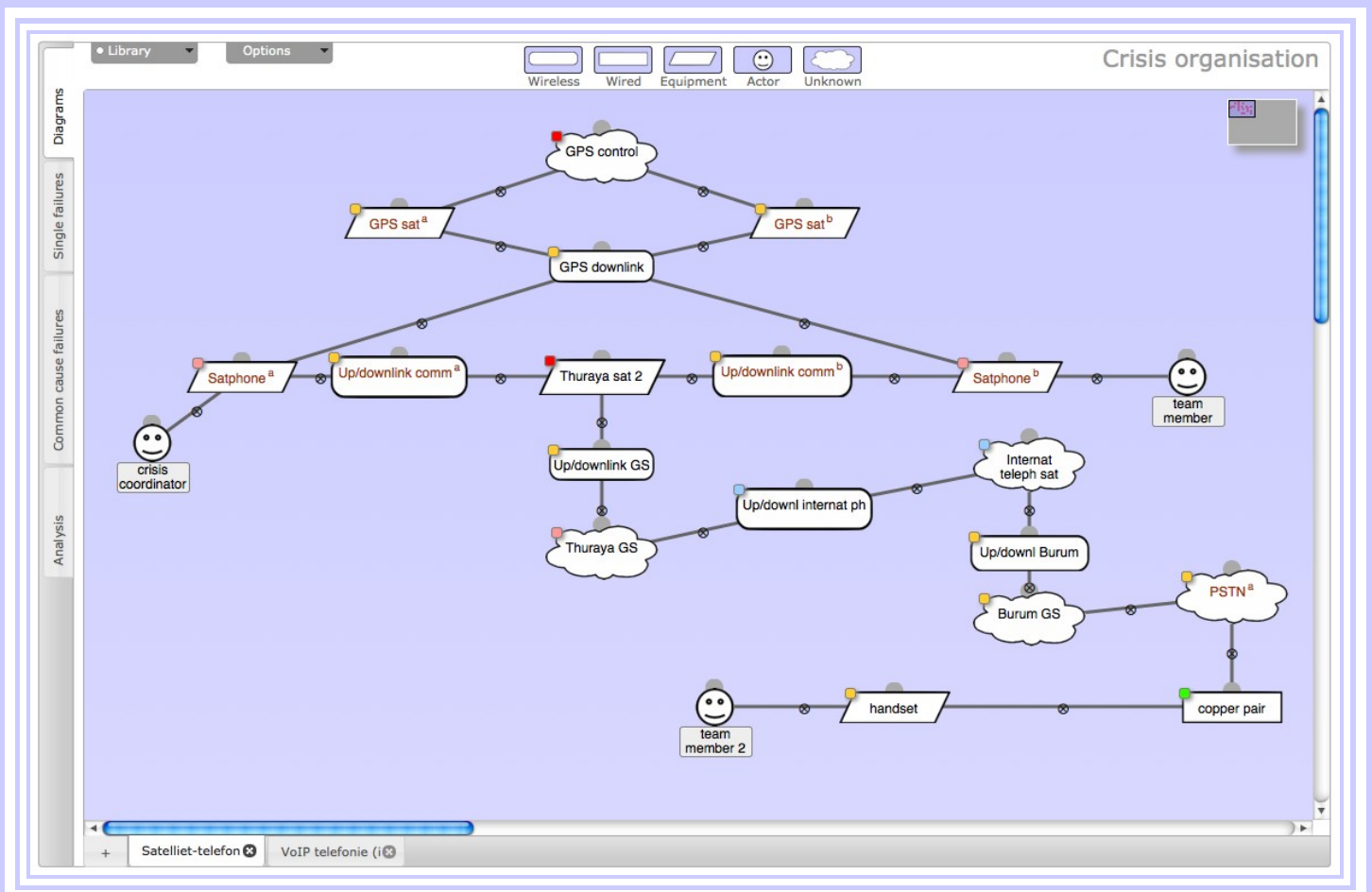


The Raster method application manual



Note: the Raster method and tool are still under development

Author: Eelco Vriezeolk

Contact: <http://wwwhome.ewi.utwente.nl/~vriezeolke/Raster/>

The Raster tool can be found at the above URL.

This work is sponsored by Radiocommunications Agency Netherlands,
and by University of Twente.

<http://www.agentschaptelecom.nl/>

<http://www.utwente.nl/>

Contents

1 Introduction	1
1.1 The problem	1
1.2 The Raster method	1
1.3 About this manual	3
1.4 Outline of this manual	3
2 The Raster method	5
2.1 Outline	5
2.2 Telecommunication service diagrams	6
2.2.1 Actors	6
2.2.2 Wired links	7
2.2.3 Wireless links.	7
2.2.4 Unknown links	8
2.2.5 Equipment	8
2.2.6 Example	9
3 Stage 1 — Initiation and preparation	11
3.1 Identify telecom services	11
3.2 Identify actors and external stakeholders	12
3.3 Describe disaster scenarios	12
3.4 Create stage 1 report	12
3.5 Obtain approval from sponsor	13
4 Stage 2 — Single failures analysis	15
4.1 Update the checklists of vulnerabilities	15
4.2 Draw initial diagrams	15
4.3 Analyse the vulnerabilities of components	16
4.3.1 Add and remove vulnerabilities	16
4.3.2 Assess vulnerabilities	17
4.3.3 Assess frequency	17
4.3.4 Assess impact	19
4.3.5 Assessing all vulnerabilities on a components	20
4.4 Expand unknown links	21
4.5 Review	21
5 Stage 3 — Common cause failures analysis	23
5.1 Create clusters	23
5.2 Analyse each cluster	24
5.3 Expand unknown links	24
5.4 Review	24
6 Stage 4 — Risk evaluation	25
6.1 Determine longlist	25

6.2 Reduce longlist to shortlist	25
6.3 Risk treatments	26
6.4 Assess social risk factors	26
6.5 Prepare final report	28
7 Executing the Raster method	29
7.1 Team composition	29
7.2 Managing work sessions	29
7.2.1 The recorder	29
7.2.2 Stage 1 — Initiation and preparation	30
7.2.3 Stage 2 — Single failures analysis	30
7.2.4 Stage 3 — Common cause failures analysis	30
7.2.5 Stage 4 — Risk evaluation	30
8 Raster tool	31
8.1 Working with the tool	31
8.2 Main views	31
8.3 Panels	32
8.3.1 The Library panel	32
8.3.2 The Options panel	33
8.4 Colour codes	34
9 Diagrams view	35
9.1 Templates	35
9.2 Checklist windows	35
9.3 Workspace	36
9.3.1 Service tabs	36
9.3.2 The scroller	36
9.3.3 Diagram nodes	37
9.3.4 Node classes	38
9.3.5 Identical nodes	38
9.3.6 Connecting nodes	38
9.3.7 Selecting nodes	39
9.3.8 The node menu	39
9.3.9 Node labels	40
9.3.10 Vulnerability assessment window	40
10 Single failures view	43
10.1 Service tabs	43
10.2 Vulnerability assessment headers	43
10.3 Vulnerability assessments	44
11 Common cause failures view	45
11.1 Vulnerability assessment headers	45
11.2 Node clusters	45
11.3 Vulnerability assessments	47

12 Analysis view	49
12.1 Failures and vulnerabilities	49
12.2 Single failures by level	49
12.3 Node counts	49
12.4 Checklist reports	50
13 Technical issues	51
13.1 Supported web browsers	51
13.2 Printing	51
13.3 Browser tabs	51
13.4 Computation of vulnerability levels	52

1 Introduction

Introduction and guide to this document.

1.1 The problem

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 crisis organisations (police, fire services, medical care, etc) and for crisis support and decision makers (National Crisis Coordination Centre, ministerial crisis centres, the Safety Regions, etc). Unfortunately, crisis organisations operate in just those circumstances in which failure of telecommunication services is most likely. A breach of a dike or an explosion in a chemical installation increases the odds that the supply of electricity or telecom switches will fail.

It is therefore important that organisations in general, and crisis organisations 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.

1.2 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.

Rather, the method 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.

The following parties are involved in applying the Raster method.

- The crisis organisation: the method is executed on request of a crisis organisation. This organisation is the requesting client of the study.
- 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 a objective and impartial assessment, as much as possible free from personal preferences or personal blind spots.

The team needs to encompass knowledge on crisis management, crisis communications, 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 typically be useful to include representatives of the crisis organisation in the team of analysts.

- The sponsor: the person or entity representing the crisis organisation for the purpose of the study. Typically this will be an official of the crisis organisation.
- 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 crisis 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.

1.3 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.

In this manual, the words 'must', 'should', and 'may' have a well-defined meaning.

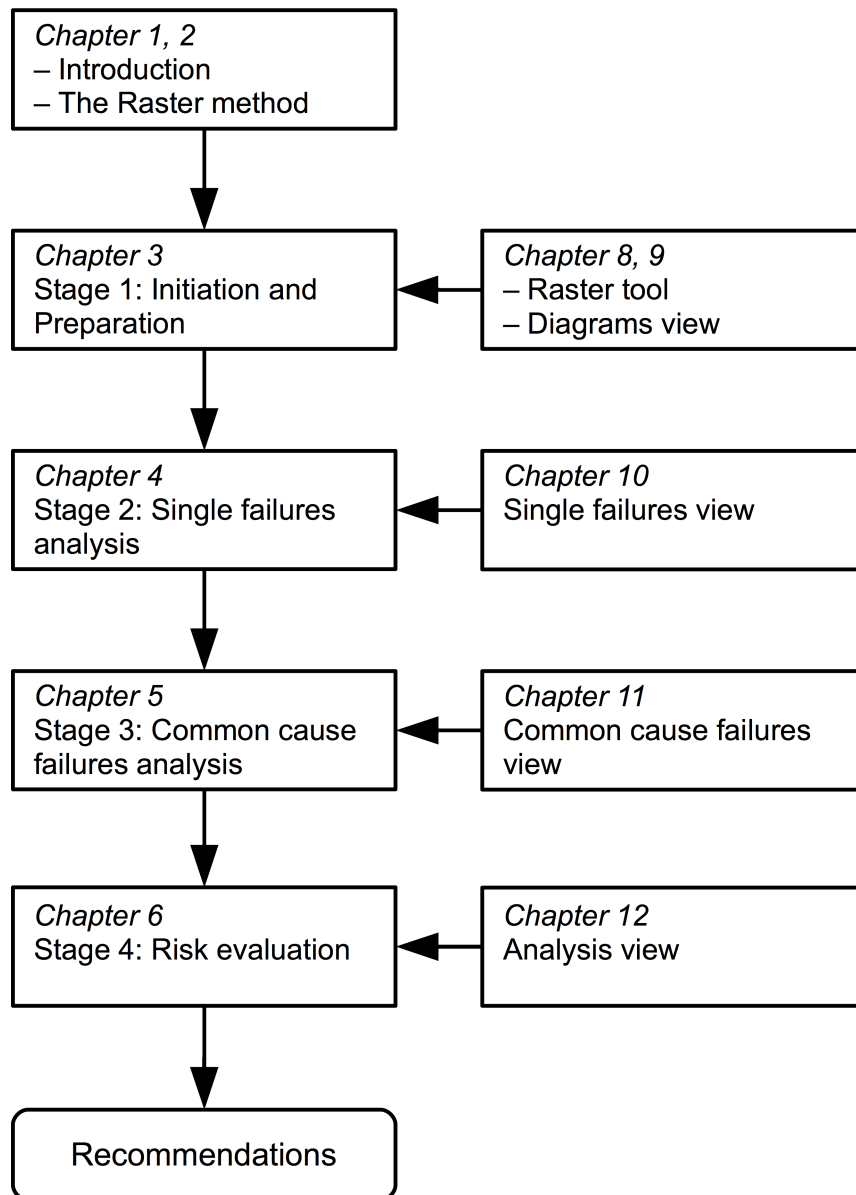
- *Must* indicates a compulsory aspect of the Raster method; under no circumstances can the activity be omitted.
- *Should* indicates a recommended activity, that should only be omitted if the implications are fully understood. This must be a conscious decision.
- *May* indicates an suggested but optional activity, that can be included or omitted at will.

Examples, notes and tips are typeset in text boxes.

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

1.4 Outline of this manual

Chapters 3 to 6 describe the Raster method; chapters 8 to 13 describe the Raster tool that aids 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 overleaf.



2 The Raster method

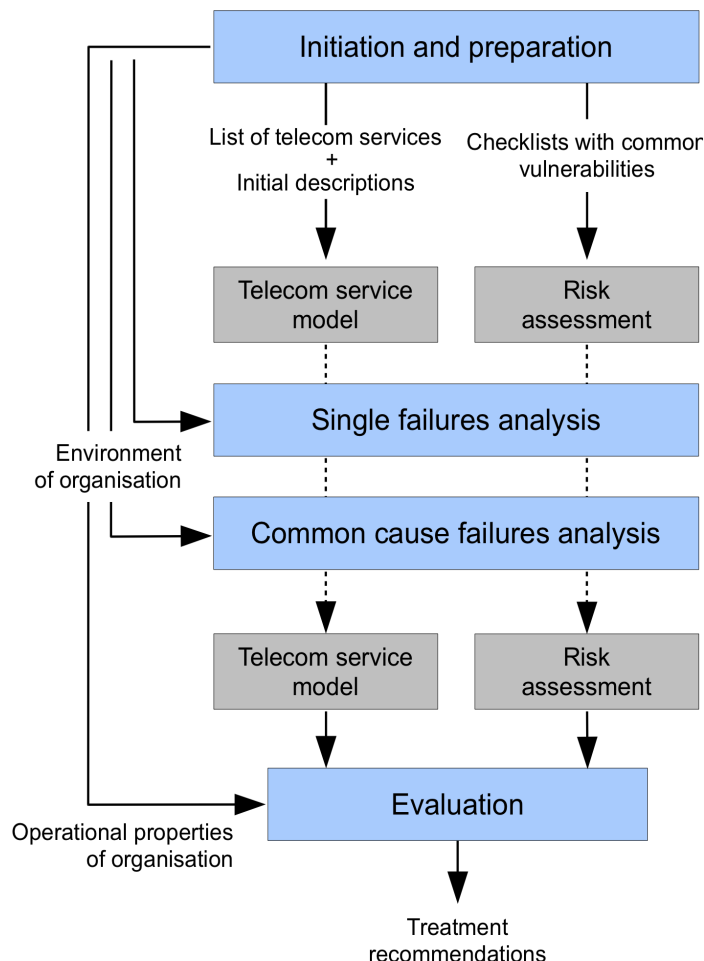
General outline of the Raster method and telecom service diagrams.

2.1 Outline

The Raster method consists of four stages.

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

The Figure below illustrates these four stages.



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 telecommunica-

tion components, including cables wireless links, or complete installations. 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.

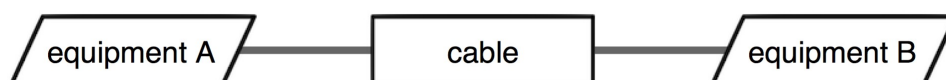
3. The Common Cause Failures Analysis stage takes closer look at failure causes that lead to the failure of multiple components at once. One example is that of independent telecom services that both have an cable in the same underground duct. A single trenching incident may cut both cables at the same 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.

Chapters 3 to 6 describe each stage in detail.

To facilitate the creating of diagrams and analysis of single and common cause failures, the Raster tool is available. This tool is described in the second part of this document, starting from Chapter 8. In principle, stages 2 and 3 can be used without the tool. However, the tool comes highly recommended and this manual assumes that the method will be used together with the tool.

2.2 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.



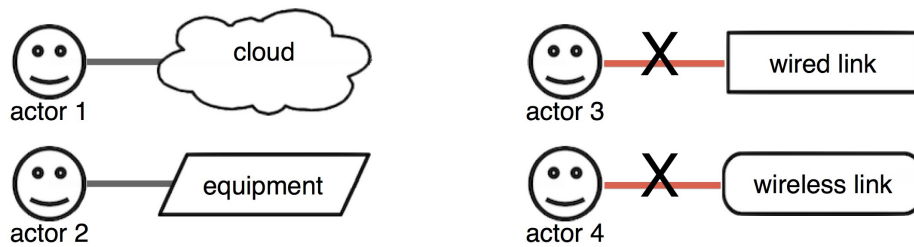
Lines are not the same as cables. When two equipment items are connected via a cable, three nodes are used as in the picture above. The line between equipment and cable shows a physical connection: the cable is plugged into the equipment.

There are five types of nodes, each identified by its unique shape.

2.2.1 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.



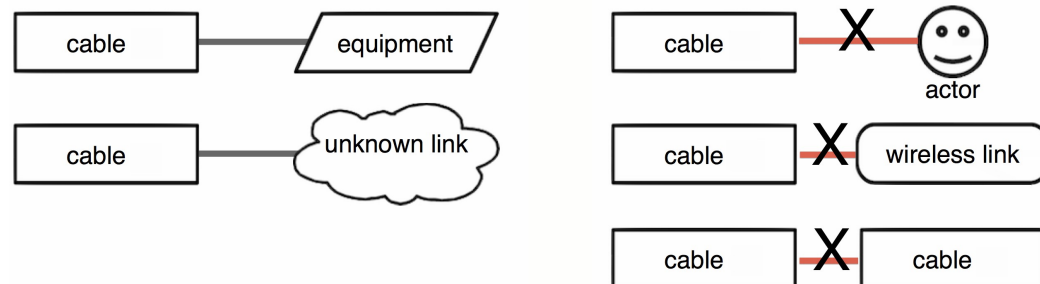


An actor can only be connected to components of type 'equipment' or 'unknown link'. Actors cannot be connected directly to wired or wireless links, and the Raster tool will not allow such connections.

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.

2.2.2 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 endpoints are not part of the wired link, and need to be modelled separately as equipment items.



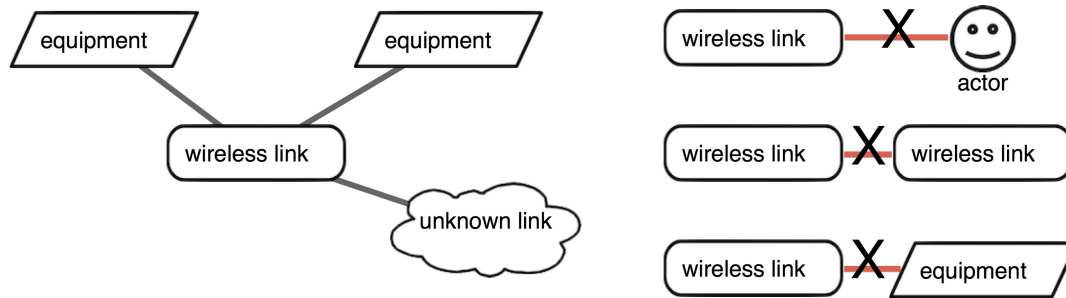
Each wired link has exactly two connections, each to a component of type either 'equipment' or 'unknown link'. To connect a wired link to an actor, wireless link, or an other wired link, place an equipment node in between.

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.

2.2.3 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.

2.2.4 Unknown links

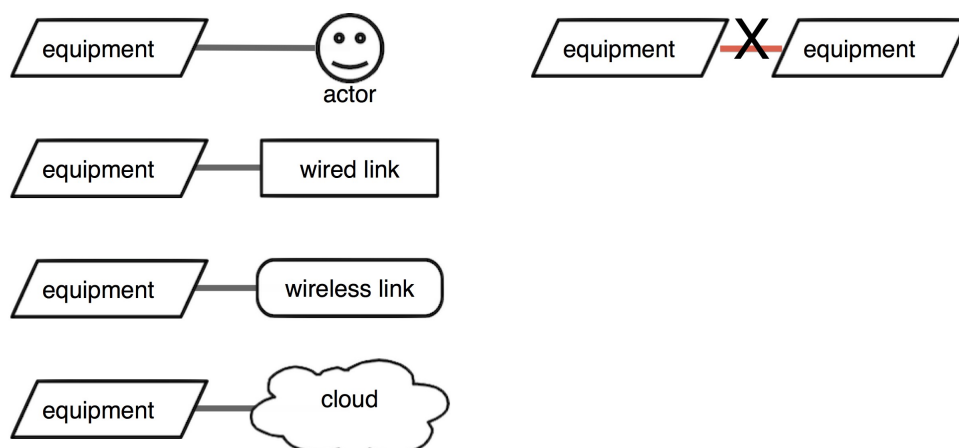
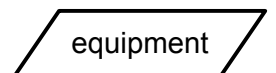
Unknown links (cloud shapes) represent parts of networks for which insufficient information is available, or that do not need to be described in detail. Unlike wired and wireless links, that represent a single communication channel, unknown links are composed of equipment and wired and wireless links.



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.

2.2.5 Equipment

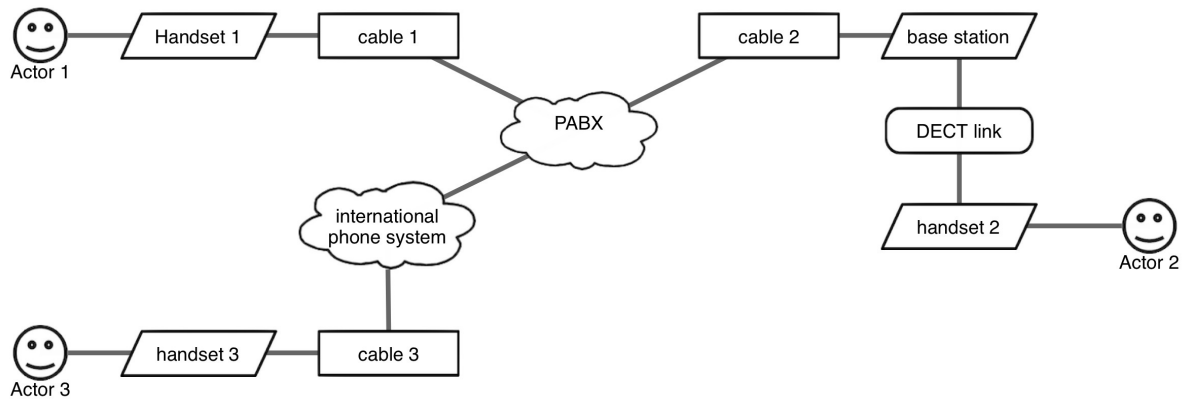
Equipment nodes represent all other physical components of telecom networks, such as switches, exchanges, routers, amplifiers, radio transmitters, radio receivers etc. An equipment node may model a single piece of equipment or an entire installation.



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'.

2.2.6 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 crisis organisation must be described in some detail. Also, the position of this crisis organisation within the wider system of crisis response must be laid out.

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 crisis 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 crisis organisations.
- 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 crisis 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 crisis 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 crisis 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 crisis 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 crisis organisation.

In the Netherlands earthquakes seldom lead to damage to infrastructures. Typically, the threat of earthquakes 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 man-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 (see section 6.5).

1. Executive summary to the Stage 1 report.
2. About the crisis organisation (internal scope):
 - a. Position within wider system of crisis response.
 - b. Sponsor, decision makers, and analysts.
 - c. Roles, tasks, and responsibilities of the crisis organisation.
 - d. Telecom services used, with a description of the implementation, role and purpose during crisis response, and fallback and backup options.
 - e. Actors, including main actors, and their roles, tasks, and responsibilities.
3. About the environment of the crisis 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 crisis 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.

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, the most common vulnerabilities of network components must be described. Checklists are used for this. A checklist contains a summary and description of common vulnerabilities. Section 9.2 describes how to adapt the standard checklists in the Raster tool.

Create a fresh Raster project (see section 8.3.1), and inspect the predefined checklist of the Raster tool, and add new vulnerabilities as deemed necessary. Good checklists make the analysis process faster and easier. The vulnerabilities on the checklists must apply to most components of that type; vulnerabilities that only apply to a few components must be omitted. It is therefore not necessary to strive for completeness when listing vulnerabilities. Any particular network component may have specific vulnerabilities that do not occur in the standard checklist. When the most common vulnerabilities are included in checklists, few special cases need to be considered.

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. As they may contain any of the other component types, all vulnerabilities on 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 or incorrect handling of handsets can be taken into account. These vulnerabilities are modelled 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 Section 9.3.1).

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 Section 9.3.

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. The initial list is a copy of the generic checklist for that type. Other vulnerabilities may exist that were not in the 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.

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.

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.

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

Both factors Frequency and Impact are split into eight classes, summarised in Tables 4.1 and 4.2. In the Raster tool each class also has an identifying colour (see section 8.4). 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 they 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 9.3.10 and 10, and section 13.4 for technical details).

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

The factor Frequency indicates the likelihood that the vulnerability will lead to an incident. All eight classes can be used for Frequency. Characteristic values for the classes high, medium, and low are given in Table 4.1.

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 component, 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.

Class	Value	Symbol
High	Once in 5 years. For 1000 identical components, each month 15 will experience an incident.	H
Medium	Once in 50 years. For 1000 identical components, each month 1 or 2 will experience an incident.	M
Low	Once in 500 years. For 1000 identical components, each year 2 will experience an incident.	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.	–

Table 4.1: Characteristic values for normal frequency classes.

Use the following four-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 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. The frequency does not reflect the likelihood that the vulnerability is triggered, but the likelihood that the vulnerability will lead to a noticeable incident. Another example is the use of premium quality components, or secure and controlled equipment rooms.

For some components monitoring can detect failures that are imminent before they occur. This also will reduce the frequency of incidents.

3. Think of reasons why this particular node should have a higher frequency than usual.

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.

4. 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 of little relevance. What is relevant is the effect to the service. The outage 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 is not considered, but may be relevant during risk evaluation (see Section 6.4).

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.

All eight classes can be used for Impact. Characteristic values for the classes high, medium, and low are given in Table 4.2.

Use the following four-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 than this initial assessment.
3. Think of reasons why the impact would be lower than the 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.

4. Decide on the impact class.

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.

<i>Class</i>	<i>Value</i>	<i>Symbol</i>
High	Long-term, but eventually repairable unavailability of the service for all actors.	H
Medium	Partial temporary unavailability of the service for some actors.	M
Low	Noticeable degradation of the service.	L
Extremely high	Very long-term or unrepairable unavailability of the service for all actors. Major redesign of the telecom service is necessary, or the service has to be terminated and replaced with an alternative.	V
Extremely low	Unnoticeable effects.	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.	–

Table 4.2: Characteristic values for normal impact classes.

The expected time to repair must also be taken into account. Repair time is expressed in the phrases “long-term”, “temporary”, and “unrepairable”.

4.3.5 Assessing all vulnerabilities on a components

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. Analytically this means that failures are no longer independent.

For a common cause failure to be possible, it is necessary that the components share a critical property. For physical events such as fire and flooding, this property is geographical distance: the components must be sufficiently close to be affected simultaneously. Other events may have a different critical property. For example, for configuration mistakes it is whether the same maintenance staff is used and for software bugs it is whether same firmware is used, regardless of geographical distance.

For each vulnerability, the critical property has a minimum effect distance. Two equipment items can only be affected by the same fire when they are in the same room, or at most in the same building. Flooding has a much larger effect area, and two components must be further apart to be immune for flooding as their common failure cause.

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 (see section 11).

Example: clusters based on *geographical distance* 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 some vulnerability in a single cluster. Based on the minimal effect distance of the critical property further subdivisions can be made, such that:

- two components in different clusters can never be affected by the same threat event,
- any two components in the same cluster may be affected by the same threat event.

Clusters may be nested. All nodes in a subcluster are members of their parent cluster as well.

Suppose that the critical property is geographical distance. All components within the same rooms can be clustered together. Then, rooms that are within the same building can be clustered into one parent cluster for each building. Then, buildings within the same city can be clustered, etc.

5.2 Analyse each cluster

To analyse a cluster the two factors Frequency and Impact must be assessed. This is done in the same way as for single failures (see section 4.3).

In this stage, the factor Frequency reflects the likelihood that *two or more* components in that cluster are affected by the same threat event. The factor Impact still indicates the overall effect on the telecom service, when the threat event leads to an incident.

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 section 4.4).

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.

The Risk Evaluation stage consists of the following steps:

1. Determine longlist
2. Reduce longlist to shortlist
3. Draft treatment recommendations
4. Assess social risk factors
5. Prepare final report

6.1 Determine longlist

Based on the information presented by the Raster tool (see section 12), 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 section 12.1). 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 Risk treatments

For each risk on the shortlist, the analysts must draft risk treatment recommendations. It is impossible to give guidelines 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 crisis organisation. However, there are four general options that must be considered:

1. **Avoid.** Remove the risk completely (proaction), or discontinue the use of the telecom service. Proaction means eliminating structural causes of accidents to prevent them from happening in the first place (e.g. by prohibiting dangerous activities in urban areas). When discontinuing a service, an alternative service will often be available. However, one 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.

6.4 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 more acceptable to external stakeholders. Analysts must therefore assess additional risk factors that influence risk perception and risk acceptance by third parties. See Table 6.1 for the list of these factors.

<i>Factor</i>	<i>Description</i>
Artificiality, immorality	“Unnaturalness” of risk sources (e.g. electromagnetic radiation from mobile telephony base stations, versus sunlight).
Benefits	Tangible and intangible beneficial effects (e.g. emergency communications, versus entertainment broadcasts).
Blame	Responsibility for damages clearly attributable to some subject, e.g. the telecoms operator.
Catastrophic potential	Fear of sudden, disruptive, large effects, as compared to risks that have a small chronic effect over a period of time.
Children	Amount of risk exposure faced by children in general.
Familiarity	Characterises the 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. Strong control can reduce the risk perception.
Media exposure	Amount of attention by the press and broadcasters.
Mobilisation	Violation of individual, social, or cultural interests and values generating social conflicts and psychological reactions by individuals or groups who feel inflicted by the risk consequences.
Personal control	Level of control that an individual stakeholder can exercise (e.g. ability to control the device and participate in communication, versus only the ability to listen).
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 (e.g. choice of a preferred handset, versus a handset prescribed by regulations).

Table 6.1: List and description of social risk factors.

The analysts must review each risk on the short list, 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 an monitoring and oversight body.

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

6.5 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 crisis organisation (internal scope):
 - a. Position within wider system of crisis response.
 - b. Tasks.
 - c. Responsibilities.
 - d. Telecom services used, together with their role and purpose during crisis response.
 - e. Main actors.
 3. About the environment of the crisis 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
 - d. Recommended risk treatment
 7. Conclusions and recommended actions
- Appendices:
8. Glossary
 9. Diagrams of telecom services
 10. Reports of single failures
 11. Reports of common cause failures

7 Executing the Raster method

Practical guidelines for execution of the Raster method.

7.1 Team composition

Two factors influence the choice and number of analysts.

1. To apply the Raster method to a crisis 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.

These factors indicate that the group of analysts should not be too small. There are disadvantages to having a large group as well. Several steps in the Raster method call for consensus. When the group becomes too large, reaching consensus will be time consuming. Therefore, the group of analysts should include experts from different fields and backgrounds, and should not exceed 10 persons.

Some analysts may opt to not actively participate in the gathering of information and analysis of vulnerabilities. A core group of analysts will then perform most of the tasks. However, it is essential that all analysts participate in all reviews, and agree to the stage results and final report.

7.2 Managing work sessions

Before a Raster project can start, all analysts must be sufficiently familiar with the method. Each analysts should have received a copy of this manual well in advance. Unless all analysts are familiar with the method, an introductory session should be held in which someone who is well acquainted with the method shows its key activities using a small mock-example.

To speed up execution of the Raster method some activities can be performed in parallel. However, the more the analysts break into separate groups, the more they will need to coordinate the integration of their intermediate results later on. After all, the Raster method leads to a single final report, on which all analysts need to agree.

7.2.1 The recorder

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.

In follow-up sessions it may be useful to distribute printouts from the Raster tool for reference (see section 13.2).

7.2.2 Stage 1 — Initiation and preparation

If some of the analysts are not yet familiar with the method, the group should not be divided. Otherwise, two groups could be formed:

1. one group to identify telecom services and actors, and
2. one group to describe disaster scenarios.

This division should only be made if the analysts expect that it will save a large amount of time. Because the Stage 1 results will be referenced throughout the study (in stages 2, 3, and 4) it is important that all analysts are intimately familiar with its contents, which may not be the case when the group is divided.

7.2.3 Stage 2 — Single failures analysis

For analysis of diagrams, the analysts may divide themselves into groups, each group analysing their own subset of telecom services. These groups must then remain in close contact, as components may be present in more than one telecom service and must be assessed in a consistent manner.

It may not be possible to complete the analysis in a single work session. After the initial diagram has been created and analysed, the analysts may decide to expand unknown links, or decide to do further investigations. It may thus require a number of work sessions to complete the single failures analysis.

7.2.4 Stage 3 — Common cause failures analysis

Common cause failures are assessed for the project as a whole, and not for individual telecom services. It is therefore not possible nor useful to divide the analysts into groups.

As with single failures analysis, multiple work sessions may be necessary to complete the analysis of common cause failures.

7.2.5 Stage 4 — Risk evaluation

All analysts must participate in creation of the longlist and shortlist. Most likely this can be completed in a single work session. Based on this shortlist social risk factors must be assessed. This assessment may require further investigation, and it may not be possible to complete this in a single work session. The analysts may decide to break into groups, each group analysing some risks from the shortlist. As with all reviews, it is essential that the assessment of social risk factors be reviewed by the entire group of analysts.

The collation of material into a final report should be done by a small team of editors. 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 6.5.

8 Raster tool

Facilitates execution of the Raster method.

To assist in performing risk evaluations using Raster, a browser based tool is available. For its URL see the inside of the front cover.

All work that you perform with the tool affects one project. A project denotes the complete risk assessment for a single organisation. Typically, a project encompasses several telecommunication services. The 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.

8.1 Working with the tool

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.

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 text file, which can then be stored and transferred as any other file. Exporting is explained in the section 8.3.1. Likewise, such a text 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.

The Raster tool requires the Chrome or Firefox browser. It does not currently work in Safari or Internet Explorer.

8.2 Main views

The tool is divided into 4 views, indicated and selected by the vertical tabs on the left-hand side.

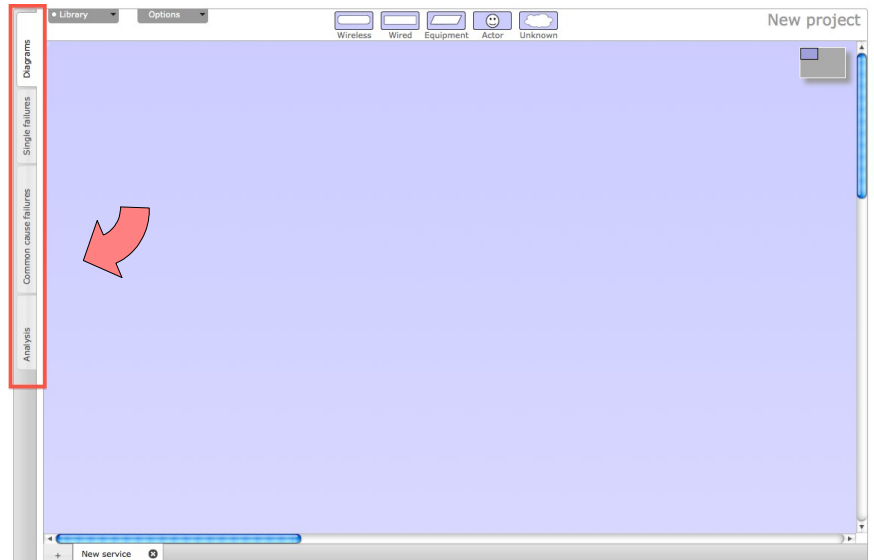
1. **Diagrams** view is used to draw and edit diagrams of telecom services.
2. **Single failures** view is used to assess failures of individual elements.

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.

You can:

- *view* a short description of each tab, by hovering (holding the mouse pointer stationary) over the tab.



8.3 Panels

There are two panels to control the tool: the Library panel and the Options panel. The panels are normally hidden, but can be opened using one of the two buttons along the top of the workspace. You can:

- *open* the panel by clicking its button.
- *close* the panel by clicking the button a second time.
- *close* the panel by clicking anywhere outside the panel.
- *swap* between panels. When one panel is open, hovering over the other button will immediately open that other panel.

8.3.1 The Library panel

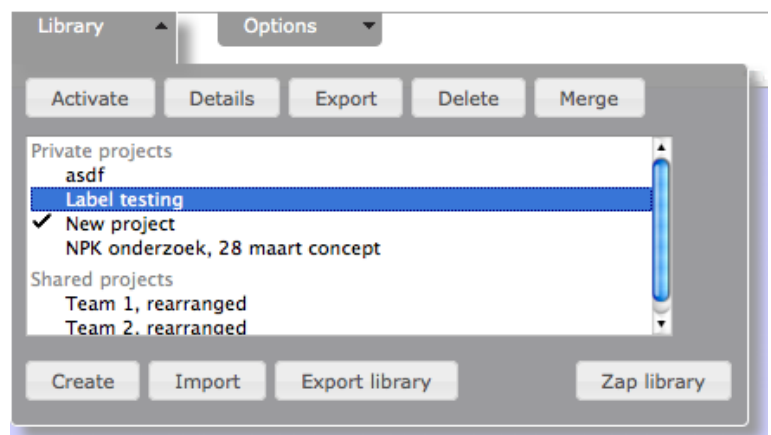
The Library panel shows a list of all projects that are currently available for viewing and editing. The project that is currently active is indicated with a checkmark.

The list of projects is divided into three sections: your private projects, shared projects that you have worked on, and other shared projects.

The highlighted project can be acted upon using the row of buttons above the list.

You can:

- *see the description* of a project, by hovering the mouse pointer over it.



- *activate* the highlighted project (to start viewing and editing it), by clicking the “Activate” button. You can also double-click the project in the list.
- *change properties* of the highlighted project by clicking the “Details” button. Projects have a name, an optional free-text description, and a sharing status (private or shared).
- *save* the highlighted project, by clicking the “Export project” button. The project will be downloaded as a file; the file-name consists of the project name and the current date and time.
- *remove* the highlighted project, by clicking the “Delete” button. If the last project in the list is deleted, it will be replaced with a blank project.
- *merge* the highlighted project into the currently active project. All services of the highlighted project will be re-created as services of the active project.

Below the project list there are buttons for actions that operate on the library itself:

- *create* a new project, using “Add empty project”.
- *import* a previously saved file, using the “Import from file” button.
- *save all* projects using the “Export entire library” button.
- *erase* all services, diagrams and projects, using the “Zap library” button. This will clear *all* information stored in this web browser. Unless you had previously exported your projects onto other storage, you will lose all your work.

Exporting the entire library is not only a convenient way to transfer your work between browsers or machines, but is also useful to create a snapshot of Raster in case of bug reports. Sometimes the tool may show “weird” error messages. Noting down the error and immediately saving the state of your work by exporting the entire library will provide valuable information to improve the tool.

8.3.2 The Options panel

The options panel provides settings and other preferences.

1. *Visual style*: The appearance of the tool can be modified by choosing one of the three styles provided.
2. *Move nodes*: Nodes in the diagram can either be moved freely to any position, or snap to fixed horizontal and vertical increments. The latter makes it easier to align diagram nodes.









3. *Vulnerability levels*: The size of the vulnerability level indicators (see 9.3.3) can be switched between large and small, or they can be hidden entirely.
4. *Labels*: The colors 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 colors when you find this too distracting, or before printing to a black and white printer.
5. *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.
6. *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.

You can always find the present document using the link “see the manual”.

The preferred size of the vulnerability level indicators and the label colors also affecting printing.

8.4 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)
	Ambiguous, the assessors have conflicting opinions (purple)
	Extremely (very) high, an extreme risk (bright red)
	High (red)
	Medium (yellow-orange)
	Low (green-orange)
	Unknown, because of lack of knowledge (sky blue).
	Extremely (ultra) low, the risk level is negligible or absent (bright green)

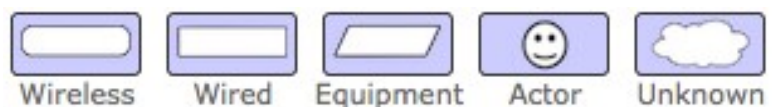
9 Diagrams view

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 a row of 5 templates, buttons to activate the Projects, Service, and Options panels, and an indicator of the active project.

9.1 Templates

Templates contain default settings for new diagram nodes. You can:



- *view* a short description of the template, by hovering (holding the mouse pointer stationary) over the template.
- *create* new nodes by dragging one of the templates into the workspace.

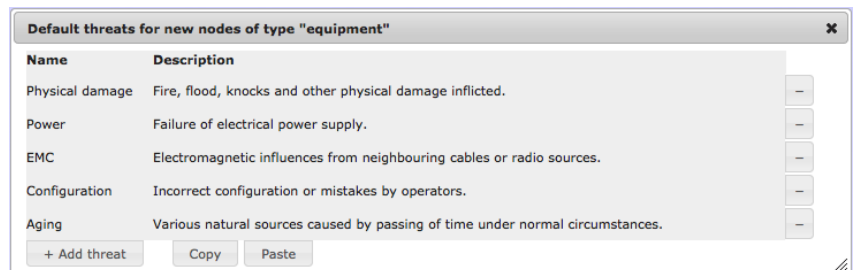
For the first three elements (wireless links, wired links, and equipment items), you can modify the predefined checklists. Click the drop-down indicator to open the checklist window for that element type.



9.2 Checklist windows

Wireless links, wired links, and equipment items each have a list of default vulnerabilities. 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)
- *remove* a vulnerability, by clicking the minus-button on the right. You will be asked to confirm the deletion.
- *add* a new vulnerability, by clicking the “+ Add vulnerability” button.
- *copy* the checklist, so that you can paste it into a vulnerability assessment for a node.
- *paste* the vulnerabilities of a vulnerability assessment.



The vulnerabilities that you create this way will be used as templates for any new element nodes that you create. Once created, each element node has its own independent list of vulnerabilities. Editing the checklists will not affect existing nodes in any way.

Suppose that you have been working on a diagram and notice the omission of a vulnerability in a checklist. Rather than adding that vulnerability to each node that you have created, you can add it to the checklist with the “+ Add vulnerability” button. To quickly update all existing nodes, you then Copy the list of vulnerabilities. Switch to the Single Failures view, and Paste the vulnerability list into each existing node of that type, and into each unknown link. When pasting, any vulnerability assessments that have been filled in will be preserved. Pasting is a quick way to correct a forgotten checklist vulnerability.

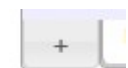
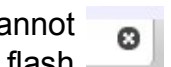
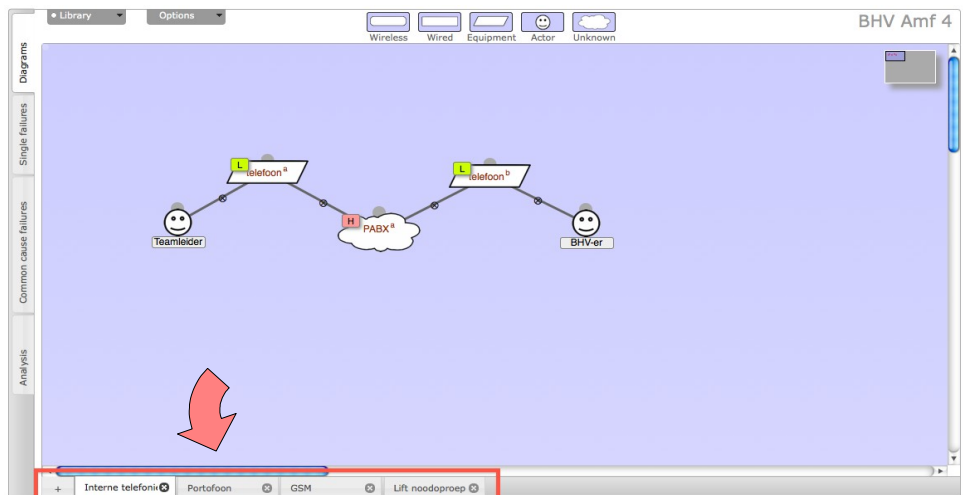
9.3 Workspace

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.

9.3.1 Service tabs

Each service has a tab at the bottom of the screen.

- You can:
- *view* the service diagram for a service, by clicking its tab.
 - *see* the full name of the service (it will be cut off beyond the close button), by hovering the mouse pointer (keeping it stationary) over the truncated name.
 - *remove* a service, by clicking the close 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. A popup window will appear, in which you can enter the new name. End by pressing the Enter key, or click the “Change name” button. Cancel by clicking the Cancel button, or press Escape.



Rename service 'New service'

Change name Cancel

9.3.2 The scroller

The workspace onto which nodes are drawn and connected, is larger than can be displayed on the screen. Use the scroller to change the current view.



The large grey area of the scroller represents the total available workspace, while the smaller blue rectangle corresponds to the area that is currently visible. 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.

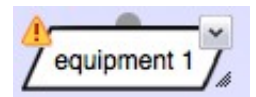
With the scroller you can:

- *move* the visible area, by dragging the blue rectangle around.
- *move* the scroller itself, when it gets in the way, by dragging the grey rectangle around.

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.

9.3.3 Diagram nodes

Each node is visually represented as a shape with its name and up to five decorations. 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.
 2. The *vulnerability level indicator* in the top-left corner indicates the overall risk level for that node, using a colour. This indicator is hidden when the warning triangle is shown.
 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.
- If you prefer a larger vulnerability level indicator, you can choose one using the Options panel. The larger size contains the first letter of the class name (H for High, M for Medium, etc).



With a node you can:

- *view* the warning report, by clicking on the warning triangle. The report is updated immediately when the status of the node changes; you do not need to click the triangle again to refresh the report.
- *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 (see 9.3.7), and drag the selection rectangle to move the selected nodes only.

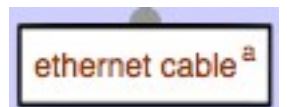
- *rename* the node, by clicking its title. Note that the area becomes orange when you hover the pointer over the title. Confirm by clicking somewhere outside the workspace, or press Enter. Cancel the action (that is, revert to the current title) by pressing Escape.
- *resize* the node, by dragging its resize handle. You can increase the size up to twice the normal size.

- *call up* the menu, by clicking the drop-down indicator. Alternatively, you can right-click anywhere on the node. Click the desired menu item; click anywhere outside the menu to cancel.
- *view* an explanation of the vulnerability level, by hovering the mouse pointer over the coloured vulnerability level indicator.

Instead of clicking the drop-down indicator, and then clicking the desired menu item, you can also press and hold the mouse button over the drop-down indicator, move the pointer to the desired menu item, and release the mouse button over that menu item.

9.3.4 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.



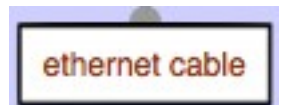
You create a node class by giving one node the same name as another node of the same type. Both nodes will be put into the class. You can add as many nodes as you need, again by renaming nodes to the name of the class.

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.

9.3.5 Identical nodes

Sometimes the same component appears in two different services. By giving the nodes the same name in each service diagram, a node class is created. To mark the node class as a single physical component instead of two similar “copies”, you 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.

9.3.6 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, you cannot connect an actor 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 *double-clicking* its disconnect button. 

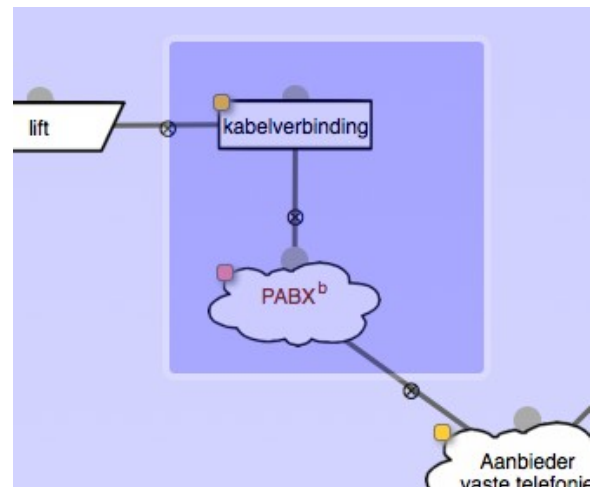
Connections cannot be moved; they automatically follow the two nodes that they connect.

It is possible to have more connections than allowed by the connection rules for that node type (see section 2.2). 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.

9.3.7 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. You can:

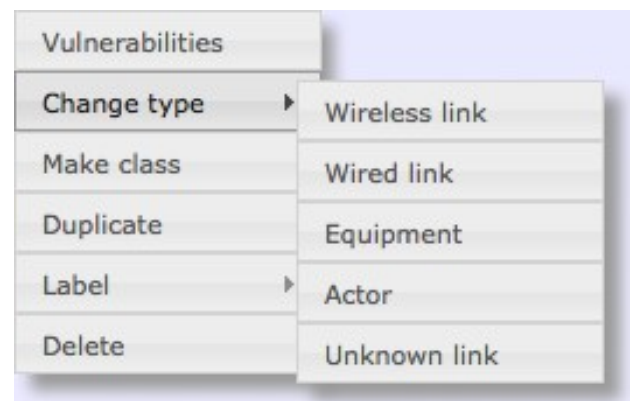
- *delete all nodes* in the selection, by *right-clicking* the selection rectangle and choosing “Delete selection” from the popup menu.
- *label all nodes* in the selection, by right-clicking the selection rectangle and choosing the appropriate label from the menu.
- *move all nodes* in the selection, by dragging the selection rectangle itself.



9.3.8 The node menu

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

- *call up* the vulnerability assessment window (see below).
- *change* the type of the node (e.g. from a wireless link into a cloud).
- *change* the type of the node class from a single identical node into a collection of similar nodes, and vice versa (see 9.3.5).
- *duplicate* the node. This will create an exact duplicate, including any vulnerabilities and assessments.
- *label* the node, using one of the 7 available labels (see 9.3.9).
- *delete* the node.



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.

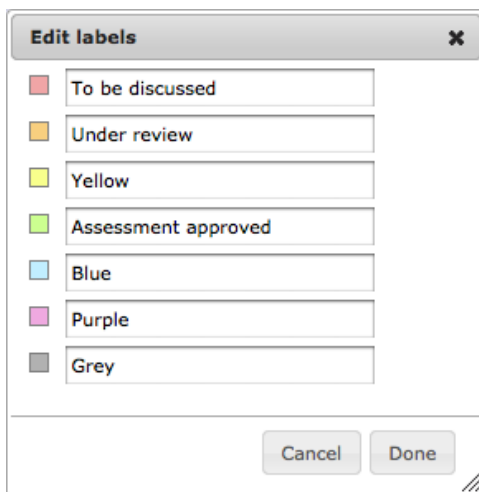
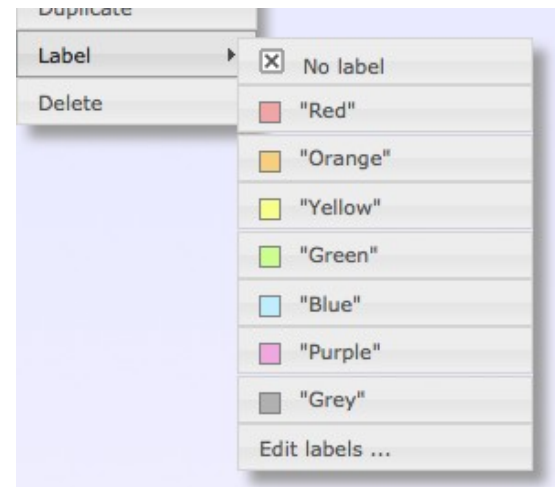
Changing the node type can be used to correct a mistake (for example, you intended to create a wired link but accidentally used the rounded rectangle, which is for wireless links).

Changing node types is also useful to convert an equipment item into a cloud, if you notice during your analysis that the situation is more complex than you previously thought.

9.3.9 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. Labels are optional, and have no relation to vulnerability assessments.

To assign a label, choose one from the Label submenu. To remove the label, choose "No label" from that menu. When a node has been given a label, that label will appear in the node menu for that node.

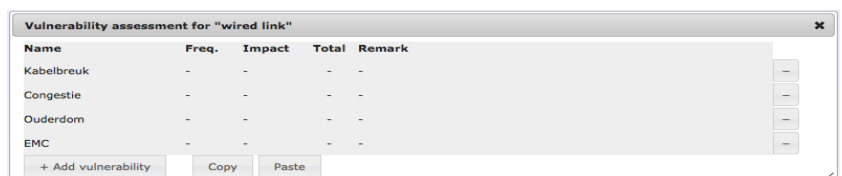


A node cannot have more than one label. Each label is visually indicated in the diagrams using a color (to disable this, use the setting in the Options panel: see 8.3.2). Note that these colors have no relation with the colors that are associated with vulnerability levels.

The labels themselves are preset to the names of their color, but can be changed by choosing "Edit labels..." from the node menu. Reset a label to its default value by making it blank.

9.3.10 Vulnerability assessment window

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).
- *view* the description of the vulnerability, by hovering the pointer over the title.
- *add* or *edit* remarks.
- *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 4.3.1 about removing vulnerabilities.
- *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.

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

Copy and Paste also functions between projects. You can copy the checklists or vulnerability assessment in one project, switch to another project, and paste into it.

10 Single failures view

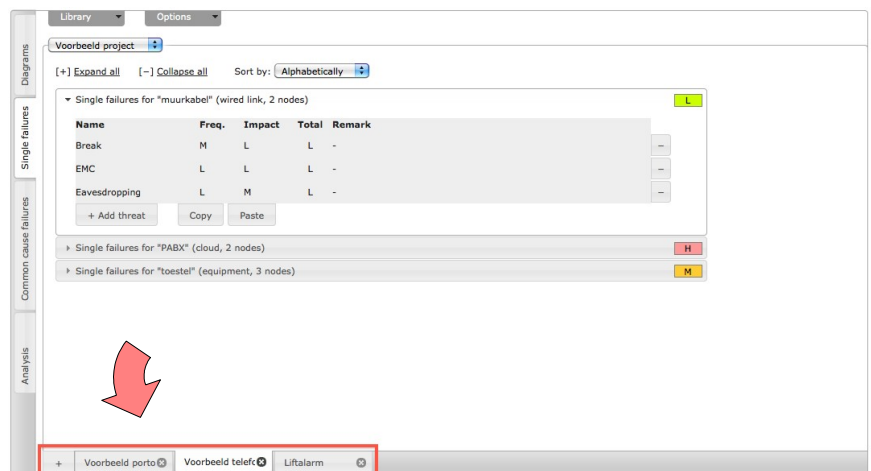
Assess single failures to components.

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

Like Diagrams view, Single failures view is divided into tabs, one for each service. You can:

- *view* the vulnerability assessments for all nodes of a service, by clicking its tab.
- *view* the full name of the service (it will be cut off beyond the close button), by hovering the mouse pointer (keeping it stationary) over the truncated name.
- *remove* a service, by clicking the close 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. A popup window will appear, in which you can enter the new name. End by pressing the Enter key, or click the “Change name” button. Cancel by clicking the Cancel button, or press Escape.



10.2 Vulnerability assessment headers

► Single failures for "muurkabel" (wired link, 2 nodes)

Each node or node class in the selected service is shown using a collapsible header.

With the header you can:

- *see* the vulnerability, the name of the node, its type, and in the case of a node class the number of nodes in that class.
- *see* if the vulnerability assessment is incomplete. 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 “-”.

- see the overall vulnerability level, in the coloured emblem on the right side of the header. Hover the mouse pointer over the colour marker to see a short description.
- *open* the vulnerability assessment, by clicking the header of a collapsed vulnerability assessment.
- *close* the vulnerability assessment, by clicking the header of an expanded vulnerability assessment.
- *collapse* or *expand* all vulnerability assessments at once, using the Collapse all and Expand all links at the top of the view.

10.3 Vulnerability assessments

When a header is expanded (opened), the full vulnerability assessment of that node becomes visible. In this area you can:

▼ Single failures for "muurkabel" (wired link, 2 nodes) L

Name	Freq.	Impact	Total	Remark
Break	M	L	L	-
EMC	L	L	L	-
Eavesdropping	L	M	L	-

+ Add threat Copy Paste

- *rename* a vulnerability, by clicking its title (press Enter/click elsewhere to confirm, press Escape to cancel).
- *view* the description of the vulnerability, by hovering the pointer over the title.
- *add* or *edit* remarks.
- *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 4.3.1 about removing vulnerabilities.
- *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, for 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 that are on the clipboard but not yet present in the destination will be created.

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 assessment headers

► Common Cause failures for "Break" (wired link)

Each common cause failure is shown using a collapsible header. With the header you can:

- see the vulnerability, and its type.
- see if the vulnerability assessment is incomplete. The marker (*Incomplete*) appears when any one vulnerability assessment in the cluster has not been completed. An assessment is complete when both the frequency and impact are set to a value other than “–”.
- see the overall vulnerability level, in the coloured emblem on the right side of the header. Hover the mouse pointer over the colour marker to see a short description.
- *open* the vulnerability assessment, by clicking the header of a collapsed vulnerability assessment.
- *close* the vulnerability assessment, by clicking the header of an expanded vulnerability assessment.
- *collapse* or *expand* all assessments at once, using the Collapse all and Expand all links at the top of the view.

11.2 Node clusters

When a header is expanded (opened), all nodes having that vulnerability are listed. Nodes can be sorted

into clusters. Each cluster has a name and member nodes, Common cause failures must be assessed for each cluster with the usual frequency and impact measures.

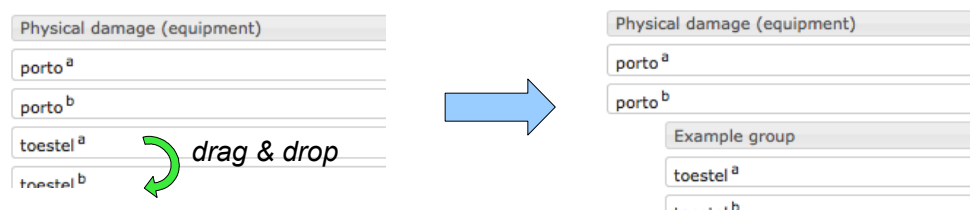
▼ Common Cause failures for "Break" (wired link)

Break (wired link)				
schacht-kabel				
muurkabel ^a				
muurkabel ^b				
Name	Freq.	Impact	Total	Remark
Break	–	–	–	–

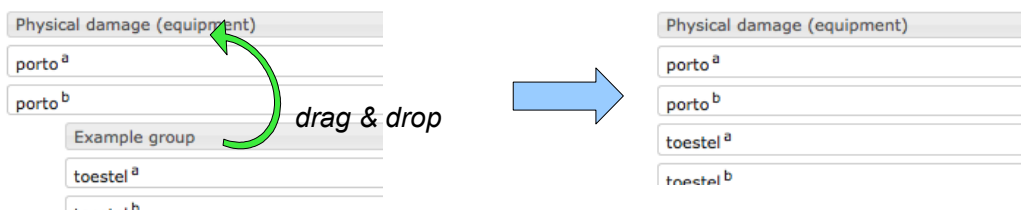
Nodes and subclusters arranged and rearranged using 'drag and drop'. Subclusters are dragged by dragging their header row. While dragging a node or subcluster, all possible drop targets light up in pale green.

You can:

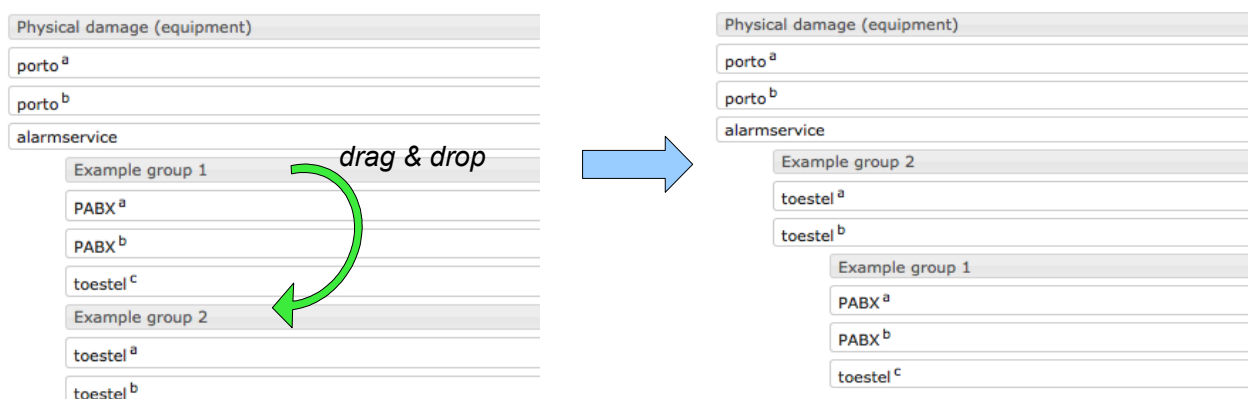
- *rename* a cluster, by clicking its title. Note that the area becomes orange when you hover the pointer over the title. Confirm the new title by clicking somewhere outside the workspace, or press Enter. Cancel the action (that is, revert to the current title) by pressing Escape. The top-most cluster is named after the vulnerability, and cannot be renamed.
- *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 member nodes will be shown beneath it, indented from the left margin.



- *move* a node, 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 below:



Each sub-cluster has a vulnerability level indicator, similar to the indicators in Single Failures view. The overall vulnerability level of the vulnerability is shown at the top, and will be visible even when the vulnerability is collapsed.

11.3 Vulnerability assessments

When a header is expanded (opened), the full vulnerability assessment of that common cause failure becomes visible.

Name	Freq.	Impact	Total	Remark
Stroomuitval	M	M	M	-
Verre buitenland	A	X	A	-
Nederland	X	M	X	-
Groningen	M	M	M	-
Server ruimte	U	L	U	-
Amersfoort	U	L	U	-
Server ruimte	L	L	L	-

In this area you can:

- *change* frequency and impact. Click to activate the selection widget. Click the widget to open it, or type the letter of your choice.
- *add* or *edit* remarks.

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

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.

Single failures	Bedieningsfout	Congestie	Congestie	Diefstal	EMC	EMC	Fysieke schade	Interferentie	Jamming	Kabelbreuk	Ouderdom	Signaal 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
base station	H			L		M							H	L	H
s onder vergunning			H				M	U					H		H

12.2 Single failures by level

These tables show an overview of all single failures. The Frequencies table shows how often each frequency was assigned in the Single Failure analysis stage, including the totals per frequency class and per node class. 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 4.3.1 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.

13 Technical issues

Using the Raster tool in a browser, and below-the-surface info.

13.1 Supported web browsers

The Raster tool was developed for Firefox 4 and later. It also works on Google Chrome, but does not work on Internet Explorer (IE9 and earlier), nor on Safari (version 5 and earlier). It has not been tested in IE10 or Safari 6 (which as of writing are only available for limited testing purposes).

When exporting projects or the entire library with Chrome it is best to set the browser to ask for a download folder, instead of using a default folder.

13.2 Printing

You can print a diagram, its list of single failures, its 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 scroller is reset to the top-left position and single or common cause failures are expanded just before printing. With other browsers, you must 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 with Raster; the printed document does not contain background images.

You can use the Options panel to set the size of the vulnerability level indicators and choose whether label colors are printed. These settings apply to both the printed and the on-screen version of the tool.

There are bugs in common web browsers. Google Chrome earlier than version 17 could not print background colours. Firefox has a minor annoyance that page breaks may appear in inconvenient places.

13.3 Browser tabs

It is possible to use multiple tabs or browser windows with Raster. This way you can view or even edit multiple projects at once. However, it is *not recommended* to view

or edit the same project in more than one window or tab. Changes made in one tab or window will not be reflected in the other window, and your project's data is likely to become corrupted. The tool will not warn you when you open the same project twice, so you must be very careful.

13.4 Computation of vulnerability levels

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

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.

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

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.

Index

A

actor, 6, 12
 main, 12
 secondary, 12
 vulnerabilities, 15
 ambiguous, **17**, 18, 21, 24, 25
 analyst, 2, 29
 editor, 30
 recorder, 29
 artificiality, 27

B

backup, 11, 25
 benefits, 27
 blame, 27
 browser, 31, 51

C

catastrophic potential, 27
 checklist, 15, 35
 children, 27
 class,
 ambiguous, **18**, 21, 24, 25
 colour, 34
 extremely high, 18, 20, 25
 extremely low, 18, 20
 high, 18, 20, 25, 56
 low, 18, 20
 medium, 18, 20, 56
 node class, 38
 not yet analysed, 18
 unknown, **18**, 21, 24, 25
 cluster, 23, 45
 colour, 34
 common cause f. analysis
 stage, 6, **23**, 30
 common cause failure, 2, 23
 connector, 37, 38
 copy and paste, rules, 44
 countermeasure, 18
 crisis organisation, 2
 critical property, 23

D

decision maker, 1, 3, 26
 diagram, 6, 15, 35

printing, 51

disaster scenario, 12, 19
 drop-down indicator, 35, 37
 duplicate, 39

E

editor, 30
 equipment, 8, 16
 expansion, 21, 24
 export, 33
 external stakeholder, 3, 26
 extremely high, 18, 20, 25
 extremely low, 18, 20

F

fallback, 11, 25
 familiarity, 27
 fear, 27
 frequency, 17, 24, 52

G

glossary, 12
 grid, 33

H

high, 18, 20, 25, 56

I

impact, 17, 19, 52
 import, 33
 initiation and preparation
 stage, 5, **11**, 30
 institutional control, 27

L

label, 39, 40
 library, 32
 erase, 33
 export, 33
 life time, 18
 longlist, 25
 low, 18, 20

M

media exposure, 27

medium, 18, 20
 mobilisation, 27
 monitoring, 19, 20

N

node, 37
 class, single, 38
 cluster, 45
 connecting, 38
 disconnecting, 39
 identical, 38
 move, 37
 node class, 38
 rename, 37
 resize, 37
 node class, 38

P

personal control, 27
 preparation (risk treatment), 26
 prevention, 26
 printing, 51
 prioritise, 25
 proaction, 26
 project, 33
 create, 15, 33
 import, 33

Q

quick win, 25, 49

R

raster method,
 outline, 5
 recorder, 29
 redundancy, 19
 repair time, 20
 resize indicator, 37
 review, 13, 21, 24, 28
 risk evaluation stage, 6, **25**, 30
 risk treatment, 26

S

scroller, 36
 shortlist, 25

single failures analysis stage, 5, 15 , 30	T	visual style, 33
snap, 33	telecom service, 11	voluntariness, 27
social risk factor, 26	templates, 35	vulnerability level indicator, 34, 37
sponsor, 3, 13, 28		
stage, common cause failures analysis, 6, 23 , 30	U	W
initiation and preparation, 5, 11 , 30	unknown, 17 , 18, 21, 24, 25	warning triangle, 37
risk evaluation, 6, 25 , 30	unknown link, 8	wired link, 7, 16
single failures analysis, 5, 15 , 30	expansion, 21, 24	wireless link, 7, 16
stage 1 report, 12	social risk factor, 12	
	V	Z
	violation of equity, 27	zoom in, 37

Please help to improve this index!

Write down and report any index entries that you find missing.

.....
.....
.....
.....
.....
.....

Quick reference

Frequency

<i>Class</i>	<i>Value</i>	<i>Symbol</i>
High	Once in 5 years. For 1000 identical components, each month 15 will experience an incident.	H
Medium	Once in 50 years. For 1000 identical components, each month 1 or 2 will experience an incident.	M
Low	Once in 500 years. For 1000 identical components, each year 2 will experience an incident.	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.	–

Impact

<i>Class</i>	<i>Value</i>	<i>Symbol</i>
High	Long-term, but eventually repairable unavailability of the service for all actors.	H
Medium	Partial temporary unavailability of the service for some actors.	M
Low	Noticeable degradation of the service.	L
Extremely high	Very long-term or unrepairable unavailability of the service for all actors. Major redesign of the telecom service is necessary, or the service has to be terminated and replaced with an alternative.	V
Extremely low	Unnoticeable effects.	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.	–

Vulnerability levels

-	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)

Overview of the Raster method

Stage 1 — Initiation and preparation	chapter 3, page 11
1. Identify telecom services	
2. Identify actors	
3. Describe disaster scenarios	
4. Create Stage 1 report	
5. Obtain approval from sponsor	
Stage 2 — Single failures analysis	chapter 4, page 15
1. Update the checklists of vulnerabilities	
2. Draw initial diagrams	
3. Analyse the frequency and impact of components	
4. Expand unknown links	
5. Review	
Stage 3 — Common cause failures analysis	chapter 5, page 23
1. Create clusters	
2. Analyse each cluster	
3. Expand unknown links	
4. Review	
Stage 4 — Risk evaluation	chapter 6, page 25
1. Determine longlist	
2. Reduce longlist to shortlist	
3. Draft treatment recommendations	
4. Assess social risk factors	
5. Prepare final report	

Suggested outline of the final report

1. Executive summary to the final report.
2. About the crisis organisation (internal scope):
 - a) Position within wider system of crisis response.
 - b) Tasks.
 - c) Responsibilities.
 - d) Telecom services used, together with their role and purpose during crisis response.
 - e) Main actors.
3. About the environment of the crisis 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
 - d) Recommended risk treatment
7. Conclusions and recommended actions
8. Appendices:
9. Glossary
10. Diagrams of telecom services
11. Reports of single failures
12. Reports of common cause failures

