Risk and Threat Assessment Integration in Systems Engineering Process

Dimitrios Koupatsiaris

Email: dkoupats@hotmail.com

Hellenic Navy

Risk/Threat Definition

- PMBOK Guide: Project risk definition.
  - Opportunities are positive risks/ Threats are negative risks.
- Risk Management Guide for US DoD Acquisition: Risk definition.
  - Threat is part of constraints that define the technical requirements to the Contractor (product Scope).
- NASA Risk Management Handbook: Risk definition.
  - Threat is a form of negative risk.
- Operations Management vs. Project Management.
- Safety vs. Security.

Risk/ Threat Disconnect

- Threat management is part of the security domain, normally utilized after the completion of a project, during normal operations.
  - Usually manages information security.
  - Even for physical security, the project as infrastructure is already completed, and changes cost.
- Argument: If a building/ vehicle/ logistic system is safe to operate, then it is also secure.
  - However, safety features are tuned to government regulations (as they apply during project construction/ manufacturing), and are not changing fast.

The six processes of Project Risk Management

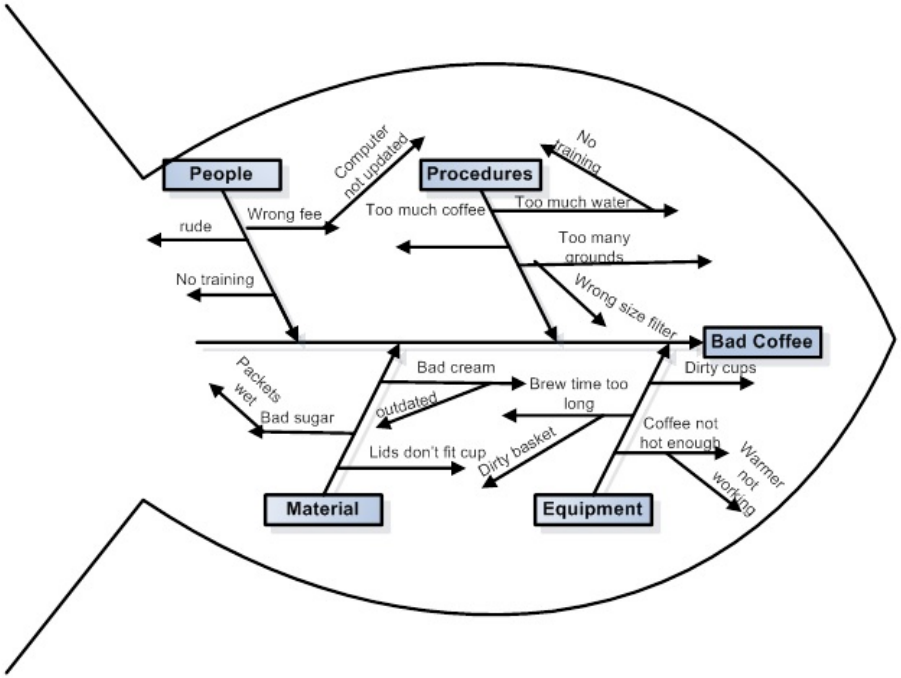
- Plan Risk Management.
- **Identify Risks.**
- **Perform Qualitative Risk Analysis.**
- **Perform Quantitative Risk Analysis.**
- Plan Risk Responses.
- Control Risks.

Risk Analysis

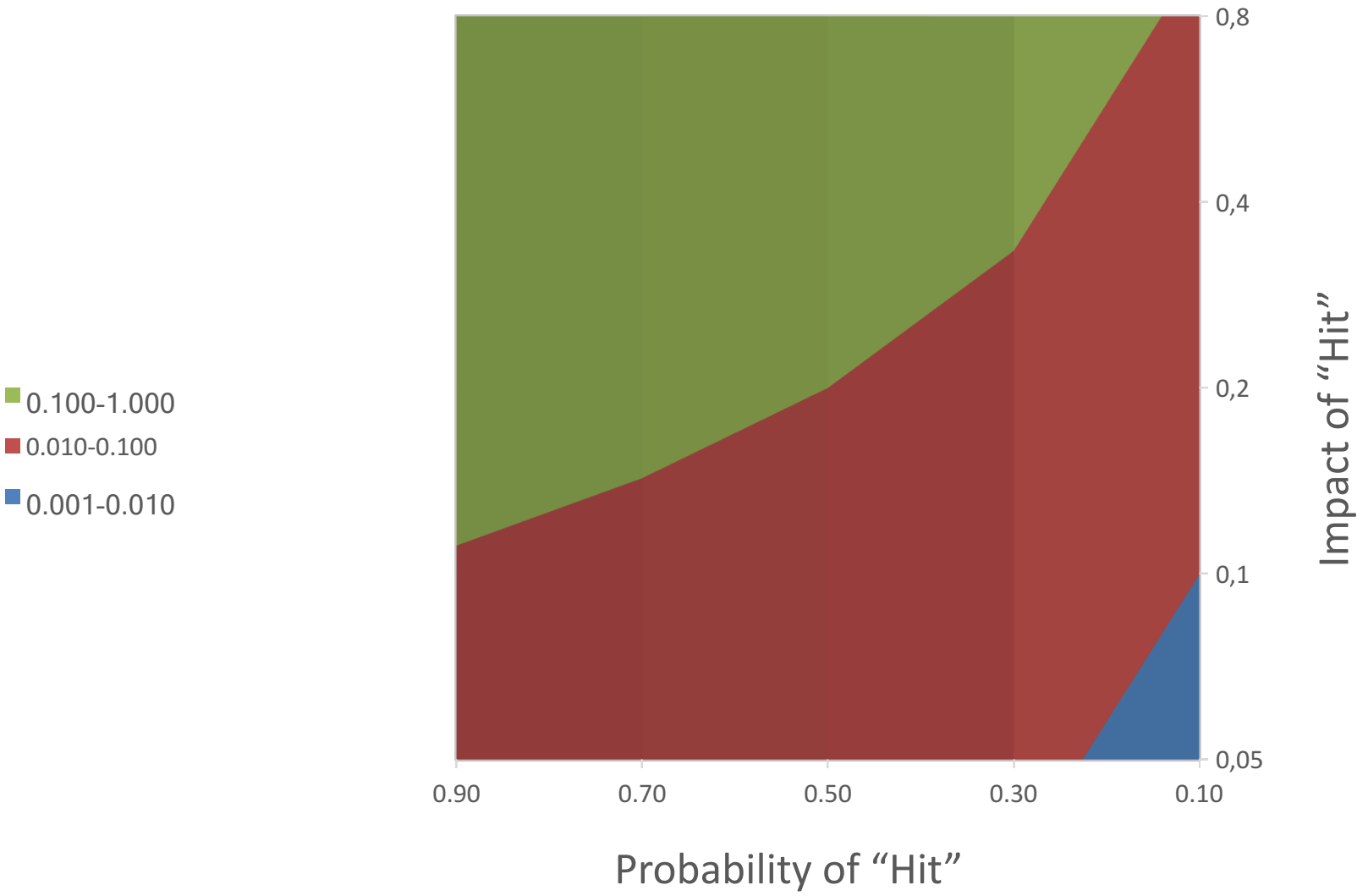
- Qualitative
  - Risk probability and impact Assessment.
  - **Probability and Impact Matrix**.
  - Risk data quality assessment.
  - Risk categorization.
  - Risk urgency assessment.
  - Expert judgment.
- Quantitative
  - Data gathering and representation.
    - Interviewing.
    - Probability distributions.
  - Risk analysis and modeling.
    - Sensitivity analysis.
    - Expected monetary value.
    - Modeling and simulation.
  - Expert judgment.

Note: Fishbone (Ishikawa) diagram

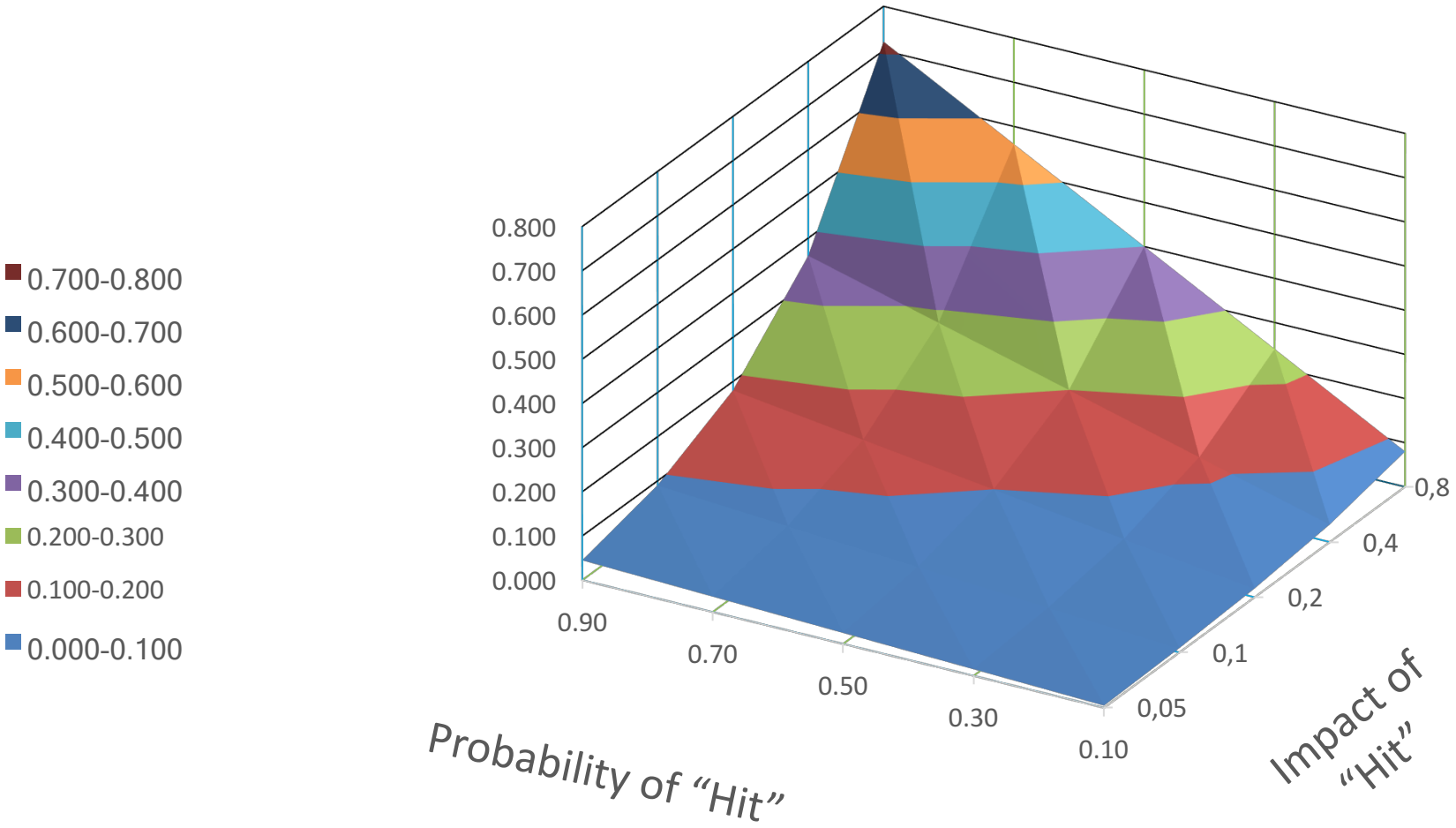
- Created by Kaoru Ishikawa, to show the causes of a specific event.
- It is a tool of Root Cause Analysis (RCA).
- It is based on the fact that an unfortunate event already took place.



Probability and Impact Matrix



Probability and Impact Matrix



P & I Matrix Math

- Joint Probability: The probability that two events take place "together".
- Statistical independence assumption between the events of "Hit" and "Impact".

$$Risk = \Pr\{H \cap I\} = \Pr\{H\} \cdot \Pr\{I\}$$

P & I Matrix Implications

- The statistical independence assumption is:
  - Convenient for the math involved.
  - Has proven value in risks where statistical independence is valid, related to safety and quality.
  - Not valid when an active adversary is involved, since an attack will be aimed at the weakest point.
- High cost of computer simulations and lack of data, leaves the estimation of probabilities to experts or stakeholders, who (wanting the project to succeed without cost overruns) can be biased on the probability of "hit" assessment.

Survivability

- The quantified ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance.
- Developed in the naval domain to assess the impact of guided missiles in naval vessels during the cold war. Mostly used in the military to assess hardened structures.
- Applicable to other areas as well.
- Closely related to availability.

Survivability, cont.

- Consists of four main system elements:
  - Detectability.
  - Susceptibility.
  - Vulnerability.
  - Recoverability.
- Principle: The possibility of a hit cannot be ruled out (the probability of being "detected" and "engaged"), however one can improve the performance of other areas.

Survivability Math

- Probability Chain Rule: permits the calculation of any member of a joint distribution, using only conditional probabilities.
- Every system element can be improved independently.
- Statistical dependence is taken into account, thus bias is less likely.
- Overall performance is achieved by the combined contribution of all elements.
- Unlike the P & I matrix, cannot be illustrated by a 2-D or 3-D surface. Utilization of graph theory and Directed Acyclic Graphs (DAG) would be helpful in this domain.

$$\Pr\{S\} = Pr\{R|V,S,D\} \cdot (1 - Pr\{V|S,D\}) \cdot (1 - Pr\{S|D\}) \cdot (1 - \Pr\{D\})$$

P & I Matrix vs Survivability

- Pros:
  - Convenient math.
  - Illustrative.
  - Proven and reliable for safety, quality.
- Cons:
  - Biased estimations.
  - Cannot model threat from an adversary.

- Pros:
  - Can model threat from an adversary.
  - Immune to bias.
  - Already used.
- Cons:
  - Strange math.
  - Difficult illustration.
  - Difficult to impose hard constraint in cost overrun.

Conclusions

- Current trend in risk management makes infrastructure security difficult to manage, due to lack of predictive robustness during construction/ manufacture.
- A possible solution would be the replacement of P & I Matrix with Survivability, when assessing possible risks during the design phase of a project.
- Although Survivability cannot exclude possible project cost overruns, can provide the means to manage threats, the probability of which was considered very low during construction/ project delivery.

Dimitrios Koupatsiaris

Email: dkoupats@hotmail.com