Analysing Non-Malicious Threats to Urban Smart Grids by Interrelating Threats and Threat Taxonomies

Alexandr Vasenev, Lorena Montoya

UNIVERSITY OF TWENTE.

Trento (IT), 15-09-2016

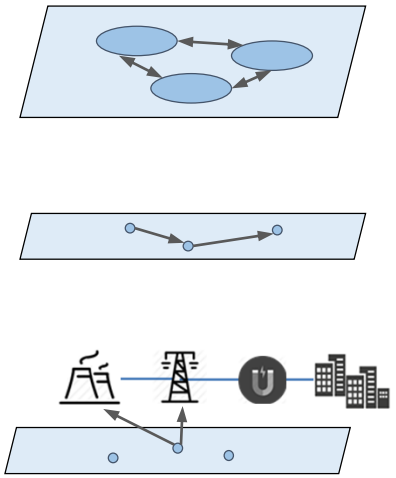
In a Nutshell

This presentation illustrates ways to look beyond a specific threat by:

(1) relating threat sources from one taxonomy to threat lists from other taxonomies;

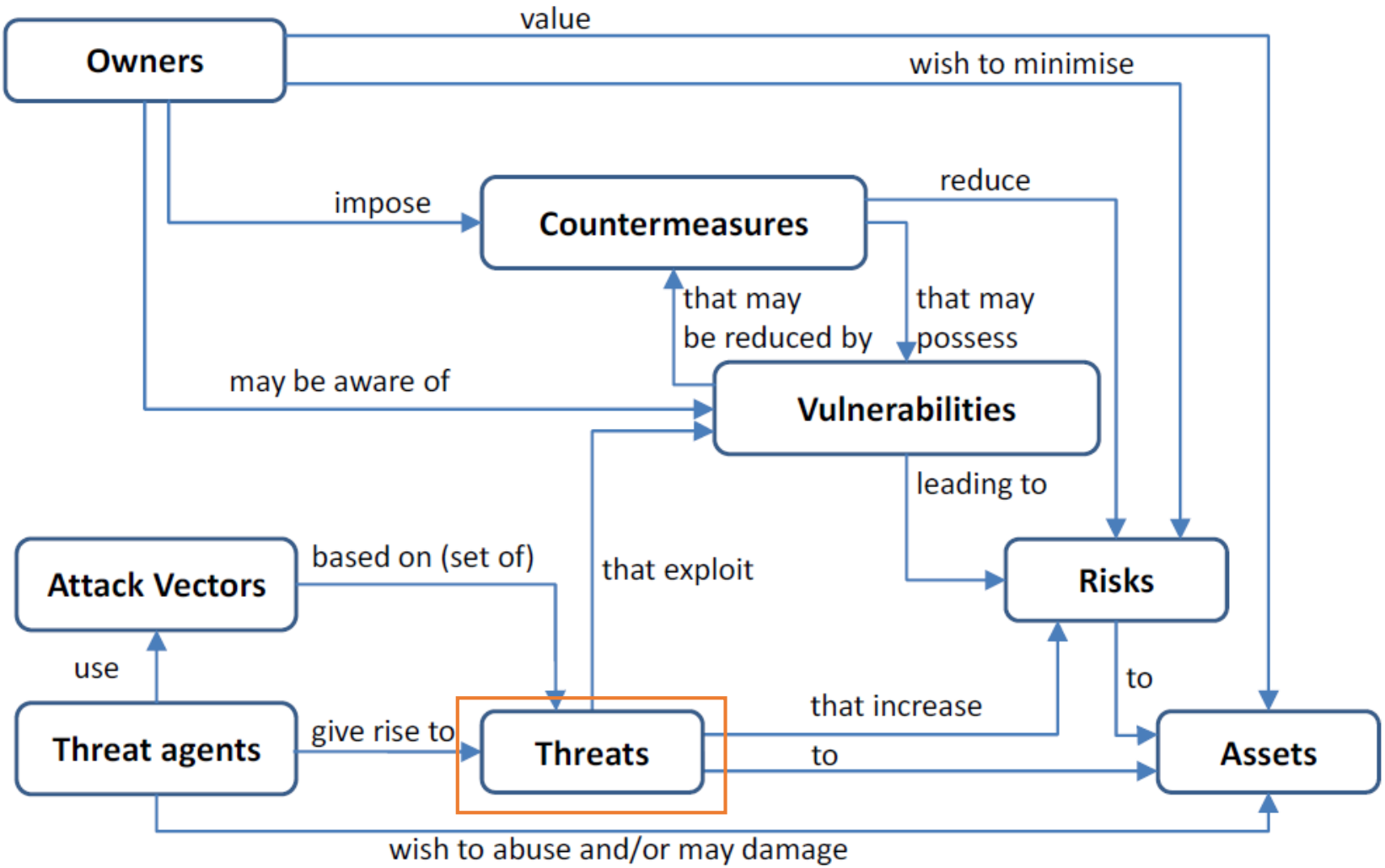
(2) analyzing how threats can be cross-related to identify possible scenarios of undesirable events; and

(3) assigning threat categories to system components.



We link taxonomies and explore a threat landscape of a grid as a complex system.

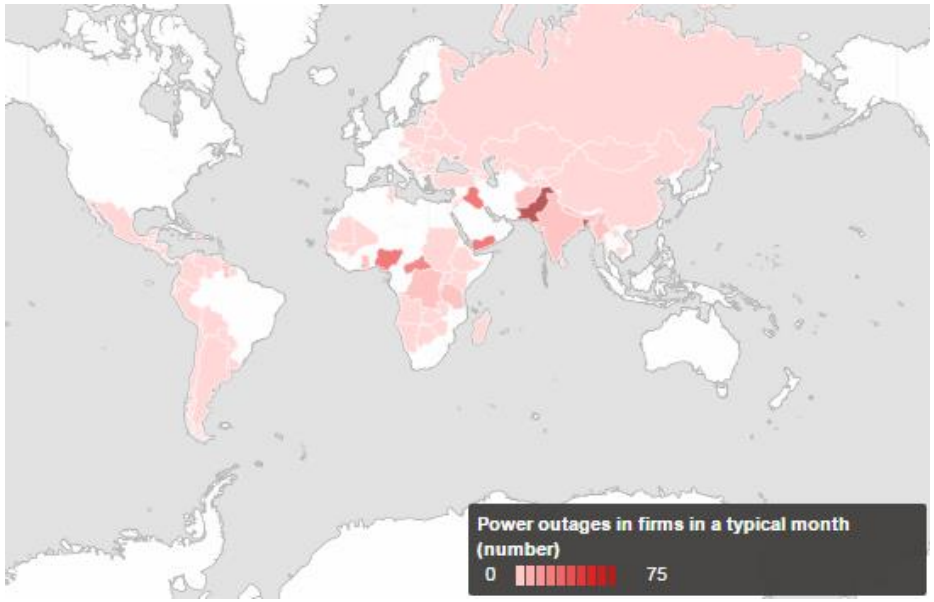
Elements of a Risk



ISO 15408:2005

Blackouts

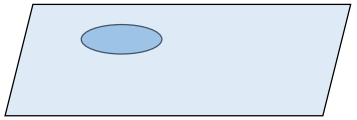
07 June 2015: Kenya (>40m people) without power for >4 hours because of a rogue monkey;
26 January 2015: terrorist attacks left 80% of Pakistan without power (~140 million people);
27 March 2015: a technical problem in one of the main power grids in North Holland caused 1 million households to be off the grid for at least one hour.



Average number of power outages that establishments experience in a typical month between 2011 and 2015 [The World Bank].

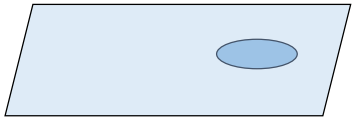
~50,000,000 people affected;
11 people died; $6 billion in damages.
Parts of Ontario suffered rolling blackouts for more than a week.

AFTER Taxonomy



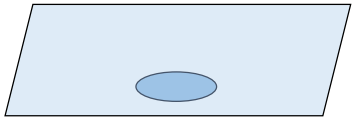
Physical threats		
	External	**Internal**
Natural	Lightings, fires, ice/snow storm, solar storms	Component faults, strained operating conditions
Man related	Unintentional damage by operating a crane, sabotage, terrorism, outsider errors	Employee errors, malicious actions by unfaithful employees
ICT threats		
	External	Internal
Natural	Ice and snow, heavy flood, fire and high temperature, geomagnetic storm	Operation out of range, internal faults, ageing
Man related	Hacker, sabotage, malicious outsider	Employee errors, malicious actions by unfaithful employees, software bugs

SESAME Taxonomy



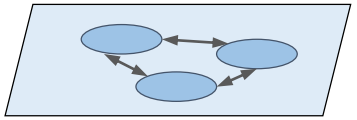
- **Nat**ural disasters:
  - Geological disasters (avalanches, earth-quakes, volcanic eruptions, landslides);
  - Hydrological disasters (floods, limnic eruptions, tsunamis);
  - Meteorological disasters (blizzards, cyclonic storms, droughts, hailstorms, heat waves, tornadoes, lighting, thunder, rainstorm);
  - Fires (wild fires);
  - Health disasters (epidemics, famines);
  - Space disasters (impact vents, solar flares, gamma ray burst);
  - Contamination.
- **Acc**idental threats:
  - Operational faults (design error, wrong decision, maintenance accident);
  - Equipment failures (technical failure, human and animal interference).
- **Mal**icious threats:
  - Physical threats (terrorists, war, sabotage);
  - Human threats (insider threats);
  - Cyber-threats (malware, terrorist hacking).

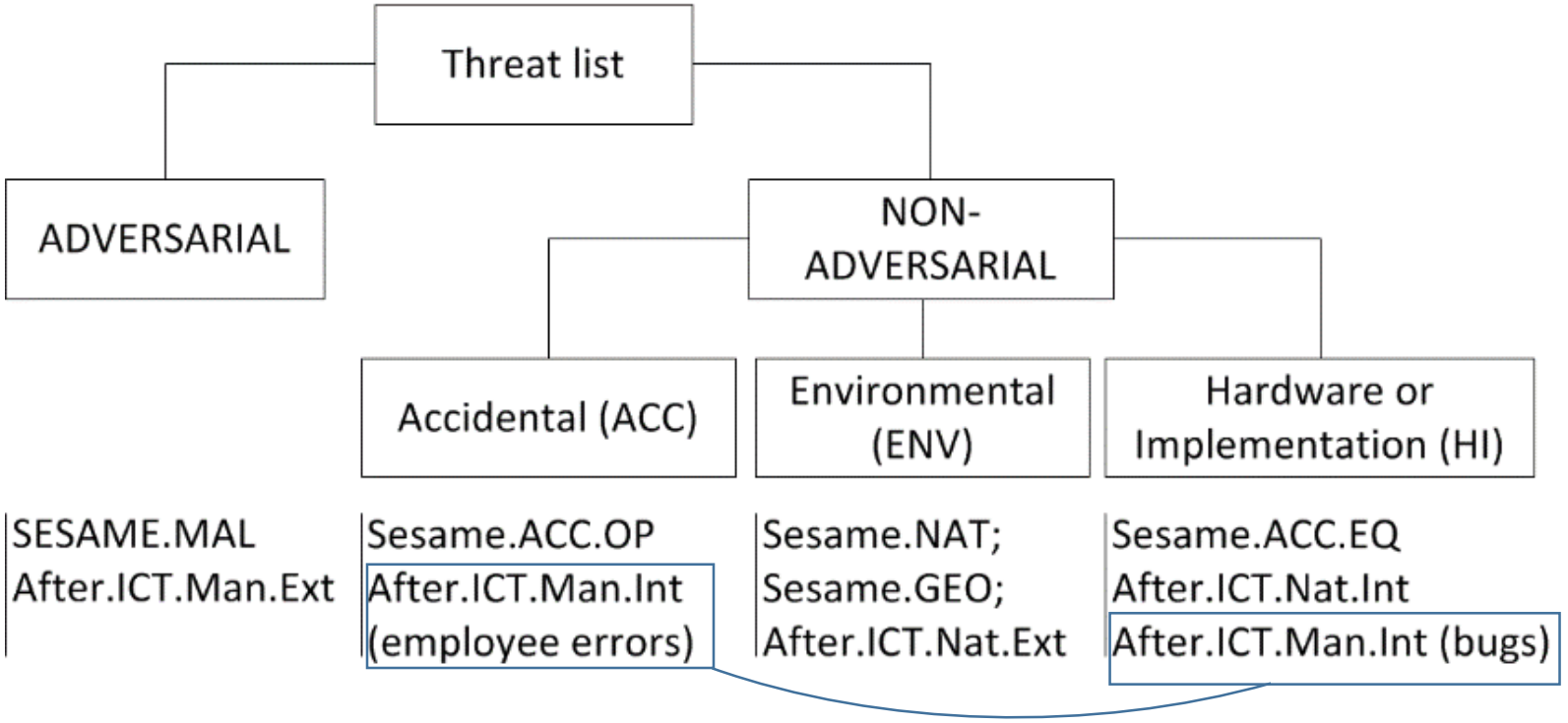
IRENE Taxonomy



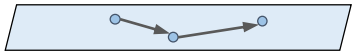
- **Adv**ersarial, such as an individual, outsider, insider, trusted insider, privileged insider, competitor, supplier, partner, customer, nation state;
- Non-Adversarial:
  - Accidental (**ACC**), e.g., mistakes made by a user or privileged user/administrator.
  - Environmental (**ENV**), including natural or man-made disaster e.g., sunspots, flood, earthquake, bombing, overrun, telecommunications infra-structure failure/outage.
  - Hardware or Implementation (**HI**) - failures of equipment (including IT, storage, processing, communications, display, sensor, controller, environmental & temperature/humidity controls, power supply), environmental controls, or software (operating system, networking, general- and mission-specific applications) due to aging, resource depletion, etc.

Interrelating Taxonomies





Interrelating Threats



Threat index	Threat event	IRENE[a] Category	Dependency
29	Spill sensitive information	ACC	Can be precursor to reconnaissance-related threats
30	Mishandling of critical and/or sensitive information by authorized users	ACC	Similarly to 29, it can lead to recon-related
31	Incorrect privilege settings	ACC	Incorrect privilege settings can directly lead to multiple other threat events, including 23 – 25
32	Earthquake at primary facility	ENV	Can lead to 33
33	Fire at primary/backup facility	ENV	-
34	Flood at primary/backup facility	ENV	-
35	Hurricane at primary/backup facility	ENV	Can lead to 33 and 34
36	Resource depletion	HI	-
37	Introduction of vulnerabilities into software products	HI	Can lead to 36
38	Disk error	HI	Can lead to 36

In relation to AFTER and SESAME:
threats 29 – 31 are internal human-related threats;
33 (Fire) and 36 – 38 – internal with no human involved;
32 – 35 – external natural threats.

Additionally: Fire can lead to resource depletion, floods can lead to fire (due to short circuits).

Modeling Grids: Elements

1. Energy provider (EP): power plants, photo voltaic energy generators, and wind farms;

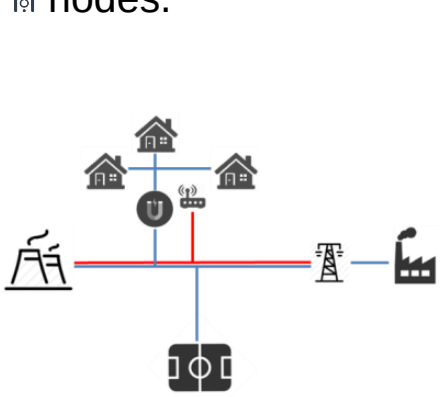
2. Connection (CON):

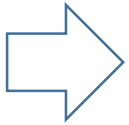
   2a. Communications: electricity, data, and micro-grid connections.

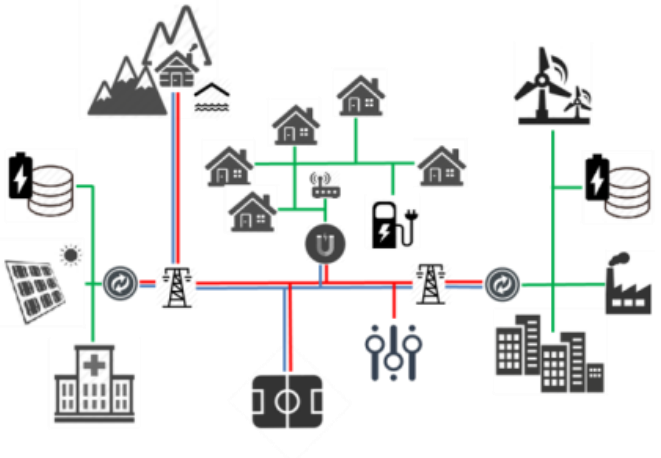
   2b. Connection nodes: connection, substation, and long-range connector ;

3. Buildings (BLD): factories, stadiums, hospitals, offices, office districts, smart homes, special buildings (e.g. police stations, fire brigades). Other specialized components include data and electricity storage, EV (electric vehicle) charging points, and access points connecting components without direct connections with the data channel.

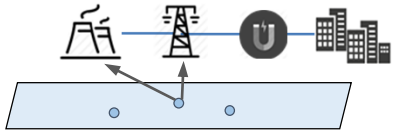
4. Data center (DAC): basic data centers and SCADA (Supervisory Control And Data Acquisition) nodes.







Relating Threat Categories to Grid Elements



Weather events ENV:
- Ice storm
- Snow storm
- Wind storm
- Lightning
- Flood
- Heat waves (cold weather)

E.g. by means of:
- Lack of cooling water
- Lack of hydro capacity

Failure of transmission (Connection CON and Data Center DAC components)

Increased demand (Building BLD components)

Failure of production (Energy production EP components)

Blackout

Accidental ACC threat events Hardware and Implementation HI threat events

Connections (CON)

Energy Production (EP)

Building (BLD)

Data center (DAC)

Conclusions

We outlined approaches useful for constructing a threat landscape for risk assessments of complex systems. By taking a grid as a case, we pointed out how to:

(1) Inter-relate grid-specific threat taxonomies;

(2) Link non-malicious threats;

(3) Relate threat categories to grid components.

Future work:

- Relate the ways to fault-error-failure-fault error propagation chain;
- Elaborate on specifics when event chains can occur;
- Consider spatio-temporal data management systems in connection to threat mapping.

Thank you for your attention!

“Analysing Non-Malicious Threats to Urban Smart Grids by Interrelating Threats and Threat Taxonomies”

a.vasenev@utwente.nl