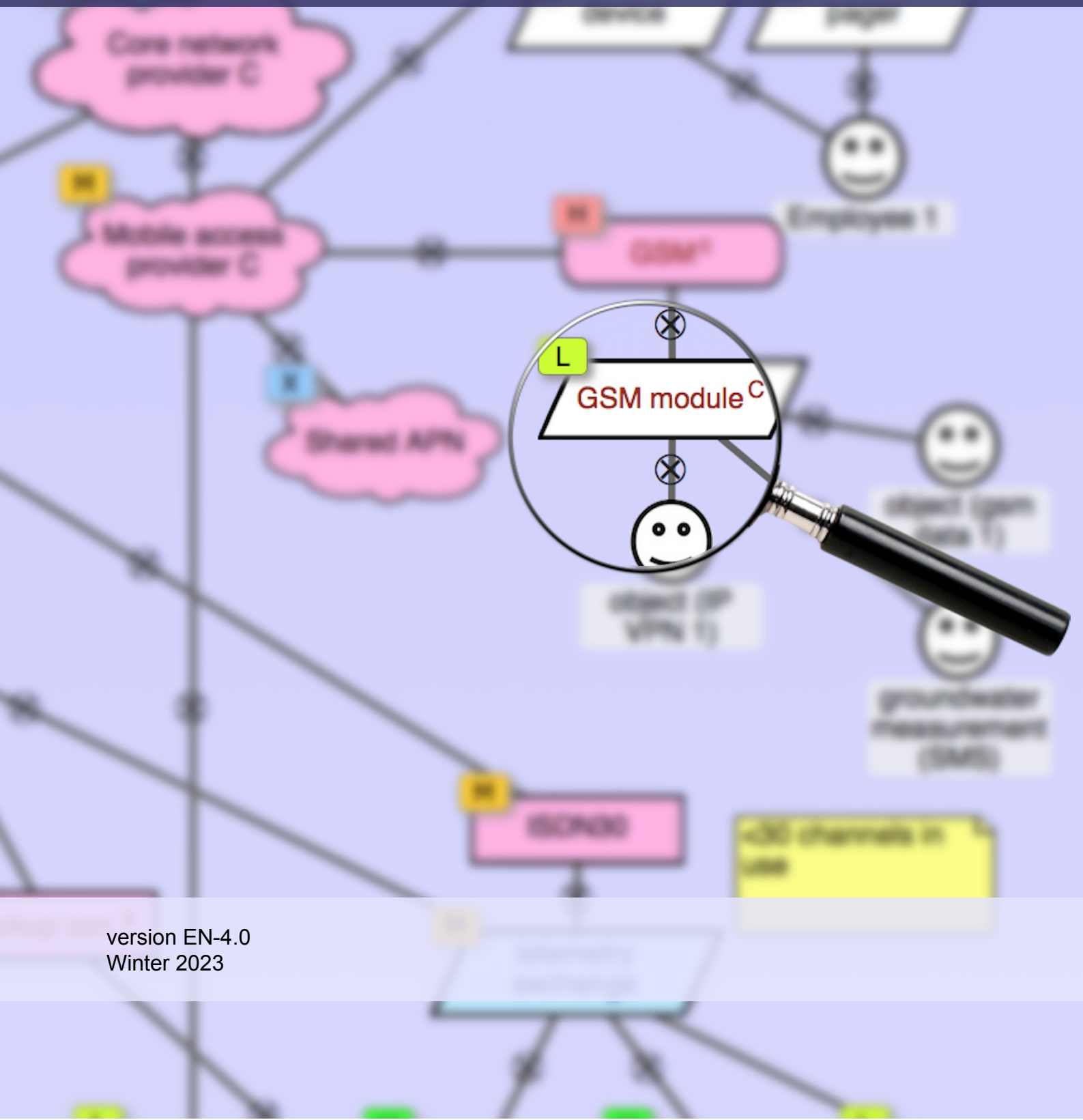


# The Raster Method application manual



# Table of contents

1	Introduction	5
1.1	The Raster method	5
1.1.1	Participants	6
1.1.2	Tool support	7
1.2	About this manual	7
2	The Raster method	9
2.1	Telecommunication service diagrams	10
2.1.1	Actors	10
2.1.2	Wired links	11
2.1.3	Wireless links	11
2.1.4	Unknown links	12
2.1.5	Equipment	12
2.1.6	Example	13
3	Stage 1 — Initiation and preparation	15
3.1	Identify telecom services	15
3.2	Identify actors and external stakeholders	16
3.3	Describe disaster scenarios	16
3.4	Create stage 1 report	16
3.5	Obtain approval from sponsor	17
4	Stage 2 — Single failures analysis	19
4.1	Update the checklists of vulnerabilities	19
4.2	Draw initial diagrams	20
4.3	Analyse the vulnerabilities of components	20
4.3.1	Add and remove vulnerabilities	20
4.3.2	Assess vulnerabilities	21
4.3.3	Assess frequency	22
4.3.4	Assess impact	24
4.3.5	Assessing all vulnerabilities on a component	26
4.4	Expand unknown links	26
4.5	Review	26
5	Stage 3 — Common cause failures analysis	29
5.1	Create clusters	29
5.2	Analyse each cluster	30
5.3	Expand unknown links	30
5.4	Review	31
6	Stage 4 — Risk evaluation	33
6.1	Determine longlist	33
6.2	Reduce longlist to shortlist	33
6.3	Make treatment recommendations	34
6.3.1	Select risk treatment option	34
6.3.2	Assess social risk factors	35
6.3.3	Review the shortlist	36
6.4	Prepare final report	37

---

7 Executing the Raster method	39
7.1 Team composition	39
7.2 Stage 1 — Initiation and preparation	40
7.3 Stage 2 — Single failures analysis	40
7.3.1 Wireless connections	40
7.3.2 Wired connections	41
7.3.3 Equipment	41
7.4 Stage 3 — Common cause failures analysis	42
7.4.1 Wireless links	42
7.4.2 Wired links	43
7.4.3 Equipment	43
7.5 Stage 4 — Risk evaluation	43
8 Raster tools	45
8.1 Working with the standalone tool	45
8.1.1 File menu	46
8.1.2 View menu	46
8.2 Working with the intranet tool	46
8.2.1 Private and shared projects	47
8.3 Toolbars	47
8.3.1 The Projects toolbar	47
8.3.2 The Home toolbar	49
8.3.3 The Settings toolbar	49
8.4 Printing	50
8.5 Main views	50
8.6 Find nodes	51
8.7 Help window	51
8.8 Colour codes	52
8.9 Keyboard shortcuts	52
9 Diagrams view	53
9.1 Templates	53
9.2 Checklist windows	53
9.3 Service tabs	54
9.4 The mini-map	54
9.5 Diagram nodes	55
9.6 Node classes	55
9.7 Identical nodes	56
9.8 Notes	56
9.9 Connecting nodes	57
9.10 Selecting nodes	57
9.11 The node menu	58
9.12 Node labels	59
9.13 Vulnerability assessment window	60
10 Single failures view	61
10.1 Service tabs	61
10.2 Vulnerability assessment	61
11 Common cause failures view	63
11.1 Vulnerability assessments	63

11.2	Nodes and node clusters	64
11.2.1	Nodes	65
11.2.2	Cluster headers	65
11.2.3	Drag and drop	66
12	Analysis view	67
12.1	Failures and vulnerabilities	67
12.2	Assessments by level	68
12.3	Node counts	68
12.4	Checklist reports	68
12.5	Longlist	68
13	Technical issues	69
13.1	The intranet tool	69
13.2	Computation of vulnerability levels	69
13.3	Creating iconsets	71
13.3.1	Creating icons and masks	71
13.3.2	iconset.json	72
13.4	Project Groups	72
13.4.1	group.json	73
13.5	Standalone configuration	74
13.5.1	prefs.json	74
13.5.2	iconsets	75

# 1 Introduction

*Introduction and guide to this document.*

Organisations use many types of telecommunication services: fixed and mobile telephony, videoconferencing, internet, encrypted links between offices, etc. In the last decade, organisations have become much more dependent on these services. Whereas in the past a telephone outage was an inconvenience, today the failure of telecom services often makes it impossible to do business at all. And as organisations move online and into the cloud, reliability of telecom services becomes even more essential.

At the same time, technological and market changes have made it more difficult to assess the reliability of telecommunication services. Networks grow continuously, new technologies replace old ones, and telecom operators outsource and merge their operations. For any end-to-end telecom service, several telecoms operators will be involved, and none of them can understand how important that service is to each customer.

This increased dependency applies even more to organisations that fulfil a vital role in society, such as fire services, medical care, water boards, utilities, banks, etc.

It is therefore important that organisations in general, and organisations that supply critical infrastructures in particular, understand the vulnerabilities and dependencies of the telecom services they use. This document describes a method, called Raster, to assist in this understanding.

The goal of Raster is that the organisation becomes less vulnerable to telecom failures. To reduce the vulnerability, the organisation must first understand what can go wrong with each telecom service they use. Also, these risks must be ranked, so that the most pressing risks can be addressed first. Raster helps a team of analysts to map and investigate one or more telecom services for an organisation. The result is a report, showing which risks should be addressed first, and why. Selection and execution of countermeasures is the next logical step, but is not part of the Raster method.

## 1.1 The Raster method

Incidents with availability of telecom services often happen because of component failures: an underground cable is damaged by a contractor, a power failure causes equipment to shut down. To prepare for these incidents, the organisation must first realise that the cable and equipment exist. An important part of the Raster method is therefore to draw a diagram showing all components involved in delivering the service.

Incidents can also happen when a single event leads to the simultaneous failure of two or more components. For example, two cables in the same duct can be cut in the same incident, or a software update can cause several servers to misbehave. These failures are called *common cause failures*, and they are dangerous because their impact can be quite large.

Major steps in the Raster method are to draw service diagrams, and to assess the likelihood and potential impact of single and common cause failures. However, unlike other methods Raster does not take a narrow numerical approach to assessing risks.

Risks with low probability and high effects are especially important. These rare but catastrophic events have been called “black swans”. Raster helps to uncover black swans in telecom services.

Risk assessments are always in part subjective, and information is hardly ever as complete as analysts would like it to be. This does not mean that biases and prejudices are acceptable. Raster tries to nudge analysts into a critical mode of thinking. Uncertainty is normal, and assessments can be explicitly marked as “Unknown” or “Ambiguous” if a more specific assessment cannot be made. Raster can be applied even when much of the desired information on the composition of telecom networks is unavailable or unknown. Missing information can be gradually added.

To avoid a narrow risk assessment, the Raster method is applied by a team of experts, each having his own area of expertise. Raster facilitates cooperation between experts of different backgrounds.

Raster facilitates the construction of a recommendation using a tested methodical analysis. This recommendation is not just based on the technical aspects of failure of telecoms services, but also takes account of the societal impact of failures, and of risk perceptions of external stakeholders.

One final remark: Raster can be deployed on its own, or as part of a company-wide risk management framework. This manual assumes a stand-alone application. When Raster is used as an element within an approach, the initiation stage (in which the scope of the study is determined) will likely need to be adapted.

### 1.1.1 Participants

The following parties are involved in applying the Raster method.

- The *case organisation*: the method is executed on request of an organisation. This organisation is the requesting client of the study.
- The *project leader*: the person facilitating the application of the method. The project leader can be one of the analysts, or focus on managing the process.
- The *analysts*: the method is executed by a group of professionals. It is essential that this group consists of multiple people. Not only does a single person seldom possess all required knowledge, it is also important that the study leads to an objective and impartial assessment, as much as possible free from personal preferences or personal blind spots.

The team needs to encompass knowledge on essential business activities and technical aspects of telecommunication networks and services. Additionally, it will be useful if team members have some experience with risk assessment, and with the Raster method in particular. Because of this range of knowledge it will be necessary to include employees of the case organisation in the team of analysts.

- The *sponsor*: the person or entity representing the case organisation for the purpose of the study. Typically this will be a manager from the case organisation. The sponsor can be one of the analysts. The sponsor is the customer to the project leader.
- The *decision makers*: the output of the method is a set of recommendations and supporting argumentation that serve as the basis for the selection of risk treatment decisions. Responsibility for the selection does not belong to the

analysts, but to the decision makers. The decision maker can be sponsor, but these roles can also be separate.

- The *external stakeholders*: this category includes all parties that are not part of the case organisation and not involved in the use of telecom services, but do have interests that may be harmed by the risks or chosen risk treatments. External stakeholders may be 'the public' in general, or a specific group such as those people living in the neighbourhood of a facility, the patients of a hospital, customers, etc.

### 1.1.2 Tool support

Software tools are available to support the application of the method. Their use is strongly recommended, and this manual assumes that one of these applications is used. There are multiple versions: there is a standalone application for Windows and MacOS, and a web-based tool that requires an intranet server. All versions function almost identically. This manual uses "the application" without specific reference to indicate that either version can be read.

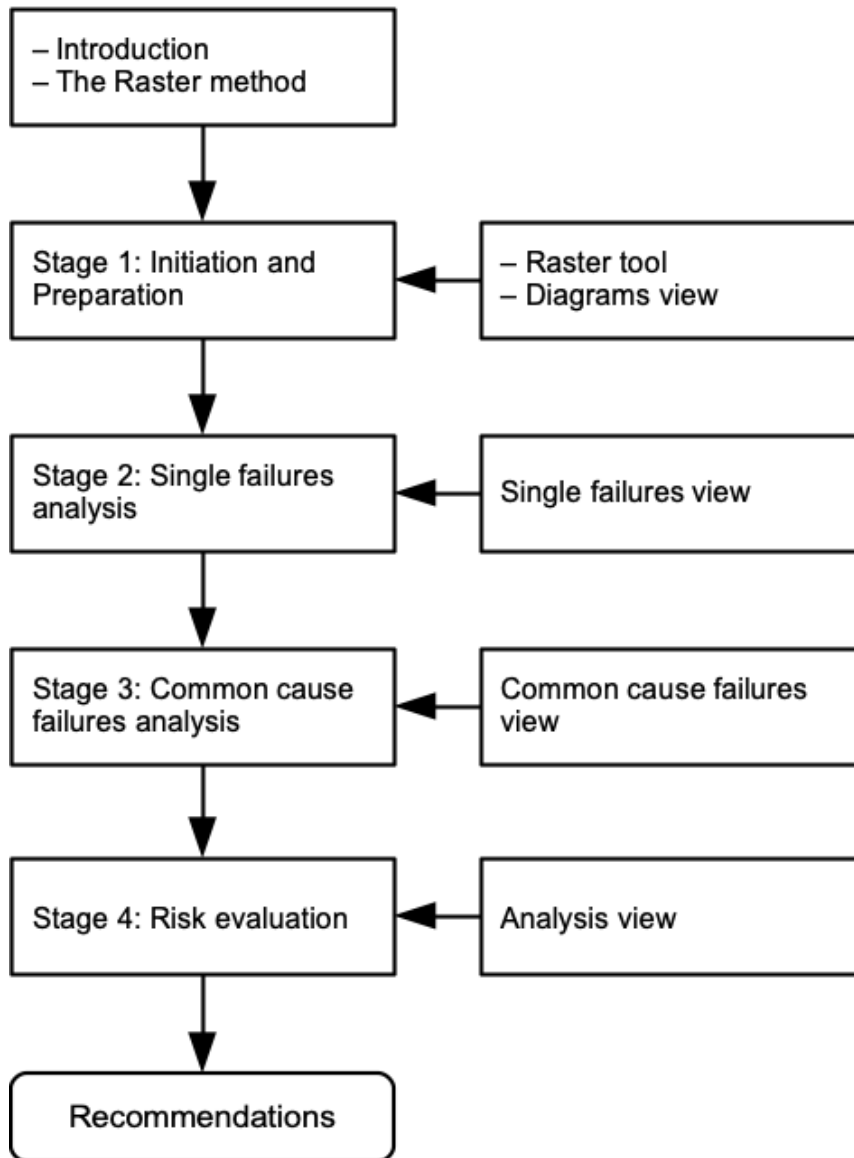
## 1.2 About this manual

This manual is for the professionals who will execute the Raster method. It explains the method and provides guidance. These professionals can either be telecom experts or experts in any other field whose expertise is needed. Examples, notes and tips are typeset in text boxes.

This would be an example, note, tip or shortcut.

The first chapters of this manual describe the Raster method; the second part describes the Raster tools that aid the creation of diagrams and the analysis of Single Failures and Common Cause Failures. When executing an analysis using Raster, you will proceed as in the figure below.

The left-hand column shows the chapters in the first part of this manual. The right-hand column shows the second part, which covers the Raster tools.



---

Author: Eelco Vriezokolk.

Contact and downloads: <https://risicotools.nl/>

Source: <https://github.com/EelcoV/RasterTool>

This work was originally sponsored by Dutch Authority for Digital Infrastructure, and by University of Twente.



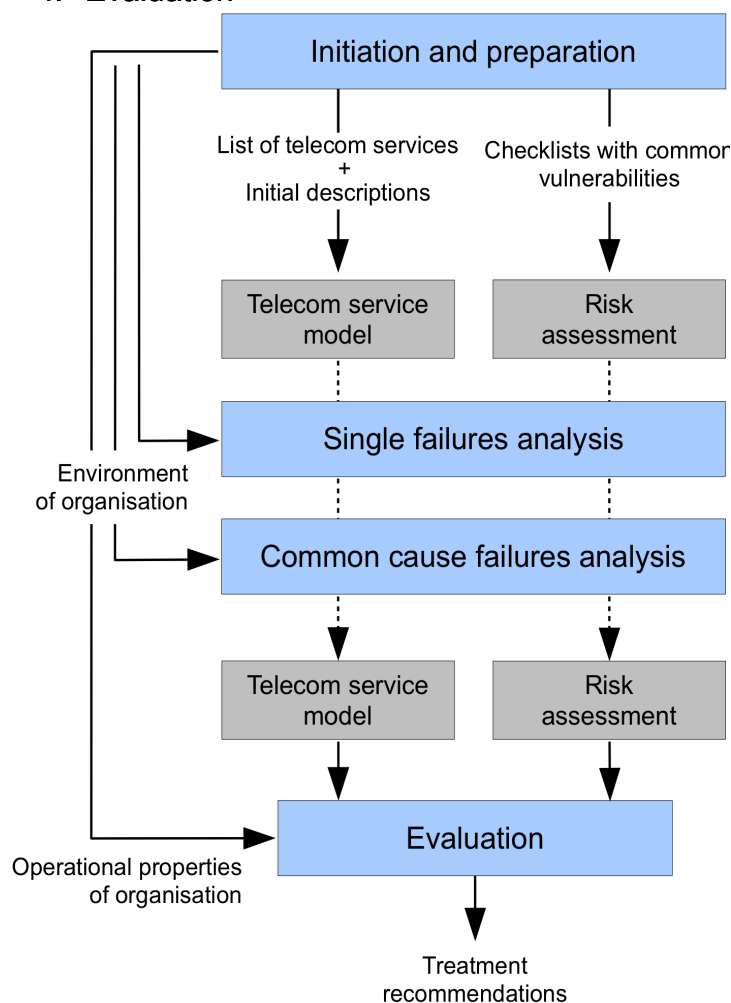
## 2 The Raster method

*General outline of the Raster method and telecom service diagrams.*

When using the Raster method, you and the rest of your team will perform a number of tasks. The method will guide you through these tasks in a methodical way, and the Raster tool will assist you in recording your progress. Based on your collective knowledge and expert judgement you will make estimates about the likelihood and impact of various vulnerabilities affecting the telecom services. Based on this analysis, you and your team will draft suitable risk treatment recommendations. The result of your efforts is a report that can be used by a decision maker to take informed business decisions about accepting, reducing, or avoiding the risks.

Raster consists of four stages, shown in the figure below.

1. Initiation and preparation
2. Single failures analysis
3. Common cause failures analysis
4. Evaluation

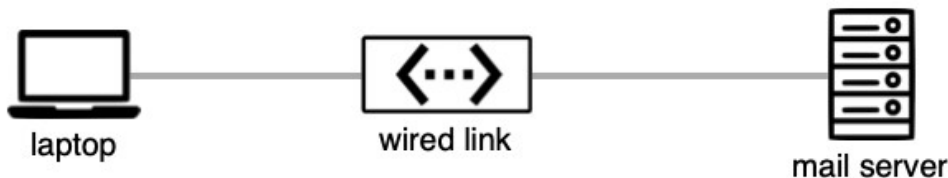


1. The Initiation and Preparation stage describes the scope and purpose of the assessment. Which telecom services are involved, which users can be identified, who are external stakeholders, and what are the characteristics of the environment in which these services are used?

2. The Single Failures Analysis stage creates a telecom service diagram for each telecom service in use. These diagrams describe the most relevant telecommunication components, including cables, wireless links, and equipment items. These components are potentially vulnerable. The diagram does not have to be complete in all details. Parts of networks that are less relevant can be captured using a single “cloud” (unknown link). For all components an assessment of all applicable vulnerabilities is done. Only independent, single failures are taken into account during this stage.
3. The Common Cause Failures Analysis stage takes closer look at failure causes that lead to the failure of multiple components at once. One example is that of independent telecom services that both have a cable in the same underground duct. A single trenching incident may cut both cables at the same time, causing both services to fail. Another example is a large-scale power outage, causing equipment over a large area to fail simultaneously.
4. The Risk Evaluation stage contains the risk evaluation and creation of the final report. The overall risk level is assessed, and recommendations are done for risk treatment. These recommendations take into account the possible reactions of external stakeholders. The recommendations and their supporting argumentation form the final output of the Raster method. [Stage 1](#), [Stage 2](#), [Stage 3](#) and [Stage 4](#) describe each stage in detail.

## 2.1 Telecommunication service diagrams

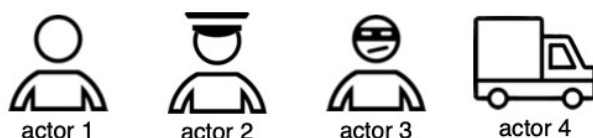
Diagrams are central to the Raster method. A telecom service diagram describes the physical connectivity between components of a telecom service. Diagrams consist of nodes that are connected by lines. Each line represents a direct physical relation. It indicates that the nodes are attached to each other. There cannot be more than one line between two nodes; nodes are either connected or they are not.



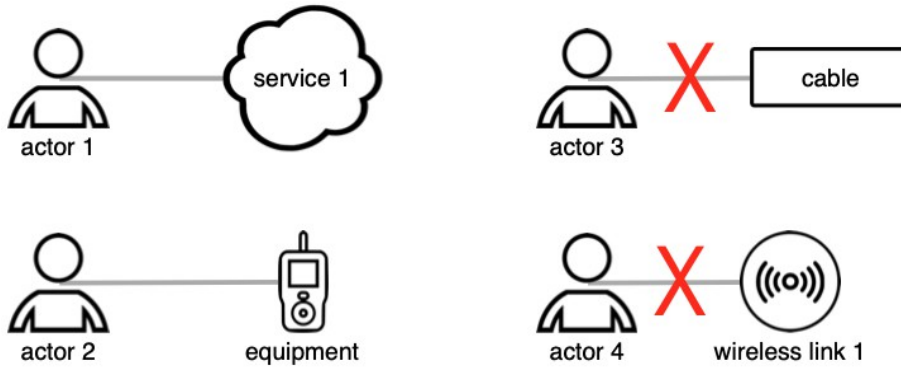
Lines are not the same as cables. When two equipment items are connected via a cable, three nodes are used as in the picture above. The line between equipment and cable shows a physical connection: the cable is plugged into the equipment. There are five types of nodes, each identified by its unique shape.

Different pictures can be used to represent nodes, depending on the icon set used by the Raster tool. The examples below use the Default icon set.

### 2.1.1 Actors



Actors represent the (direct) users of telecom services. An actor can represent a single individual, or a group of individuals having the same role, e.g. 'journalists' or 'citizens'. Maintenance personnel are not modelled as actors, as they do not participate in communication.



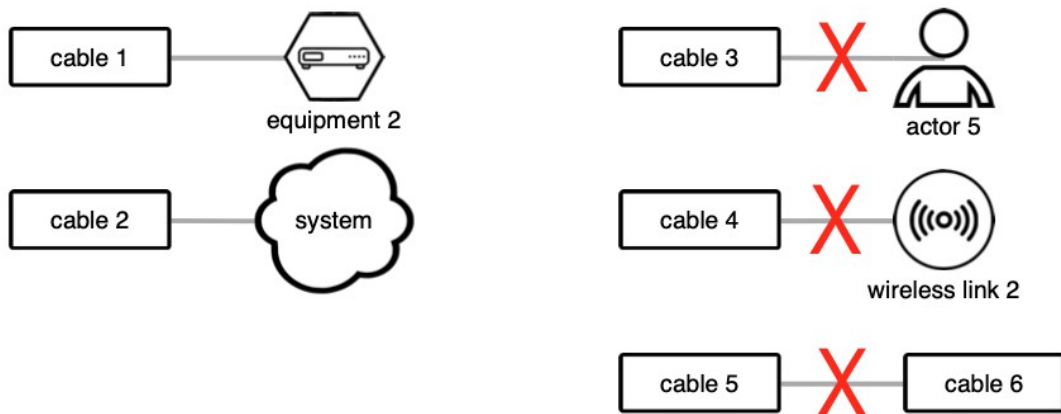
An actor can only be connected to components of type 'equipment' or 'unknown link'. Actors cannot be connected directly to wired or wireless links, and the Raster tool will not allow such connections.

There must be at least two actors in the diagram. There must at least be a person communicating, and one other person to communicate with.

### 2.1.2 Wired links



Wired links represent passive, physical cables, including their connectors, fittings and joints but excluding any active components such as amplifiers or switches. Fiber optic cables, coaxial cables, and traditional telephony copper pairs are typical examples of wired links. The two equipment items connected by the link are not part of the wired link itself, and need to be included in the model separately, either as equipment items or unknown links.



Each wired link has exactly two connections, each to a component of type either 'equipment' or 'unknown link'. To connect a wired link to an actor, wireless link, or another wired link, place an equipment node in between.

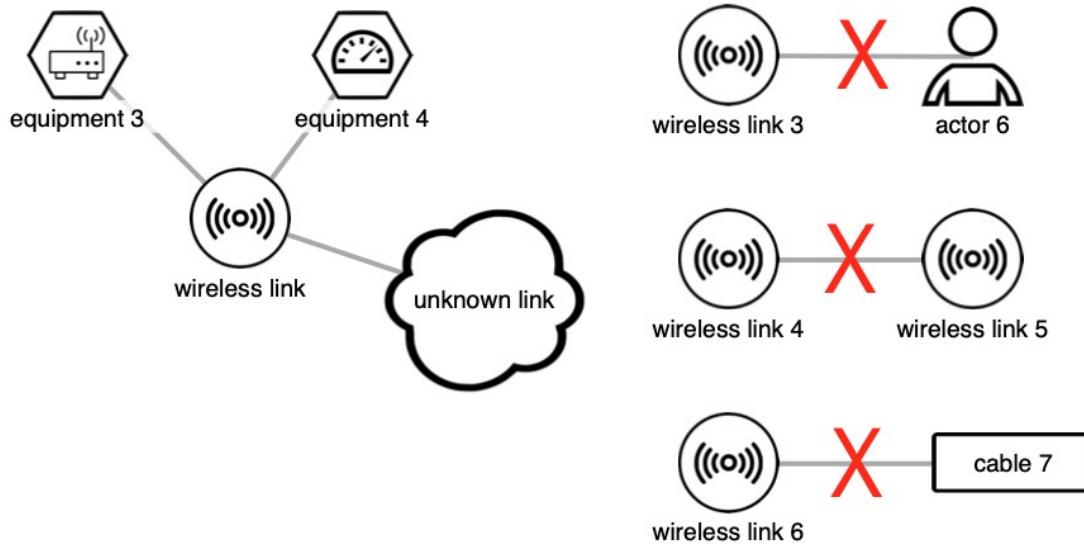
Each wired link has some fixed capacity, a physical location (including a height above or below ground level). These properties need to be known in sufficient detail.

### 2.1.3 Wireless links



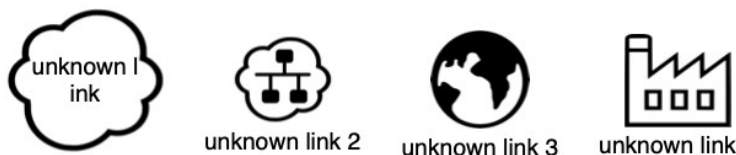
Wireless links represent direct radio connections, excluding any intermediate components. The transmission and reception installations are not part of the wireless link, and have to be modelled separately as equipment items. A wireless link can connect two or more nodes.

Each wireless link has a fixed capacity, but unlike wired links a wireless link does not always have a fixed location. Transmitters and receivers can be mobile or nomadic. The coverage area depends on factors such as transmission power and antenna properties. Wireless links have a fixed frequency or band. All of these properties need to be described in sufficient detail.



Each wireless link has at least two connections, each to a component of type either 'equipment' or 'unknown link'. It can have more than one, as in the example above. To connect a wireless link to an actor, equipment, or an other wireless link, place an equipment node in between.

### 2.1.4 Unknown links



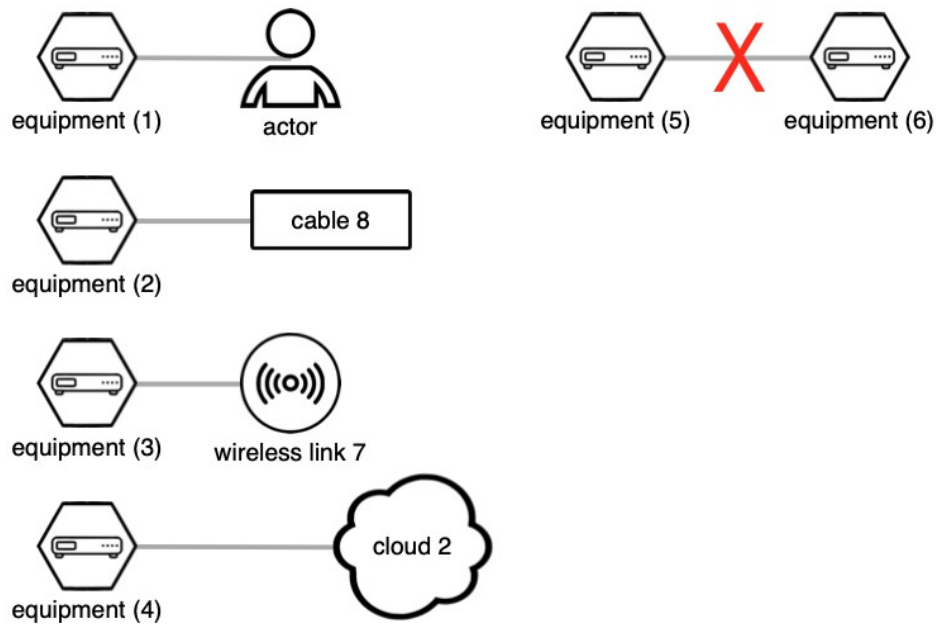
Unknown links (cloud shapes) represent parts of networks for which insufficient information is available, or that do not need to be described in detail. Unlike wired and wireless links, that represent a single communication channel, unknown links are composed of equipment and wired and wireless links.

Because unknown links are collections of equipment and wired and wireless links, they can be used in any place where these nodes can be used. In short, unknown links can connect to any other node type. Also, unknown links can be connected to any number of nodes.

### 2.1.5 Equipment



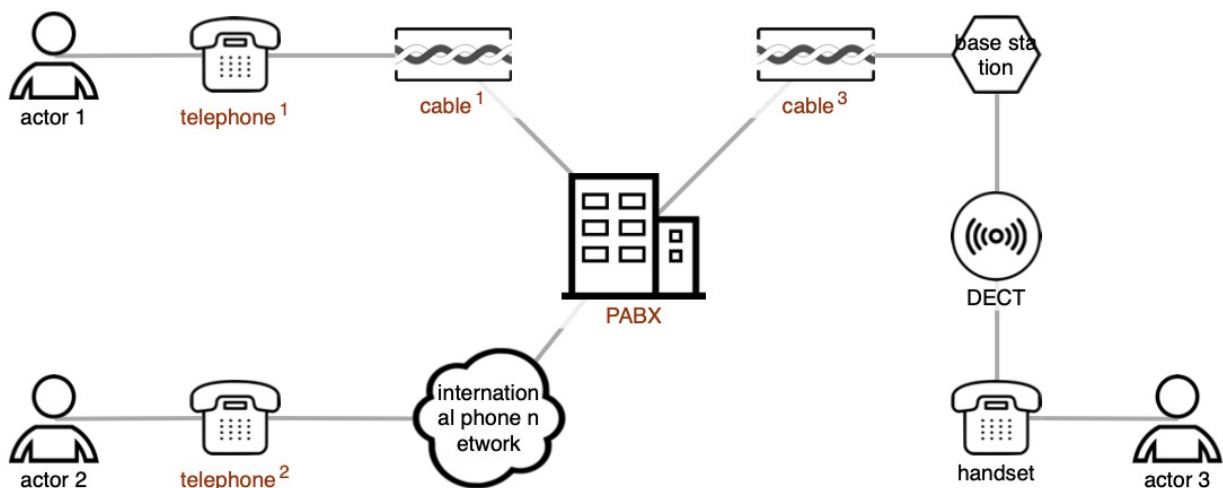
Equipment nodes represent all other physical components of telecom networks, such as switches, exchanges, routers, amplifiers, radio transmitters, radio receivers etc. An equipment node may model a single piece of equipment or an entire installation.



Each equipment node must be connected with at least one other component. An equipment node cannot be connected directly to another node of type 'equipment'.

### 2.1.6 Example

The figure below shows an example of a valid telecom service diagram. The diagram shows three actors, communicating via telephony. Two actors are connected to the same private exchange (PABX); the third actor is abroad. One actor uses a wireless DECT handset and base station, the others use fixed handsets. We have no knowledge (yet) of the other portions of the network, other than that some PABX must exist, and some kind of international telephony network to facilitate the calls.





# 3 Stage 1 — Initiation and preparation

*Define shared purpose and bounds to the study.*

Before the study is started its scope must be made clear to the analysts and to the sponsor. The responsibilities and tasks of the case organisation must be described in some detail. Also, the position of the organisation within the wider system of suppliers, customers and stakeholders must be laid out.

In stage 1 you will collect the information that you need to complete the other stages. The result is a report and agreement from the sponsor to proceed.

The Initiation and Preparation stage consists of the following steps:

1. Identify telecom services
2. Identify actors
3. Describe disaster scenarios
4. Create Stage 1 report
5. Obtain approval from sponsor

## 3.1 Identify telecom services

Create a list of all telecommunication services that are used by the case organisation. This list must be exhaustive. If a service is accidentally omitted, no risk assessment will be performed on it, and dependencies between the service and other services will not be discovered. As a result, decision makers may take unnecessary or ineffective countermeasures, or overlook necessary countermeasures.

To create the list of telecom services, the following information sources may be useful:

- The initiating problem statement, project initiation document, or request for proposals.
- Interviews with executives and operational staff from the case organisation.
- Observation of operational staff in exercises or real-life operations.
- Disaster preparedness plans.
- Reports or evaluations of past exercises.
- Internal formal procedures, operational guides, process manuals.
- Reference materials used during crisis response.

Briefly describe each telecom service. At this stage it is not yet necessary to describe the technical implementation, but if information is available on such items as handsets, terminals, or links, then this should be included in the descriptions.

If a telecom service acts as backup to some other telecom service, or when the service itself has fallback options, then these must be described as well.

The descriptions must also include the relevance of the telecom service to the operations of the organisation. That is, is the service essential, or merely a 'nice to have'?

It will also be useful at this stage to start a glossary of abbreviations and definitions of special terms that may not be clear to all analysts, or to the sponsor.

## 3.2 Identify actors and external stakeholders

List, for each telecom service, the actors who may make use of that service. Main actors are members of the case organisation. All other actors are secondary actors. Actors can be the initiating party of communication session (calling party) or the receiving party (called party), or both.

List all external stakeholders to the case organisation.

Actors and external stakeholders may be identified using the same information sources as listed above for telecom services.

## 3.3 Describe disaster scenarios

Before the analysis can start, it must be clear to which threats this organisation may be exposed. For example, the in-company fire service in charge of chemical plant safety will be confronted with different potential disasters than a crisis team controlling the spread of agricultural diseases. The latter is unlikely to be affected by violent destruction of hardware. Consequently, the threats to their telecom services will be very different in nature.

The threats to telecom services and their mechanisms must be described in as much detail as possible. Disaster scenarios describe the threats, their effects and mechanisms, their likelihood, and the required response from the case organisation.

In the Netherlands tornados seldom lead to damage to infrastructures. Typically, the threat of tornados will therefore be excluded from disaster scenarios. Flooding from sea or riverbeds, however, are quite common, and will likely be included.

For some studies intentional human-made events (crime, terrorism) are highly relevant. For other studies it may suffice to focus on accidental events only. The scope of the study need not be limited to technical aspects. When describing a disaster, the effects that it will have on telecom components is the most important part. To better understand the reactions of the general public it may be useful to also include some graphic descriptions of events that could be experienced by citizens, or that could be published in the media. This may facilitate the assessment of social risk factors in the Risk Evaluation stage.

It may be possible to reuse disaster scenarios from previous risk assessments, thus shortening the amount of work needed.

## 3.4 Create stage 1 report

The results from Stage 1 must be recorded because the analyst will need to refer to this information during subsequent stages.

The following is a common outline of the output document of the Initiation and Preparation stage. This report forms the introduction to the [final report](#).

1. Executive summary to the Stage 1 report.
2. About the case organisation (internal scope):
  - a. Position within wider system of stakeholders.
  - b. Sponsor, decision makers, and analysts.
  - c. Roles, tasks, and responsibilities of the case organisation.



- d. Telecom services used, with a description of the implementation, role and purpose, and fallback and backup options.
- e. Actors, including main actors, and their roles, tasks, and responsibilities.
3. About the environment of the case organisation (external scope):
  - a. Disaster scenarios, with descriptions.
  - b. External parties with whom the main actors may communicate, and other external stakeholders.
4. Glossary.

### 3.5 Obtain approval from sponsor

All analysts must participate in a review of the Stage 1 report. All analysts must agree on its contents by consensus.

The Stage 1 report must then be presented to and discussed with the sponsor. The list of telecom services may contain unexpected services. The unexpected appearance of a service is informative, since it indicates that the risk assessment and preparation of the case organisation are insufficient, and that disaster response plans are incomplete.

The results of the Initiation and Preparation stage determine to a large extent the course of the risk assessment in the later stages. It is therefore important that the sponsor also agrees to the outcome of this stage, and gives formal agreement to the resulting documentation. As a consequence, the documents must be understandable to non-experts. A glossary may be helpful to that effect. Also, an executive summary should be written.



## 4 Stage 2 — Single failures analysis

*Describe telecom service networks and analyse vulnerabilities of components.*

In this stage you will create a telecom service diagram for each telecom service, and assess the vulnerabilities on each of its components. This will give you a good understanding of the inner workings of each telecom service, and a first impression of its risks.

The result will be recorded in the Raster tool: telecom service diagrams and assessment of Frequency and Impact on vulnerabilities of diagram components.

The Single Failures Analysis stage consists of the following steps:

1. [Update the checklists of vulnerabilities](#)
2. [Draw initial diagrams](#)
3. [Analyse the vulnerabilities of components](#) (assess frequency and impact)
4. [Expand unknown links](#)
5. [Review](#)

### 4.1 Update the checklists of vulnerabilities

Based on the disaster scenarios that were described in Stage 1, you must describe the most common vulnerabilities of network components. Checklists are used for this. A checklist contains the name and description of the most common vulnerabilities. Good checklists make the analysis process faster and easier.

Create a fresh Raster project (see [The Projects toolbar](#)), and inspect the predefined checklist for each type (see [Checklist windows](#)). Add new vulnerabilities as deemed necessary. Include vulnerabilities that apply to most components of that type; omit vulnerabilities that only apply to a few components. The checklists do not have to be complete; any particular network component may have specific vulnerabilities that do not occur in the checklist. However, when the most common vulnerabilities are included in checklists, few special cases need to be considered.

Vulnerabilities can be *natural* or *malicious*. Natural vulnerabilities are unpredictable random events, sometimes caused by inattentiveness or other non-intentional human actions. Examples include fires, power failures, or equipment defects. Malicious vulnerabilities are bad-faith actions by people with the express purpose of causing harm, often exploiting weaknesses in the organisation's defenses. Examples include theft and cybercrime. Natural and malicious vulnerabilities differ in their frequency and consequences.

There are three checklists, one each for equipment, wired and wireless links. For actor components no checklist exists. Vulnerabilities of actors are outside the scope of the Raster method. Also, unknown links do not have a separate checklist. They may contain any of the other component types, and therefore all vulnerabilities of the three checklists may apply to unknown links.

Vulnerabilities of actors are not taken into account. For example, Raster does not handle an actor misinterpreting a received message. However, configuration errors, incorrect handling of handsets or cyber crimes can be taken into account. These vulnerabilities are modelled in Raster as part of equipment components, not as part of the actor responsible for them. Maintenance personnel are not included in the diagrams as actors.

## 4.2 Draw initial diagrams

In the Raster tool, create a diagram tab for each telecom service (see [Service tabs](#)). When two services have a lot of components in common, it may be more convenient to combine those services into a single diagram. This avoids components from appearing in more than one diagram, but does tend to make the diagram more complex.

For example, if the office LAN is used for VoIP telephony too, it is more convenient to combine telephony and office automation into one diagram.

Then, for each telecom service, draw an initial diagram based on the information that is currently available. The diagrams will likely not be very detailed yet. At the very least all actors involved with the service must be drawn. Note that it is always possible to create a diagram; if absolutely no information is available beyond the actors involved then the actors can simply be connected using an unknown link (“cloud” symbol). Drawing and editing diagrams using the Raster tool is explained in [Workspace](#).

When creating diagrams, the following guidelines may be helpful:

- A cable containing multiple fibers or strands should be modelled as a single wired link. Two cables in the same duct should be modelled by two wired links in the diagram.
- Point-to-multipoint connections should be modelled using a single wireless link, but may sometimes be more conveniently modelled using separate wireless links to each receiving node. If you know in advance that the link to each individual node is subject to identical risks, then for simplicity a single wireless link should be used.
- Equipment components can be a single device, or an entire installation. For example, a small telephone exchange may be modelled as a single equipment node. However, installations such as these contain multiple cables and sub-components. Often it is not necessary to model these cables and equipment items separately. When an installation is separated over multiple rooms or when wireless links are used then the sub-components should be modelled separately. Alternatively, an unknown link may be used instead of an equipment item.

## 4.3 Analyse the vulnerabilities of components

This activity must be performed for each component in turn. Each step, a component is selected for analysis.

### 4.3.1 Add and remove vulnerabilities

Inspect the listed vulnerabilities of the component. Other vulnerabilities may exist that were not in the general checklist. These vulnerabilities must be added. The disaster

scenarios that were prepared in Stage 1 must be used as guidance in decisions to add vulnerabilities.

Example: Telecommunication satellites are vulnerable to space debris. This vulnerability does not apply to any other kind of equipment, and will therefore not be in the equipment checklist. On the other hand, satellites are not vulnerable to flooding. Therefore “Collision with space debris” must be added, and “Flooding” must be removed from the list of satellite vulnerabilities.

A vulnerability must not be removed unless it is clearly nonsensical, e.g. configuration errors on devices that do not allow for any kind of configuration, or flood damage to a space satellite. To be removed, a vulnerability must be physically impossible, not just very unlikely in practice. In all other cases the frequency and impact of the vulnerability should be assessed (although they can both be set to Extremely low), and the vulnerability must be part of the review at the end of Stage 2.

When a vulnerability is removed, that node will also not be shown in the list for common cause failures. That is another reason not to remove vulnerabilities.

It is important that vulnerabilities that are merely unlikely but not physically impossible are retained in the analysis, because such vulnerabilities could have an extremely high impact. Low-probability/high-impact events must not be excluded from the risk analysis.

### 4.3.2 Assess vulnerabilities

When the list of vulnerabilities for the component is complete, each vulnerability must be assessed. The analysts, based on their collective knowledge, estimate two factors:

1. the likelihood (frequency) that the vulnerability will lead to an incident, and
2. the impact of that incident.

Both factors Frequency and Impact are split into eight classes. The classes do not correspond to ranges (a highest and lowest permissible value); instead they mention a typical, characteristic value for the class. The selection of the proper class may require a discussion between analysts. Analysts must provide convincing arguments for their choice of class.

Sometimes a factor (a likelihood or impact) is extremely large, or extremely small. Extremely large values are not simply very big, but too big to fit in the normal scale, unacceptably high and intolerably high. Likewise, extremely small values are outside the scale of normal values, and sometimes may safely be ignored. Extreme values fall outside the normal experience of analysts or other stakeholders, and normal paths of reasoning cannot be applied.

If no consensus can be reached between the analysts, the class *Ambiguous* must be assigned. In the remarks the analysts should briefly explain the cause for disagreement, and the classes that different analysts would prefer to see.

A limited amount of uncertainty is unavoidable, and is normal for risk assessments. However, when uncertainty becomes too large, so that multiple classes could be assigned to a factor the class *Unknown* must be assigned.

The Raster tool assists in recording the analysis results. The tool will also automatically compute the combined vulnerability score for each vulnerability, and the overall vulnerability level for each node (see sections [Vulnerability assessment window](#) and [Single failures view](#); for technical details see [Computation of vulnerability levels](#)).

Do not blindly trust your initial estimate of frequency and impact. You must not rely only on information that confirms your estimate, but also actively search for contradicting evidence.

### 4.3.3 Assess frequency

For natural vulnerabilities the factor Frequency indicates the likelihood that the vulnerability will lead to an incident with an effect on the telecom service. All eight classes can be used for Frequency (see [Frequency table](#)).

A frequency of “once in 50 years” is an average, and does not mean that each 50 years an incident is guaranteed to occur. It may be interpreted as:

- The average timespan between incidents on a single component is 50 years.
- For a set of 50 identical components, each year on average one of them will experience an incident.
- Each year, the component has a 1 in 50 chance of experiencing an incident.

When the life time of a component is 5 years (or when the component is replaced every 5 years) the frequency of a vulnerability can still be “once in 500 years”.

Example: a component is always replaced after one year, even if it is still functioning. On average, 10% of components fail before their full year is up. The general frequency for this failure is therefore estimated as “once in 10 years” even though no component will be in use that long.

Note that this value is between the characteristic values for High and Medium. The analysts must together decide which of these two classes is assigned.

**Natural frequencies:** characteristic values for frequency classes of natural vulnerabilities.

Class	Value	Symbol
High	Once in 5 years. For 100 identical components, each month 1 or 2 will experience an incident.	H
Medium	Once in 50 years. For 100 identical components, each year 2 will experience an incident.	M
Low	Once in 500 years. For 100 identical components, one incident will occur every five years.	L
Extremely high	Routine event. Very often.	V
Extremely low	Very rare, but not physically impossible.	U
Ambiguous	Indicates lack of consensus between analysts.	A
Unknown	Indicates lack of knowledge or data.	X
Not yet analysed	Default. Indicates that no assessment has been done yet.	–

The likelihood of malicious vulnerabilities is not based on chance (as is the case for natural vulnerabilities), but is based on the difficulty of the action and on the determination and capabilities of the attacker. An attack that requires modest

capabilities could already prove too demanding for a casual customer or employee. On the other hand, even a difficult attack may will be within the reach of skilled state-sponsored hackers. The Raster method is based on the most skilled attacker to the organisation, the *worst plausible attacker*.

***Worst plausible attackers: descriptions, motivations and goals.***

Customers, employees	Unskilled, lightly motivated by opportunity or mild protest (e.g. perceived unfair treatment).
Activists	Moderately skilled, aiming for media exposure to further their cause or protest. Visible impact.
Criminals	Highly skilled, motivated by financial gains (e.g. ransomware).
Competitors	Highly skilled, aiming to obtain trade secrets for competitive advantage. Avoid visible impact.
State-sponsored hackers	Very highly skilled, motivated by geopolitical advantages. Avoid visible impact.

In the Raster tools you set the worst plausible attacker as part of the [project properties](#). Since this is a property of the entire project, you only need to select the appropriate difficulty level of the exploit, as per the table below.

***Malicious frequencies: characteristic values for frequency classes of malicious vulnerabilities.***

Class	Value
Very difficult	Exploit requires skill, custom attack tools, long preparation time and multiple weaknesses and zero-days.
Difficult	Exploit requires skill, some customized attack tools and long preparation time
Easy	Tools exist to execute the exploit. Basic skills required.
Trivial	Requires no skill or tools at all.
Nearly impossible	Exploit may be possible in theory, but consensus is that exploit is infeasible.
Ambiguous	Indicates lack of consensus between analysts.
Unknown	Indicates lack of knowledge or data.
Not yet analysed	Default. Indicates that no assessment has been done yet.

Use the following three-step procedure to determine the factor Frequency:

1. Find the frequency class that applies to this type of node in general.

This can be based on, for example, past experience or expert opinion. If available, MTBF (mean time between failures) figures or failure rates should be used.

2. Think of reasons why this particular node should have a lower or higher frequency than usual.

Existing countermeasures may make the frequency lower than usual. For example, if an organisation already has a stand-by generator that kicks in when power fails, then the frequency of power failure incidents is thereby reduced. Remember that the frequency does not reflect the likelihood that the vulnerability is triggered, but the likelihood that the vulnerability will lead to an incident.

For some components monitoring can detect failures that are imminent before they occur. This also will reduce the frequency of incidents. Another example is the use of premium quality components, or secure and controlled equipment rooms. All of these measures make incidents less likely.

The disaster scenarios may be an indication that the frequency should be higher than usual. In crisis situations it is often more likely that an incident will occur. For example, power outages are not very common, but are far more likely during flooding disasters. These disasters themselves are very uncommon. The overall frequency is therefore determined by:

- the likelihood of power outages during normal circumstances, and
- the likelihood of power outages during a flood, combined with the likelihood of flooding.

3. Decide on the frequency class for this particular node.

Typically either Low, Medium, or High will be used. If neither of these accurately reflect the frequency, one of the extreme classes should be used. If no class can be assigned by consensus, one of Ambiguous or Unknown should be used.

#### 4.3.4 Assess impact

The factor Impact indicates the severity of the effect when a vulnerability does lead to an incident. This severity is the effect to the service as a whole, not its effect to the component that experienced the vulnerability. For example, a power failure will cause equipment to stop functioning temporarily. This is normal, and in itself of little relevance, unless it has an effect on the availability of the telecom service. The power failure could cause the service to fail (if the equipment is essential), but could also have a no effect at all (if the equipment has a backup). Or any effect in between.

Only the effects on the telecom service must be taken into account in this stage. Loss of business, penalties, and other damage are not considered, but may be relevant during risk evaluation (see [Assessing social risk factors](#)).

The damage may be caused by an incident that also affects other components of the same telecom service. For example, a cable may be damaged by an earthquake; the same earthquake will likely cause damage to other components as well. However, this additional damage must not be taken into account. Only the damage resulting from the damage to this component must be considered. The next stage, common cause failures analysis, takes care of multiple failures due to a single incident.

The impact of some vulnerability on a component covers:

- only effects to the service, not the effects to the component itself,
- only effects to the service, not subsequent damage to the organisation,
- only effects due to damage this single component, not effects due to the failure scenario.



All eight classes can be used for Impact. Characteristic values for the classes high, medium, and low are given in Table .

Use the following three-step procedure to determine the factor Impact:

1. Choose the impact class that most accurately seems to describe the impact of the incident.
2. Think of reasons why the impact would be higher or lower than this initial assessment.

Existing redundancy can reduce or even annul the impact. For example, a telecom service may have been designed such that when a wireless link fails, a backup wired link is used automatically. The impact of the wireless link failing is thereby reduced.

Monitoring and automatic alarms may reduce the impact of incidents. When incidents are detected quickly, repairs can be initiated faster. Keeping stock of spare parts, well trained repair teams, and conducting regular drills and exercises all help in reducing the impact of failures and must be considered in the assessment. On the other hand, absence of these measures may increase the impact of the incident.

3. Decide on the impact class.

Typically either Low, Medium, or High will be used. If neither of these accurately reflect the impact, one of the extreme classes should be used. If no class can be assigned by consensus, one of Ambiguous or Unknown should be used.

**Impact classes:** *Characteristic values, for natural and malicious vulnerabilities.*

Class	Value	Symbol
High	Partial unavailability, if unrepairable. Total unavailability, if long-term.	H
Medium	Partial unavailability, if repairable (short-term or long-term). Total unavailability, if short-term.	M
Low	Noticeable degradation, repairable (short-term or long-term) or unrepairable.	L
Extremely high	Very long-term or unrepairable unavailability.	V
Extremely low	Unnoticeable effects, or no actors affected.	U
Ambiguous	Indicates lack of consensus between analysts.	A
Unknown	Indicates lack of knowledge or data.	X
Not yet analysed	Default. Indicates that no assessment has been done yet.	–

It typically does not matter for the selection of impact class whether some or all actors are affected. All actors are important; they would not appear in the diagram otherwise. However, if the analysts agree that only very few actors are affected they can select the next lower class (e.g. Low instead of Medium).

The meaning of “short-term” and “long-term” depends on the tasks and use-cases of the actors. A two minute outage is short-term for fixed telephony but long-term for real-time remote control of drones and robots.

“Degradation” means that actors notice reduced performance (e.g. noise during telephone calls, unusual delay in delivery of email messages), but not so much that their tasks or responsibilities are affected.

“Partial unavailability” means severe degradation or unavailability of some aspects of the service, such that actors cannot effectively perform some of their tasks or responsibilities. For example: email can only be sent within the organisation; noise makes telephone calls almost unintelligible; mobile data is unavailable but mobile calls and SMS are not affected. Actors can still perform some of their tasks, but other tasks are impossible or require additional effort.

“Total unavailability” means that actors effectively cannot perform any of their tasks and responsibilities using the telecom service (e.g. phone calls can be made but are completely unintelligible because of extremely poor quality).

“Extremely high” means that if the incident happens the damage will be so large that major redesign of the telecom service is necessary, or the service has to be terminated and replaced with an alternative because repairs are unrealistic.

#### 4.3.5 Assessing all vulnerabilities on a component

The overall vulnerability level of a component is defined as the worst vulnerability for that component. If some of the vulnerabilities are not assessed (no frequency or impact have been set on them), they will not contribute to the overall vulnerability level. It can thus be a useful time-saver to skip assessment of unimportant vulnerabilities.

It is very important that all vulnerabilities with High and Extremely high impact are assessed fully. This is true even when their Frequency is low.

### 4.4 Expand unknown links

When an unknown link receives an overall vulnerability level of Ambiguous or Unknown, the analysts must decide whether or not to expand the node. Expansion means that the internal make-up of the node is examined; the unknown link is removed from the diagram, and its constituent parts are added to the diagram as individual equipment items, wired and wireless links, and possibly further unknown links. Expansion adds more detail to the model, and results in additional diagram components. The vulnerabilities to these new components must also be analysed, as for any other diagram component.

It is not always necessary to expand unknown links. If the analysts think that the effort involved in expansion is too large, or that it will not lead to more accurate or insightful results then expansion should be omitted.

### 4.5 Review

When all components have been analysed, a review must take place. All analysts must participate in this review. The purpose of the review is to detect mistakes and inconsistencies, and to decide whether the Single Failures Analysis stage can be concluded.

If any of the components has an overall vulnerability level of Ambiguous or Unknown, the analysts must decide whether or not to conduct further investigation, in order to

assess the vulnerabilities to that node with greater certainty. If the analysts think that the effort involved is too large, or that it will not lead to more accurate or insightful results then the component should be left as is.

If the analysts decide to redo some part of the Single Failures Analysis stage, then they should again perform a review afterwards. This review may be omitted when the analysts agree that all changes are minor.



# 5 Stage 3 — Common cause failures analysis

*Determine and analyse common cause failures.*

A common cause failure is an event that leads to the simultaneous failure of two or more components. For example: two cables in the same duct can both be cut in a single incident; multiple equipment items may be destroyed in a single fire.

For a common cause failure to happen, the affected components must be within range of each other, according to a critical property. For physical failure events such as fire and flooding, this property is geographical proximity: the components must be sufficiently close to be affected simultaneously. For configuration mistakes it is the similarity in maintenance procedures. For software bugs it is whether related firmware versions are used, regardless of geographical distance. Other events may have different critical properties.

For each failure scenario, the critical property has a maximum effect distance. Two equipment items can only be affected by a minor fire when they are in the same room; for a major fire the effect distance is larger, but still limited to perhaps a single building. Flooding has a much larger effect area, and two components must be further apart to be immune from flooding as their common failure cause.

In stage 3 you will make groups of components that fall within the same range of a critical property. You will do this for each vulnerability separately. For each cluster you will then assess the Frequency and Impact of a common cause failure affecting the components in that cluster. The clusters and their assessments will be recorded in the Raster tool. The result is an improved and refined risk assessment.

The Common Cause Failures Analysis stage consists of the following steps:

1. [Create clusters](#)
2. [Analyse each cluster](#)
3. [Expand unknown links](#)
4. [Review](#)

## 5.1 Create clusters

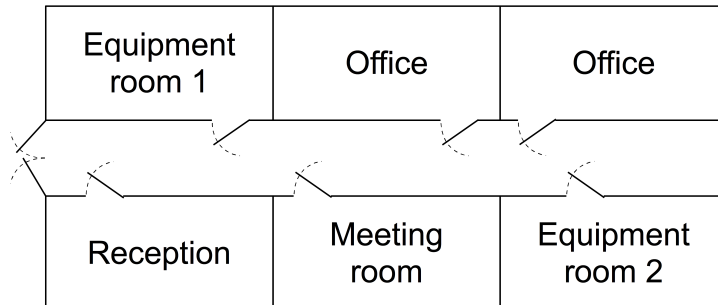
The Raster tool automatically lists each vulnerability in use, provided that that vulnerability occurs for at least two components. For each such vulnerability, the analyst must create clusters based on the critical property.

Example: clusters based on *geographical proximity* can be used for fire, flood, power outage, cable breaks, and radio jamming (per frequency band).

Clusters based on *organisational boundaries* can be used for equipment configuration, ageing, and software bugs. Initially, the Raster tool places all components that have the same vulnerability in a single cluster. Based on the effect distance of failure scenarios further subdivisions can be made, such that:

- each cluster represents a class of failure scenarios that are similar in location and effect area.
- a failure scenario for a cluster can never affect components outside that cluster.
- any two components in the same cluster may be affected by the same failure scenario simultaneously.

It is possible for a larger cluster to entirely include a smaller cluster. Clusters may thus be nested. All nodes in a subcluster are members of their parent cluster as well.



For example, the figure to the right shows an office floor plan with two equipment rooms. Three possible clusters are:

1. Equipment room 1 – small fires, affecting components in equipment room 1 only.
2. Equipment room 2 – small fires, affecting components in equipment room 2 only.
3. Entire office – large fires, affecting all components in all rooms.

Cluster 3 then contains subclusters 1 and 2. Note how each cluster is specific to one vulnerability (fire), and covers scenarios that have the same location and effect area.

The Raster tool is used to create clusters in the [Common cause failures view](#).

## 5.2 Analyse each cluster

To analyse a cluster the two factors Frequency and Impact must be assessed. This is done in a similar way as for single failures (see [Analyse the vulnerabilities of components](#)).

In this stage, the factor Frequency reflects the likelihood that *two or more* components in that cluster are affected by the failure scenario. It is not required that all components in the cluster are affected. An impact class applies if the failure scenario affects one or more telecom services. For example: when the simultaneous failure of three components in a cluster would cause long-term unavailability of one telecom service, then the impact class High should be assigned to that cluster.

The Raster tool will automatically compute the vulnerability level of any parent clusters, including the top level vulnerability.

## 5.3 Expand unknown links

When a cluster containing unknown links receives an overall vulnerability level of Ambiguous or Unknown, the analysts must decide whether or not to expand those unknown links. This is analogous to expansion in the Single Failures Analysis stage (see [Expand unknown links](#)).

Note that it is not always necessary to expand unknown links. If the analysts think that the effort involved in expansion is too large, or that it will not lead to more accurate or insightful results then expansion should be omitted.

Expansion adds new components to the diagram. These new components need to be analysed for single failures. This means that part of Stage 2 needs to be redone for these components. It also means that some clusters receive new member nodes. The analysis of these clusters must be revisited.

### 5.4 Review

During the final review all analysts must discuss the results of the analysis of single and common cause failures. Special care must be taken to ensure that all assessments are consistent. The next stage must only be started when all analysts agree on the analysis results.

If any of the clusters has an overall vulnerability level of Ambiguous or Unknown, the analysts must decide whether or not to conduct further investigation, in order to be able to assess the common cause failures within that cluster with greater certainty. If the analysts think that the effort involved is too large, or that it will not lead to more accurate or insightful results then the component should be left as is.

If the analysts decide to redo major parts of the common cause failures analysis, then they should perform another review afterwards.





## 6 Stage 4 — Risk evaluation

*Prioritise and evaluate risks, and make treatment recommendations.*

When all single and common cause failures have been analysed, a list of the most serious risks can be made. The Raster tool assists the initial effort for this stage. Quick wins can be determined automatically, and simple “what if” analysis is available.

During this stage you make a judgement of which risks you consider to be too large. You write down arguments for your choice and propose risk treatments. You take into consideration both your assessment of vulnerabilities that affect the availability of telecom services and your expectation of reactions of other stakeholders to risk treatments. The result is a report to the sponsor, outlining, explaining and justifying your recommendations.

The Risk Evaluation stage consists of the following steps:

1. Determine longlist
2. Reduce longlist to shortlist
3. Make treatment recommendations, considering social risk factors
4. Prepare final report

### 6.1 Determine longlist

Based on the information presented by the Raster tool (see [Analysis view](#)), a longlist of the most serious risks must be compiled. These risks are:

- the combination of a single vulnerability and a single component, such as “power failure at the PABX”, or
- the combination of a single common cause failure vulnerability and a single cluster, such as “fire at equipment in the facilities room”.

It is up to the analysts to judge which risks are serious enough to be placed on the longlist. However, the list should include the “quick wins” reported by the Raster tool (see [Failures and vulnerabilities](#)). Quick wins are those vulnerabilities that by themselves determine the overall vulnerability level of a component. Reducing that vulnerability would immediately reduce the overall level.

Other good candidates for inclusion on the longlist are those risks that were computed as Extremely high or High, as well the risks that were computed as Ambiguous or Unknown.

### 6.2 Reduce longlist to shortlist

The longlist must be prioritised. Prioritisation requires more information than can be found in the diagrams and vulnerability assessments. For example, information on control relationships between components, or information about redundancy, cannot be found in the diagrams but is very important for risk prioritisation. Also, telecom services are not all equally important. Therefore, a risk that was assessed as “high” occurring in a service that is useful but non-essential may be listed below a risk that was assessed as “medium” to a vital service. The priority may further be affected by the service acting as backup to another service, or having fallback options itself.

All analysts must collectively examine each risk on the longlist. Based on consensus, risks may be raised or lowered on the list, or may be removed altogether. The result of this process is a prioritised shortlist of risks for which the analysts agree that risk treatment is warranted.

## 6.3 Make treatment recommendations

It is not the responsibility of the analysts to decide on how risks on the shortlist will be treated. The sponsor or decision maker will be responsible for these measures. However, the analysts do have the responsibility for providing them guidance, and to make reservations for the uncertainty in their assessments and limits to their knowledge.

For each risk on the shortlist, the analysts must give risk treatment recommendations. It is impossible to give a procedure for this, as the suitable treatment for a risk depends very much on the type of service, the nature of the risk, and the circumstances of the case organisation.

### 6.3.1 Select risk treatment option

In general, four general risk treatment options exist:

1. **Avoid.** Remove the risk completely (proaction), or discontinue the use of the component or service altogether. Proaction means eliminating structural causes of accidents to prevent them from happening in the first place (e.g. avoiding radio interference by replacing a wireless link by a wired link). When discontinuing an entire service, an alternative service will often be available. However, you should be careful to replace a service with known risks for a new one with unknown risks.

Even when no alternative is available it may still be worth considering discontinuing use of the telecom service when the risk cannot be avoided. Rather than using a service that may fail unexpectedly, it may be preferable to not use the service at all to avoid unpleasant surprises at inopportune moments during crisis response.

2. **Reduce.** Make the risk more acceptable, by reducing either its likelihood (frequency) or impact. These activities encompass prevention and preparation. Prevention means taking measures beforehand that aim to make accidents less likely, and to limit the consequences in case incidents do occur (e.g. by imposing smoking restrictions and using fire-retardant materials). Preparation means ensuring the capacity to deal with accidents and disasters in case they do happen (e.g. by holding regular fire drills).
3. **Transfer.** Pass the risk to another party. Typical examples of risk transfer are insurance, or maintenance contracts whereby faulty equipment is replaced with spares on short notice. Risk transfer in effect buys certainty, by transferring the uncertainty to another party in return for payment.
4. **Retain.** Accepting the risk, in an informed decision. Reasons for accepting risks may be that other options would be too costly, that the likelihood is deemed to be very low, or simply the lack of suitable alternatives. In all cases it is much preferable to knowingly accept a risk rather than being confronted with it.

**Social risk factors:** list and description of social risk factors.

Artificiality, immorality

“Unnaturalness” of risk sources.

Benefits	Tangible and intangible beneficial effects.
Blame	Responsibility for damages attributable to some actor.
Catastrophic potential	Fear of sudden, disruptive, large effects.
Children	Amount of risk exposure faced by children in general.
Familiarity	Extent to which the risk is perceived as common and well known.
Fear	Characterises the amount of fear.
Institutional control	Close, effective monitoring of risks by authorities, with the option of intervention when necessary.
Media exposure	Amount of attention by (social) media.
Mobilisation	Potential for protests and active opposition.
Personal control	Level of control that an individual stakeholder can exercise.
Violation of equity	Discrepancy between those who enjoy the benefits and those who bear the risks.
Voluntariness	Amount of free choice an individual has in being exposed to the risk.

### 6.3.2 Assess social risk factors

The draft treatment of risks on the shortlist may lead to criticism by other stakeholders. The opinions of these stakeholders must be considered before final treatment recommendations are formulated. Otherwise, decision makers may unexpectedly have to deal with societal opposition, possibly forcing them to opt for a sub-optimal treatment that is nevertheless more acceptable to external stakeholders. Analysts must therefore assess additional risk factors that influence risk perception and risk acceptance by third parties. See the table of [social risk factors](#).

*Artificiality* applies to situations where people oppose a technology because it is unnatural. For example, electromagnetic radiation from mobile telephony base stations is more often considered 'harmful', whereas natural sunlight is more often considered 'healthy'. However, there is scientific consensus that ill effects from electromagnetic radiation have not been demonstrated, whereas the incidence of skin cancer is cause for serious concern. Related to this issue is that of immorality. *Immorality* play a role when technological solutions go against people's ethical or moral principles.

*Benefits* can counterbalance the availability risks on the shortlist. Risky situations can be acceptable when the (perceived) benefits outweigh the (perceived) risks. For example, construction of a high broadcasting tower may meet with less opposition if it will be used for emergency communications instead of entertainment broadcasts.

*Blame* can sometime be apportioned to some actor (e.g. a telecoms operator), but natural risks cannot be blamed on anyone in particular. Risks without blame are often more acceptable than risk caused by some explicit actor.

*Catastrophic potential* makes risks less acceptable. The menace of wide-spread, large-scale destruction, regardless of likelihood, makes risks less tolerable. On the other hand, risks that have a small chronic effect over a period of time are often more easily accepted.

*Children* influence risk perception, sometimes in dramatic ways. People have strong feelings when children are affected by risks.

*Familiarity* with a risk may lead to complacency. The reverse is also true: novel risks may be less tolerable, simply because they are less well-known.

*Fear* is a general factor, related to catastrophic potential and familiarity. Strong feelings of fear decrease risk acceptance.

*Institutional control* can reassure people that risks are handled diligently. Sufficient trust in institutions is a prerequisite. When trust in institutions is low, risks will be perceived to be higher.

*Media exposure* can lead to increased perception of likelihood. Few people experience risks first-hand, and wide coverage by broadcasting or social networks can increase risk perception.

*Mobilisation* potential is relevant to decision makers. The 'nimby' phenomenon ("not in my backyard") reflects mobilisation by nearby residents. Risks may provoke wide-spread and vocal opposition, making them less acceptable to decision makers.

*Personal control* refers to the amount of influence individuals can exert over the risky situation. For example, the risk of disturbances in communication are more acceptable when the user has the ability to control the device and participate in communication, instead of having only the passive ability to listen.

*Violation of equity* occurs when the benefits and the adverse effects are unevenly distributed. Opposition will be strong if the beneficiaries do not experience adverse effects at all.

*Voluntariness* is related to personal control. For example, people can choose whether or not to use a mobile phone, but construction of a mobile antenna mast in their neighbourhood is imposed upon them. Lack of voluntariness makes risks less acceptable.

### 6.3.3 Review the shortlist

The analysts must review each risk on the shortlist, to determine whether social risk factors may have a significant impact. This consists of the following steps:

1. Predict in what forms the risk factor would be expressed for various external stakeholders. For example, would it lead to a tarnished public image, reduced funding, or perhaps active opposition?
2. Assess the influence that this would have on the ability of decision makers to defend their choice of risk treatments. Can they easily deflect criticism, or will they be forced to select an alternative treatment?
3. Assess how the influence of the risk factor could be mitigated in advance, for example by informing stakeholders in advance, ask for their approval, or having them participate in a monitoring and oversight body.

If necessary, risk prioritisation should be adjusted and additional or different risk treatments should be recommended.

## 6.4 Prepare final report

The analysts have now collected all information for the final report. Not only can they present a prioritised shortlist of most serious risks with treatment recommendations, but they can also provide arguments for their proposals.

This final report must be reviewed by all analysts, and it must be approved by consensus before it is presented to the sponsor. The study is thereby concluded. A suggested outline of the final report is shown below.

1. Executive summary to the final report.
2. About the case organisation (internal scope):
  - a. Position within wider system of stakeholders.
  - b. Tasks.
  - c. Responsibilities.
  - d. Telecom services used, together with their role and purpose.
  - e. Main actors.
3. About the environment of the case organisation (external scope):
  - a. Disaster scenarios.
  - b. External parties with whom the main actors may communicate.
4. Roles and stakeholders
5. Telecom services
  - a. Diagram with explanation (once for each service)
  - b. Important risks (single failures and common cause failures)
6. Risk shortlist, with for each risk:
  - a. Description
  - b. Relevant social risk factors
  - c. Justification for risk priority, uncertainty, and limits to knowledge
  - d. Recommended risk treatment
7. Conclusions and recommended actions

Appendices:

1. Glossary
2. Reports of single failures
3. Reports of common cause failures



# 7 Executing the Raster method

*Practical guidelines for execution of the Raster method.*

## 7.1 Team composition

The execution of the Raster method is a project that requires a suitable project leader. The project leader should possess the following skills:

- able to effectively lead project meetings.
- ample experience with the Raster method.
- sufficient knowledge of IT and telecommunication technology.

In project meetings, the project leader ensures that each participant receives opportunities to contribute, and that all points of view are discussed. When necessary, the project leader queries statements, to improve on opinions and assessments. The project leader does not have to be a telecommunication expert, but should possess sufficient knowledge of IT and telecoms to lead the discussions. The project leader can participate as one of the analysts, or concentrate on managing the project.

Three factors influence the choice and number of analysts.

1. To apply the Raster method to an organisation, expertise from various fields of study is essential. Analysing threats to telecom service components requires in-depth knowledge of telecoms engineering, crisis management, political and legal issues, and the preferences of external stakeholders. No analyst can be expected to be expert in all these fields.
2. Raster requires analysts to make assessments about uncertain scenarios, often without access to all desired information. This inevitably means that assessments are partly subjective. By including several analysts from different backgrounds, the amount of subjectivity can be kept in check.
3. Several steps in the Raster method call for consensus. When the group becomes too large, reaching consensus will be time consuming.

These factors indicate that the group of analysts should not be too small, but also not too large. The group should include experts from different fields and backgrounds, and should not exceed 10 persons.

Before a Raster project can start, an introductory session should be held in which the project leader shows the key activities using a small mock-example.

It is often useful to use a *core team*. The core team consists of the two or three most experienced analysts, plus the project leader. The responsibility of the core group is to execute most of the operational tasks, so that the other analysts can restrict their involvement to providing their specific knowledge.

During stages 2 and 3 one of the analysts should be appointed as recorder. The responsibility of the recorder is to record the diagrams and the assessments of vulnerabilities to components using the Raster tool. The recorder should use a computer connected to a projector, so that all analysts in the room can view a common, central display of the tool. The project leader may perform the recorder role.

Because the recorder notes all assessments, he or she will be the best placed to detect inconsistencies in assessments. The recorder should take special care to notice inconsistent scores between components, and bring these up for discussion. For example, if some vulnerability is scored as Medium in one component but as Low in another, similar component, the group should discuss whether one of these scores may have to be adjusted.

In follow-up sessions the recorder may find it useful to distribute printouts from the Raster tool for reference.

## 7.2 Stage 1 — Initiation and preparation

If a core group is used, the core group will take care of Stage 1. The results are then presented during the first project meeting, so that the other analysts can contribute.

## 7.3 Stage 2 — Single failures analysis

Most commonly, the analysis cannot be completed in a single work session. To make the most effective use of the expertise of the analysts, the project leader decides which telecommunication services and components are examined in the project meetings. The goal is to discuss as many points of view as possible, in order to understand each others arguments for frequency and impact assessments. Based on this insight, the core group can then examine and assess the remaining components. Those results are then presented during the next meeting, and discussed briefly. Then the single failures of the next batch of components are discussed. This procedure is repeated until all single failures are assessed. It is not unusual that two to three project meetings are needed.

In the assessments of frequency and impact, already implemented risk treatments are taken into account. Existing measures may reduce the frequency of vulnerabilities, their impact, or both. Because of a backup power generator, for example, power supply will fail less often. The use of a smart phone cover will reduce the possibility that a smart phone is physically damaged. The generator and the cover will not prevent the loss of external power or dropping of a phone, but help to prevent it from leading to an incident, which is the meaning of Frequency.

Impact is reduced by measures that provide alternatives, or backup options. For example, a stand-by server that takes over from the main server when it fails. Or the use of two cable connections, so that in case of a cable break service continues at half capacity.

During assessments it is of prime importance to keep the definitions of frequency and impact classes in mind. The precise definition of the various vulnerabilities must be used consistently as well. The recorder or project leader must monitor consistency.

The following clarifications to the standard vulnerabilities may be useful. Suggestions for additional vulnerabilities are provided as well.

### 7.3.1 Wireless connections

Examples included mobile telephony (GSM, UMTS, LTE), WiFi, cordless DECT telephones, bluetooth, wireless audio and video connections, access cards for electronic locks, two-way radios and remote controls.



*Interference.* Unintentional interference by a radio source using the same frequency band. WiFi, for example, can be disturbed by other transmitters in the same frequency band, or even by a badly shielded microwave oven. Interference is often unpredictable, and of short duration.

*Jamming.* Intentional interference by a third party. For example, someone deliberately tries to disrupt mobile telephony. Jammers are sometimes used by criminals to prevent tracing and detection. Jamming may last for a long time, and is often difficult to locate and remove.

*Congestion.* The amount of traffic offered exceeds the capacity of the link. WiFi connections can become very slow on busy locations; mobile telephony can become troublesome when a large group of people start calling or use social media simultaneously, for example during a festival or an incident. Congestion is often brief, but can persist during large incidents.

*Signal weakening.* Loss of signal strength through distance or blocking by buildings, trees, etc. In modern buildings mobile signal strength is often low, due to thin metal foil in insulating glazing. In basements or underground parking lots the use of mobile phones and two-way radios may be impeded by weak signals. Often users know at which locations they can expect signal weakening.

### 7.3.2 Wired connections

Indoor examples include cords, network cables and patch cables. Outdoor examples include fiber optic, coax or traditional copper cables running above ground or below ground. Wired connections do not include power cords; vulnerabilities to power cords are included in equipment power loss.

*Break.* Cable damaged by natural events, trenching during construction work, anchors (for marine cables or cables under rivers or canals), weak contacts (corrosion, loose connectors) or other external influences. Especially for patch cables it is common that the wrong cable is unplugged during maintenance. This type of mistake can also be included in cable breaks.

*Congestion.* The amount of traffic offered exceeds the capacity of the link. This vulnerability is similar to congestion on wired links. Base your assessments on the true capacity, not on theoretical capacity. Fiber optic cables can handle enormous throughput, but when a contract for 2 Mbps has been agreed with the supplier, the data speed will be limited to 2 Mbps. Often the impact of congestion is noticeable at 50% load. An example of congestion is the scenario whereby all office PCs simultaneously attempt to download their monthly patches.

*Cable aging.* Insulation weakens with age. This is an issue mostly with outdoor cables that are exposed to the elements. Cable ageing expresses itself in noise or disruptions. A cable that gets cut and disconnected due to ageing is considered a cable break instead.

*Additional vulnerabilities.* Some cables are susceptible to electromagnetic interference, meaning that the cable acts as an antenna to nearby transmitters or other equipment.

### 7.3.3 Equipment

*Physical damage.* Fire, flood, water from fire fighters, knocks and other physical damage inflicted. Physical damage involves unusual external influences. For example,

a user drops his mobile phone or radio, a cup of coffee is spilled over a laptop, or the automatic fire sprinklers are activated.

*Power.* Failure of electrical power supply. For battery-powered devices this means that the battery is empty. If backup power is available, the frequency of power failures is reduced; because of the backup, the power supply to the device is not cut. A power incident only occurs when also the backup power cuts out. A defect in the power supply unit inside a device can be considered as power failure, not as Malfunction. Accidental switch-off and accidental unplugging of the power plug can be considered power failure, not as Configuration error. The vulnerability of power failure can be removed when the device does not have a power cord nor battery. This applies, for example, to WiFi access points or IP phones that use Power of Ethernet (PoE).

*Configuration.* Incorrect configuration or mistakes by operators or users. Examples include hardware configuration (switches, volume controls) or software configuration. Devices can be configured by the end user, by an IT department or an external service organisation. Complex devices such as smart phones or laptops contain many settings that can possibly be misconfigured by end users, causing malfunction of the device. The IT department may roll out a faulty patch to PCs under their control, causing malfunction of all office computers. A mobile two-way radio can be set to the wrong channel, or its volume can be dialled down, causing a message to be missed. Unintended switching off of devices is most commonly regarded as Power failure. Only the most simple devices do not have configuration settings. Sometimes devices are set up once before deployment, and never reconfigured thereafter. For these devices the vulnerability Configuration can be removed too.

*Malfunction.* Failure of an internal module without a clear external cause, possibly by aging. Malfunction involves failures without an apparent cause; devices have a limited lifetime. Even new devices can fail within their warranty period. Malfunction and Physical failure are similar, and their impact will often be identical. Their frequencies typically differ.

*Additional vulnerabilities.* At some locations theft is an issue. Some devices are more attractive to thieves than others. Overheating may be an issue. If the environmental controls fail in a large data centre, the consequences will be high. Also, like wired connections devices can be susceptible to electromagnetic interference.

## 7.4 Stage 3 — Common cause failures analysis

The following information may help with choosing the critical property and the classification of components into clusters. Each cluster has a corresponding story or failure scenario. For example: “when the power fails in this room, all these devices will stop functioning”. Creating such stories makes for a good check; if you cannot think of a plausible story, the cluster classification is probably incorrect.

### 7.4.1 Wireless links

*Interference.* The critical property is the frequency band, together with geographical proximity. For two wired links to be affected by the same radio source, that source must be transmitting on a near frequency, and be relatively close.

*Jamming.* Most jammers operate on a single frequency band. Because the use of a jammer is intentional, the motive of the person jamming is relevant. Most jammers have a limited range. Clusters can be organised based on “who may want to jam communication where, and for which motive?”

**Congestion.** Congestion is mostly temporary. When there is a high amount of activity in the neighbourhood, the mobile or private networks may become congested. Congestion may therefore affect multiple frequency bands simultaneously (GSM, UMTS and LTE, for example). Depending on the technology used, congestion may be local or affect the entire telecommunication service.

**Signal weakening.** This vulnerability is mostly limited to mobile devices. A common cause failure requires one person using two devices is at a spot with poor coverage (for example, using a mobile phone and a two-way radio), or that two users are at such a spot.

## 7.4.2 Wired links

**Break.** The critical property is geographical proximity; cables sharing the same location can be damaged simultaneously by external influences. Cables below the ground often follow the same route, or share a common duct underneath roads or canals.

**Congestion.** As for wired links.

**Cable ageing.** The critical property can be whether the cable is used above the ground, below the ground or indoor. If the age of the cables is known, a subdivision based on age can be used.

## 7.4.3 Equipment

**Physical damage.** For fixed equipment the critical property is geographical proximity. Mobile devices have their own cluster, with possibly subclusters for different types of users.

**Power.** For fixed equipment the critical property is geographical proximity. Mobile devices have their own cluster; subclusters can be created according to battery life.

**Configuration.** The critical property is who controls or can change the configuration settings: the IT department, an external service organisation, professional end users or common users. Computers are maintained by the IT department, but their users can often change settings (accidentally) as well. In this case, assign the device to the most vulnerably cluster.

**Malfunction.** Devices are often bought in batches. It is not impossible for multiple devices to fail (roughly) simultaneously. Age is a relevant property, but the kind of use and treatment are relevant as well. Devices that experience rough handling will have a higher probability of sudden malfunction than devices at a fixed location.

Often a single project meeting suffices, after which the core team completes the assessment of common cause failures.

## 7.5 Stage 4 — Risk evaluation

Most commonly the compilation of the longlist and reduction into the shortlist can be completed in a single project meeting. It is also possible for the core group to prepare their choice for discussion. Social risk factors must be assessed for each of the risks on the shortlist.

The collation of material into a final report can be prepared by the core team. Much of the Stage 1 report can be reused, and printouts from the Raster tool can be used for the appendices suggested in the template in section [\*Prepare the final report\*](#).

# 8 Raster tools

*Facilitate execution of the Raster method.*

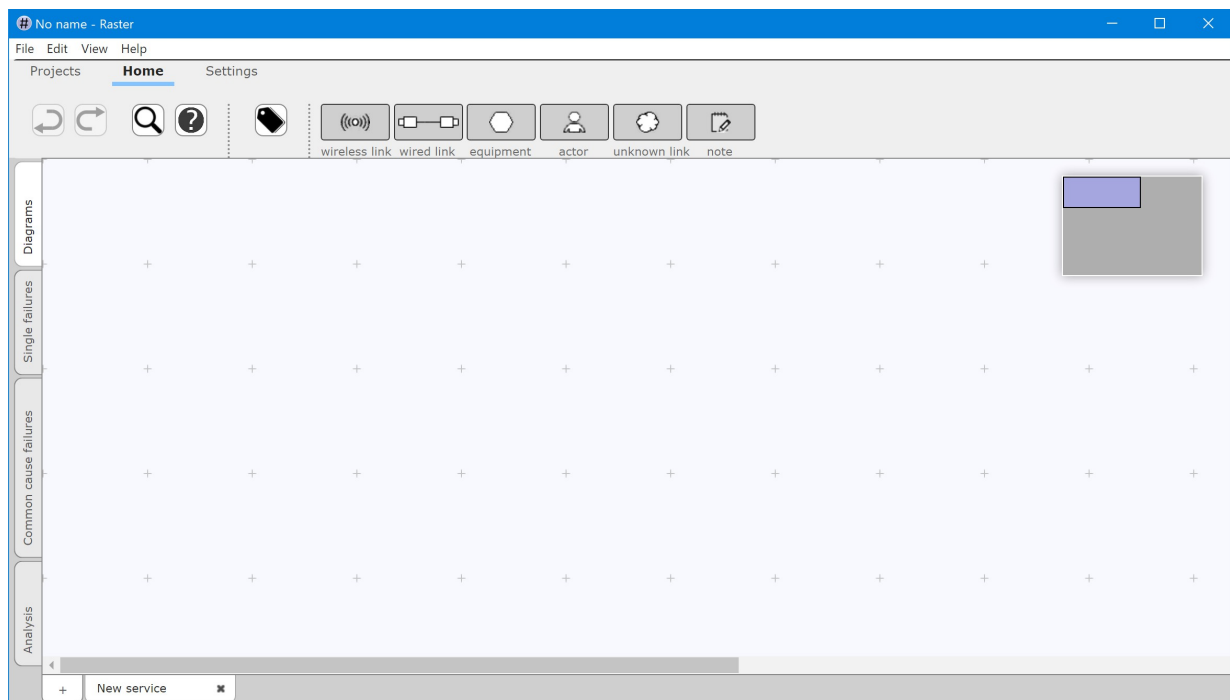
To assist in performing risk evaluations using Raster, two free tools are available. See <https://risicotools.nl/> for download locations.

The first tool is a standalone MacOS or Windows application that edits Raster project files stored on a local or network drive. The second tool is web based. It is to be installed on an intranet server and allows access to shared projects from any web browser on the local network. In both tools, a *project* contains the complete risk assessment for a single organisation. Typically, a project encompasses several telecommunication services.

With minor differences, both tools work in the same way. One major difference with the intranet tool is that multiple analysts can work on the same project simultaneously; each change is shared with other members instantly and automatically. [Working with the standalone tool](#) and [Working with the intranet application](#) describe the specifics of the standalone and intranet tool respectively. The rest of the chapter and the subsequent chapters apply to both tools.

In both tools, hovering the pointer over a button or item will usually show a popup with a brief explanation of its function.

## 8.1 Working with the standalone tool

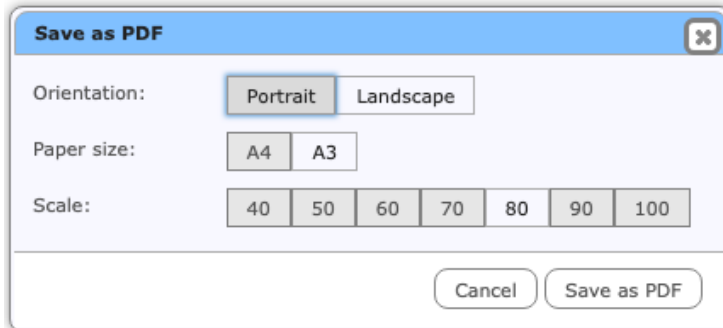


The standalone tool operates on project files stored on local or network drives. Project files are opened, edited and saved very much like how you edit text documents or spreadsheets. Pictured above is the Windows version of the tool.

### 8.1.1 File menu

The File menu is used to open, save, and print project files.

You can save your current view as a PDF file. To save a diagram, its list of single failures, the list of common cause failures, or the tables in the Analysis view, use the option “Save as PDF” in the File menu. This option will always save the current view. Your preferences from the Settings toolbar and View menu will be respected.



Before you save, review the PDF settings. You can:

- choose *orientation* (Portrait or Landscape). Landscape (wide) orientation is often best for diagrams; Portrait (tall) is often best for all other views.
- choose *paper size*. Use A3 for large diagrams, A4 for any other views.
- choose the *scale*. 80% to 100% is often best, but to fit large diagrams on a single sheet you may have to go down to 40% scaling.

### 8.1.2 View menu

The View menu is used to change layout and preferences. The first section contains the same functions as the [Settings toolbar](#): Labels, Vulnerability levels and the Mini-map. The items on the second section can also be found in the toolbars: Find (on the Home toolbar), Edit labels (on the Home toolbar in Diagrams view), Project details (on the Projects toolbar).

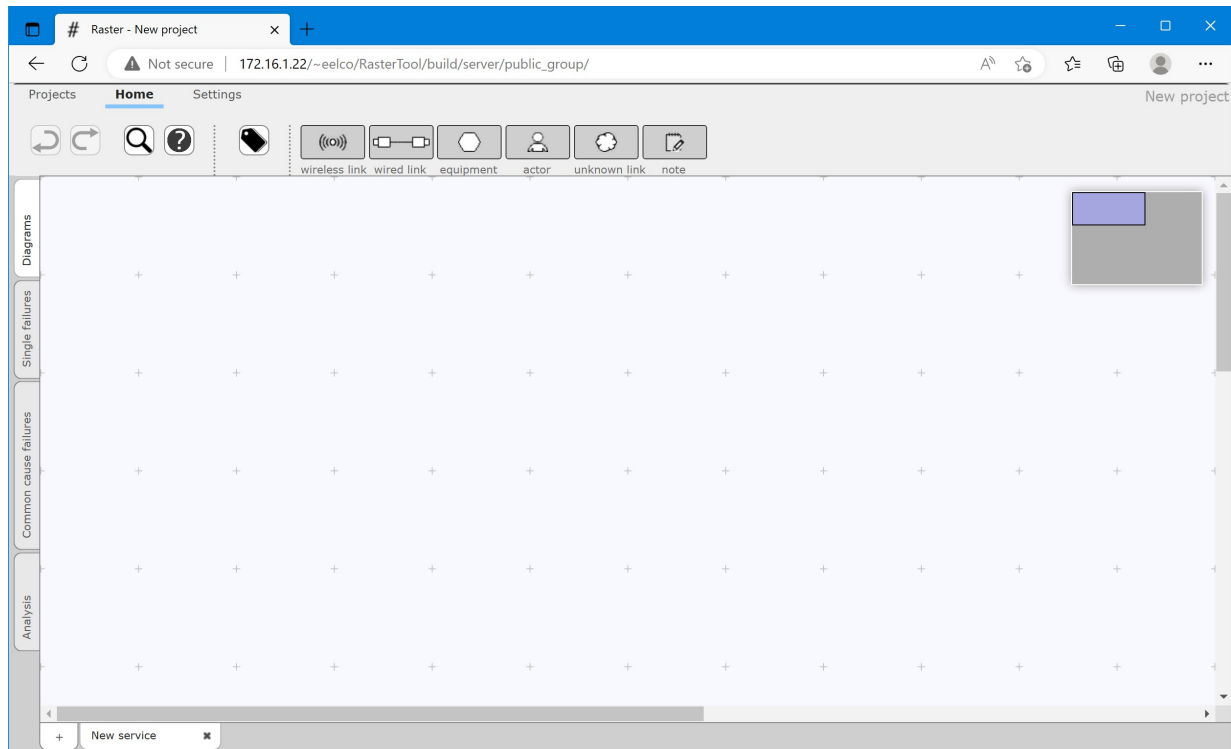
You can change:

- *Zoom*: increase or decrease the size of diagrams or text. For large diagrams it may be useful to shrink the text and images to fit more of them on the screen.
- *Full screen*: expand the tool to make it use all available screen space.

## 8.2 Working with the intranet tool

The intranet tool can handle multiple projects, but only one can be active at any time. Multiple analysts can work on the same project simultaneously; each change is shared with other members automatically.

Pictured below is the intranet tool, running in Edge.



The editing that you perform is recorded instantly. This means that if you close your browser window none of your work is lost. When you visit the tool's URL again, the state of your workspace will be fully restored. It is therefore also not necessary to save your work, or to open a file before commencing work.

### 8.2.1 Private and shared projects

Projects can be private or shared. *Shared projects* can be edited by multiple people at the same time. Any changes you make to a shared project are immediately propagated to all other people currently editing the same project; any changes that they make are immediately reflected in your own browser.

*Private projects* are not visible to other people, and are never stored on the server. When you work on a private project and visit the tool's URL from a different machine, or even using a different browser on the same machine, your previous work is not restored. This does not mean that your work is lost; it is tied to one particular browser. To transfer a private project between machines or browsers, or if you wish to share your projects with a co-worker, you must export that project. By exporting, all data of the project is saved into a project file, which can then be stored and transferred as any other file. Exporting is explained in [The Project toolbar](#). Likewise, such a project file can be imported using the Import function. After importing, any changes will again be recorded instantly. However, they will not affect the file; the file is not modified until you decide to export again.

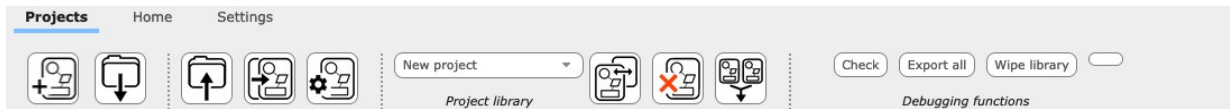
## 8.3 Toolbars

At the top there are toolbars to control the tools: [Projects](#), [Home](#) and [Settings](#).

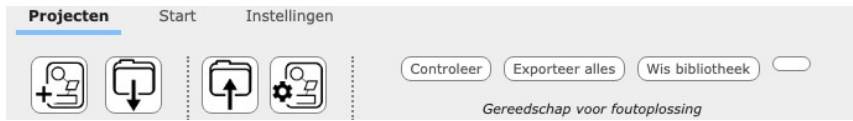
### 8.3.1 The Projects toolbar

Use the Project toolbar to add, remove, modify and swap between projects. The intranet tool and the standalone tool have slightly different toolbars.

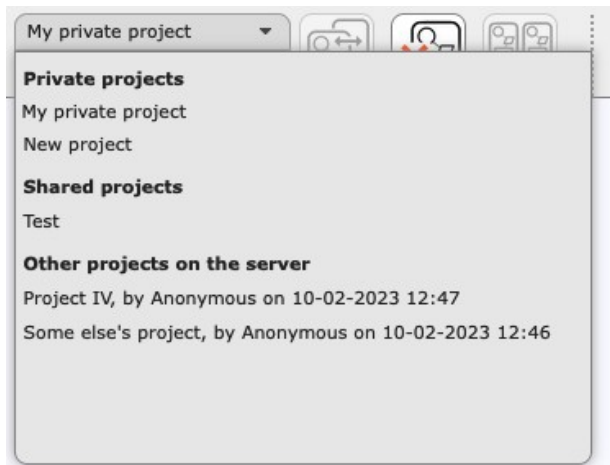
For the intranet tool:



For the standalone tool:



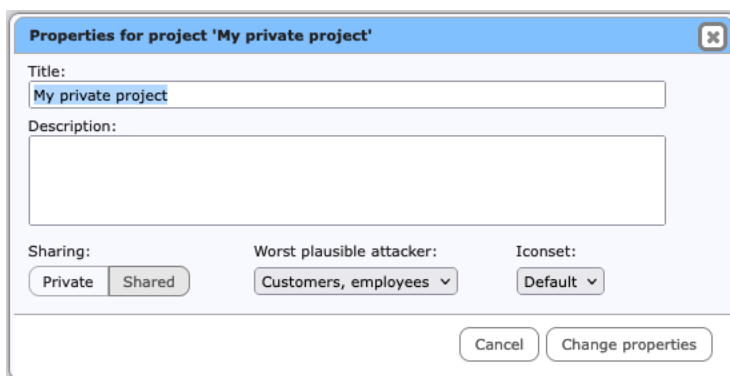
The *Project library* shows a list of all projects that are currently available for viewing and editing. The list of projects is divided into three sections: your private projects, shared projects that you have worked on, and other shared projects.



The selected project can be acted upon using the three buttons to the right. You can:

- *activate* the project, to start viewing and editing it.
- *remove* the project.
- *merge* the project into the currently active project. All services of the highlighted project will be re-created as services of the active project.

The project properties allow you to change important aspects of your project.



- change the *name* or *description* of the project.
- change whether the project is *private* or *shared*; see [Private and shared projects](#)
- set the *worst plausible attacker* for cybersecurity vulnerabilities. See XXX
- change the *icon set* for the project.

Icon sets contain graphical representations of components in your diagrams. By default the icon sets Classic and Default will be installed. You can create your own icon sets, or extend the predefined ones (see XXX).

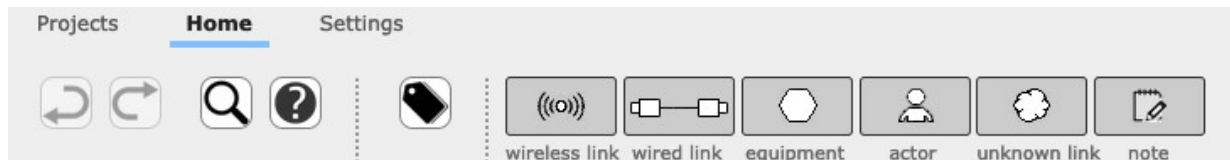


The Projects toolbar may contain functions for debugging. These are temporary, and can be ignored.

### 8.3.2 The Home toolbar

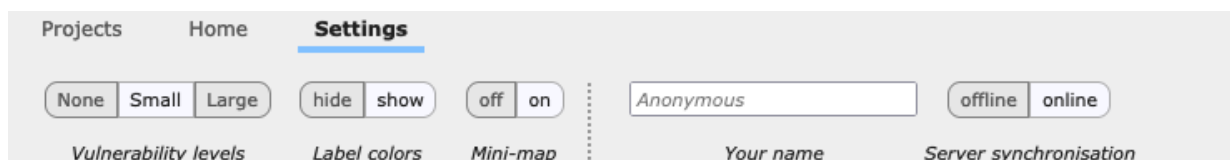
The Home toolbar is used for editing and viewing information. It is the same for the intranet and standalone tools. The first section is fixed, and contains the Undo, Redo, Find and Help buttons.

The second section contains buttons for each of the four views. Below is the toolbar for Diagrams view.

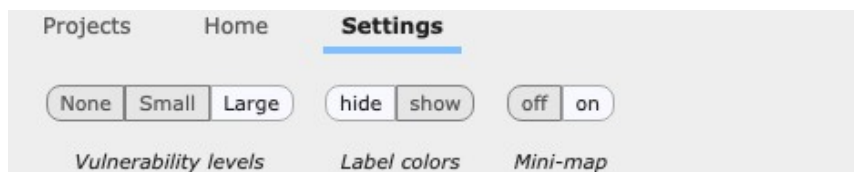


### 8.3.3 The Settings toolbar

The Settings toolbar provides settings and other preferences. The one from the intranet tool is below.



The standalone tool has a smaller toolbar.



- **Vulnerability levels:** The size of the vulnerability level indicators (see [Diagram nodes](#)) can be switched between large and small, or they can be hidden entirely.
- **Labels:** The colours that are associated with labels can either be hidden or shown. When hidden, nodes are always painted in plain black and white, as if no label was assigned to them. Hide the label colours when you find this too distracting, or before printing to a black and white printer.
- **Minimap:** Hide or show the minimap during editing or before printing.

The preferred size of the vulnerability level indicators and the label colours also affect printing.

The intranet tool has two extra settings.

- **Your name:** The server stores the name of the last person to modify a shared project, together with the date of modification. Enter your name here; this is purely informational.
- **Network connection:** The network connection to the server is normally automatically set to either offline (disconnected) or online (connected). You can (re-)enable communication with the server by switching to online.

## 8.4 Printing

You can print a diagram, its list of single failures, the list of common cause failures, and the tables in the Analysis view. The print view looks very different from the normal screen display; the tabs, buttons and other user interface elements will not show up in the printed document.

When using Firefox, the mini-map is reset to the top-left position and single or common cause failures are expanded just before printing. With other browsers, you may have to do this manually. You can use the “Expand all” function before printing.

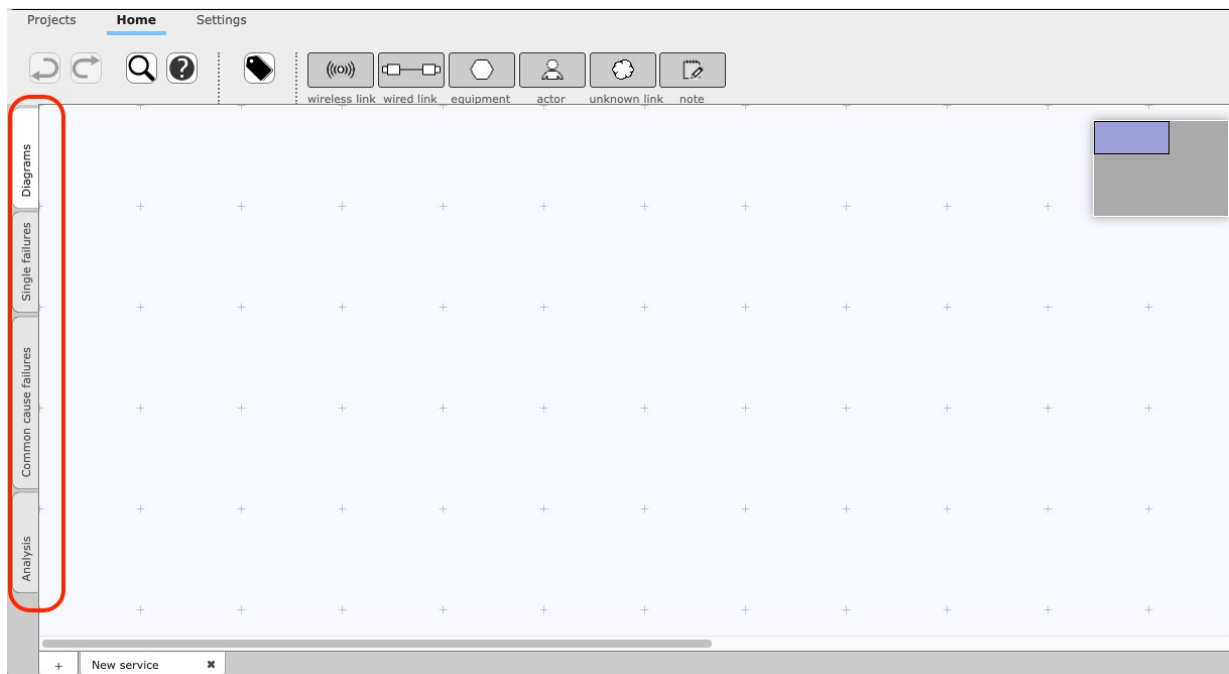
When printing the diagrams, it is best to set the paper size to A3 and landscape orientation. A4 paper may suffice for smaller diagrams. The Single Failures and Shared Failure views are best printed using portrait orientation. You may need to shrink the printout to make it fit the paper, using the printing features of your web browser.

Make sure that the printing of background colours is enabled in your web browser, otherwise the risk classification indicators will all show as white. The option to print background *images* is not relevant; the printed document does not contain background images.

You can use the [Settings toolbar](#) to set the size of the vulnerability level indicators and choose whether label colours are printed. These settings apply to both the printed and the on-screen version of the intranet tool.

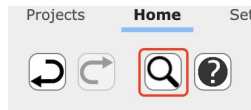
## 8.5 Main views

Both the standalone tool and the intranet tool are divided into 4 main views, indicated and selected by the vertical tabs on the left-hand side.

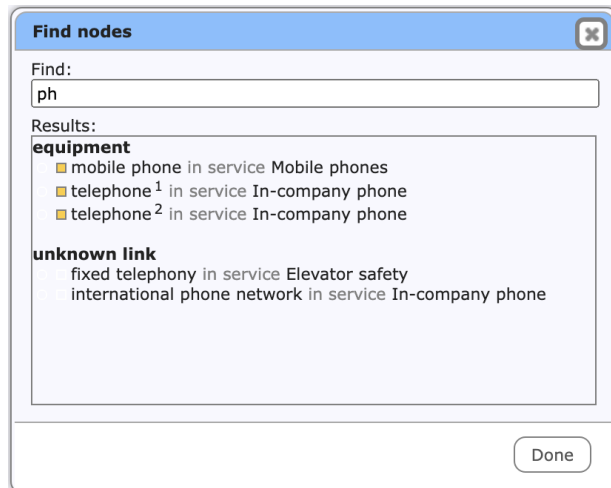


1. [Diagrams view](#) is used to draw and edit diagrams of telecom services.
2. [Single failures view](#) is used to assess failures of individual elements.
3. [Common cause failures view](#) is used to assess common cause failures.
4. [Analysis view](#) is used to view reports on completed diagrams, and to see the effects of individual vulnerabilities on overall vulnerability levels.

## 8.6 Find nodes



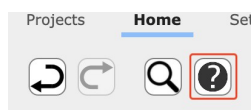
When diagrams get larger and the number of diagrams increases, it can become more difficult to remember in which service nodes are located, and what their names were. Use the looking glass icon to call up a search window.



Search results will be presented as you type. The overall vulnerability level (when available, as a coloured square) and label colour (if set, as a coloured circle) will be shown.

Click one of the search results to reveal that node in the diagram. The tool will jump to the diagram view and will mark the node using a frame.

## 8.7 Help window

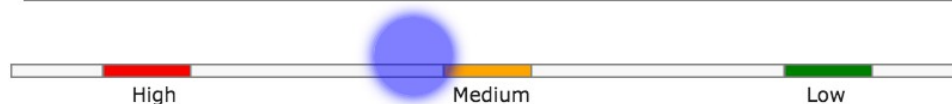


The Help window shows the definitions of the Frequency and Impact classes, and provides tips and other information on the tool. Open the Help window using the question mark button.

Since it is important that the definitions of the classes are applied consistently, it is useful to have this reference close at hand.

Assessing Frequencies may be challenging for the analysts. The Help window therefore offers a calculation tool.

I have  identical nodes, and  
 every  week  
 are affected.



If the organisation deploys 60 tablets, of which two fail each year, then the calculator helps to determine that this poses a Medium frequency.

## 8.8 Colour codes

In several locations colours are used to indicate the overall vulnerability level for a node. If size permits, a letter is also shown. The following letter and colour combinations are used:

- Not yet analysed, no assessment has been done yet (white)
- A Ambiguous, the assessors have conflicting opinions (purple)
- V Extremely (very) high, an extreme risk (bright red)
- H High (red)
- M Medium (yellow-orange)
- L Low (green-orange)
- X Unknown, because of lack of knowledge (sky blue).
- U Extremely (*ultra*) low, the risk level is negligible or absent (bright green)

## 8.9 Keyboard shortcuts

### *General shortcuts*

Ctrl-Z	Undo
Ctrl-Y	Redo
Ctrl-Shift-Z	Redo
Ctrl-F	Open the <a href="#">Find window</a>
Ctrl-L	Open the <a href="#">label window</a>
F1	Open the <a href="#">help window</a>
Ctrl-1	Go to <a href="#">Diagrams view</a>
Ctrl-2	Go to <a href="#">Single failures view</a>
Ctrl-3	Go to <a href="#">Common cause failures view</a>
Ctrl-4	Go to <a href="#">Analysis view</a>
tab	Cycle between toolbars

MacOS-users can use the Cmd key instead of the Ctrl key.

### *Shortcuts for nodes on the Diagrams view.*

<	Label the node with the previous label from the list (see <a href="#">Node labels</a> ).
>	Label the node with the next label from the list (see <a href="#">Node labels</a> ).
F2	Rename the node, or edit the note.
Delete, Backspace	Remove the node.
Enter, Return	Open the <a href="#">vulnerability assessment window</a> , or edit the note.

## 9 Diagrams view

Create telecom service diagrams.

The centre of this area is occupied by the workspaces in which telecom service diagrams are drawn. Below this area is a row of tabs, to create an additional service and to switch between services. Above this area you find buttons to activate the Library and Options panels, a row of templates, and the name of the active project.

### 9.1 Templates



Templates contain default settings for new diagram nodes. You create new nodes by *dragging one of the templates* into the workspace.



For the first three elements (wireless links, wired links, and equipment items), you can modify the predefined checklists. Click the edit indicator (the box with three dots) to open the checklist window for that element type.

### 9.2 Checklist windows

Common vulnerabilities for all nodes of type 'wired link'			
+ Add vulnerability			
Cause	Name	Description	
	Break	Cable damaged by natural events, aging, trenching, anchors, or other external influence.	⊗
	Congestion	The amount of traffic offered exceeds the capacity of the link.	⊗
	Denial of service	Intentional congestion (DDOS).	⊗

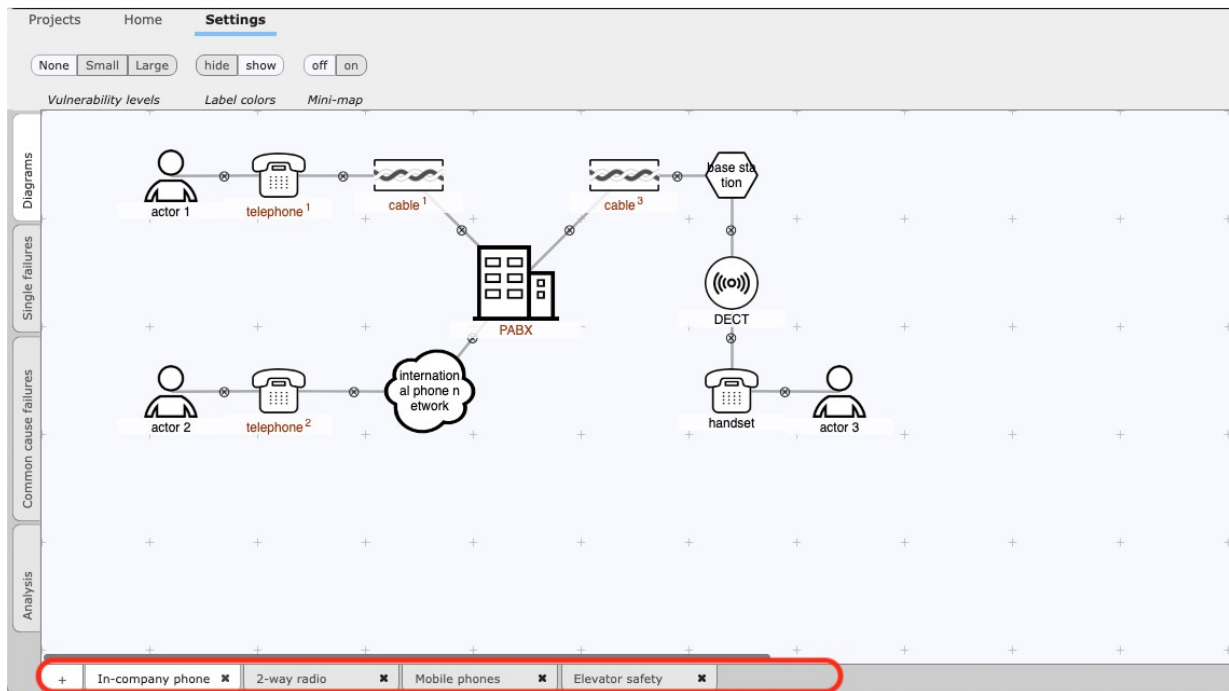
Wireless links, wired links, and equipment items each have a list of common vulnerabilities. These vulnerabilities apply to all nodes of that type. In the checklist window you can:

- *modify* the name or description of a vulnerability by clicking that item (press Enter/click elsewhere to confirm, press Escape to cancel)
- modify the type between *natural* and *malicious* using the icons on the left.
- *remove* a vulnerability, by clicking the minus-button on the right.
- *add* a new vulnerability, by clicking the “+ Add vulnerability” button.
- *reorder* the vulnerabilities, by dragging them into the desired order.

Any changes you make will affect all current and future nodes as well.

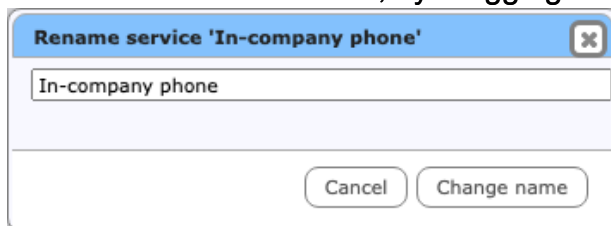
## 9.3 Service tabs

The workspace is the areas where the diagrams for telecommunication services are drawn. A project consists of one or more services. For each service, you can draw a telecom service diagram, and perform vulnerability assessments on nodes.



Each service has a tab at the bottom of the screen. You can:

- **remove** a service, by clicking the close (“cross”) button on its tab. Note that you cannot remove the last service of a project. If you try to, the workspace will flash briefly.
- **add** a new service to the active project, by using the plus-button.
- **rename** a service, by *double-clicking* its name. The popup window shown below allows you to enter the new name.
- **re-order** the services, by dragging the tabs into the desired order.



## 9.4 The mini-map



The workspace onto which nodes are drawn and connected, is larger than can be displayed on the screen. Use the mini-map to change the current view. The large grey area of the mini-map represents the total available workspace, while the smaller blue

rectangle corresponds to the area that is currently visible (the workspace). Each red dot is one of the nodes in the diagram. Each red dot outside the blue rectangle indicates a node that is currently not visible.

Drag the visible area, by dragging the blue rectangle around. Or move the mini-map itself when it gets in the way, by dragging the grey rectangle around. You can also [switch the mini-map off](#) on the Settings toolbar.

When your diagram gets large, you can use the Zoom In, Zoom Out functions of your browser to fit more of the diagram onto the screen. The View-menu of the standalone tool also contains a Zoom function.

## 9.5 Diagram nodes

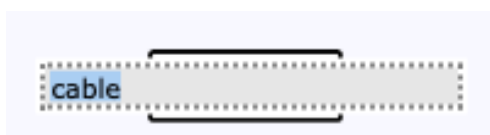
You create new diagram nodes by dragging them from the templates at the top of the screen. Each node is visually represented as a shape with its name inside or below, and up to five decorations that will become visible when you approach the node with the mouse.. Clockwise, starting from the top left corner:



1. The *warning triangle* in the top-left corner indicates that the node has too few or too many connections. View the warning report, by clicking on the warning triangle.
2. The *vulnerability level indicator* in the top-left corner indicates the overall risk level for that node, using a colour. You can [change the size](#) of the vulnerability level indicator.
3. The round *connector* at the top middle is used to link nodes together.
4. The *drop-down indicator* in the top-right invokes a menu with actions.
5. The *resize indicator* in the bottom-right allows the size of the node to be adjusted.

Move the node to another location on the workspace by dragging it around.

There are two ways to move more than one node at the same time. Hold the shift key while dragging a node to move all nodes in the diagram. Alternatively, [create a selection](#), and drag the selection rectangle to move the selected nodes only.



Rename a node by clicking its title. Note that the area becomes blue when you hover the pointer over the title. Confirm by clicking somewhere outside the workspace, or press Enter. Cancel the action (that is, revert to the current title) by pressing Escape.

## 9.6 Node classes



Nodes that are very similar can be made into a *node class*. Node classes are marked by a dark red colour. All nodes of a class share a single assessment of vulnerabilities. To be able to distinguish individual nodes in a class, each node is automatically assigned a letter, shown to the right of the name. This letter can be changed to something more meaningful using the “Change suffix” option of the node menu.

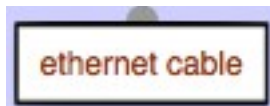
You create a node class by giving one node the same name as another node of the same type. Both nodes will be put into the class. You can add as many nodes as you need, again by renaming nodes to the name of the class. Node names are case-insensitive. This means that “internal cable” and “Internal Cable” represent the same name, and therefore form a node class.

**Warning:** by placing a node in a node class you discard all vulnerability assessments of that node. The node will adopt the vulnerability assessments of the class.

Note that a node class can span more than one service; nodes of the same class can appear within more than one service (of the same project). There are no actor classes.

When a member node of a node class is renamed, it will cease being a member and will become an individual node again. To rename all members of the node class collectively, use the “Rename class” option of the node menu.

## 9.7 Identical nodes



Within a service each physical component can only appear once. The same physical component may however appear in two different services. To indicate this, use the following procedure.

First, create a node class by giving the nodes the same name in each service diagram. Then, to mark the node class as a single physical component instead of two similar “copies”, use its popup menu item “Make single”. Note that the title of single nodes is still shown in red, but that the superscript letter is omitted.

‘Make single’ can only work when the nodes in the class are in separate services. When the node class has more than one node in a service, the node will flash to indicate that it cannot be converted to a single node.

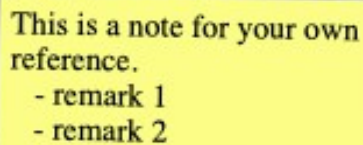
To revert to a node class, use the popup menu item “Make class” on a single node.

## 9.8 Notes



For your convenience notes can be added to a diagram. You add a note by dragging its template onto the workspace, just as you do for diagram nodes.





This is a note for your own reference.

- remark 1
- remark 2

Notes can contain any text. You can resize notes, change their text, duplicate them, delete them, and label and colour them in the same way as for diagram nodes. The text of notes cannot be marked up (bold, font sizes, etc).

## 9.9 Connecting nodes

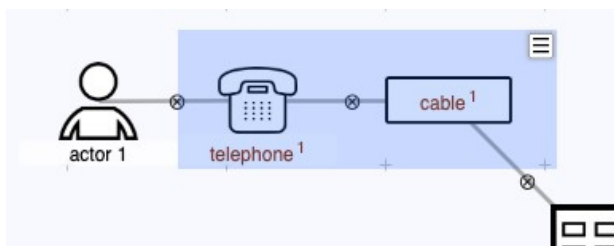
Nodes can be connected by dragging the connector (the round decoration at the top of the node) onto another node. If no connection is possible (for example, actors cannot be connected directly to a wireless link), both nodes will flash briefly and no connection will be made. With connections you can:

- *connect* the node to another node, by dragging from its connector at the top. The connector will enlarge when the mouse pointer hovers over it.
- *disconnect* two nodes, by clicking its disconnect button. The disconnect button appears in the middle of the connection when you approach it with the mouse.

Connections cannot be moved; they automatically follow the two nodes that they connect.

It is possible to have more connections than allowed by the connection rules for that node type (see [Telecommunication service diagrams](#)). This may be useful during editing. You will need to remove extra connections later on, for the diagram to be valid. Meanwhile, the node will show a warning triangle.

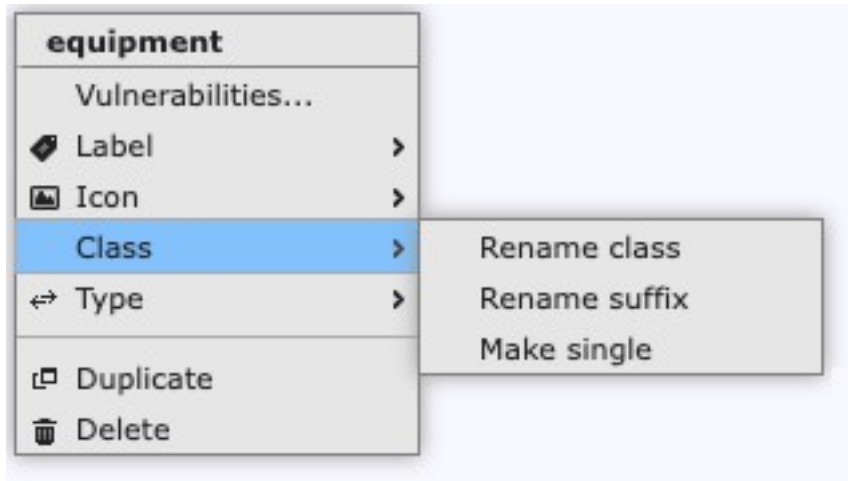
## 9.10 Selecting nodes



A set of nodes can be selected, and moved or deleted as a group. Click and drag anywhere on the workspace outside a node to create a selection. While dragging, a blue rectangle indicates the current selection. Move all nodes in the selection by dragging the selection rectangle itself.

Call up the selection menu using the menu indicator in the top-right corner, or by clicking the right mouse button. Use the menu to delete all nodes in the selection, or to label them collectively.

## 9.11 The node menu



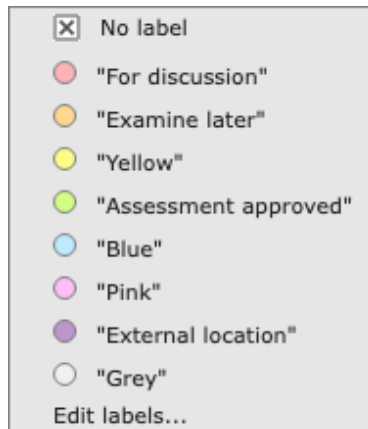
The popup menu allows several operations to act on a node:

- *call up* the [vulnerability assessment window](#).
- *label* the node, using one of the 8 [available labels](#).
- change the *icon* of the node, depending on the current [icon set](#).
- For nodes that belong to a node class:
  - *change the name* of all nodes in the node class. Renaming a single member will make that node fall out of the node class. Use this menu item to rename all member nodes collectively.
  - *change the suffix* from the default of a single letter ('a', 'b', 'c', ...) to something more meaningful, such as an abbreviation of the location of the component.
  - *change* the type of the node class from a single identical node into a collection of similar nodes, and vice versa (see [Identical nodes](#)).
- *change* the *type* of the node (e.g. from a wireless link into a cloud).
- *duplicate* the node. This will create a node class.
- *delete* the node.

Changing the node type can be used to correct a mistake, for example to convert an equipment item into a cloud, if you notice during your analysis that the situation is more complex than you previously thought. Note that the vulnerability assessments will not be preserved when changing the node type. Typically, it is not possible to preserve vulnerability assessments, as nodes of different types tend to have very different default vulnerabilities.

Changing the type to something different and back again is a quick way to reset all vulnerability assessments for that node.

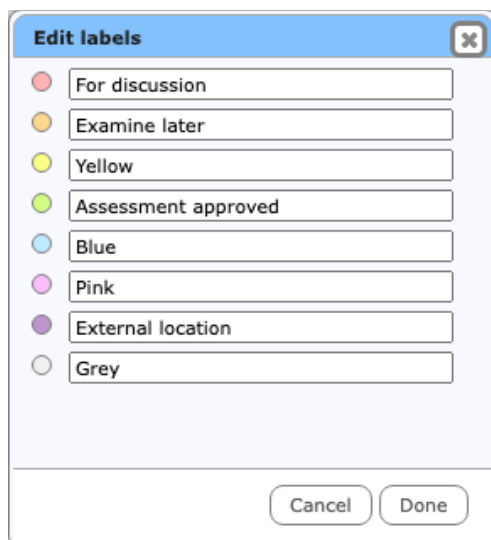
## 9.12 Node labels



You can use labels to organise nodes. For example, you can label nodes to mark them as 'under review' or to record additional information that is not normally part of the diagrams, such as ownership, responsibility or physical location. Each label is visually indicated in the diagrams using a colour (to disable this, use the setting in the [Settings toolbar](#)). Note that these colours have no relation with the colours that are associated with vulnerability levels.

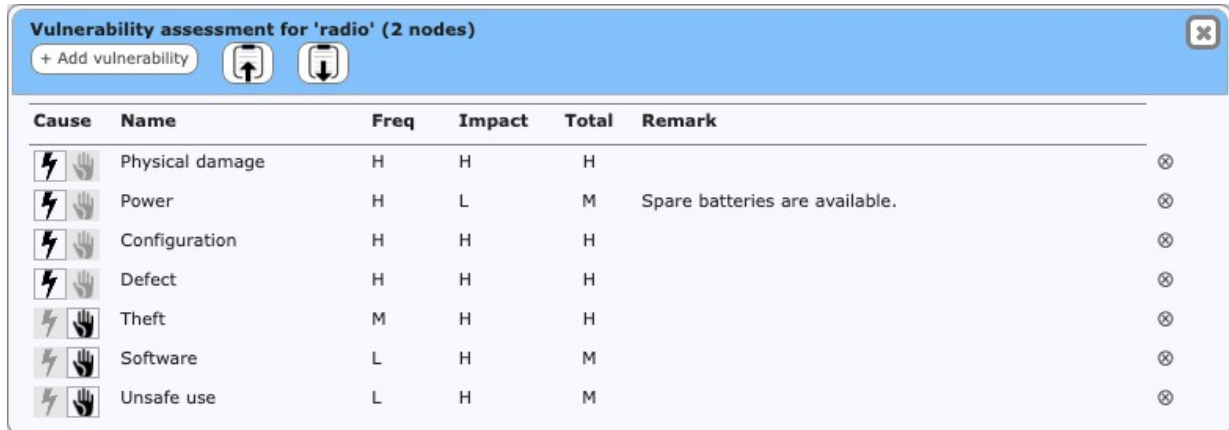
To assign a label, choose one from the Label submenu. To remove the label, choose "No label" from that menu. A node cannot have more than one label.

Labelling nodes is also very useful when clustering nodes in common cause failures view (see [Create clusters](#)).



The labels themselves are pre-set to the names of their colour, but can be changed by choosing "Edit labels..." from the node menu, or using the Label button on the [Home toolbar](#). Reset a label to its default value by making it blank.

## 9.13 Vulnerability assessment window



Cause	Name	Freq	Impact	Total	Remark	
	Physical damage	H	H	H		
	Power	H	L	M	Spare batteries are available.	
	Configuration	H	H	H		
	Defect	H	H	H		
	Theft	M	H	H		
	Software	L	H	M		
	Unsafe use	L	H	M		

The vulnerability assessment window is called up using the node menu on diagram nodes (except actors). In the vulnerability assessment window, you can add, remove, and assess vulnerabilities to the node. In this window you can:

- *rename* a vulnerability, by clicking its title (press Enter/click elsewhere to confirm, press Escape to cancel). The name change will apply to all other nodes and (if applicable) to the checklist as well.
- modify the type between *natural* and *malicious* using the icons on the left.
- *add* or *edit* remarks. Remarks are very useful to explain why this particular assessment was chosen.
- *reorder* vulnerabilities, by dragging them into the desired order.
- *change* frequency and impact. Click to activate the selection widget. Click the widget to open it, or type the letter of your choice.
- *remove* a vulnerability, by clicking the minus-button on the right. See the warning in [Adding and removing vulnerabilities](#) about removing vulnerabilities.

Using the buttons in the toolbar, you can:

- *add* a new vulnerability, by clicking the “+ Add vulnerability” button.
- *copy* all vulnerabilities onto a clipboard, using the Copy button.
- *paste* a previously copied set of vulnerability assessments, using the Paste button.

Be careful when pasting vulnerability assessments; these three rules are used:

1. Vulnerabilities that were present (based on their name) in the source as well as the destination will be combined.
2. On combination, if the probability or impact has been set in both the source and destination, the worst value will be used.
3. Any vulnerabilities listed in the source but not yet present in the destination will be created.

It is not yet possible to add/edit descriptions for vulnerabilities, other than using the checklists.

# 10 Single failures view

Assess single failures to components.

In the “Single failures” view you can assess all vulnerabilities that affect a single node. This offers similar functionality as the vulnerability assessment window in the diagram workspace, but shows the assessment of more than one node.

## 10.1 Service tabs

The screenshot shows the 'Single failures' view in a software application. The interface includes a top navigation bar with 'Projects', 'Home', and 'Settings'. Below this is a toolbar with 'Collapse all', 'Expand all', 'Alphabetically', 'by Type', and 'by Vulnerability level'. The main content area is divided into three sections: 'Diagrams', 'Single failures', and 'Common cause failures'. The 'Single failures' section is currently active and displays a list of services with their associated vulnerabilities. The services are: 'Single failures for "base station" (equipment)' (Incomplete), 'Single failures for "cable" (wired link, 2 nodes)' (M), and 'Single failures for "DECT" (wireless link)' (H). The 'DECT' section is expanded, showing a table of vulnerabilities.

Cause	Name	Freq	Impact	Total	Remark
⚡	Interference	L	L	L	
⚡	Signal weakening	H	L	M	
⚡	Jamming	H	M	H	

Below the table, there are buttons for '+ Add vulnerability', 'Up', and 'Down'. At the bottom of the interface, there is a row of service tabs: 'In-company phone', '2-way radio', 'Mobile phones', and 'Elevator safety'. The '2-way radio' tab is highlighted with a red circle.

Like Diagrams view, Single failures view is divided into to tabs, one for each service. You can [add, remove, rename and reorder](#) services in the same way as in the Diagrams view.:

## 10.2 Vulnerability assessment

The screenshot shows a detailed view of the 'Single failures for "DECT" (wireless link)' section. The header indicates the status as 'Incomplete' and includes a red 'H' marker. Below the header is a table of vulnerabilities.

Cause	Name	Freq	Impact	Total	Remark
⚡	Interference	L	L	L	⊗
⚡	Signal weakening	H	-	-	⊗
⚡	Jamming	H	M	H	⊗

Each node or node class in the selected service is shown using a collapsible header. The marker *Incomplete* appears when any one vulnerability assessment for that node or node class has not been completed. An assessment is complete when both the frequency and impact are set to a value other than “-”. Open or close the vulnerability assessment by clicking the header. The buttons *Collapse all* and *Expand all* on the Home toolbar will open or close all vulnerability assessments at once.

When a header is expanded (opened), the full vulnerability assessment of that node becomes visible. This works in the same way as in the [vulnerability assessment window](#) in Diagrams view.



# 11 Common cause failures view

*Cluster components and assess common cause failures.*

In the common cause failures view, you assess the possibility of two or more nodes failing simultaneously. Most often, two nodes must be sufficiently close together before a single event can make both fail. For example, two equipment items in the same building will fail in a single area-wide power failure.

The common cause failure view does not have tabs for each service. Common cause failures are assessed for the project as a whole. This assessment is done once for each vulnerability, as long as that vulnerability occurs at least twice in the project. Vulnerabilities that occur only for a single node are not shown; for a common cause failure event to happen, at least two nodes must be involved.

## 11.1 Vulnerability assessments

Each vulnerability is presented using a header, followed by assessments for each cluster and finally by the nested list of clusters and nodes.

Cause	Name	Freq	Impact	Total	Remark
	Physical damage	L	M < H	L	
	└ City	L	H	M	
	└└ Office	M	M	M	
	└└└ Equipment room 1	L	M	L	
	└└└ Equipment room 2	L	H	M	
	└ Branch office in other c...	L	M	L	

Each common cause vulnerability is shown using a collapsible header. The marker *Incomplete* appears when any one cluster has not been assessed. An assessment is complete when both the frequency and impact are set to a value other than “—”. Open or close the common cause assessment by clicking the header. You can collapse or expand all assessments at once, using the *Collapse all* and *Expand all* buttons on the Home toolbar.

When a header is opened (expanded), a table of vulnerability assessments of clusters is shown below it. Lines indicate the structure of clusters-within-clusters. In this area you can rename a cluster, by clicking its title (press Enter/click elsewhere to confirm, press Escape to cancel). Note that the root cluster always has the same name as the vulnerability itself, and cannot be renamed. You can change the frequency and impact. Click to activate the selection widget. Click the widget to open it, or type the letter of your choice. You can also add or edit remarks.

The frequency assessment of clusters is often lower than the frequencies for the individual components in the cluster. That is because the failure scenario is more involved and larger. But if the vulnerability leads to an incident, the impact for the common cause failure should be at least the highest impact for the components of the clusters.

Suppose that failure of a router will lead to long-term unavailability of a telecom service. The impact class for that is High. Simultaneous failure of that router and another component will also lead to long-term unavailability, and should therefore also be assessed at least as High.

The Raster tool will show a warning when the impact has such a lower limit. When an impact below this limit is assigned, a warning will be shown (see below).

The screenshot shows a table titled "Common Cause failures for 'Physical damage' (equipment)". The table has columns for Cause, Name, Freq, Impact, Total, and Remark. The 'Impact' column has a dropdown menu set to "M Medium". A callout box on the right contains the text: "The impact should be at least High, because the following nodes have that impact for single failures." followed by a bulleted list containing "radio<sup>b</sup>". A lightbulb icon with a checkmark is next to the callout box.

Cause	Name	Freq	Impact	Total	Remark
⚡	Physical damage	L	M Medium		
⚡	City	L	H	M	
⚡	Office	M	M	M	
⚡	Equipment room 1	L	M	L	
⚡	Equipment room 2	L	H	M	
⚡	Branch office in other c...	L	M	L	

To show the contents of all clusters for a vulnerability click its header. The currently selected header is drawn in blue. The contents are then shown on the right.

## 11.2 Nodes and node clusters

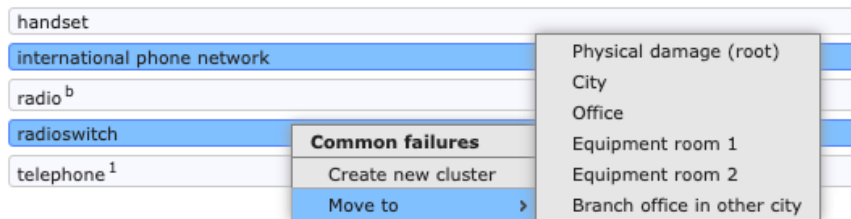
The screenshot shows a hierarchical tree structure of nodes and clusters. The root node is "Physical damage (equipment)". It has several sub-nodes: "City", "Branch office in other city", "handset", "international phone network", "radio<sup>b</sup>", "radioswitch", and "telephone<sup>1</sup>". The "City" node is expanded to show "Office" and "Equipment room 1". "Office" is further expanded to show "Equipment room 2", "base station", and "PABX". "Equipment room 2" is expanded to show "Mobile network operator" and "mobile phone". "Equipment room 1" is expanded to show "elevator" and "fixed telephony". "Branch office in other city" is expanded to show "cloud" and "telephone<sup>2</sup>".

All nodes subject to the vulnerability are listed to the right the table of vulnerability assessments. Initially all the nodes as shown in a single list, sorted by label and by name. There are two mechanisms to sort nodes into clusters: by using the menus or by 'drag and drop'. Either way you can group nodes into clusters, and rearrange nodes and clusters in a nested structure.



## 11.2.1 Nodes

Each node is shown using a simple white row. You can select one or more nodes, and use the popup menu to move the selection into a new or existing cluster.



You can:

- *select* a single node, by clicking it. The node is highlighted in blue to indicate that it is now selected.
- *select* or *unselect* individual nodes, by clicking the node while holding the Control key (on Windows) or the Command key (on Mac OS X).
- *select a series* of nodes, by clicking an unselected node while holding the Shift key. All nodes between the last selected node and the current node become selected.
- *unselect* all nodes, by clicking somewhere on the workspace.

To move all currently selected nodes, use the right mouse button to call up the popup menu.

- *Create new cluster.* Use this menu item to move the selected nodes into a new cluster. The new cluster will become a subcluster in the cluster in which the last nodes was selected.
- *Move to:* Move the selected nodes into an existing cluster.

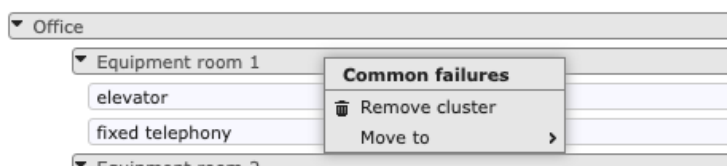
Note that after moving nodes, any clusters with less than two nodes or subclusters remaining will automatically be cleaned up.

## 11.2.2 Cluster headers

Each cluster has a grey header; the nodes in that cluster are listed below the header, after the subclusters (if any). Unlike nodes, cluster headers cannot be selected.

Open or close the cluster, by clicking the header (either on the triangle or to the right of the title). Rename the cluster by clicking its title. Note that the root cluster cannot be closed nor renamed; it always has the same name as the vulnerability itself.

To move or remove a cluster, use the right mouse button to call up the popup menu.

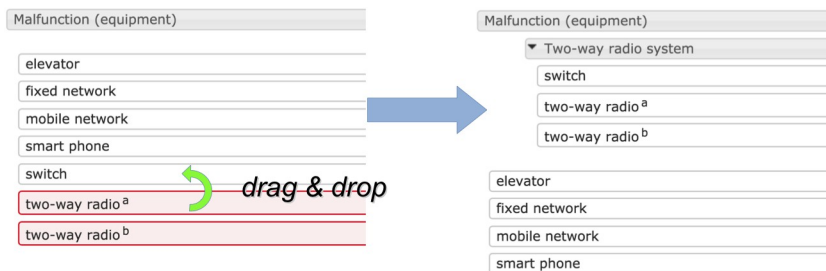


- *Remove cluster.* Use this menu item to dissolve the cluster. All nodes in the cluster will be moved into the parent cluster.
- *Move to:* Make the cluster a subcluster of an existing cluster. Note that after moving clusters, any clusters with less than two nodes or subclusters remaining will automatically be cleaned up.

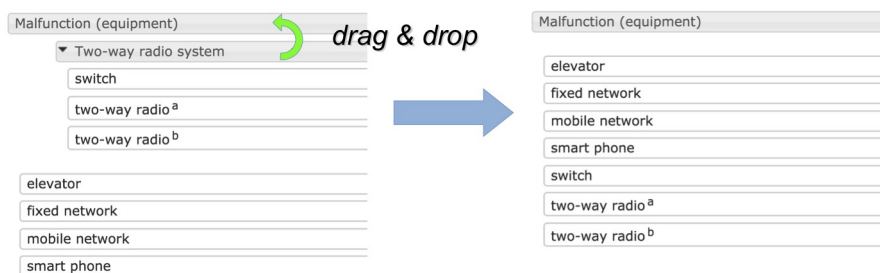
### 11.2.3 Drag and drop

Nodes and clusters can also be arranged and rearranged using 'drag and drop'. Clusters are dragged by dragging their header row. While dragging a node or cluster, all possible drop targets light up in pale green. You can first select a number of nodes, then drag them collectively. You can:

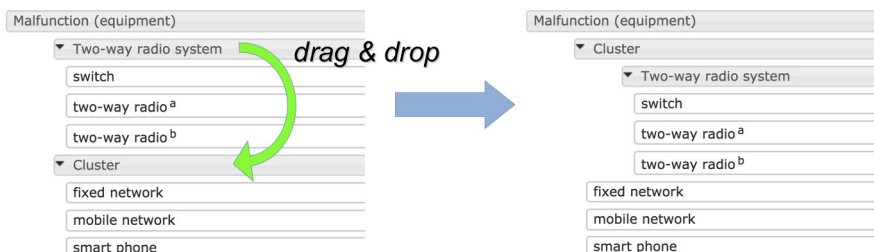
- **create** a new subcluster, by dragging a node onto another node. Both nodes must belong to the same cluster, and will be combined into a new subcluster thereof. See the picture below. The new cluster will get a default name, and the two nodes and all other selected nodes will be shown beneath it, indented from the left margin.



- **move** a node or selection, by dragging it onto the header of any cluster.
- **remove up** a cluster (dissolve it), by dragging the cluster header onto the header of its parent, as illustrated below. The nodes in the cluster will be merged with the parent cluster. When a group is removed, the assessment for that group will be lost.



- **move** a cluster, by dragging its header onto the header of any cluster except its direct parent. The cluster will become a subcluster of the cluster on which it was dropped, as illustrated:



# 12 Analysis view

View reports and assist in risk evaluation of the project.

The analysis view contains a number of reports, some of them interactive, that are useful in preparing the longlist and shortlist during the Risk Evaluation stage. Tabs along the bottom give access to various tools and reports.

## 12.1 Failures and vulnerabilities

Single failures	Bedieningsfout	Congestie	Congestie	Diefstal	EMC	EMC	Fysieke schade	Interferentie	Jamming	Kabelbreuk	Ouderdom	Sigmaal afzwakking	Stroomuitval	Veroudering	Overall	
raadloze verbinding			H				A	U			L				H	reduced
Mobiele Aanbieder)	M	M	M	X	U	U	H	X	L	X	U	L	H	U	X	
portofoon	H			L	X		L						M	L	H	reduced
base station	H			L		M							H	L	H	
s onder vergunning		H					M	U					H		H	

This table shows a condensed overview of all vulnerabilities against the single failures and common cause failures. It allows you to quickly visualise the most critical nodes.

This table is interactive. You can:

- *ignore* a vulnerability, by clicking it. The square will colour white with a red border to indicate its status. If ignoring this vulnerability would cause the overall vulnerability level to change, the marked *reduced* appears on the right hand side of the row.
- *include* an ignored vulnerability, by clicking it.
- *include* all ignored vulnerabilities, using the “clear exclusions” button.
- *show* all quick wins automatically, by clicking the “show Quick Wins” button.

Quick wins are those vulnerabilities that by themselves determine the overall vulnerability level. Reducing that vulnerability would immediately reduce the overall level. Quick wins are therefore a useful priority for risk treatment.

## 12.2 Assessments by level

Frequencies		Impacts							Overall levels	
Single vulnerability frequencies		U: Extremely low	L: Low	M: Medium	H: High	V: Extremely high	X: Unknown	A: Ambiguous	?: Undetermined	Total
Configuration (equipment)	1	11	5	3		1			1	22
Flooding (equipment)	15	1	1				1		1	19
Malfunction (equipment)		8	12				1		1	22
Other (equipment)		1	1							2
Physical damage (equipment)	5	11	4			1			1	22
Power (equipment)	1	14	4	1			1		1	22
Congestion (wireless link)	1	3	4				1		1	10
Interference (wireless link)	1	6	1			1			1	10
Jamming (wireless link)	1	6	1			1			1	10
Signal weakening (wireless link)	1	2	4	1			1		1	10
Ageing (wired link)	3	9	3			1			1	17
Break (wired link)	2	5	7				1		2	17
Congestion (wired link)		10	2			1			1	14
<b>Total</b>	<b>31</b>	<b>87</b>	<b>49</b>	<b>5</b>	<b>0</b>	<b>12</b>	<b>0</b>	<b>0</b>	<b>13</b>	<b>197</b>

These tables show an overview of all assessments. The Frequencies table shows how often each frequency was assigned in the Single Failure and Common Cause Failures stage, including the totals per frequency class and per node class (both as numbers and visually). The Impacts table does the same for impact assignments. The last table shows the combined vulnerability levels. All tables are informational.

## 12.3 Node counts

This table shows the number of occurrence for each node type, for each service and for the project as a whole. It is purely informational.

## 12.4 Checklist reports

Two overviews help determine how useful the checklists were, and what vulnerabilities were added during the Single Failures stage.

Removed vulnerabilities: lists all vulnerabilities that are present in the checklist for a component, but not on the component itself. Section [Adding and removing vulnerabilities](#) warned that vulnerabilities should only be removed when physically impossible. This report helps to verify this.

Custom vulnerabilities: lists all vulnerabilities that are present for a component, but not in its corresponding checklists. This is purely informational.

## 12.5 Longlist

This longlist view selects all single and common cause vulnerabilities above a chosen level. This can serve as a good first attempt at the [longlist in Stage 4](#). Often, the list of all High vulnerabilities together with all Unknown and Ambiguous vulnerabilities can be used as the longlist.

# 13 Technical issues

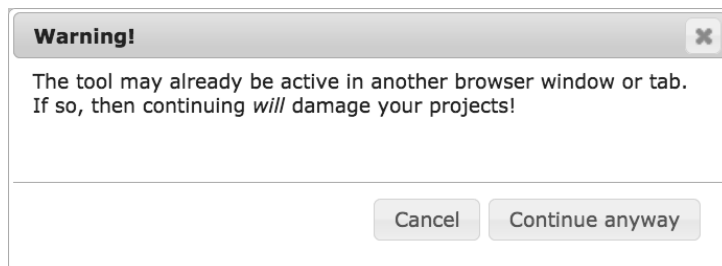
*Some technical below-the-surface info.*

## 13.1 The intranet tool

The intranet tool was developed for recent versions of Firefox, Google Chrome, Safari, and Edge. It will work with all browsers in the same way, with only minor differences. Internet Explorer is not supported.

The interface will use the preferred language setting of your web browser. Currently, only Dutch and English (the default) are available. Configure the language preferences in your web browser to choose the interface language.

It is not possible to use Raster in multiple tabs or windows of the same browser. When Raster is active in more than one browser window or tab, your project data will get damaged and you will likely lose all your work. The tool will warn you when it may already be running in another tab.



In rare cases you may see this warning even though no other instance of the Raster tool is active. This may happen, for example, when the browser crashed and could not exit cleanly. When this happens, make absolutely clear that Raster is not running elsewhere before continuing.

It is, however, possible to use Raster with two separate browsers on the same computer. For example, once in Firefox and once in Chrome. If the project is not private but shared (see [Working with the intranet application](#)), then it is possible to work on the same project simultaneously. Shared projects can also be viewed and edited from two computers simultaneously.

## 13.2 Computation of vulnerability levels

For malicious vulnerabilities the frequency depends on both the worst plausible attacker and the level of difficulty, as in the table below.

	customers, employees	activists	criminals	competitors	state actors
Trivial	H	H	H	H	V
Easy	M	H	H	H	H
Difficult	L	M	M	H	H
Very difficult	L	L	L	M	M
Nearly impossible	U	L	L	L	M

The following table describes the way that the Raster tool computes a vulnerability level from a frequency and impact class.

	A	A	A	A	A	A	A	A	A
	-	-	-	-	-	-	-	-	A
	X	X	X	X	X	X	X	-	A
	V	A	V	V	V	V	X	-	A
	H	U	M	H	H	V	X	-	A
	M	U	L	M	H	V	X	-	A
	L	U	L	L	M	V	X	-	A
Impact	U	U	U	U	U	A	X	-	A
	U	L	M	H	V	X	-	A	
									Frequency

As can be seen from the table, the inner part for frequency and impact L, M, and H match expected damage, even though frequency and impact are not fully numerical. These three classes represent modest values, for which 'frequency times impact' assessment is suitable.

When impact is extremely high (V), it does not matter what the frequency is, as the risk is unacceptable at any probability. When frequency is extremely high (i.e. near certainty), we are almost certain that damage will arise, and are therefore obliged to prepare countermeasures. In this case the risk will also be unacceptable.

When the impact is extremely low (i.e. nearly absent, symbol U), we do not really care whether the incident happens; the risk will always be extremely low to us. The same consideration applies for situations where the frequency is extremely low.

These considerations are ambiguous when one of frequency or impact is V, and the other U. However, we do have a class for ambiguity, namely A.

When either the frequency or the impact is not known, the combination also cannot be known. In these combinations, we always want to preserve ambiguity, as we believe that information to be highly relevant to decision makers. When an undetermined value (the minus symbol in the table) is involved, the result must also be undetermined as that value could turn out to be ranked as ambiguous rather than simply unknown; until we assess the value of that factor, the result of the combination is still undetermined. When neither the value A nor - is appropriate, the combination is ranked as a 'plain' unknown (symbol X).

The overall vulnerability score for a node is computed by taking the 'maximum' vulnerability score of all vulnerabilities on that node. The vulnerability levels, in order from lowest to highest, are:

(lowest) - U L M H X A V (highest)

Note that here also the symbol – indicates the 'not yet analysed' level.

## 13.3 Creating iconsets

An iconset is a collection of cartoon-style images to create Raster diagrams. You can create your iconsets. Use the Default iconset as an example.

Each iconset should be stored in its own directory inside the `iconset` directory. The name of the directory should match the name of the iconset. The iconset must contain a description in JSON format; the file must be called `iconset.json`; e.g. for iconset `Medical` the description must be stored in `iconset/Medical/iconset.json`. See below for the definition of the the `iconset.json` file.

Icons have a type (either wired link, wireless link, equipment, unknown link or actor). There must be one or more icons for each type. For each icon there must be two files: the icon and its icon mask. If no mask is specified, the mask is assumed to have the same name as its icon but with `-mask` appended (and with the same extension). In addition to the icon and the mask, the first icon of each type must specify the template-image (the user drags the template from the toolbar onto the workspace to create new nodes). If no template image is specified, then the name is assumed to be the icon name with `-template` appended.

E.g;

- icon `machine.png` will have the default mask `machine-mask.png`, and the default template will be `machine-template.png`.
- icon `tube.jpeg` will have the default mask `tube-mask.jpeg`, and the default template will be `tube-template.jpeg`.

Files for icons, masks and templates may be stored in the iconset directory (at the same level as `iconset.json`) or in subdirectories.

### 13.3.1 Creating icons and masks

Icon and mask images typically have transparent areas. The icon is displayed on a colored background. Some areas of the icon will have the background color. The mask image determined the extent and size of the background. Non-transparent areas of the mask will take the background color, transparent areas of the mask will remain transparent. The icon is drawn on top of its background.

- Outlines and areas that must always be visible in the foreground color: include these in the icon.
- Areas that should be visible in the background color: make these transparent in the icon, and non-transparent in the mask.
- Areas that should always be transparent: make these transparent in the icon *and* in its mask.

### 13.3.2 iconset.json

This must be a valid JSON file, containing a single object. Some of the (sub-)fields are multi-language strings. Multi-language strings are objects in which property names are (capitalized) language codes, and property values are the string in that language. E.g. `{"EN": "This is an example", "NL": "Dit is een voorbeeld"}` Fields are mandatory, unless specified as optional.

#### Fields

1. `setDescription`: Multilanguage string (optional), a phrase describing this iconset.
2. `icons`: Array of icon descriptions; see below.

The first five icons in the array *must* be of types `tEQT`, `tWRD`, `tWLS`, `tUNK`, `tACT`, in that order. Any additional icons must be specified after these five.

#### Icon descriptions

1. `type`: String, one of `tWLS`, `tWRD`, `tEQT`, `tUNK`, `tACT`.
2. `image`: String, the name of the image file.
3. `mask`: String (optional), the name of the mask file. Default = derived from the image filename.
4. `template`: String (optional), the name of an image file that can be used as the template image. Default = derived from the image filename.
5. `name`: Multi-language string (optional), description of this icon. Default = image filename.
6. `width`: integer (optional), the default width of the icon in pixels. Default = 100. Allowed range is 20..200
7. `height`: integer (optional), the default height of the icon in pixels. Default = 30. Allowed range is 10..100
8. `title`: String (optional), location of the title, one of `inside`, `below`, `opleft`. Inside: the title is centered horizontally and vertically within the icon. Below: the title is drawn centered and below the icon. Opleft: the title is aligned to the left margin, and vertically aligned at the top. Default = `inside`.
9. `margin`: String (optional), left and right margin of the title as a percentage of the icon width. Does not apply when title = below. Increase the margin to fit the title inside the icon. Default = 0.
10. `offsetConnector`: real number between 0.00 and 1.00 (optional). The connector is always drawn at the top of the icon; this offset specifies its horizontal location: 0.00 means at the extreme left, 0.5 means centered, 1.0 means at the extreme right. Default = 0.5.
11. `maintainAspect`: boolean (optional). If false, the width and height can be adjusted independently. Default = true.

Make sure that `iconset.json` is a valid JSON file. Raster will report parsing errors in the Developer tools|Console.

## 13.4 Project Groups

This section applies to the intranet tool, not to the standalone tool.

A *group* is a separate area in which projects can be stored on the web server. The group's directory can be protected using the web server's access authorization; a sample `htaccess` file is provided as an example. Although groups are mainly useful for Shared projects, all Private projects belong to a specific group as well.



The default group is called `public_group` and has no access control; the web server administrator can override this if required.

To create a new project group (called `samplegroup` in these instructions):

1. Duplicate the `public_group` directory structure as a new directory `samplegroup`. All files should be readable by the web server; the directory `SharedProjects` should be writable.
2. Set access permissions, if required.
3. Add one or more iconsets, if required.
4. Create a suitable project to be used as the template (starting point for new projects), if required.
5. Inspect and modify the settings file `group.json` if required.

### 13.4.1 `group.json`

The settings for a group are stored in a JSON configuration file. Currently the file may contain these fields:

- *classroom*: (boolean, default is `false`) If true, classroom functionality is enabled on this group. See below.
- *template*: (string, default is "Project Template") The name of the project that will be used as the starting point when a new project is created, instead of a blank project. Set to "" to disable the template.
- *iconsets*: (array of strings, default is ["Default"]) The names of the available iconsets; the first set will be used for new projects. If a `template` is specified, the iconset in the template project takes precedence for new projects. See the `Iconsets.md` for details.
- *localonly*: (boolean, default is `false`) If true, projects cannot be retrieved nor stored on the server. The template will still be used, if present. If this set, only private projects will be possible.

A template is most useful to define default iconset, vulnerabilities and labels, instead of the builtin defaults. It is possible, although perhaps less useful, to include services and nodes in the template.

If no shared project with the template name exists, an empty project (with builtin defaults) will be used instead.

#### The `classroom` option

For training purposes it may be useful to provide sample projects to the students, which the students should not be able to modify. This can be achieved by setting the `classroom` property to `true`. When classroom functionality is enabled, opening a shared project will create a new private copy instead. This way each student can open the projects provided by the course teacher, and make their own personal changes.

Students cannot set their private projects to shared, to prevent them from uploading their work for others to see. You can think of the `classroom` option as "can retrieve but cannot store".

Note: when classroom functionality is enabled, shared projects will be called "Exercises" in the project library on the Projects toolbar.

#### The `localonly` option

When `localonly` is set to `true`, the server offers even less functionality. No project can be stored on the server, as is the case when `classroom` is `true`. But in addition, no projects will be retrieved from the server. The list of projects in the Projects toolbar will

only show private projects. However, the template project will still be retrieved from the server if `localonly` is set.

You can think of the `localonly` option as “cannot retrieve and cannot store”.

### Preparing the web server

To put the course materials (with the `classroom` option) and/or template on the web server, first temporarily disable the `classroom` and `localonly` properties by setting them to `false` in the `group.json` file. Then create your projects, and share them (in the project properties using the tool) to upload them to the server. Edit as required. Finally, when all is set, edit `group.json` again to set `classroom` or `localonly` options to `true`.

When either the `classroom` or `localonly` option is true, the SharedProjects directory on the web server can be made read-only.

### Iconsets for project groups

Additional iconsets can be installed in two locations: either in the `img/iconset` directory or in the group’s directory. Iconsets installed in `img/iconset` are available to all groups on the server. Iconsets installed in a group’s directory are available to projects in that group only. In either case it is not sufficient to install the iconset files on the web server: it must also be explicitly enabled using the `iconset` field in `group.json`.

Installing a new iconset therefore requires two steps: copying the new set into the `iconset` directory (either under `img` or in the group’s directory), then edit the `group.json` file accordingly.

## 13.5 Standalone configuration

This section applies to the standalone tool, not to the intranet tool.

There are a few advanced settings that can be modified by editing the `prefs.json` configuration file. This file is stored in the user’s application data directory:

- On Windows: `%APPDIR%` (most often `C:\Users\«username»\AppData\Roaming\Raster`).
- On MacOS: `Library/Application Support/Raster` in the user’s home directory.

### 13.5.1 prefs.json

The file `prefs.json` is used by the Raster application to save user preferences between sessions. This is a plain JSON file, and the two relevant properties are:

- `disablehardwareacceleration`: Set this to `false` to *enable* hardware acceleration. It is disabled by default for maximum compatibility.
- `iconsets`: This is an array of strings that specifies the names of the available iconsets. The the first name will be used for new projects. To disable the “default” iconset and only allow iconset “myicons”, use the following line:
 

```
"iconsets": ["myicons"]
```

## 13.5.2 iconsets

Each project will use one iconset for its diagrams. Two iconsets are provided: “Default” and “Classic”. You can create and add additional iconsets; see the file `Iconsets.md` for details. Additional iconset must be stored in the user’s application data directory, inside the `iconset` directory. The `iconset` directory does not exist by default; create it before adding custom iconsets.