e-Resilience Survivability and Availability Exercise: the RASTER Method

Subregional workshop on implementation of the Asia-Pacific Information Superhighway for achieving the Sustainable Development Goals in Pacific island countries

20 November 2018
Nadi, Thailand

Nuwan Waidyanatha
Senior Research Fellow
nuwan@lirneasia.net

LIRNEasia
Pro-poor. Pro-market.

BCP

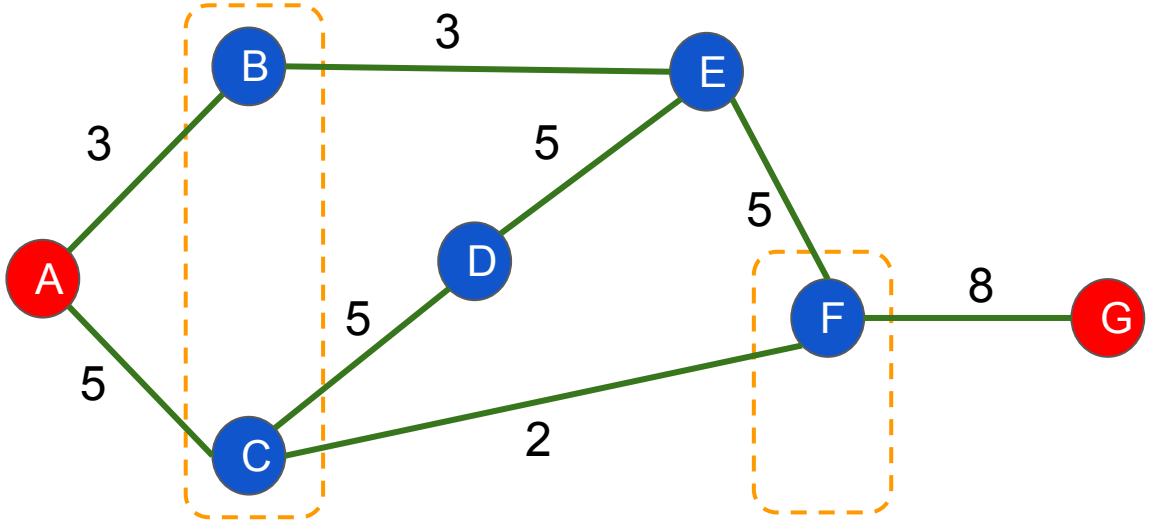
QUESTIONNAIRE

https://goo.gl/47cV5x

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 quite what we are after) but important for APPs to work everywhere
  - Survivability and availability during incidents (i.e. robustness)

Points of Failure and Impact



Either failure types can cause 100% downtown and maximize impact on business continuity

- Common point of failure - single event that affects a collection of nodes
  - E.g. power outage
- Single point of failure - single event affects a one nodes
  - E.g. physical damage
- Impact is the minimum cut that affects the maximum flow
  - E.g. removing node E forces to use a lower bandwidth edge CE

Raster Methodology

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

Raster facilitates the:

- Uncovering of “black swans”
  - Risk with low probability and high impact (or effects)
  - Basically, rare catastrophic events that bring your comms down to their knees.
- Preparation of recommendation using a tested methodical analysis:
  - 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

Raster past projects

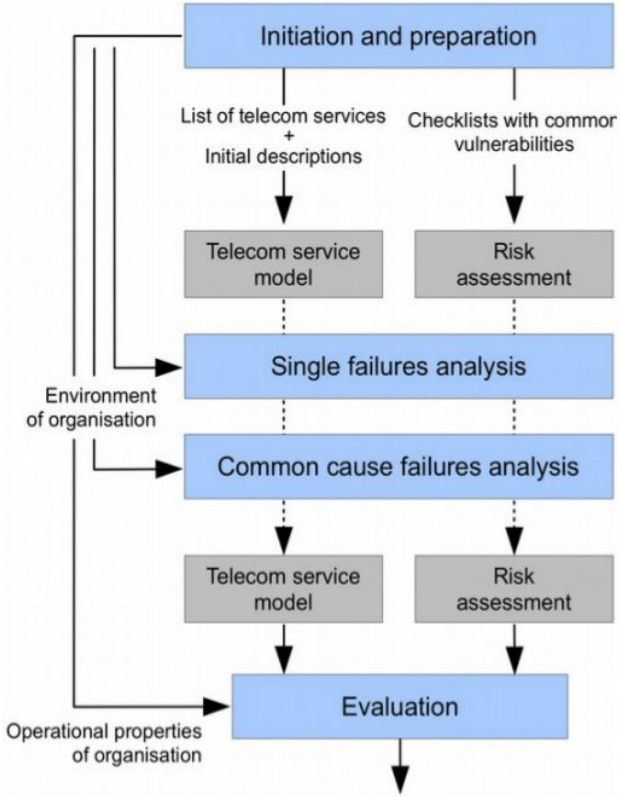
1. Diversity: commercial and non-commercial, health care, public administration, industry.
2. Regional fire and emergency service: after a recent reorganisation and redesign of internal IT systems.
3. Regional water board and flood protection agency: an old organisation (>100 years) that had many “old 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.

How is it done

1. Applied by a team of experts:
    1.1. Case Organization, Sponsor (responsible person), and Decision Makers
    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 affect business as usual?)

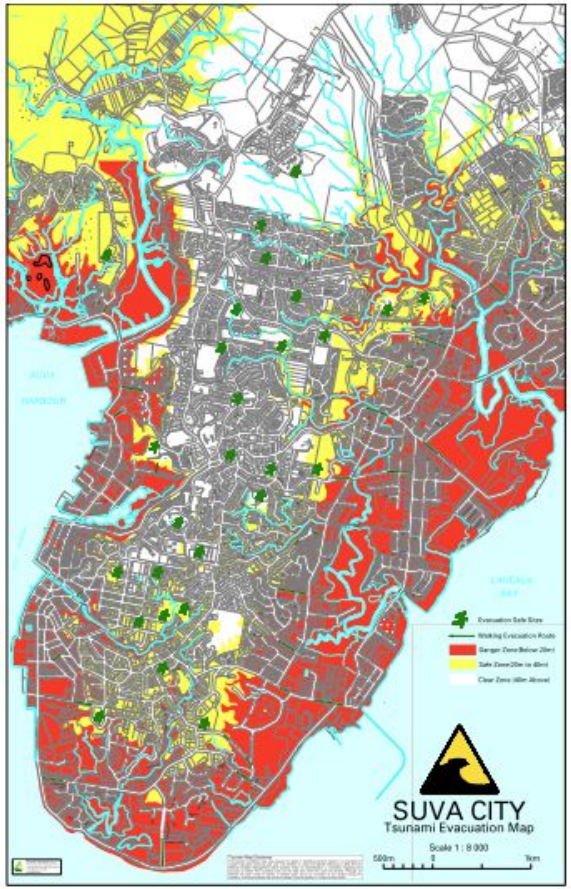
Class	Description	Symbol
Extremely High	Very long term, unrepairable and unavailable (> 06 months) 100% of the actors are affected	V
High	Unavailable and if unrepairable then has a long term effect (< 01 month) 50% of the actors are affected	H
Medium	Partially unavailable and if unrepairable then has a medium term effect (< 01 day) 10% of the actors are affected	M
Low	Partially unavailable and if unrepairable 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

Analysis and Report

1. Why do we need this emergency communication service? Or what is the purpose?
2. What are the criteria or factors that the emergency communication should address?
3. What are the emergency communication system components and services?

Tsunami Risk Profile for Fiji (the Purpose)

- Waves potentially affecting Fiji
  - Are Generated by earthquakes or submarine landslides
  - may vary from a few millimetres to 23 metres in height (NDMO, 2017)
  - Arrive within several minutes with less than a 5 minute warning window
- Danger zone for “coastal and maritime” areas
  - Under 10 meter coastal/maritime
  - Less than 1.0 Kilometer from the shoreline
- Danger zone for “river banks”
  - Under 10 meter above sea level
  - Less than 3.0 Kilometers from the shoreline



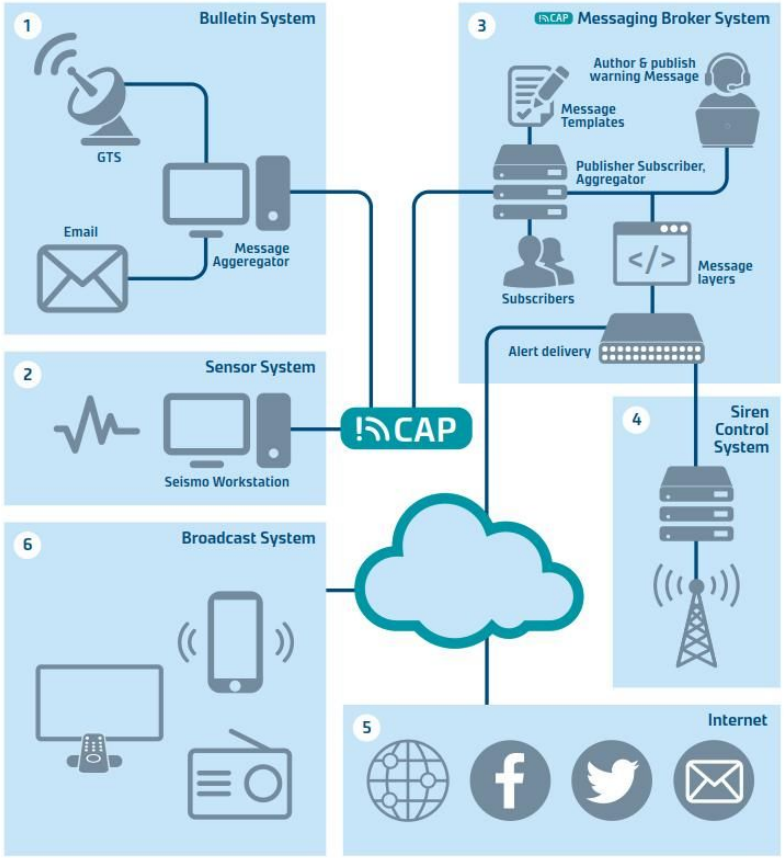
Criteria Assessment

1) Transmission type - Nature of the communication service (siren system, cell broadcast)
2) Limitations - A short summary of the main limitations of the mechanism
3) Time-frame - How long will it reasonably take to prepare and send a warning via the mechanism and for it to be received?
4) Alerting and instruction - Can the mechanism be used for alerting, for instruction, or for both?
5) Effectiveness for residents - Effectiveness of the mechanism for the normal resident population (wake up at the middle of the night)
6) Effectiveness for transients - Effectiveness of the mechanism for people that are unfamiliar with the area or local arrangements, e.g. tourists
7) Effectiveness for institutions - Effectiveness of the mechanism for people that are inside institutions like work places, places of learning, hospitals and prisons
8) The vulnerable & immobile - Effectiveness of the mechanism for people that are suffering from some type of disability, e.g. the blind, deaf and elderly

Criteria Assessment

9) Robustness and resilience - Vulnerability of the mechanism
10) Continued effectiveness - Ongoing effectiveness of the mechanism after the first warning has been issued, e.g. can it be utilised for further information send out?
11) Geographical suitability - Suitability or unsuitability of the mechanism for different geographical features
12) Population density - Suitability of the mechanism for high and low density areas
13) Cost basis - The basis on which cost is estimated
14) Cost - Approximate estimates based on research as at early 2017. These estimates are not regarded adequate for final decision making
15) Target population - The particular segment or part of the population that the mechanism will be able to reach (coastal communities in Suva)
16) Hazard applicability - How applicable is the mechanism to warning of tsunami hazards?

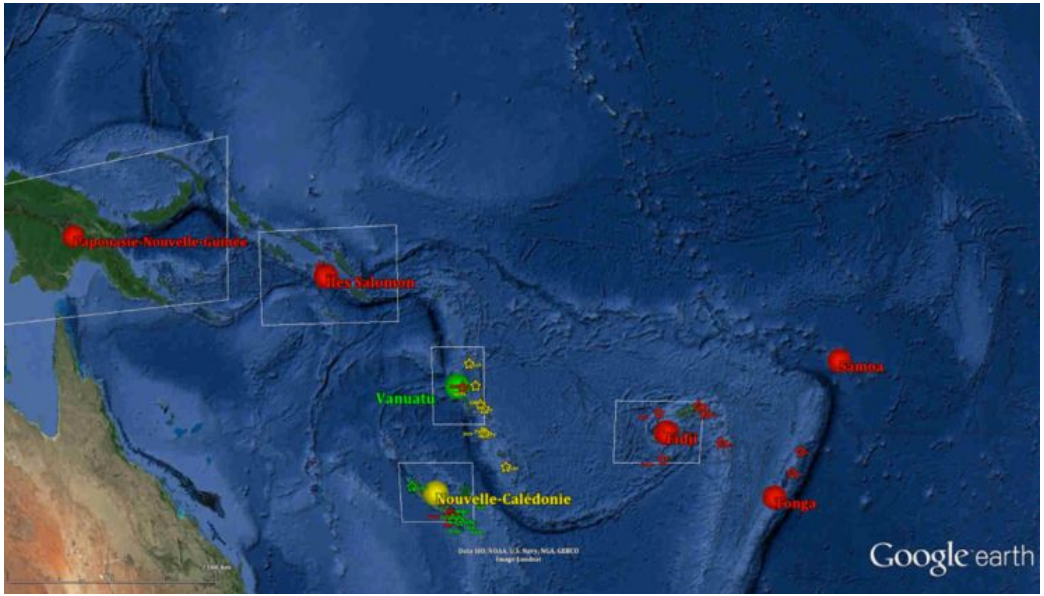
Suva Tsunami Universal Mass Notification System

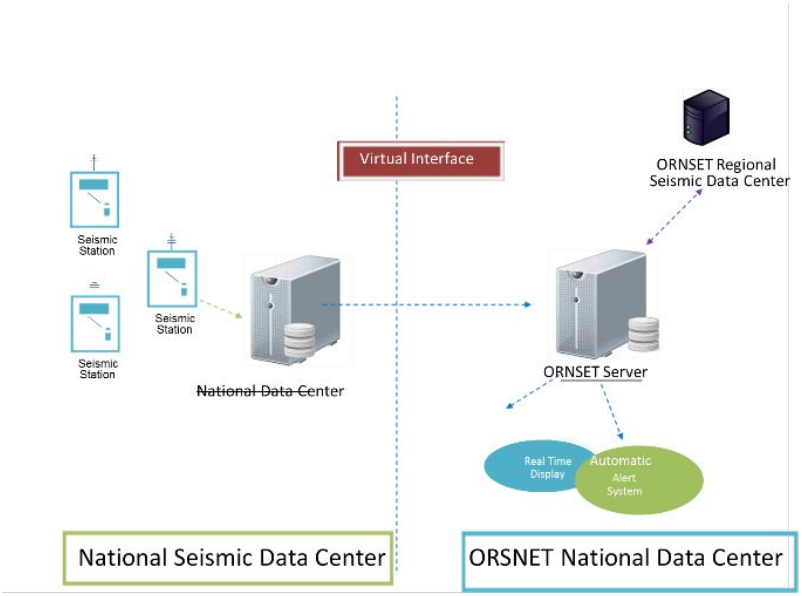


Universal Mass Notification System (UMAS) has multiple SERVICES:

- *S1*: Receiving hazard information through Global Telecommunication System (GTS) and Email (e.g. PTWC)
- *S2*: Seismic networks (e.g. sea leve gauges, buoys)
- *S3*: Authoring CAP messages using the broker and message delivery
- ***S4*: Addressable Siren towers and activation**
- S5: Interned media - http posts, social media, email
- *S6*: RSS Feeds to support Cell Broadcast, Television, and FM Radio

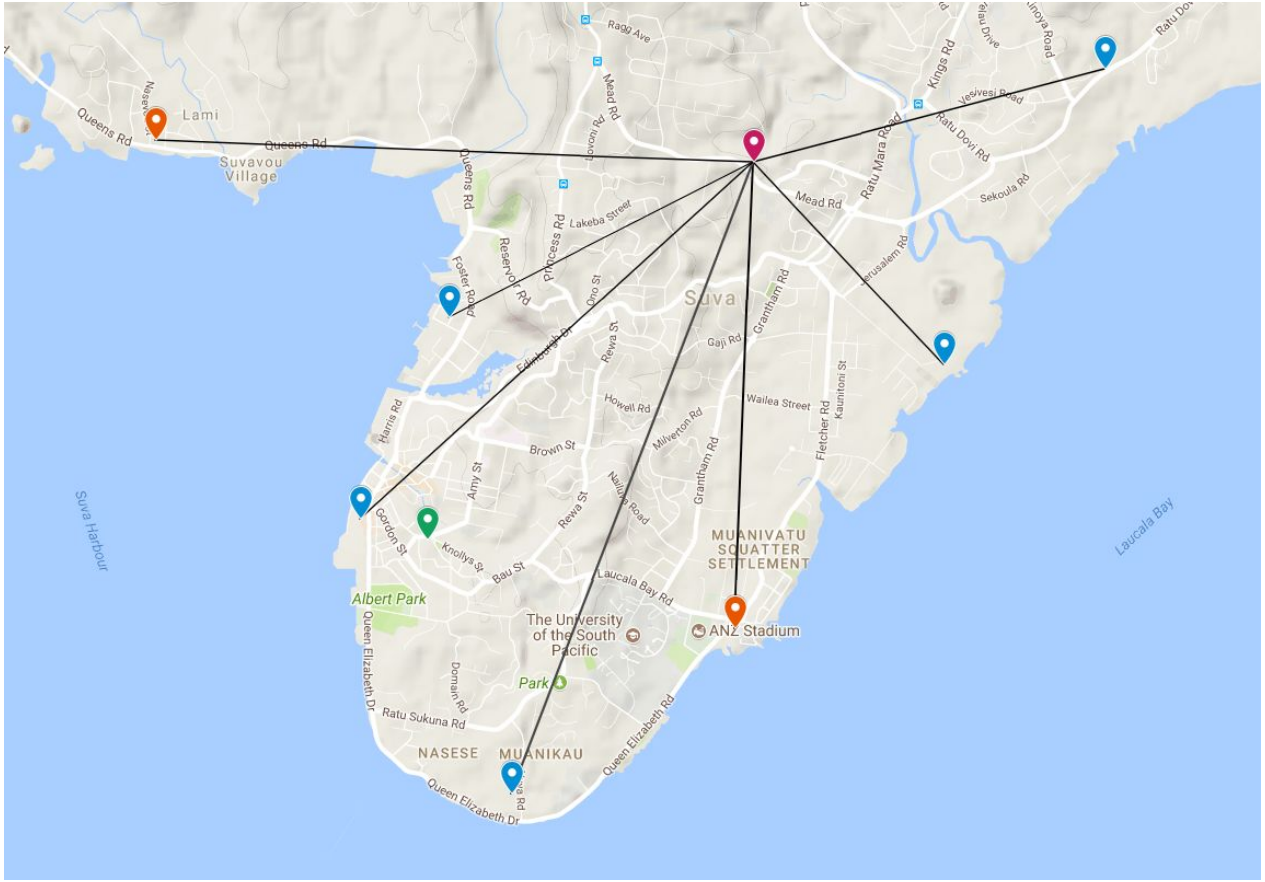
Oceania seismic network (earth observation



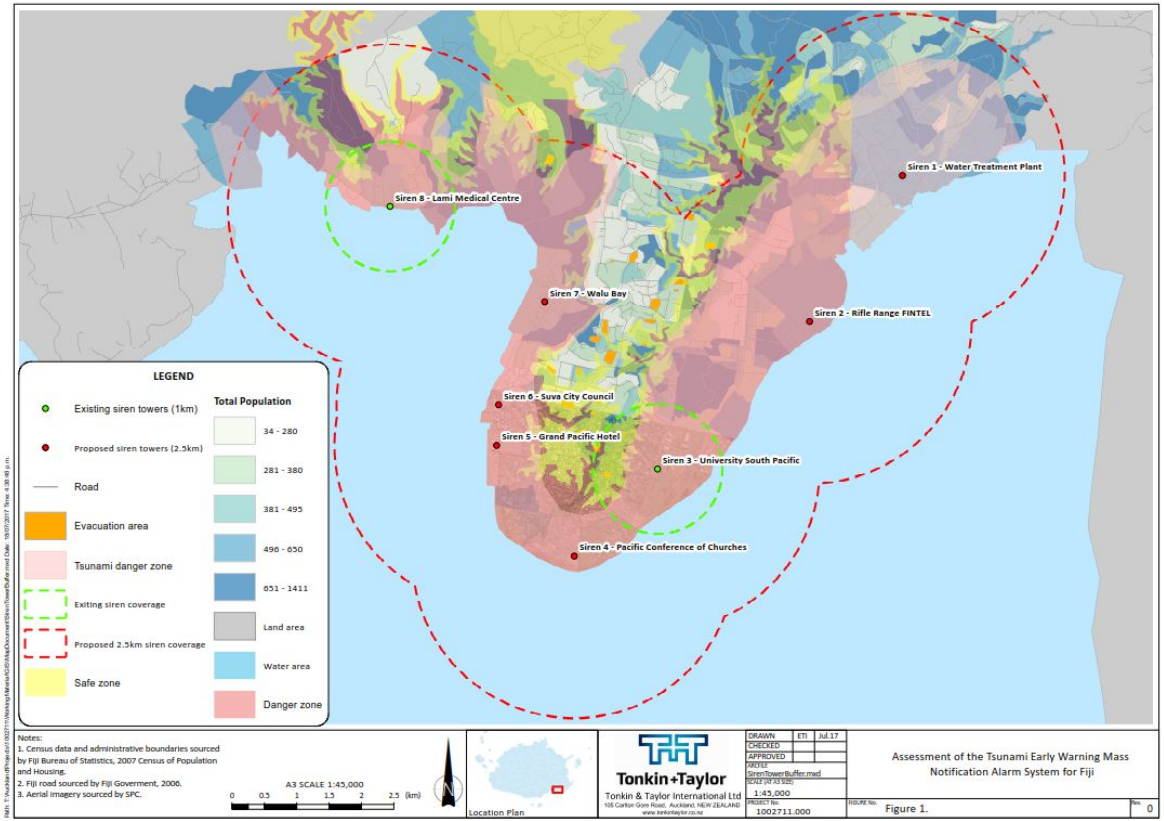


Mineral Resources Department

Existing and Proposed Sirens



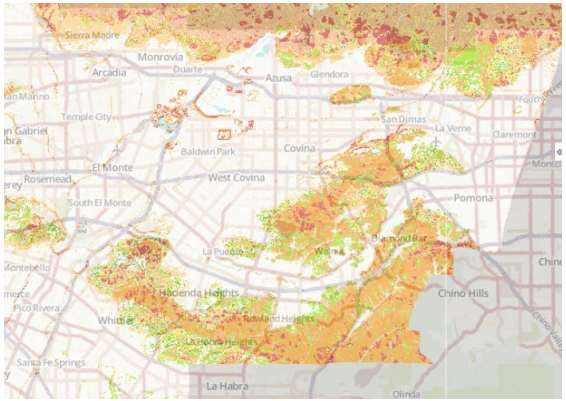
Risk analysis of the Tower through risk zone



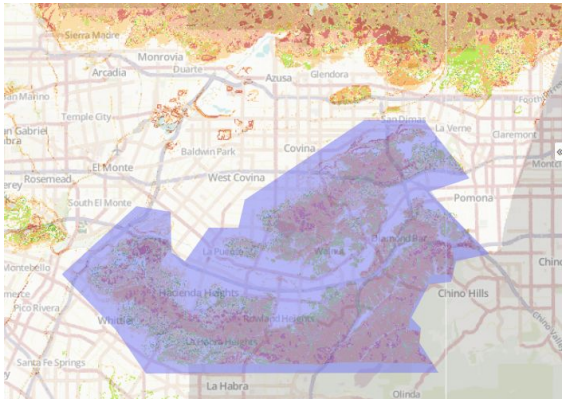
Are the towers 10m above sea level?

Do the tower audio range cover 1 - 3 Km range?

What are there vulnerabilities (e.g. severe weather, storms, cyclones)



Using hazard, vulnerability, and exposure to identify risk (e.g Landslide prone area)



Define a risk-based predefined alert area to use when issuing heavy rains and landslide warnings

Overlay with telecommunications signal coverage data to ensure warnings go through to intended recipients


TRIO TAXIS - LAMI
3361911, 3361579
9392045
7761249
9674643
ITS OUR PLEASURE DOING BUSINESS WITH YOU


WHELEN
TECH

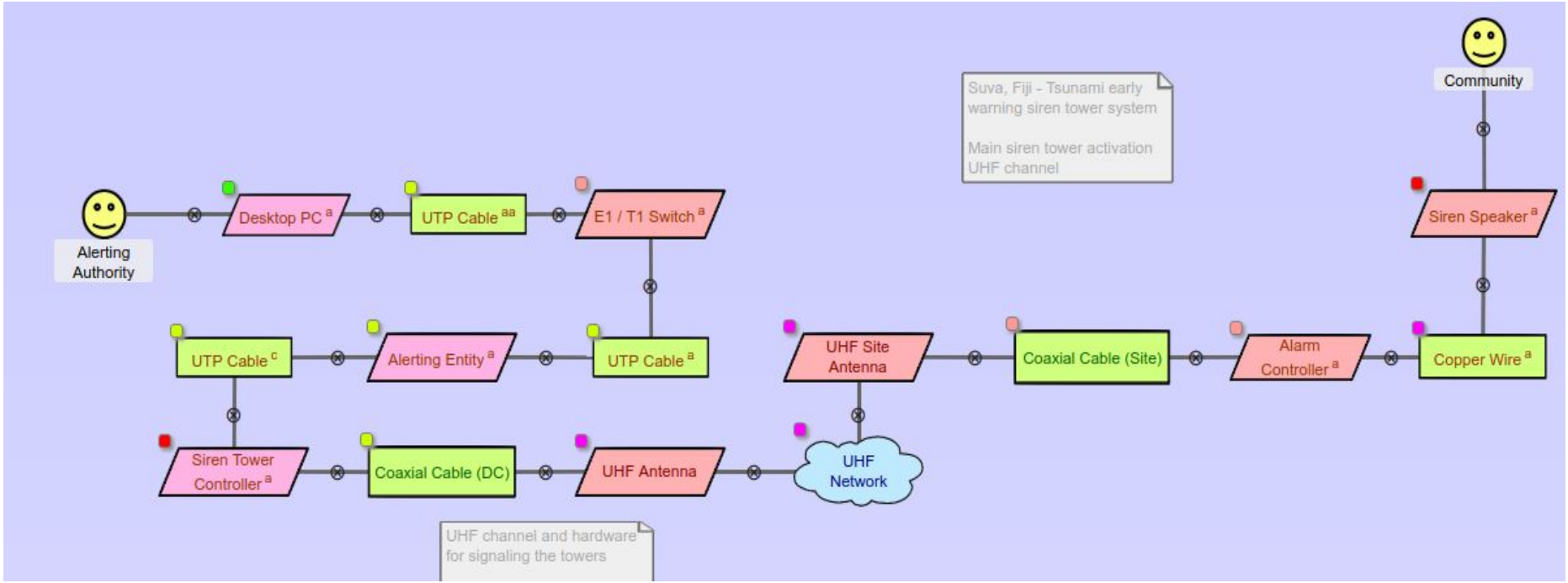
Risk Frequency (how often does it occur)

Class	Description	Symbol
Extremely High	Once a (01) days, routine event ~~For 100 identical components 10 will experience an incident~~	V
High	Once in 10 days, happens often ~~For 100 identical components 10 will experience an incident~~	H
Medium	Once in 06 months, not frequent but an incident does occur ~~For 100 identical components 1 will experience an incident in 1 year~~	M
Low	Once a (01) years, rarely ~~For 100 identical components, 1 will experience an incident in 5 years~~	L
Extremely Low	Once in 10 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

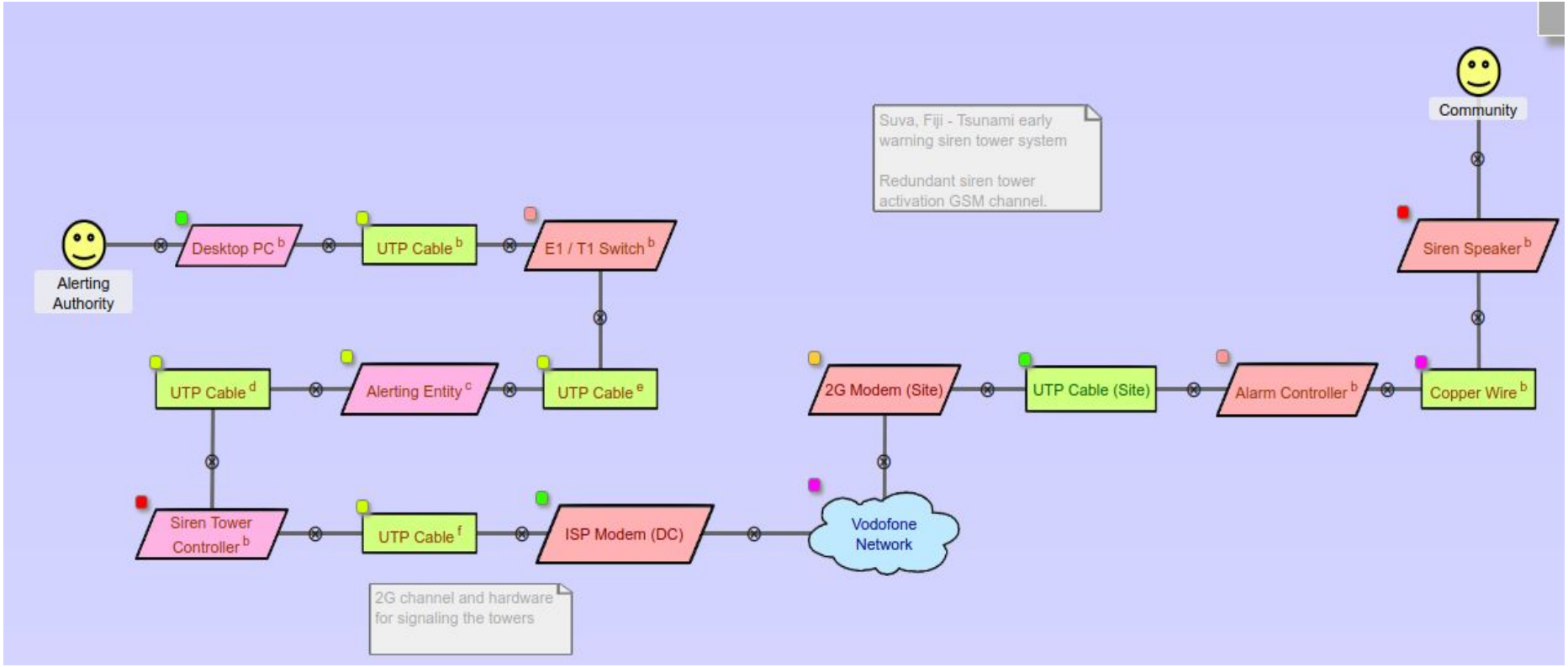
Risk Impact (How does it affect business as usual?)

Class	Description	Symbol
Extremely High	Very long term, unrepairable and unavailable (> 03 months) ~~100% of the actors are affected~~	V
High	Unavailable and if unrepairable then has a long term effect (< 01 month) ~~50% of the actors are affected~~	H
Medium	Partially unavailable and if unrepairable then has a medium term effect (< 01 day) ~~10% of the actors are affected~~	M
Low	Partially unavailable and if unrepairable 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

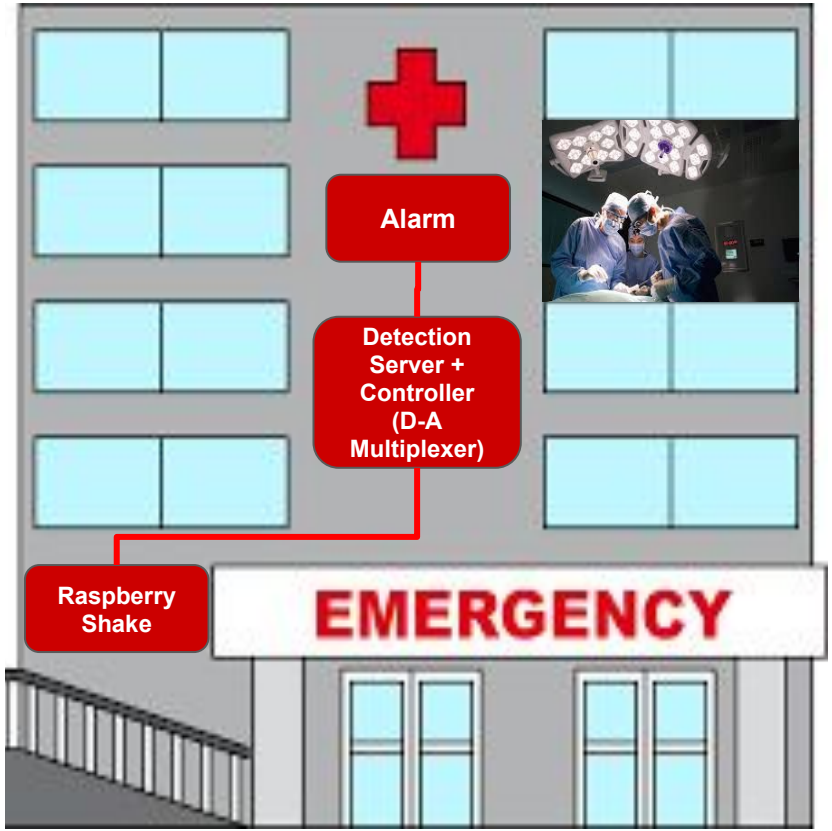
UHF-based siren activation



Redundant 2G-based Siren Activation



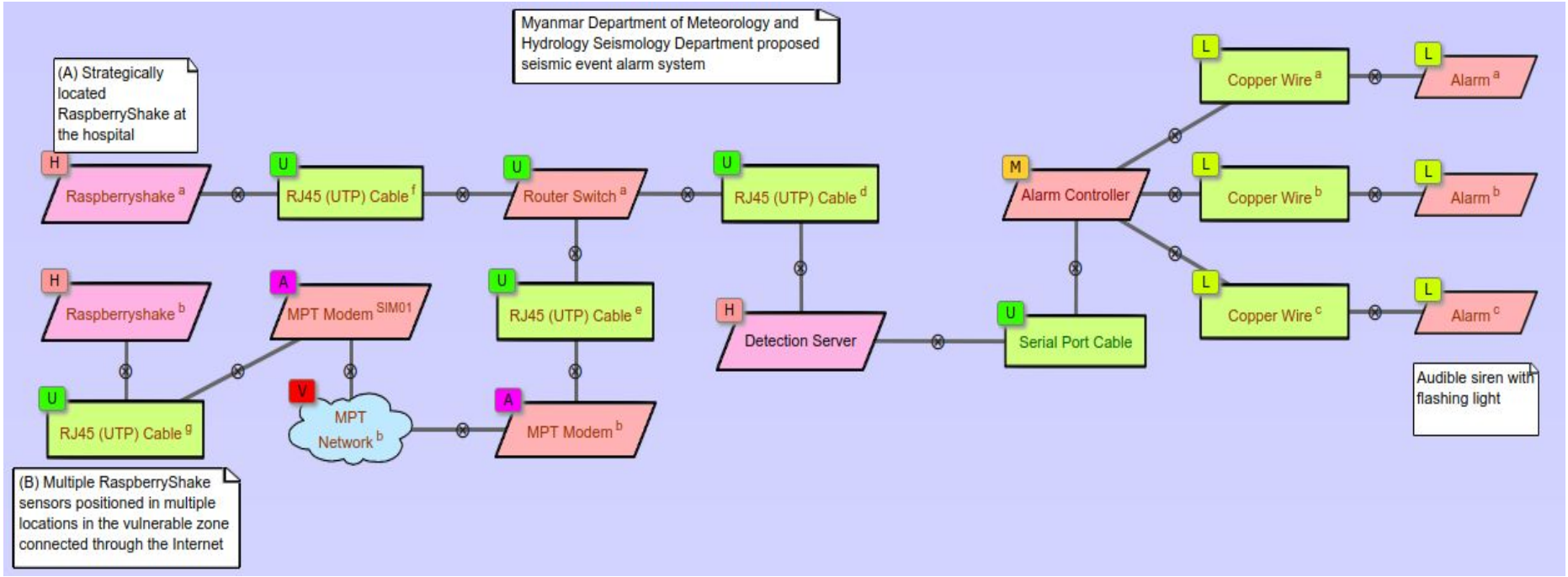
RaspberryShake Alarm



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

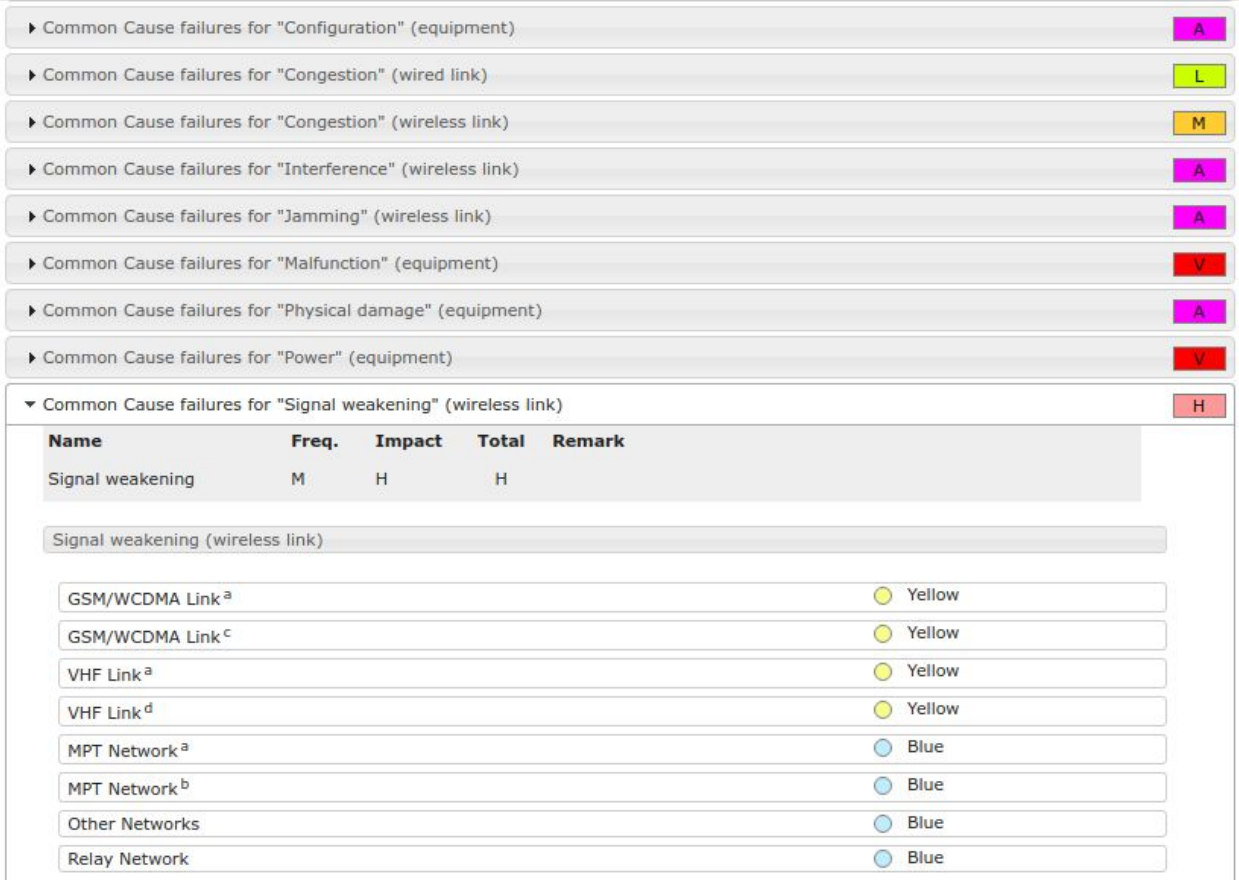
▸ Single failures for "Alarm" (equipment, 3 nodes)	Red	L
▸ Single failures for "Alarm Controller" (equipment)	Red	M
▸ Single failures for "Copper Wire" (wired link, 3 nodes)	Green	L
▸ Single failures for "Detection Server" (equipment)	Purple	H
▾ Single failures for "MPT Modem" (equipment, 3 nodes)	Red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

Name	Freq.	Impact	Total	Remark
Physical damage	U	U	U	
Power	U	V	A	
Configuration	U	L	U	
Malfunction	U	L	U	

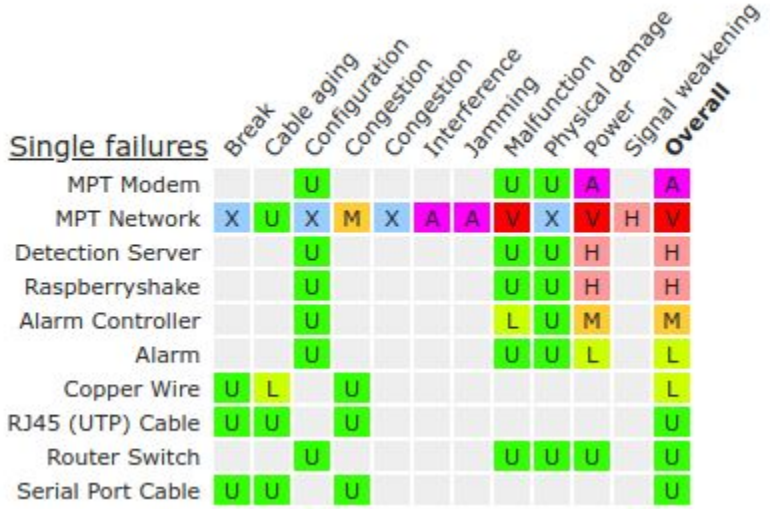
+ Add vulnerability | Copy | Paste

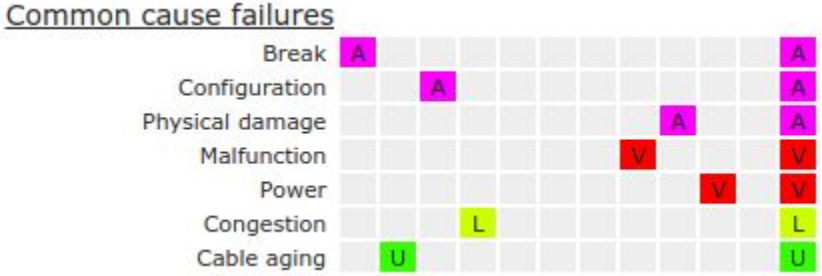
▸ Single failures for "MPT Network" (cloud, 2 nodes)	Blue	V
▸ Single failures for "Raspberryshake" (equipment, 2 nodes)	Purple	H
▸ Single failures for "RJ45 (UTP) Cable" (wired link, 7 nodes)	Green	U
▸ Single failures for "Router Switch" (equipment, 2 nodes)	Red	U
▸ Single failures for "Serial Port Cable" (wired link)	Green	U

Common Failures



Analysis of the Single and Common Failures





- 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

Group exercise using Raster - Instructions

1) Break into groups of 3-4 by country or organization or roles/responsibilities; assign a group name A - F.
2) Designate the following roles to members of the group;
    a) One person to control the Raster tool
    b) One person to prepare the report
    c) One person to present the report
3) Identify a common theme for all groups (e.g early warning, incident reporting - police, fire, ambulatory services, or relief management)
4) Design the diagram with telecom services, conduct the analysis, and prepare the report (you have 3 minutes to present)

Thank You

Nuwan Waidyanatha

Senior Research Fellow

nuwan@lirneasia.net

LIRNEasia

Pro-poor. Pro-market.