Safety and Security – Contradictions or Synergies?

Why look at safety / security metrics?

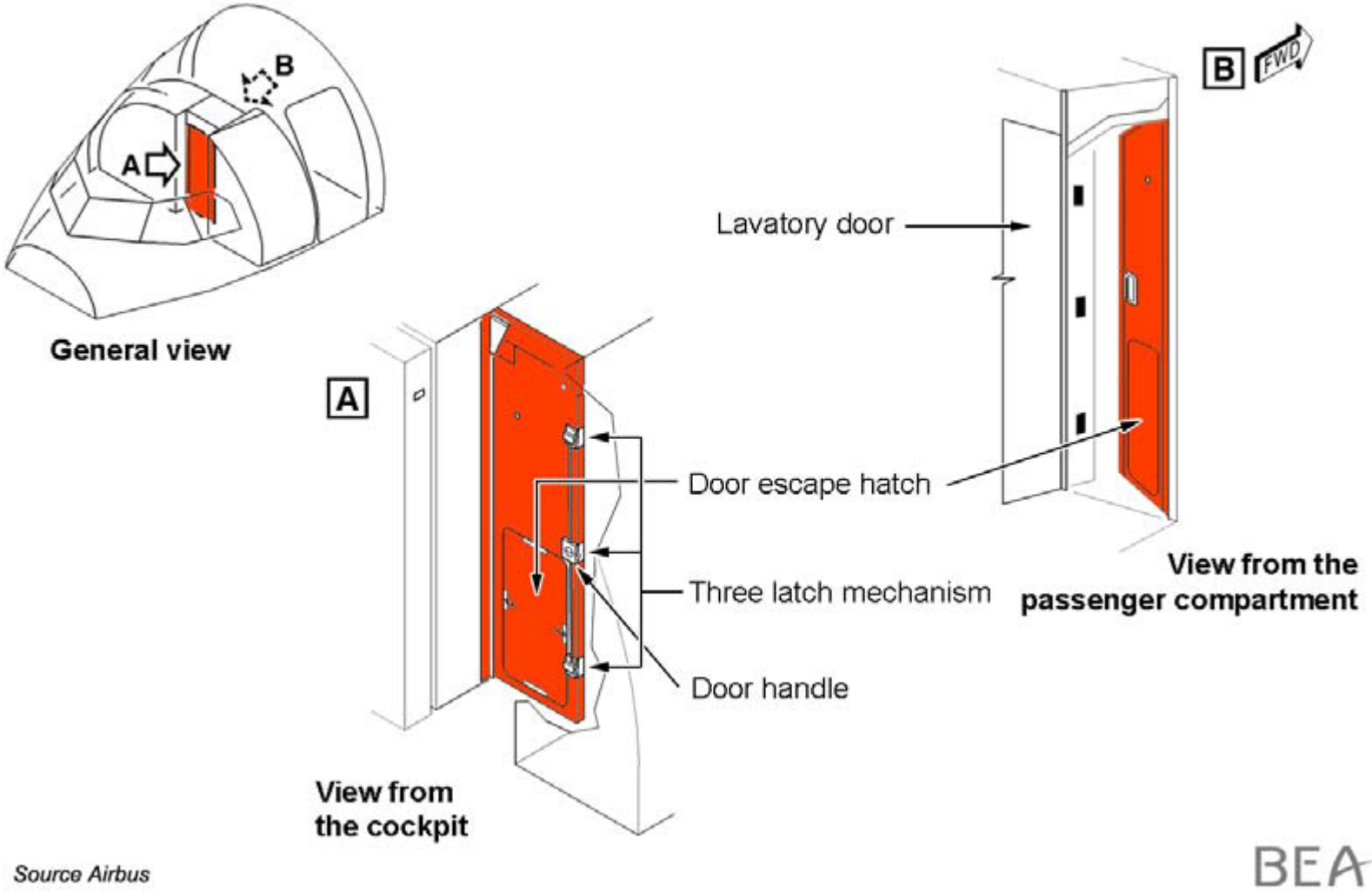
Introduction to GSI

Kai-Dietrich Wolf

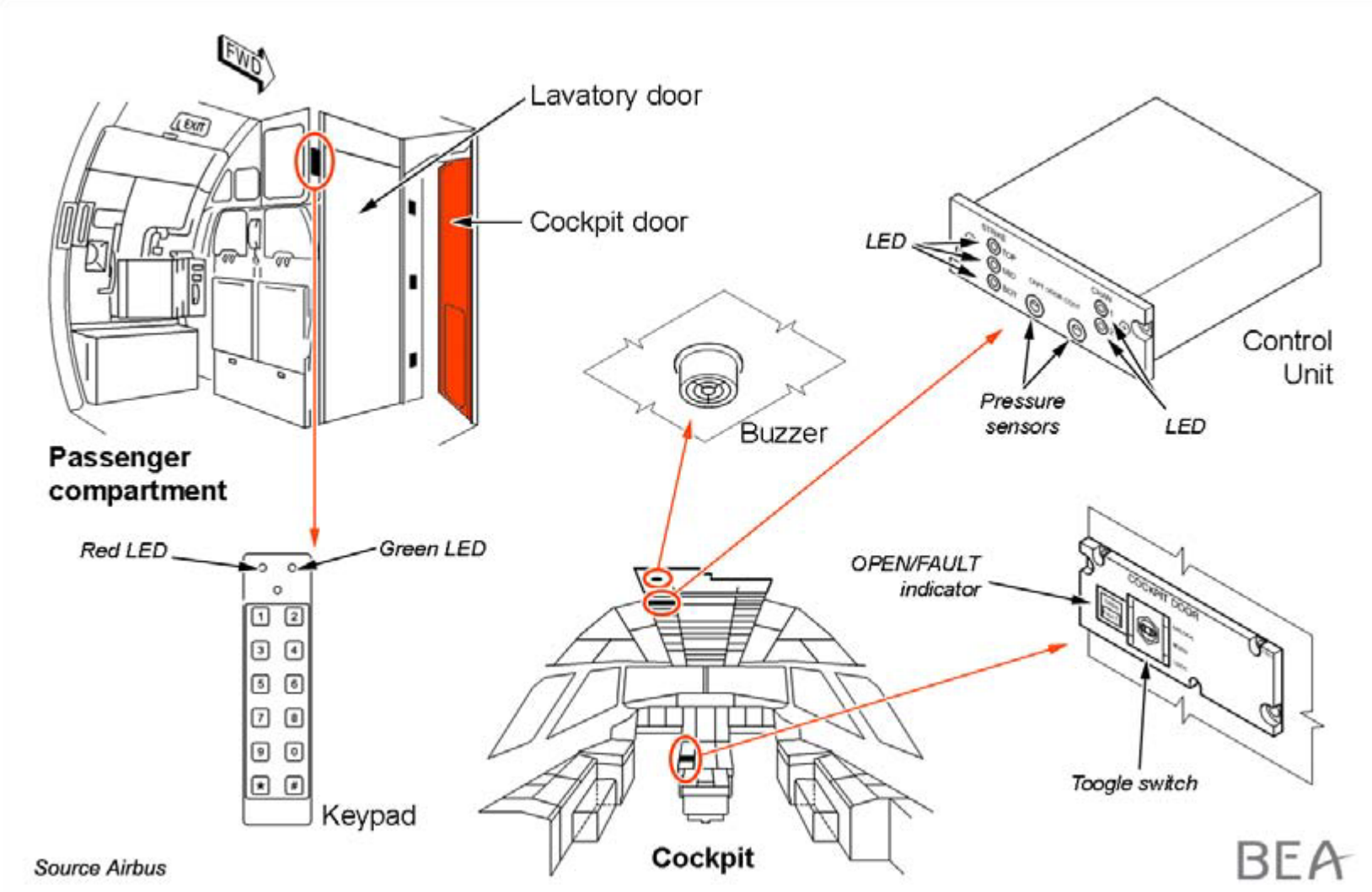
2021/09/03

Institut für Sicherungssysteme iSS

Safety & Security – Germanwings Flight 9525 Crash



Safety & Security – Germanwings Flight 9525 Crash



Safety & Security: Challenges of Today and Tomorrow

Increasing IOT integration leads to:

- Need for **encrypted communication** and **authentication**
- **IT-security** (and embedded security) as an **integral part** of technology
- Integration also **links safety and security functions** and requirements

Global threat scenarios will put **more emphasis on (physical + IT) security**:

- Integration and innovative technologies induce **new attack modes** but also **new defence measures**
- **„Critical“** supply, communication and transport **infrastructures** are getting into public focus
- **Substantial need to invest** in security (+safety) measures

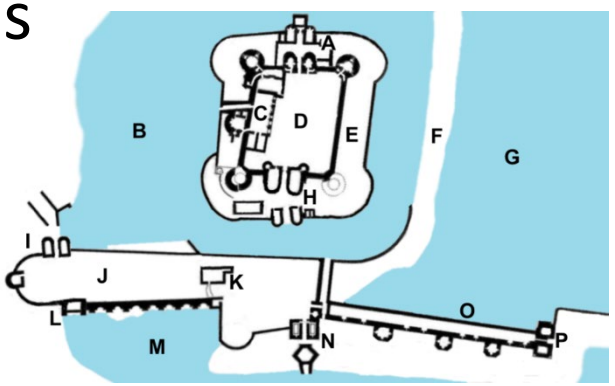
➢ We will less and less be able to afford a separate consideration of safety and security in future!

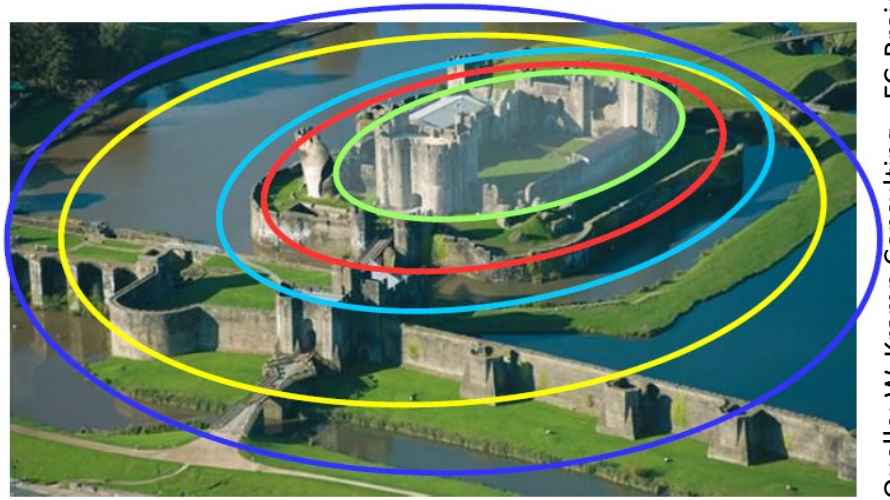
Defense in Depth (DiD)

- Physical Protection – Main Effects

- attack(er)s are **delayed** by barriers and can be **detected** early enough to deploy successful **intervention** measures before the assets are reached
- **guidance of** individuals and vehicles
- **access control**

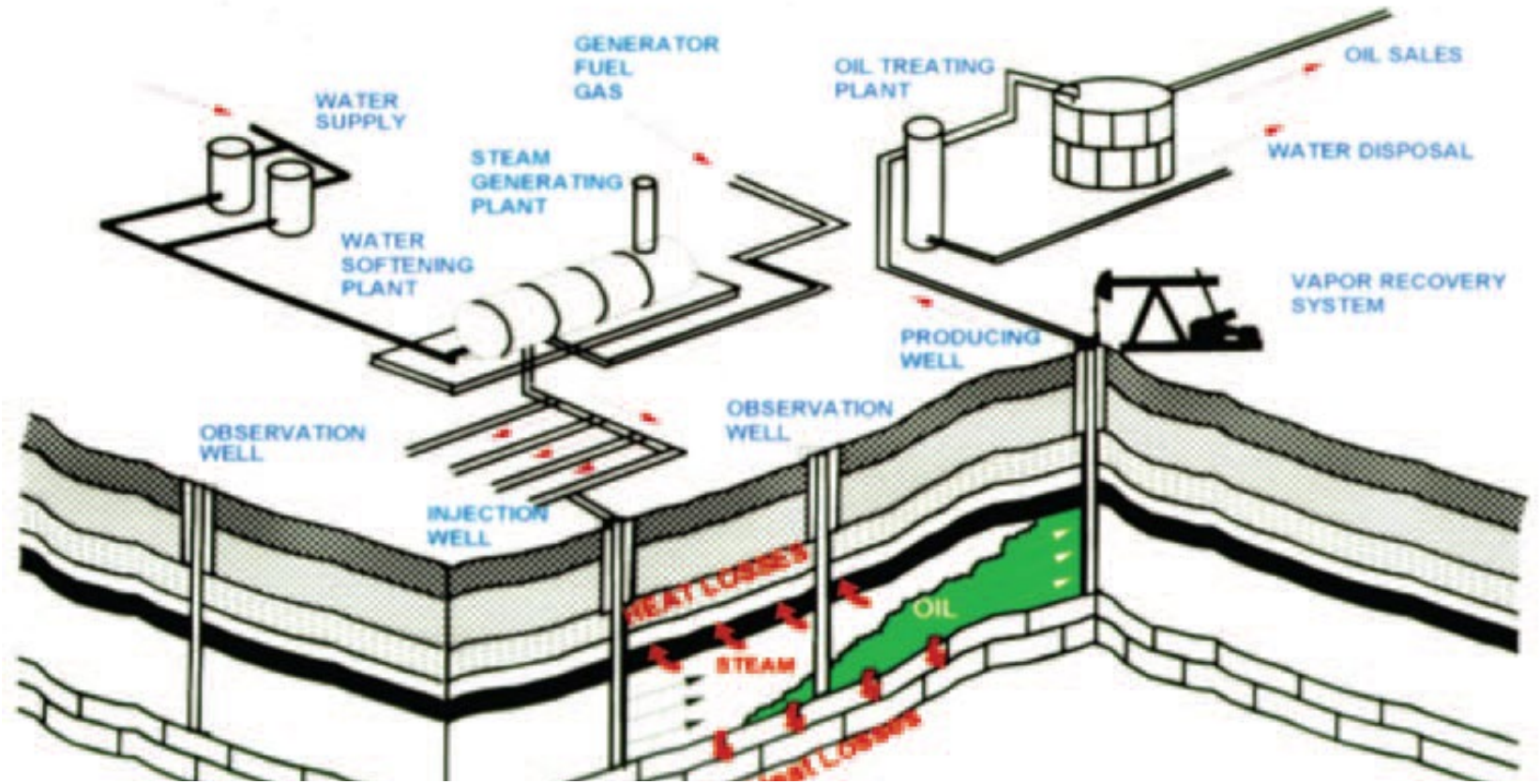
- Caerphilly Castle, South Wales





Quelle: W. Kramp Consulting, „EC-Projekt-II-NRW – Prävention Einbruch", 2016

Physical Security Assessment:
Assets in (critical) Infrastructures

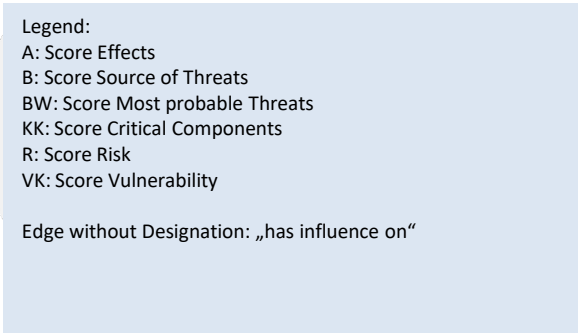


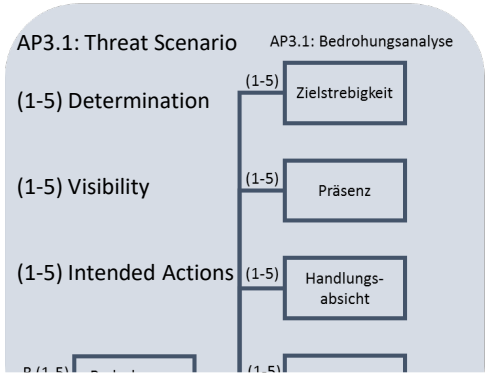
What are the consequences of a > 24h power outage in a megacity??
YES – we are vulnerable!

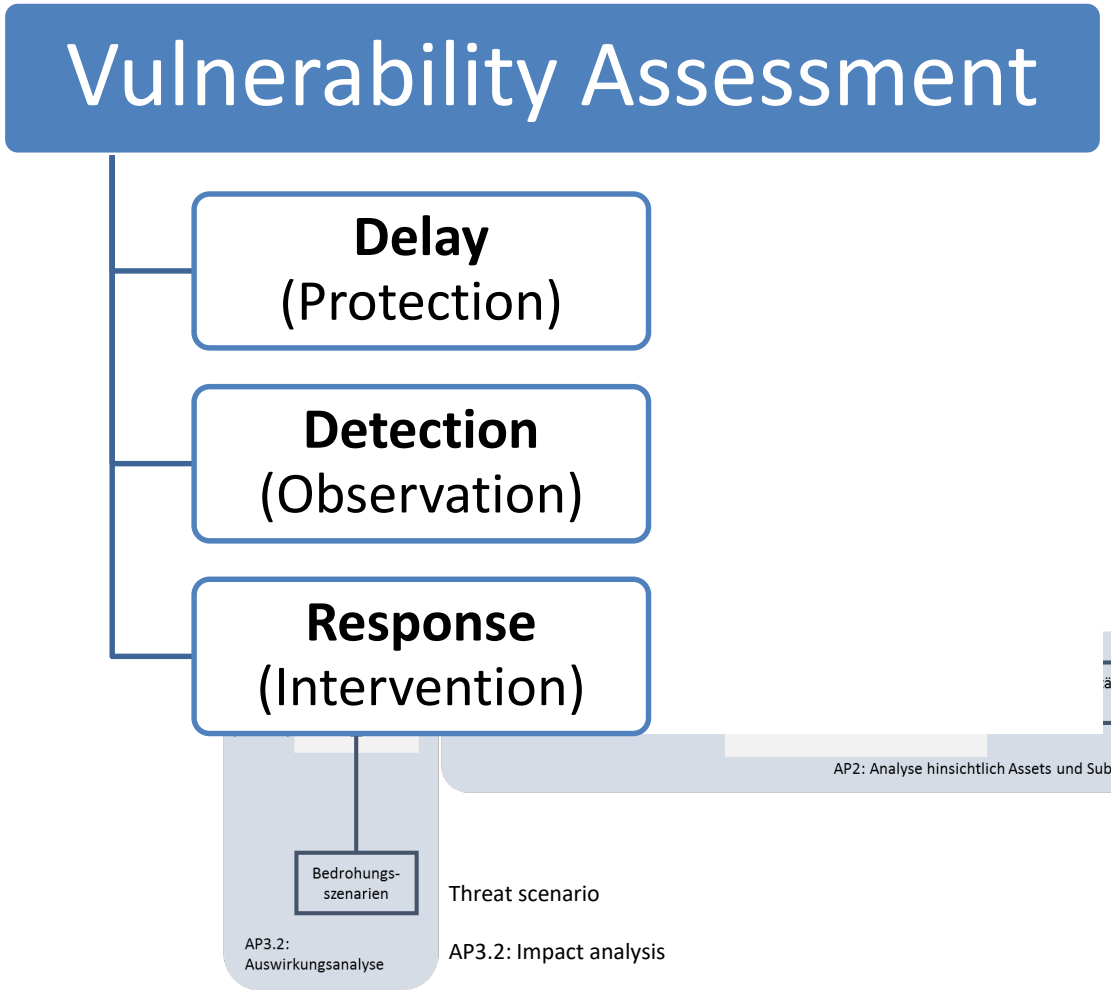
State of the Art: Harnser Model **(semi-quantitative)**

DuPont Scheme

- Assessing influencing factors on discrete scales (i.e.: 1 – 5)
- Qualitative ranking of individual asset risks (scenario-based)







Harnser Group (Ed.) 2010: *A Reference Security Management Plan for Energy Infrastructure*. Brussels: European Commission.

Risk Assessment (simplified)

RISK = Probability x Consequence

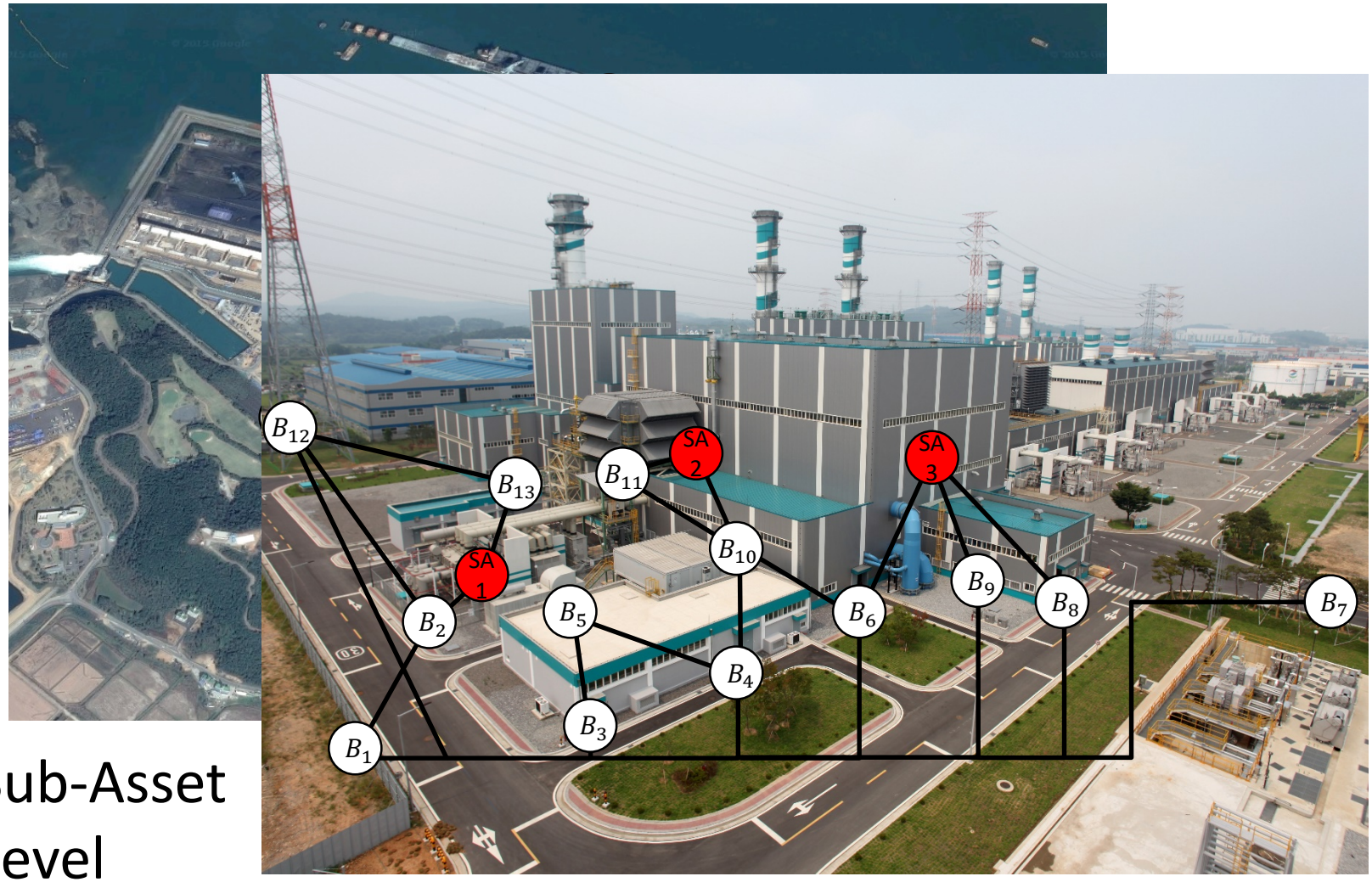
In **Physical Security**:

RISK = Threat x Vulnerability x Consequence

Mitigation via:

Prevention	Security Measures (Detection, Delay, Response)	Resilience

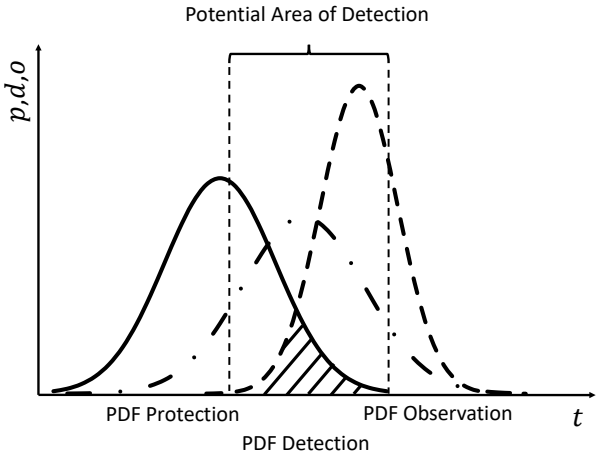
Quantitative Analysis of Physical Vulnerability

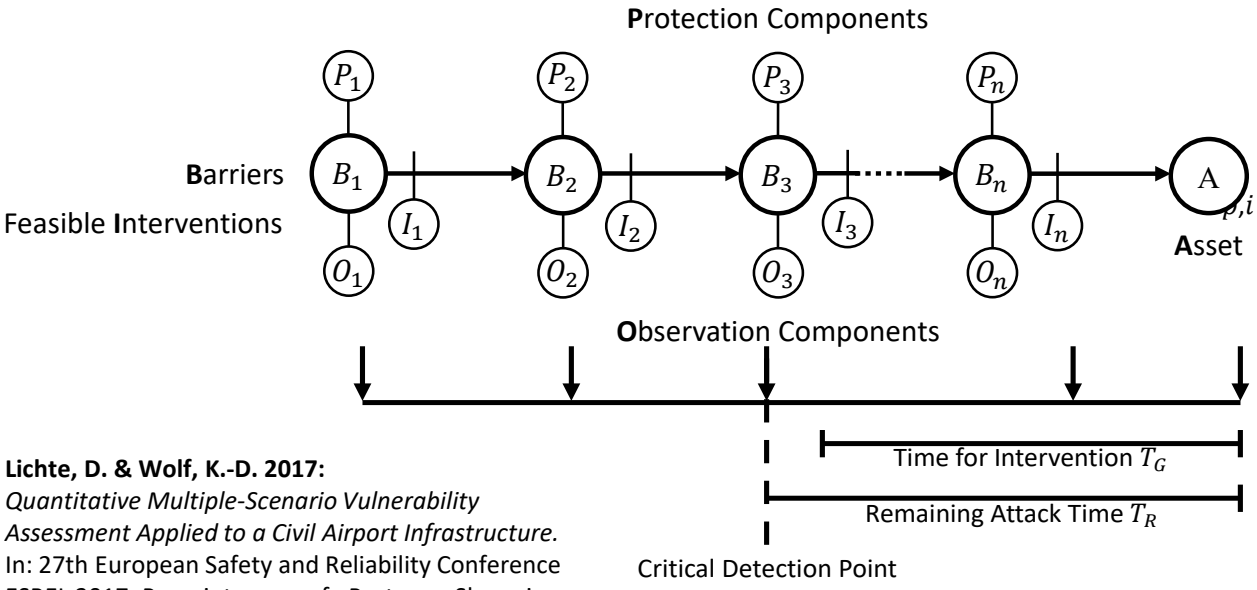


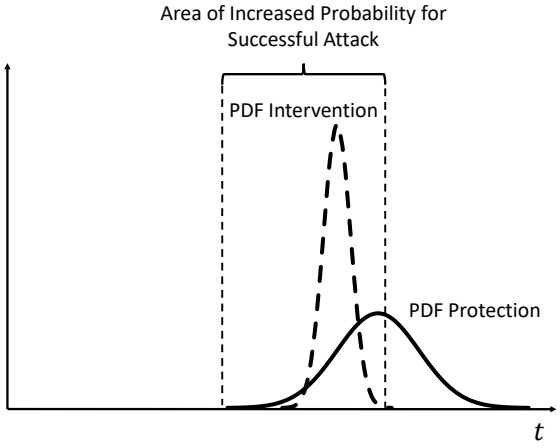
Sub-Asset Level

Quantitative Vulnerability Assessment in Physical Security

- Barrier-oriented
- Based on time metric
- Using conditional probabilities
- Considering uncertainties







Lichte, D. & Wolf, K.-D. 2017:
Quantitative Multiple-Scenario Vulnerability Assessment Applied to a Civil Airport Infrastructure.
In: 27th European Safety and Reliability Conference ESREL 2017, Proc. intern. conf., Portoroz, Slovenia.

Outlook: Safety & Security in Smart Environments

- Increasing Distribution of Smart Home Components
- Concepts of „Assisted Living“

http://www.loxone.com

Concept:
Smart Door

- Identification of safety/security scenario
- **Balancing of measures** is necessary!

- Complex Systems with a great number of components
  - Cyber Physical Systems / Systems of Systems

- Increasing number of safety & security tradeoffs
- No simple technological solution (decoupling) available

How should a smart door „behave“?
If e.g.:

- **There are individuals in the house?**
- **...no individuals are at home?**

BACKUP

Scenario-spanning Quantitative Risk Analysis (QRA): **Uncertainty** in Risk Contributions

R = **T**hreat x **V**ulnerability x **C**onsequence

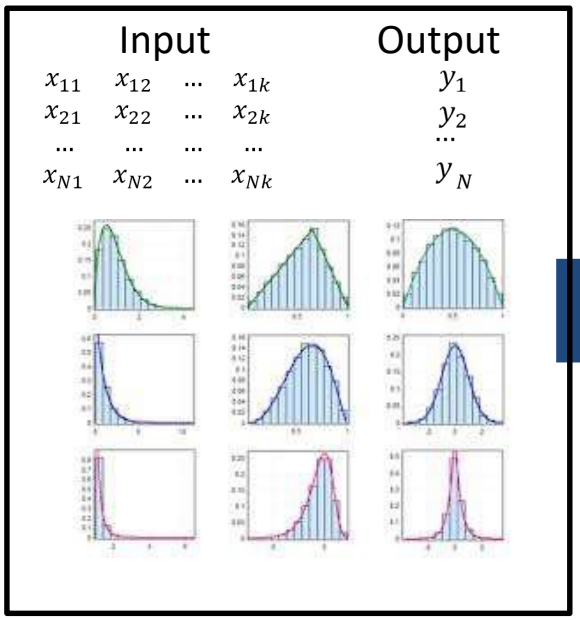
- **To what extent** (how precise or imprecise – i.e. arithmetic average, variance, etc.) are the single contributions T, V, C (or further) known?
- Which **approaches and methods** may be used to evaluate and model vulnerability (in the generalized sense) as a technical, complex quality of systems or processes?

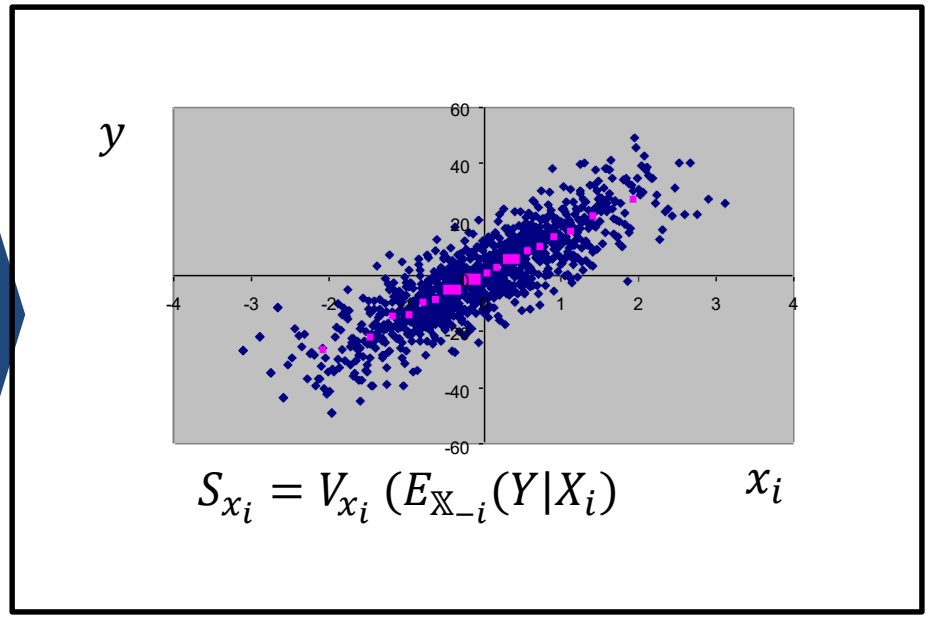
The **different disciplines of safety & security** as well as different **contributions of risk** to the overall risk

$R_{Ges} = R_1 + R_2 + R_3$ will **require different answers!**

Simulation & Uncertainty Analysis of Quantitative Models

- Monte-Carlo Model Simulation
- **Variance Based Sensitivity Analysis** (First & Total Order)
- Analysis of Uncertainties in assessment & available data





Conclusion

- **Integrated Assessment of safety and security** in the future is needed
- **Balancing** of safety and security risk can be accomplished via scenario-spanning **quantitative risk analysis**
- **Decoupling of scenarios** may be possible
- Quantitive risk models require an **objective metric**
- **Uncertainties** must be carefully considered
  - In many (most) cases an authoritative decision based on quantitative analysis **will not be possible**
  - Uncertainty analysis will show that
- **Ethical Questions** must be adressed (this is another talk)