

Securing continuity and Availability

Risk-wise Assessment and Step-wise Resolution (RASTER)

APrIGF 2018
Porto Vila, Vanuatu



Ministerie van Economische Zaken
en Klimaat



Agenda

- Introductions & quick intro to IOT and Risk, show video
- Naveed Haq (ISOC)
 - ISOC cyber security agenda
- Jackson Miake (OGCIO)
 - development and implementation of Vanuatu's ICT & telecommunications policies
 - drafting the Vanuatu cybersecurity bill and advocating it through the legislative process
- Eecho Vriezokolk (University of Twente)
- Nuwan Waidyanatha (LIRNEasia)
 - Overview of availability, survivability and the Raster tool
 - Demonstrate the Myanmar use-case with Raster
 - Discuss and analyze the Vanuatu use-case with Raster
- Shazna Zuhyle (LIRNEasia)
 - Broadband Internet availability in Asia and the Pacific

IOT and Organizations

- In the past a telecommunications outage was an inconvenience, today they, often, makes it impossible to do business
- unavailability of telecom services often happens with component failure
 - Access to networks (not what we are after) but important for APPs to work everywhere
 - Survivability and availability during incidents (i.e. robustness)

Raster past projects

1. Diversity: commercial and non-commercial, health care, public administration, industry.
2. Regional fire and emergency service: after a recent reorganisation and redesign of internal IT systems.
3. Regional water board and flood protection agency: an old organisation (>100 years) that had many “old fashioned” workarounds for telecom failure, and therefore highly resilient.
4. Local municipality: human-induced earthquakes, and their effect on underground infrastructures.
5. Industrial area: shared services to several chemical factories, after internal relocation of fire and emergency services.
6. Elderly health care: transition towards home-care and increasing use of eHealth technologies increase dependency on telecommunication.
7. Regional airport: non-safety critical operations affect the commercial viability of the airport. Special interest on service level agreements.
8. Festivals and events: ensuring visitor safety during large temporary events (e.g. music festivals).
9. Electrical grip operator: interdependency between electricity and telecommunication during repairs and maintenance.
10. Process industry: move towards Industry 4.0, increased use of sensors and Internet of Things technologies increase the dependency on telecommunications.

Lessons learned

1. Older organisations have an advantage: there is still a collective memory of how primary processes were conducted before IT and automation. Fallbacks are still present. New organisations are often IT-only.
2. Technical organisations are better equipped to assess telecom risks. Health care, for example, require more support than industry.
3. Risk treatment: often organisational, and far less often technical. For example: use of paper files as fallback, having extra personnel on site.
4. Old technology is not necessarily more risky, provided that you ensure: ongoing training, maintenance, and availability of spare parts.
5. Risk assessment can be done by any organisation, using the knowledge of existing employees. Anyone can contribute. But it does require an experienced moderator / project leader.
6. When automating an existing process, do try to retain the old manual system, as it provides an excellent fallback. When buying new shoes, keep the old ones as spares.
7. The more reliable infrastructure becomes, the higher the impact of (rare) failures. Reliability breeds complacency, lack of preparation. Incidents at least have a beneficial effect in that they do shake up policy makers.

Raster Methodology

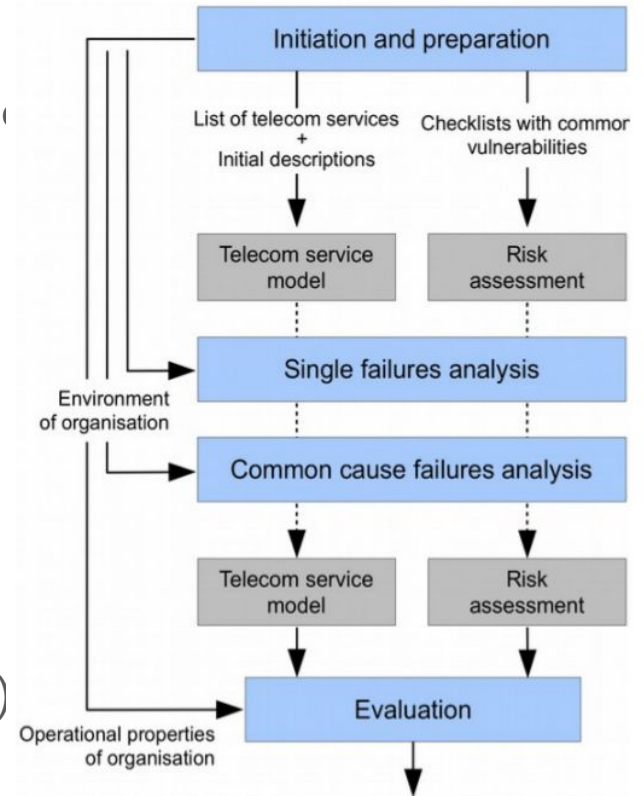
The goal of Raster is to make the organisations becomes less vulnerable to teleco failures by first understand what can go wrong with each telecom service they use.

Raster facilitates the:

- construction of a recommendation using a tested methodical analysis
- recommendations are prepared:
 - based on the technical aspects of failure of telecoms services
 - also takes account of the societal impact of failures, and
 - risk perceptions of external stakeholders.

How is it done

1. Applied by a team of experts:
 - 1.1. Case Organization, Sponsor (responsible person), and
 - 1.2. Project Manager & Analyst(s)
 - 1.3. Team members & external Stakeholders
2. Initiation & Preparation
 - 2.1. Identify telecom services
 - 2.2. Identify team & procedures
3. Single Failure Analysis (component-wise)
4. Common cause Failure Analysis (cluster-wise)
5. Risk Evaluation (recommendations)



Social Risk Factors

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

Evaluation - telecom impact to organizational impact

1. Risk of failure is limited to the telecommunication service itself.
2. Risk evaluation translates this into risk to the organisation.
3. Four steps:
 - a. Determine a longlist.
 - b. Combine and select the longlist into a shortlist.
 - c. Determine social risk factors, prioritise the shortlist, and make treatment recommendations.
 - d. Final report.

Risk Assessment Procedure

1. Pick the class that typically applies to items of this kind and usage.
 - a. Think of reasons why the frequency/impact could be higher in this case.
 - b. Think of reasons why the frequency/impact could be lower in this case.
2. Making estimates is a group effort.
 - a. Pool your expertise, convince using arguments, reach consensus.
 - b. Make reasonable assumptions.
 - c. When uncertain, or when consensus cannot be reached, then mark as “Unknown”.
 - d. When consensus cannot be agreed, pick “Ambiguous”.
 - e. High uncertainty and lack of consensus are valid outcomes!

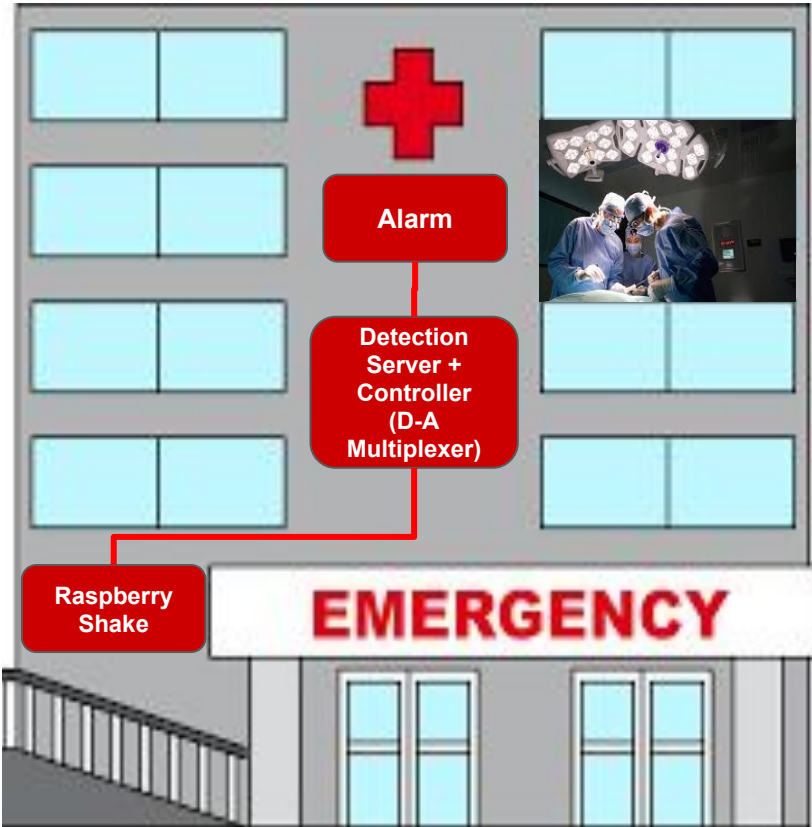
Risk Frequency (how often does it occur)

Class	Description	Symbol
Extremely High	Once in 10 days, routine event	V
High	Once in 06 months, happens often For 100 identical components 10 will experience an incident	H
Medium	Once in 12 months, not frequent but an incident does occur For 100 identical components 1 will experience an incident in 1 year	M
Low	Once in 05 years, rarely For 100 identical components, 1 will experience an incident in 5 years	L
Extremely Low	Once in 50 years, very rare For 100 identical components, 1 will experience an incident in 5 years	U
Ambiguous	Indicates lack of consensus among analysts	A
Unknown	Not yet analyzed, indicated lack of knowledge	X

Risk Impact (How does it effect business as usual?)

Class	Description	Symbol
Extremely High	Very long term, unreparable and unavailable (> 06 months) 100% of the actors are affected	V
High	Unavailable and if unreparable then has a long term effect (< 01 month) 50% of the actors are affected	H
Medium	Partially unavailable and if unreparable then has a medium term effect (< 01 day) 10% of the actors are affected	M
Low	Partially unavailable and if unreparable then has a short term effect (< 1 hour) 1% of the actors are affected	L
Extremely Low	Unnoticeable effect No actors are affected	U
Ambiguous	Indicates lack of consensus among analysts	A
Unknown	Not yet analyzed, indicated lack of knowledge	X

RaspberryShake Alarm



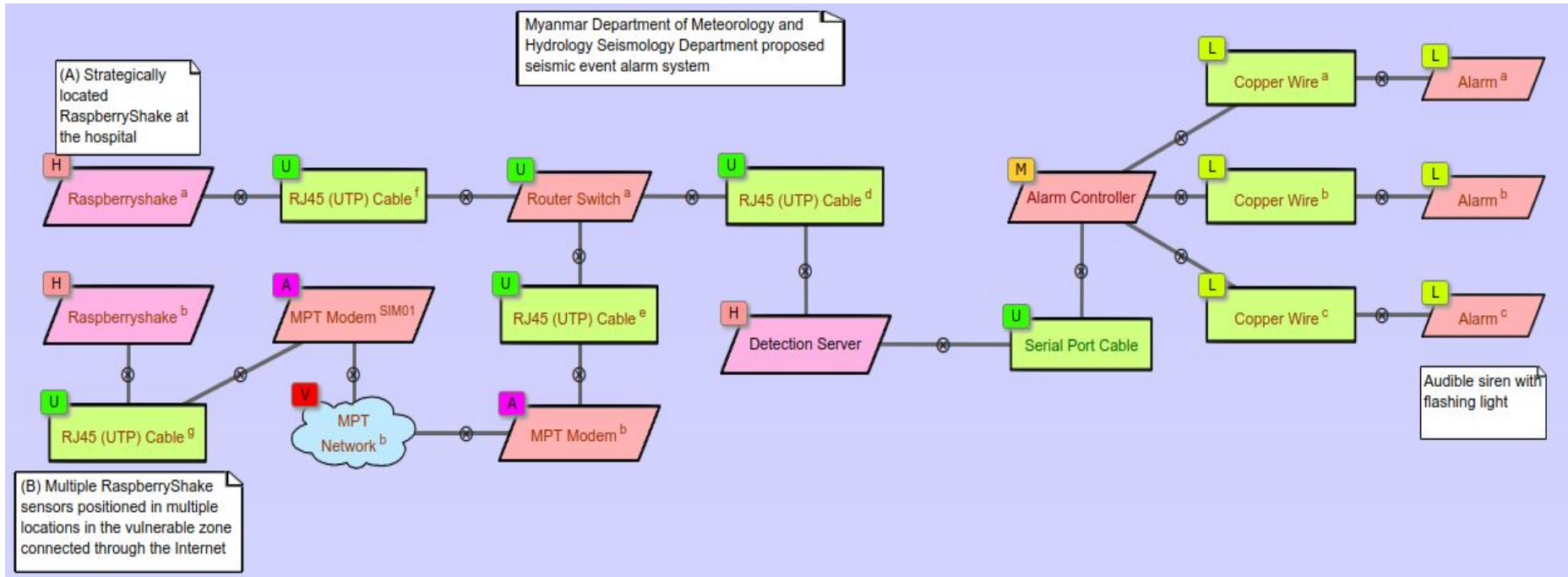
making use of the Primary earthquake wave to forewarn hospital staff to, example:



- Prevent surgical accidents by forwaning, with an audible siren and flashing lights,
- Stop elevators at the next floor



Raster diagram - earthquake alarm system



Single Failures

- ▶ Single failures for "Alarm" (equipment, 3 nodes) ● Red L
- ▶ Single failures for "Alarm Controller" (equipment) ● Red M
- ▶ Single failures for "Copper Wire" (wired link, 3 nodes) ● Green L
- ▶ Single failures for "Detection Server" (equipment) ● Purple H
- ▼ Single failures for "MPT Modem" (equipment, 3 nodes) ● Red A

Name	Freq.	Impact	Total	Remark
Physical damage	U	U	U	-
Power	U	V	A	-
Configuration	U	L	U	-
Malfunction	U	L	U	-
- ▶ Single failures for "MPT Network" (cloud, 2 nodes) ● Blue V
- ▶ Single failures for "Raspberrysake" (equipment, 2 nodes) ● Purple H
- ▶ Single failures for "RJ45 (UTP) Cable" (wired link, 7 nodes) ● Green U
- ▶ Single failures for "Router Switch" (equipment, 2 nodes) ● Red U
- ▶ Single failures for "Serial Port Cable" (wired link) ● Green U

Common Failures

▶ Common Cause failures for "Configuration" (equipment)	A			
▶ Common Cause failures for "Congestion" (wired link)	L			
▶ Common Cause failures for "Congestion" (wireless link)	M			
▶ Common Cause failures for "Interference" (wireless link)	A			
▶ Common Cause failures for "Jamming" (wireless link)	A			
▶ Common Cause failures for "Malfunction" (equipment)	V			
▶ Common Cause failures for "Physical damage" (equipment)	A			
▶ Common Cause failures for "Power" (equipment)	V			
▼ Common Cause failures for "Signal weakening" (wireless link)	H			
Name	Freq.	Impact	Total	Remark
Signal weakening	M	H	H	
Signal weakening (wireless link)				
GSM/WCDMA Link ^a				Yellow
GSM/WCDMA Link ^c				Yellow
VHF Link ^a				Yellow
VHF Link ^d				Yellow
MPT Network ^a				Blue
MPT Network ^b				Blue
Other Networks				Blue
Relay Network				Blue

Analysis of the Single and Common Failures

Single failures	Break	Cable aging	Configuration	Congestion	Congestion	Interference	Jamming	Malfunction	Physical damage	Power	Signal weakening	Overall
MPT Modem		U						U U A				A
MPT Network	X	U	X	M	X	A	A	V X V	H	V		V
Detection Server		U						U U H				H
Raspberrysake		U						U U H				H
Alarm Controller		U						L U M				M
Alarm		U						U U L				L
Copper Wire	U	L		U								L
RJ45 (UTP) Cable	U	U		U								U
Router Switch			U					U U U				U
Serial Port Cable	U	U		U								U

Common cause failures

Break	A											A
Configuration			A									A
Physical damage									A			A
Malfunction								V				V
Power										V		V
Congestion				L								L
Cable aging		U										U

- MPT network malfunctioning, power, and signal weakening are the key single component failures
- Power and equipment malfunctions are the common failures that can be fixed for quick wins

Engage participants in the analysis and decisions

1. Assign roles

1.1. Speakers:

1.1.1. Sponsors, facilitating the project

1.1.2. Analyst / Raster method facilitator

1.2. Participants:

1.2.1. Team of experts who know about Power, Configuration, Damage

1.2.2. Decision-makers approving the recommendations

2. Define the single and common failure vulnerabilities

3. Analyze to decide on recommendations (quick wins)