihood rating per threat scenario is derived from the exposure rating and exploitability rating through the mapping table given in Figure 9. The likelihood rating consists of the five values *Very unlikely*, *Unlikely*, *Possible*, *Likely*, *Very likely*.

		Exposure Rating		
		High	Medium	Low
Exploitability/Simplicity Rating	High	Very likely	Likely	Possible
	Medium	Likely	Possible	Unlikely
	Low	Possible	Unlikely	Very unlikely

Figure 9: Likelihood Mapping Table

2.3.2.2 Rating the Impact of a Threat Scenario

The threat scenario contains the violation of a protection goal. The impact from the violation of protection goal is rated in 'Step 3: Specify protection goals and impacts'. The impact level of the violation of the protection goal is used as the impact level of the threat scenario.

The description of the threat scenario has to be sufficiently detailed to understand how the attack causes the violation of the protection goal.

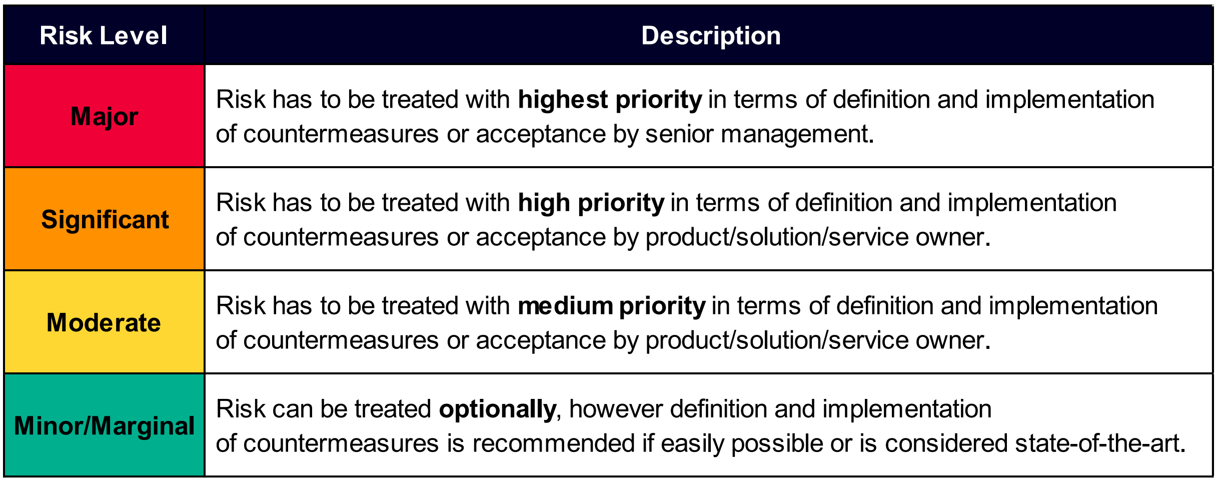
If some participants in the workshop find that the impact level assigned to the violation of the protection goal does not match their expectation of impact level for the threat scenario, the reason should be analysed. Typically, the violation of the protection goal has to be split into several cases with different impact ratings. For example, it might be necessary to differentiate between the targeted manipulation of data and the 'blind' manipulation of the same data, as the former usually causes higher impact than the latter. In that case, the protection goals and impacts have to be updated accordingly.

In some cases, the same attack action could violate several protection goals, the protection goal with the maximum impact has to be selected. For later re-assessments, it is useful to document all violated protection goals.

2.3.2.3 Deriving the Risk Level for a Threat Scenario

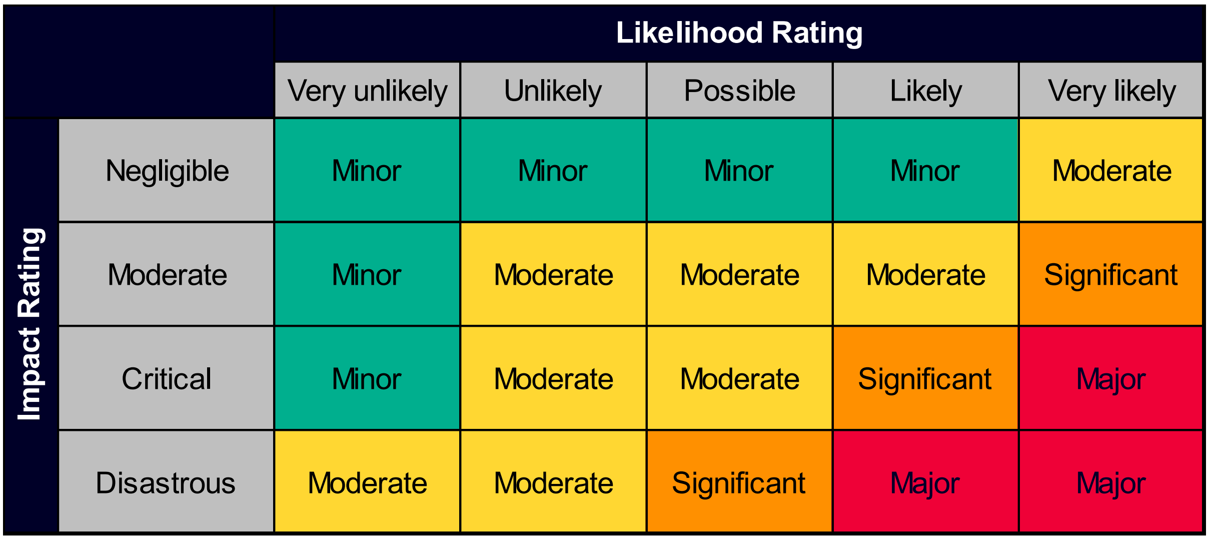
The TRA method uses four security risk levels: *Minor/Marginal, Moderate, Significant and Major.* They are symbolized by the colours green, yellow, orange, or red, as shown in the risk level description in Figure 10. The security risk level can be used to prioritize the risk treatment. The descriptions are generic and can be adapted according to the specific security risk acceptance criteria and associated management responsibilities of an organizational unit.

The security risk level of a threat scenario is determined from the likelihood and the impact ratings by a mapping in the form of a 4x5 matrix, shown in Figure 11. For example, a threat scenario with the likelihood rating *'Possible'* and impact rating of *'Critical'* would result in a risk level *'Moderate'*. The risk rating mapping matrix can be adapted according to the PSS risk management strategy of the organizational unit.



Risk Level	Description
Major	Risk has to be treated with **highest priority** in terms of definition and implementation of countermeasures or acceptance by senior management.
Significant	Risk has to be treated with **high priority** in terms of definition and implementation of countermeasures or acceptance by product/solution/service owner.
Moderate	Risk has to be treated with **medium priority** in terms of definition and implementation of countermeasures or acceptance by product/solution/service owner.
Minor/Marginal	Risk can be treated **optionally**, however definition and implementation of countermeasures is recommended if easily possible or is considered state-of-the-art.

Figure 10: Risk Level Description



		Likelihood Rating				
		Very unlikely	Unlikely	Possible	Likely	Very likely
Impact Rating	Negligible	Minor	Minor	Minor	Minor	Moderate
	Moderate	Minor	Moderate	Moderate	Moderate	Significant
	Critical	Minor	Moderate	Moderate	Significant	Major
	Disastrous	Moderate	Moderate	Significant	Major	Major

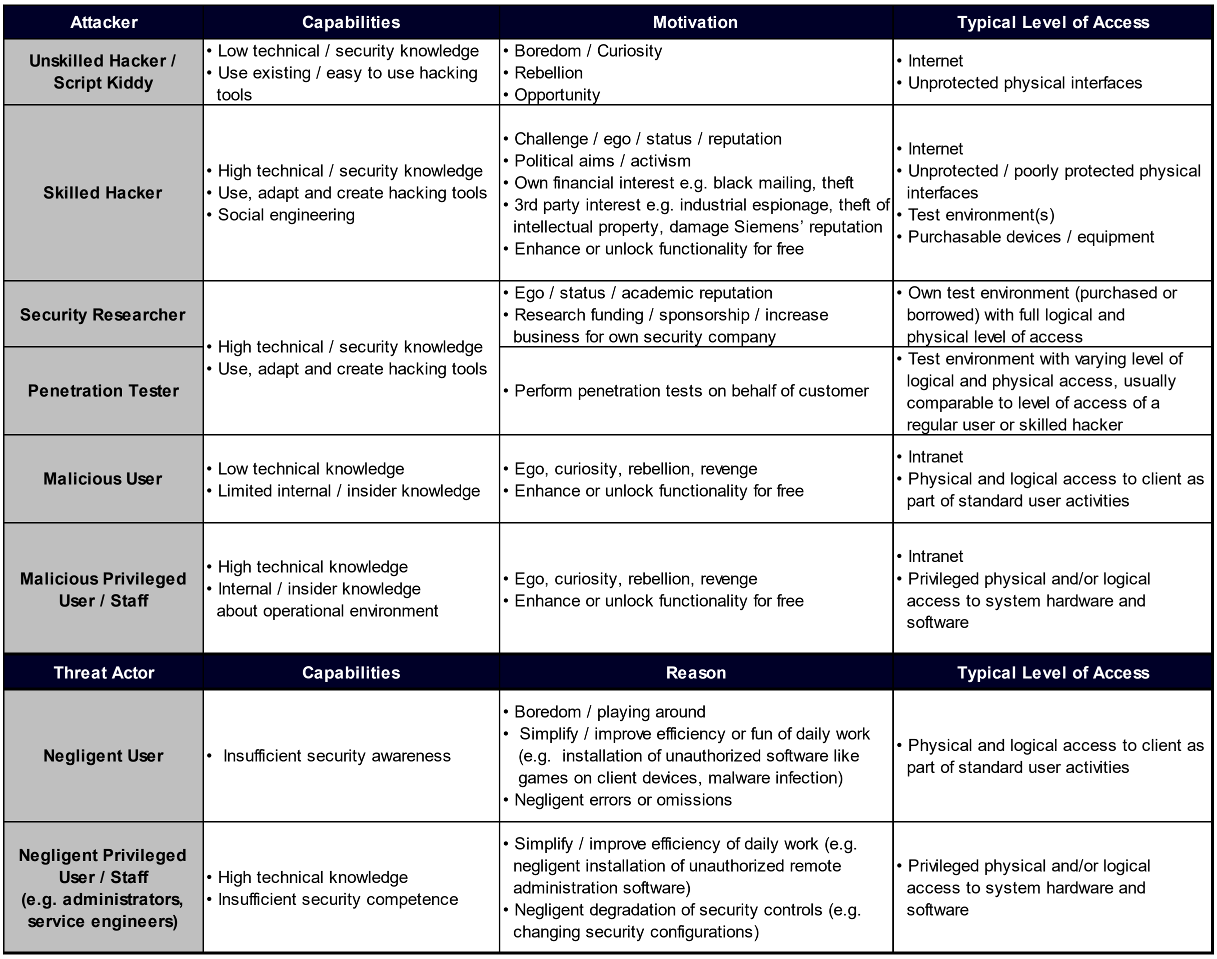
Figure 11: Risk Rating Mapping Table

After security risk treatment has been decided, and countermeasures in the form of requirements, design change requests or changes to the customer documentation have been specified the same rating approach can be used to re-rate a threat under consideration of the defined countermeasures. Typically, technical countermeasures reduce the exploitability. Additional assumptions on the intended operational environment could lower the exposure. In most cases, the impact rating will remain unchanged as this considers the impact given that an attack was successful, independent of the likelihood of being successful.

2.3.2.4 Attacker Types (Optional)

An attacker type is not a mandatory part of the description of a threat scenario but can be useful in some cases to improve the description of a threat scenario.

The TRA method provides a list of six attacker types and two threat actor types. Each type is characterized by capabilities, motivation, and the typical level of access to the system (see Figure 12). While attackers attack a system intentionally threat actors do not have malicious intents but could enable attacks through negligent behaviour.



Attacker	Capabilities	Motivation	Typical Level of Access
Unskilled Hacker / Script Kiddy	• Low technical / security knowledge • Use existing / easy to use hacking tools	• Boredom / Curiosity • Rebellion • Opportunity	• Internet • Unprotected physical interfaces
Skilled Hacker	• High technical / security knowledge • Use, adapt and create hacking tools • Social engineering	• Challenge / ego / status / reputation • Political aims / activism • Own financial interest e.g. black mailing, theft • 3rd party interest e.g. industrial espionage, theft of intellectual property, damage Siemens' reputation • Enhance or unlock functionality for free	• Internet • Unprotected / poorly protected physical interfaces • Test environment(s) • Purchasable devices / equipment
Security Researcher	• High technical / security knowledge • Use, adapt and create hacking tools	• Ego / status / academic reputation • Research funding / sponsorship / increase business for own security company	• Own test environment (purchased or borrowed) with full logical and physical level of access
Penetration Tester		• Perform penetration tests on behalf of customer	• Test environment with varying level of logical and physical access, usually comparable to level of access of a regular user or skilled hacker
Malicious User	• Low technical knowledge • Limited internal / insider knowledge	• Ego, curiosity, rebellion, revenge • Enhance or unlock functionality for free	• Intranet • Physical and logical access to client as part of standard user activities
Malicious Privileged User / Staff	• High technical knowledge • Internal / insider knowledge about operational environment	• Ego, curiosity, rebellion, revenge • Enhance or unlock functionality for free	• Intranet • Privileged physical and/or logical access to system hardware and software
Threat Actor	**Capabilities**	**Reason**	**Typical Level of Access**
Negligent User	• Insufficient security awareness	• Boredom / playing around • Simplify / improve efficiency or fun of daily work (e.g. installation of unauthorized software like games on client devices, malware infection) • Negligent errors or omissions	• Physical and logical access to client as part of standard user activities
Negligent Privileged User / Staff (e.g. administrators, service engineers)	• High technical knowledge • Insufficient security competence	• Simplify / improve efficiency of daily work (e.g. negligent installation of unauthorized remote administration software) • Negligent degradation of security controls (e.g. changing security configurations)	• Privileged physical and/or logical access to system hardware and software

Figure 12: Attacker types

The attacker types are implicitly used in the likelihood rating in the following way: The capability level, and the willingness to spend a lot of effort and resources are reflected by the exploitability rating of a threat. The level of access needed for the attack is reflected in the exposure rating. Hence adding an attacker type to a threat scenario is redundant in most cases. But in some cases, it makes sense split a threat scenario into two versions for different attacker types, because that makes the attack actions more specific. For example, an unskilled hacker performs 'blind' manipulation that is easy to do, while a skilled hacker uses advanced tools and effort for targeted manipulation.

The motivation of an attacker is not used in the likelihood rating, as motivation is volatile and difficult to assess. In addition, in some cases there is an overlap with impact.

At the same time, it is useful that the participants in a TRA are aware of the different kind of attackers that are to be expected in the different zones of the system. For example, attackers of the type Privileged User / Staff have access to internal, trusted zones. Explicitly thinking of such attacker types helps to identify corresponding threat scenarios.

2.4 Required Roles and Responsibilities per TRA Step

It is important to ensure that persons with sufficient expertise participate in a TRA in addition to the fixed role of TRA moderator and security specialist. This section describes the typical roles, required expertise and responsibilities that are necessary for each TRA step.

2.4.1 Roles

Roles have different names in different contexts, so here only typical names can be provided, and a transfer to the roles in an actual project needs to perform.

From the TRA perspective, roles fall onto different categories, which are described in the next subsections.

2.4.1.1 Technical roles

PLM process	**PM process**
Architect	Technical lead engineer
Key developer	Commissioning engineer
Tester	Service engineer
	Process specialist (employed by asset owner or intermediates)

2.4.1.2 Business roles

PLM process	**PM process**
Product owner	Project leader
Product manager	Service engineer
Project manager	Customer, asset owner

2.4.1.3 Domain expert roles

Legal expert
Safety expert

2.4.2 Required Roles and Responsibilities during the Preparation

Method Step	**Leading roles**	**Expertise and responsibility**
Step 1) **Create system overview**	Leading technical role	Has the technical knowledge about the system to create the system overview

	TRA moderator	Has TRA expertise to ensure the system overview contains the necessary information as required for the preparation and the workshop
Step 2) Specify scope and intended operational environment	Business roles Leading technical role	Specify scope of the TRA Provide an understanding of the intended operation environment at asset owner's site(s)
	TRA moderator	Has TRA expertise to ensure that the scope and the assumptions on the operational environment are sufficiently documented.
Step 3) Specify protection goals and impacts	Business roles	Has a good understanding of business purpose and the domain of the target of analysis and uses that for specifying protection goals and rating impacts. Decides on budget and decides on security risk acceptance according to the PSS risk management process. Lists the key data and functionalities of the target of analysis.
	Domain expert roles	Support the understanding and the rating of impacts.
	Leading technical roles	Lists the key data and functionalities of the target of analysis.
	TRA moderator	Has TRA expertise to ensure that protection goals and violations are stated, and the impact rating is consistent.
Step 4) Document sub-units	Leading technical roles	Has the technical knowledge about the target of analysis to provide the security-relevant details about the sub-units.
	TRA moderator	Uses the TRA moderation expertise to ensure that relevant aspects of the sub-units are documented.
	Security expert	Asks about potential security weaknesses in sub-units.

Table 1: Roles and responsibilities for preparation

2.4.3 Required Roles and Responsibilities in the TRA Workshop

Method Step	**Roles**	**Expertise and responsibility**
Step 5) Identify and analyze threats	All technical roles	Know possible entry points and possible security weaknesses and identify threat scenarios accordingly. Analyze whether and how protection goals can get violated through attacks.
	Security specialist	Knows typical attacks and security weaknesses and asks questions to find out whether these apply to the target of analysis.
	TRA moderator	Supports with the TRA moderation expertise to make sure that threat scenarios are completely specified and documented.
Step 6) Rate likelihood and impact to derive risk	All technical roles	Know technical details about the target of analysis and the intended operational environment and have good understanding of the organizational aspects of the intended operational environment, to support the exposure and exploitability rating.
	Security specialist	Has profound security know-how and knowledge about attackers and available tools to rate the exploitability of threat scenarios. Supports the exploitability rating.
	TRA moderator	Uses TRA moderation expertise to ensure that the reasoning for ratings is documented and that the rating schemes are applied consistently.

Table 2: Roles and responsibilities during workshop

Appendix A: Conformance Mapping with Standards

2.5 ISO/IEC 27005

The following table provides a conformance mapping of the methodology described in this document with the ISO/IEC 27005:2018 security risk management activities. As stated in the introduction, the scope of this document does not include security risk treatment and acceptance, and hence some requirements of the standard are out of scope for this document. However, the additional notes indicate how such requirements are addressed at Siemens Companies.

ISO/IEC 27005 activity	Section in this document	Additional notes
7 Context establishment		
7.1 General considerations	Out of scope of this document	
7.2 Basic criteria		
7.2.1 Risk management approach	Out of scope of this document	
7.2.2 Risk evaluation criteria	Section 2.2.3 provides risk evaluation criteria in the form of impact categories for the violation of protection goals.	
7.2.3 Impact criteria	Section 0 provides impact criteria in the form of a default impact scheme.	
7.2.4 Risk acceptance criteria	Section 0 defines a scale for risk levels and provides default risk acceptance criteria.	
7.3 Scope and boundaries	Section 2.2 provides guidance how to specify the scope of specific TRAs in terms of system overview and intended operation environment.	
7.4 Organization for information security risk management	Section 2.4 lists roles and responsibilities for TRA.	
8. Information security risk assessment		
8.1 General description of information security risk assessment	Section 2.3.1 and 2.3.2 describe how to identify, analyze, and rate risks.	
8.2 Risk identification		
8.2.1 Introduction to risk identification		

8.2.2 Identification of assets	Section 2.2.3 describes how to identify critical data and functionality assets, and state protection goals for these assets	
8.2.3 Identification of threats	Section 2.3.1 describes how to systematically identify threats for the defined TRA scope in its intended operational environment. Threat catalogs or security weakness catalogs that could be used are listed. Section 2.3.2.4 provides attacker types and describes how to use them for threat identification.	
8.2.4 Identification of existing controls	Existing controls of the system are described as part of the system overview (Section 2.2.1) or in the sub-unit description (Section 2.2.4) Special aspects of controls that are relevant for the exploitability rating are described in the comment of the rating (Section 0). Controls that are assumed in the intended operational environment are captured by assumptions (Section 2.2.2). A TRA tool is used to document new controls.	Existing controls are documented as part of the system overview, the sub-unit description or as assumptions.
8.2.5 Identification of vulnerabilities	Section 2.3.1 describes the identification of security weaknesses part of the identification and analysis of threat scenarios.	
8.2.6 Identification of consequence	Section 2.2.3 describes how to identify impacts for violation of protection goals.	
8.3 Risk analysis		
8.3.1 Risk analysis methodologies	This document defines the methodology (qualitative)	
8.3.2 Assessment of consequences	Section 2.2.3 describes how to rate impacts for violation of protection goals. Section 0 states that impact levels for violation of protection goals are used to rate impact of threat scenarios. Section 0 describes how to summarize impacts per sub-unit.	
8.3.3 Assessment of incident likelihood	Section 0 describes how to rate the likelihood of a threat scenario with a provided likelihood rating scheme.	
8.3.4 Level of risk determination	Section 0 describes the risk levels and contains the risk matrix to derive the level of risk of a threat scenario.	

8.4 Risk evaluation	The prioritized risk list that is the output of a TRA, as described in Section 0., is the basis for risk evaluation.	
9 Information security risk treatment		
9.1 General description of risk treatment	Out of scope	
9.2 Risk modification	A TRA tool is used to document risk treatment per threat scenario, and to determine the level of the residual risk.	
9.3 Risk retention		
9.4 Risk avoidance		
9.5 Risk sharing		
10 Information security risk acceptance	A TRA tool is used to document acceptance of residual risks per threat scenario.	
11 Information security risk communication and consultation	Out of scope of this document	
12 Information security risk monitoring and review		
12.1 Monitoring and review of risk factors	Out of scope of this document	
12.2 Risk management monitoring, review and improvement	Out of scope of this document	

Table 3: Conformance mapping to ISO 27005:2018

2.6 IEC 62443-4-1

The following table provides a conformance mapping of the methodology described in this document with the requirements of IEC 62443-4-1.

IEC 62443-4-1 Requirement SR-2	System overview for target area "Development of component" See section 0: System overview for target area "Development of component"	Threat identification
a) correct flow of categorized information throughout the system;	**Data flows** between the interfaces of services and data stores as well as external systems. Examples are API calls, data base queries, and HTTP communication with Web applications. The protocol used in the data flow should be annotated.	
b) trust boundaries	Security zones of the technical environment, **and trust boundaries** between the zones.	
c) processes	**SW-services** with their interfaces, e.g. APIs or user interfaces	
d) data stores	**Data stores**, e.g., file shares, database and shared memory, with their interfaces.	
e) interacting external entities	External systems that are connected through data flows	
f) internal and external communication protocols implemented in the product	Data flows between the interfaces of services and data stores as well as external systems. Examples are API calls, data base queries, and HTTP communication with Web applications. **The protocol used in the data flow should be annotated**.	
g) externally accessible physical ports including debug ports;	**Physical interfaces** of a device, e.g., USB ports, ports for memory cards, and debug ports.	
h) circuit board connections such as Joint Test Action Group (JTAG) connections or debug headers which might be used to attack the hardware	Physical interfaces of a device, e.g., USB ports, ports for memory cards, and debug ports. **This includes circuit board connections like JTAG.**	
i) potential attack vectors including attacks on the hardware, if applicable		*See section 2.3.1:* *Step 5: Identifying and Analyzing Threat Scenarios* Approaches for the systematic identification and analysis of threat scenarios:

		1) Analyze all interfaces of sub-units for possible attack actions at that interface. ... The systematic identification of threat scenarios can be supported by taxonomies or catalogs. • Taxonomies of attack actions or threats, see STRIDE or an approach described by authors from Siemens, help to cover the different types of attack. • Catalogs that list common attack actions in detail can be used as knowledge repositories, see e.g., ATT@CK by Mitre, the TOP 10 Threats and Countermeasures by BSI, or CAPEC.
j) potential threats and their severity as defined by a vulnerability scoring system (for example, CVSS);		The risk level of a threat scenario is rated as described in *section 2.3.2: Step 6: Rating Likelihood and Impact to Derive Risk*. The rating scheme uses similar factors as CVSS.
k) mitigations and/or dispositions for each threat;		Security measures to mitigate threats are determined after the TRA. Threats with high security risk level have to be mitigated according to the PSS risk management strategy of the organizational unit.
l) security-related issues identified;		*See section 2.3.1: Step 5: Identifying and Analyzing Threat Scenarios* Approaches for the systematic identification and analysis of threat scenarios: 3) Consider possible security weaknesses. The systematic identification of threat scenarios can be supported by taxonomies or catalogs.

		• Lists of typical security weaknesses are available, e.g. the OWASP Top Ten or ISO 27005 Annex D.1. A gap analysis with respect to security requirements lists like IEC 62443-3-3 or the SANS CIS Controls is proven way to detect security weaknesses.
m) external dependencies in the form of drivers or third-party applications (code that is not developed by the supplier) that are linked into the application		*See section 2.2.2:* Step 2: *Specifying Scope and Intended Operational Environment* List the third-party sub-units, and state whether a TRA or security documentation exists for each.

2.7 IEC 62443-2-4

The following table provides a conformance mapping of the methodology described in this document with the requirements of IEC 62443-2-4.

IEC 62443-2-4 requirement SP.03.01	IEC 62443-2-4 notes	Mapping
BR The service provider shall have the capability to conduct a security risk assessment of the Automation Solution or contribute to (participate in) a security risk assessment conducted by the asset owner or its agent.	...the service provider has an identifiable process for performing or contributing to a risk assessment	The TRA method provides a method for security risk assessment. The workflows for risk assessment are integrated in the PM process of the organizational unit.
	... the service provider might be asked to provide detailed knowledge of the Automation Solution and its components	Step 1, 2 and 4
	... the service provider might be asked to provide ..... information about threats and/or vulnerabilities	Step 5
RE(1) The service provider shall inform the asset owner of the		Workflows for security risk communication and acceptance are integrated in

results of security risk assessments that it performs on the Automation Solution, including risk mitigation mechanisms and procedures.		the PM process of the organizational unit.
RE(2) The service provider shall have the capability to verify that security architecture reviews and/or security assessment and/or threat analysis of the control system used in the Automation Solution have been conducted by a third party		Workflows for security assessments and review are integrated in the PM process of the organizational unit.

Appendix B: Terminology

The terms used in the TRA method are explained in Section 1.4. This appendix provides some further explanations. The following UML diagram summarizes the terms and their relationships.

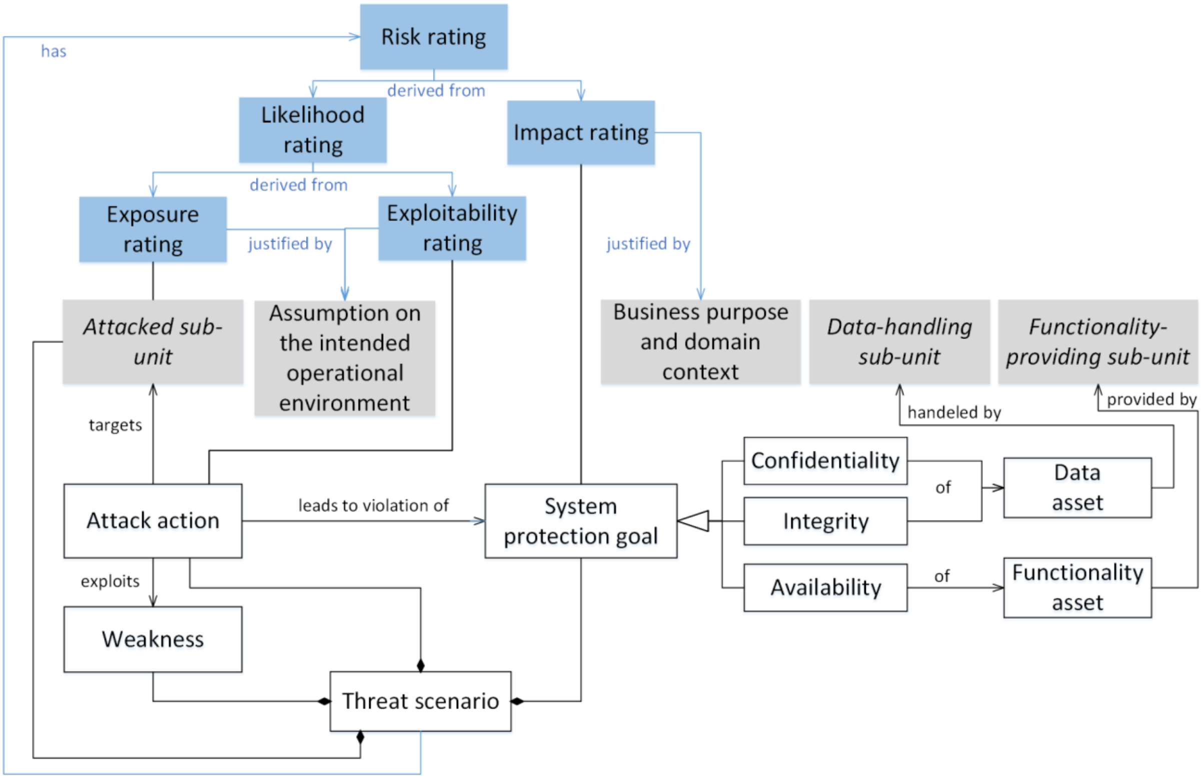


Figure 13: UML diagram illustrating the terminology of the TRA method

The terms shown in Figure 13 have been derived from terms and definitions of ISO/IEC 27000, ISO/IEC 27005, IEC 62443 and NIST 800-30. These standards use divergent sets of terms, so a choice had to be made.

For example, IEC 62443 uses the term **Threat scenario** as well, corresponding to the term 'Incident scenario' in ISO/IEC 27005, while the combination of a 'Threat source', 'Threat event', 'Vulnerability', 'Predisposing conditions' and 'Adverse impact' is called a 'Generic risk model' in NIST 800-30.

The term **Attack action** corresponds to the terms 'Method', 'Circumstance', 'Event' and 'Action' in these standards. The more specific wording of Attack action reflects the fact that the presented TRA method focuses on threats caused by human threat actors, i.e. attackers, rather than environmental threats.

In ISO/IEC 27005 and in NIST 800-39, the term 'Vulnerability' is used, which corresponds to **Weakness**. The latter has been chosen to differentiate from vulnerabilities in the sense of CVE[11].

In the presented TRA method, likelihood is rated in terms of the factors **Exposure** and **Exploitability**, as explained in Section 0. The use of different factors for likelihood is common in TRA methodologies, but again the naming of the factors varies. In the presented TRA method, the factors have been chosen with the goal to avoid overlaps and dependencies, as this helps users to do the rating. The term **Exposure** is very similar to the metric 'Attack Vector' in CVSS v3.1[12], which can take the values Network, Adjacent, Local, and Physical. Sometimes the term 'Risk exposure' is used – this corresponds to **Risk rating** in the presented method. The term **Exploitability** matches well with a combination of the CVSS v3.1 metrics 'Attack Complexity', 'Privileges required' and 'User interaction'.

The use of the protection goal categories of confidentiality, integrity and availability is a key concept in ISO/IEC 27005. There it is stated that consequences (impact) of loss of confidentiality, integrity and availability should be identified. A **System protection goal** is a protection goal category together with a data or functionality asset.

Figure 13 also shows the associations with the system overview. Note that the entities with names in *italics* are abstract. Depending on the scope, sub-units could, e.g., be hosts, embedded devices, dataflows, data-stores, interfaces of SW-services, physical interfaces, or network devices.

[11] https://cve.mitre.org/

[12] https://www.first.org/cvss/