HAZARD = potential source of danger

DANGER = state, circumstance or action that may cause damage

Hazard
↓
Resistance + Exposure | System (Vulnerabilities) ⟹ Vulnerability assessment

RESILIENCE = Coping capacity + Recovery

↳ The ability of the system to sustain external and internal disruptions without discontinuity of performing the system's function or, if the function is disconnected, to fully recover the function rapidly.

RISK = Hazard + Uncertainty + consequences ⟹ Risk assessment

(Accident scenario) (Probability) (Damage caused)

S , P , X

(Analysis of the system performance under undesired conditions)

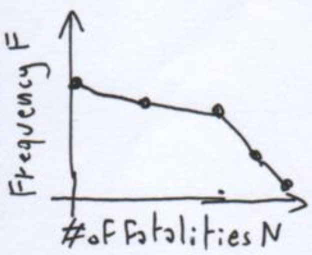
Probabilistic Risk Assessment

Knowledge:
- Hazards probability
- Experts

→ System Risk model ⟹ RISK MEASURES (Uncertainty is represented probabilistically)

UNCERTAINTY → Aleatory
UNCERTAINTY → Epistemic

F/N Graph:



Risk matrix:

STRATEGIES → Risk assessment informed: For knowledgeable problems
STRATEGIES → Robustness, resilience-based: For unknown problems

COMPLEX SYSTEM:
- Many interacting components
- Components of heterogeneous type
- Hierarchies of subsystems
- Interactions across different scales of space and time
- Rules are dynamic and complex
- Interactions are fluid and not obvious
- No central organizing principle
- Interaction with environment

↓

Dependencies & Interdependencies

⇒ Risk management decisions have to be taken on the basis of not-knowing

Global Risk
- De-localization: causes and consequences not local
- Incalculableness: of consequences
- Non-compensability ⇒ principle of precaution

⇒ Resilience implies to anticipate, prevent, mitigate, recover from risks
There will always be unforseen events.

RESILIENCE = Absorb, adapt + Recover
- Amount of changes that can be absorbed
- Capacity for learning and adaptation
- Capacity for self-organization
- Speed/time to return to equilibrium

Resilience assessment framework: to evaluate resilience w.r.t. specific hazards that can be modeled

Resilience strategies: (System specific)
- Enhance resilience awareness
- Share information
- Make integrated decision makings
- Train staff and managers
- Harden system components
- Adjust system topology
- Control system demand level
- Deploy backup systems (redundancy)
- Optimize repair sequence

Complex system representations: → Improve reliability
→ Defining structural, logical and functional relations among components

FAULT TREE

- "Logical" method → apt to representation
  → capture the logic of the functioning/dysfunctioning of a complex system
  → Identify the combinations of failures of elements leading to the loss of system function

⇒ Quantify the probability of the top event with mathematical framework

Cut set = logic combinations of primary events which render true the top event

Minimal cut sets = cut sets such that if one of the events is not verified, then the top event is not verified

(components appearing in low order m.c.s. or in many m.c.s. are most critical)

Rare event approximation: $P(\text{Top event}) \leq \sum_{j=1}^{mcs} P(M_j)$

Advantages:

- Modelization via few, simple logic operations
- Elements are put in a well-defined structure
- Minimal cut sets allow to identify critical components

Limitations:

- Additional factors not included
- Identify m.c.s. can be difficult for large systems
- Difficult to build the FT with many components
- No flexibility when adding new components
- No accounting for the strength of the relationships

EVENT TREE

- "Logical" method

a) System event tree
b) Phenomenological event tree

⇒ Identify possible scenarios developing from an accident initiator
→ One event tree for each accident initiator

FT and ET are failure-oriented approaches.

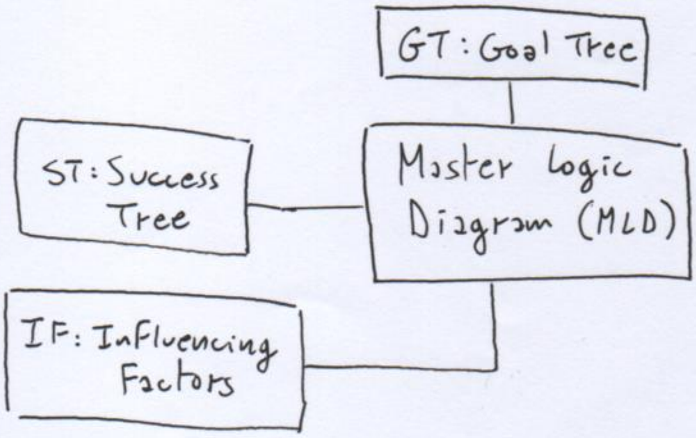
Limitations:
- Impossible to enumerate all failure scenarios
- Difficulty in defining all the events probability

GTST

Goal-oriented approach → Comprehensive knowledge
Goal-oriented approach → Quantitative analysis

⇓

Top-down perspective



- Show dependencies
- Describe causal effects of failures

Different components can have different weights

- Assigned by experts
- Assigned with simulations of threats on the system and their effects

Advantages:

- Comprehensive knowledge of the system
- Understanding of system structure
- Dynamic behavior modeling
- Cause-effect reasoning
- Possibility to be combined with other representation methodologies
- The flow can be partitioned in the system

Limitations:

- Difficult to build for large systems
- Unclear representation when a sequential importance of the demand is not considered
- Need of computer-aid tools for complex GTST-(D)MLD

COMPLEXITY THEORY

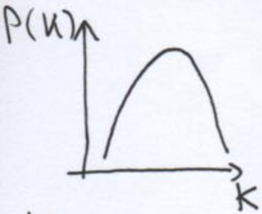
ASSESS VULNERABILITIES
- BRUTE FORCE: SIMULATION OF THE CRITICAL INFRASTRUCTURE (NOT PRACTICAL)
- USE OF HIGHLY SIMPLIFIED MODELS

COMPLEX GRAPH: CONTAINS MANY DIFFERENT SUBGRAPHS
HAS IRREGULAR, COMPLEX AND DYNAMICAL STRUCTURE

NETWORK STATIC STRUCTURE ANALYSIS
- → TOPOLOGICAL ANALYSIS → SHAPE OF THE NETWORK
- → WEIGHTED ANALYSIS → EMBED SOME OF THE PHYSICS

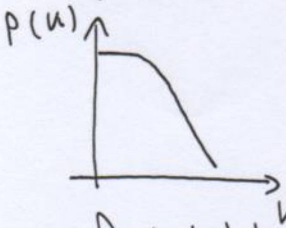
DEGREE: # OF NEIGHBORS (K)
DEGREE DISTRIBUTIONS:

Poisson:



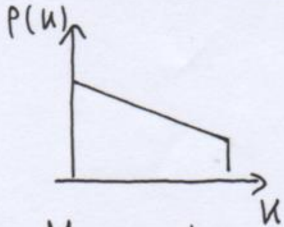
Many nodes with K=mode and the others have decreasingly more or less K

Exponential:



Probability of K bigger than the peak decreases exponentially
⇓
If a node is removed, the connection is still good
↓
Robustness to attacks and random faults

Power law: ("Scale-Free")



Many nodes with few connections
Few nodes with many connections
⇓
Attacks to hubs cause severe damages,
Random faults are likely to happen on not-important nodes

To understand connection of neighbors:

clustering coefficient $$C_i = \frac{\#\text{edges connecting the neighbors of } i}{\max \#\text{edges that could connect the neighbors}}$$

Average clust. coeff.: $$C = \frac{1}{N} \sum_i C_i$$

WEIGHTS are introduced to account for lengths and capacities of edges
There are different weights, used depending on the cases

Global efficiency $$E[G] = \frac{\sum_{ij} \varepsilon_{ij}}{N(N-1)}$$

In a neighborhood: $$E[G_i] = \frac{\sum_{mn \in Neigh} \varepsilon_{mn}}{K_i(K_i-1)}$$

VULNERABILITY INDEX

$$V^* = \frac{E[G] - E[G^*]}{E[G]}$$

G^* is network after disconnection of a link

CENTRALITY MEASURES

Topological degree centrality

$$C_i^D = \frac{\sum a_{ij}}{N-1}$$

Highest importance to the node with more first neighbors

Topological closeness centrality

$$C_i^C = \frac{N-1}{\sum d_{ij}}$$

Identify the nodes which on average need fewer steps to communicate with the other nodes

Topological betweenness centrality

$$C_i^B = \frac{\sum \frac{m_{jk}(i)}{m_{jk}}}{(N-1)(N-2)}$$

A node is central if it is traversed by many of the shortest paths connecting pairs of nodes

Topological information centrality

$$C_i^I = \frac{E[G] - E[G^*(i)]}{E[G]}$$

Relates a node importance to the ability of the network to respond to the deactivation of the node

---

In general, centrality measures:
- Rely on the topology of the network to qualify the importance of elements
- Quantify the importance of an element location w.r.t. a given network performance
- Originated in social network analysis, they quantify the role of an element in the interaction and communication occurring

---

DYNAMIC MODELING OF CASCADING FAILURE PROPAGATION IN NETWORK SYSTEMS

- Identify operating conditions that lead to cascade
- Identify indicators of criticality

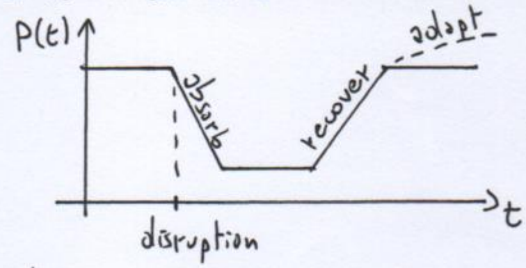
MODEL FOR PROPAGATION: Flow-based failure propagation

- COMMON CAUSE FAILURES: result from a single root cause
- CASCADING FAILURES

(Islanding)

DECISION ANALYSIS

Resilience concerns the whole evolution dynamic:

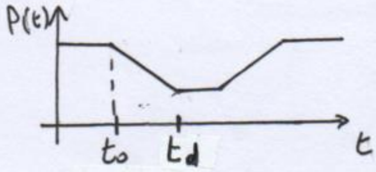


↓ Risk ↗ Resilience

4R:
- Robustness
- Rapidity
- Redundancy
- Resourcefulness

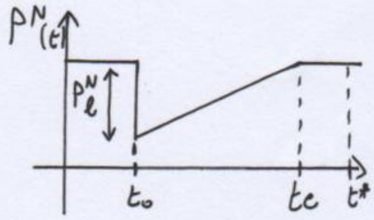
Resilience metrics:

HENRY
$$R(t) = \frac{P(t) - P(t_d)}{P(t_0) - P(t_d)}$$



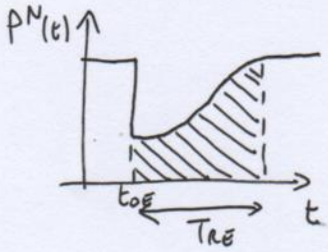
t_0 = disruption
t_d = lowest performance

ZOBEL
$$R = \frac{T^* - P_l^N \cdot \frac{T}{2}}{T^*} = 1 - \frac{P_l^N T}{2T^*}$$



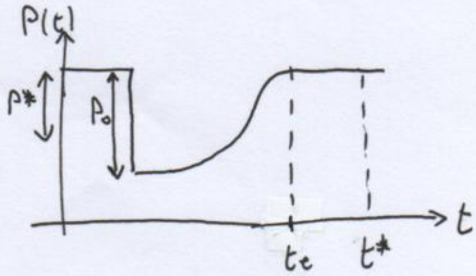
P_l^N = loss of normalized P
t_0 = minimum $P(t)$
t_e = recovery
t^* = given upper bound to t_e
$T = t_e - t_0 \quad T^* = t^* - t_0$

BRUNEAU
$$R = \int_{t_{0E}}^{t_{0E}+T_{RE}} \frac{P^N(t)}{T_{RE}} dt$$



CHANG
$$R = P_r(P_0 < P^* \text{ and } t_e < t^*)$$

where P_0 = initial performance loss
P^* = maximum acceptable loss
t_e = time of recovery
t^* = maximum acceptable time of recovery



Resilience assessment
- Statistical methods
- Simulation-based methods
- Worst-case analysis methods

e.g. game theory worst case assessment framework
WORST CASE ⇒ No need to guess what scenario will happen

PRE-EVENT STRATEGIES vs POST-EVENT STRATEGIES

↑

Don't know what the attacker will do

↓

Prepare resilience using:
- Simulations of large number of attacks
- Reinforcement learning