Hazard Analysis of IT Systems
Towards a joint technical language with regard to „safety & security hazards“

Arslan Brömme
Dipl.-Inform. B.Sc.

Faculty of Informatics
University of Hamburg

broemme@informatik.uni-hamburg.de

GI FB Sicherheit – Schutz und Zuverlässigkeit **Workshop on**
„Joint Terminology for Safety and Security“
July 12, 2002, Frankfurt a.M., Germany

Plan of the Talk

1. *Introduction*
2. *Safety & Security Hazards*
3. *Safety & Security Hazard Analysis Techniques*
4. *Summary and Conclusions*

1. Introduction

General Workshop Mission:

Enable discussion on a joint technical language (nomenclature, terminology) for the research area of dependable IT systems

- **Safety**
  - **failure → robustness (fault tolerance, redundancy)**
  - **availability of system (functions)**
  - **aspects of system design and usability**

- **Security**
  - **attack -> „patchability" (protection, recovery)**
  - **availability of system (functions)**
  - **aspects of system design and usability**

2. Safety & Security Hazards (1)

What is a failure ?

Failure is the nonperformance or inability of the system or component to perform its intended function for a specified time under specified environmental conditions.

- **Type 1:**
  intended, designed and constructed behavior does not satisfy the system goal (systemic failure)

- **Type 2:**
  operation does not follow the original design (e.g. caused by environmental disturbances)

[Leveson 95]

2. Safety & Security Hazards (2)

What is an attack [against security]?

Any (intended) activities against systems' security properties like

- ***integrity (e.g. man in the middle)***
- ***authenticity (e.g. spoofing)***
- ***confidentiality (e.g. sniffing)***
- ***availability (e.g. denial of service)***
- ***...***

2. Safety & Security Hazards (3)

What is a [safety] hazard ?

A hazard is a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead inevitably to an accident (loss event).

[Leveson 95]

- ***Successful attacks against e.g. the availability lead to failures which can lead to loss events but not accidently.***

  => What is a security hazard ?

  => What is a „safety & security hazard" ?

} Defs TODO

2. Safety & Security Hazards (4)

Assumption:

Failures and attacks are elements of a defined set of „safety & security hazards".

Statement #1: ***„A hazard can result in a hazard."***

a) An attack can result in a failure.

- ***intended malfunction***
- ***destruction***

b) A failure can result in an attack.

- ***exploit***

2. Safety & Security Hazards (5)

c) A failure can result in an attack which can result in a failure ...

- ***chain of hazards***
- ***mass mailing malware***
- ***(d)dos***

d) A failure can result in a failure.

- ***fault intolerance***
- ***accident***

e) An attack can result in an attack.

- ***intrusion response***

2. Safety & Security Hazards (6)

Statement #2: *„A hazard needs not to be known."*

a) A failure needs not to be known.
- *failure types 1 and 2*

b) An attack needs not to be known.
- *intrusion detection systems (using heuristics)*
- *firewalls*

2. Safety & Security Hazards (7)

Statement #3: *„A hazard analysis can help to detect hazards."*

a) A failure analysis can help to detect failures.

- *different types of safety hazard analysis:*

  - *Preliminary Hazard Analysis (PHA)*
  - *System Hazard Analysis (SHA)*
  - *Subsystem Hazard Analysis (SSHA)*
  - *Software Hazard Analysis (SHA)*
  - *Operating Hazard Analysis (OHA)*
  - *Maintenance Hazard Analysis (MHA)*
  - *Fault Hazard Analysis (FHA)*
  - *...*

2. Safety & Security Hazards (8)

- *different types of safety hazard analysis techniques:*
  - *Fault Tree Analysis (FTA)*
  - *Cause Consequence Analysis (CCA)*
  - *Management Oversight and Risk Tree Analysis (MORT)*
  - *Event Tree Analysis (ETA)*
  - *Hazards and Operability Analysis (HOA)*
  - *Interface Analysis (IA)*
  - *Failure Mode and Effects Analysis (FMEA)*
  - *Failure Modes, Effects, and Criticality Analysis (FMECA)*
  - *Fault Hazard Analysis (FHA)*
  - *State Machine Hazard Analysis (SMHA)*
  - *Task and Human Error Analysis (THEA)*
  - *...*

2. Safety & Security Hazards (9)

b) An attack analysis can help to detect attacks.

- ***chosen categories of attack damages:***

  - ***attacker receives information about target***
  - ***access to network resources***
  - ***access to local resources***
  - ***loss of availability***
  - ***loss of data integrity during transmission***
  - ***loss of data confidentiality during transmission***
  - ***loss of local data integrity***
  - ***loss of local data confidentiality***
  - ***loss of authenticity***
  - ***denial of service***

[Schnell et al 01]

2. Safety & Security Hazards (10a)

- ***Types of attacks and attack levels:***
  - ***passive***
    - ***sniffing***
  - ***active***
    - ***disconnection***
    - ***modification***
    - ***falsification***
  - ***attack levels (network/local)***
    - ***low***
    - ***medium***
    - ***high***

[Schnell et al 01]

2. Safety & Security Hazards (10b)

- ***Examples for network attack levels (network):***
  - ***low***
    - ***spoofing, wrong IP parameters,***
    - ***(syn) flooding/attacks,***
    - ***ping of death, tunneling, ...***
  - ***medium***
    - ***DNS attacks/spoofing,***
    - ***FTP port number guessing and connection, ...***
  - ***high***
    - ***mail spoofing,***
    - ***distributed/coordinated attacks,***
    - ***applications, ...***

[Schnell et al 01]

2. Safety & Security Hazards (11)

c) A failure analysis can help to detect attacks.

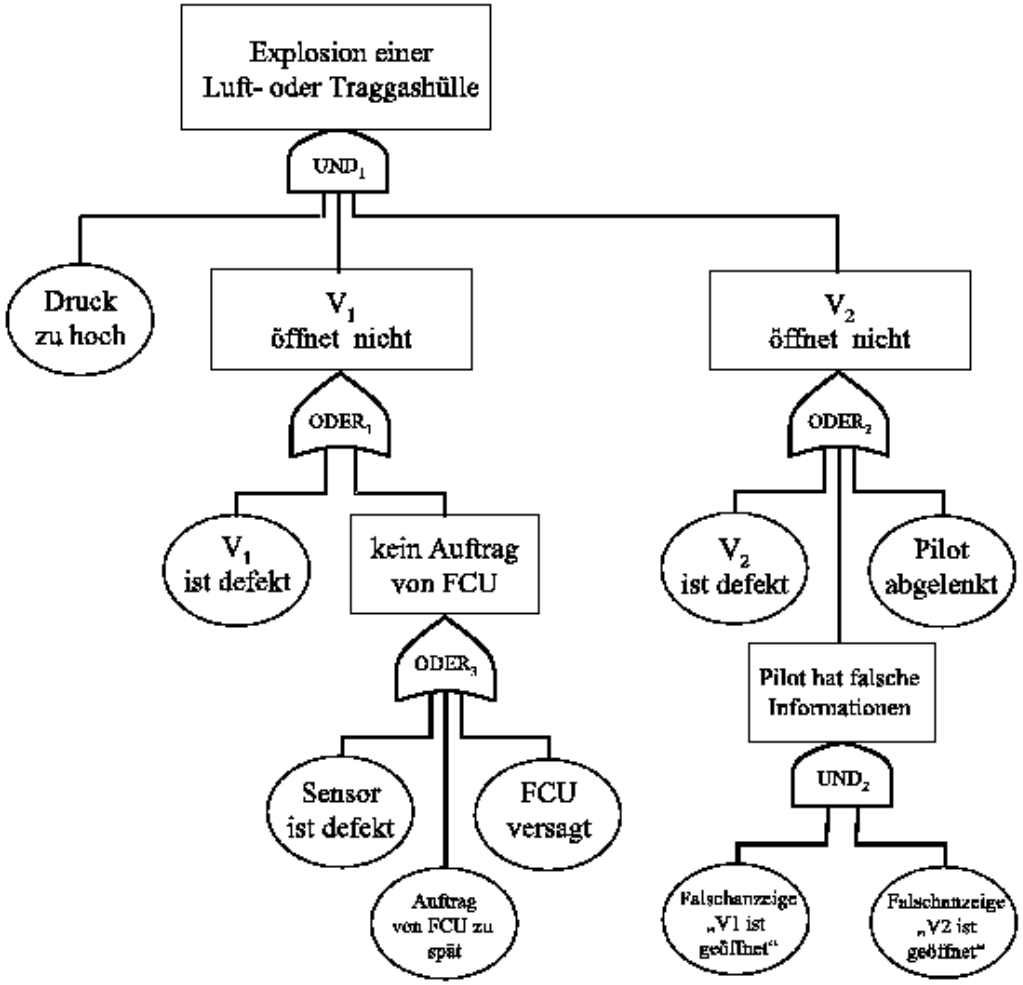
- ***combination of a) and b)***

d) An attack analysis can help to detect failures.

- ***combination of a) and b)***

3. *Safety & Security Hazard Analysis Techniques (1)*

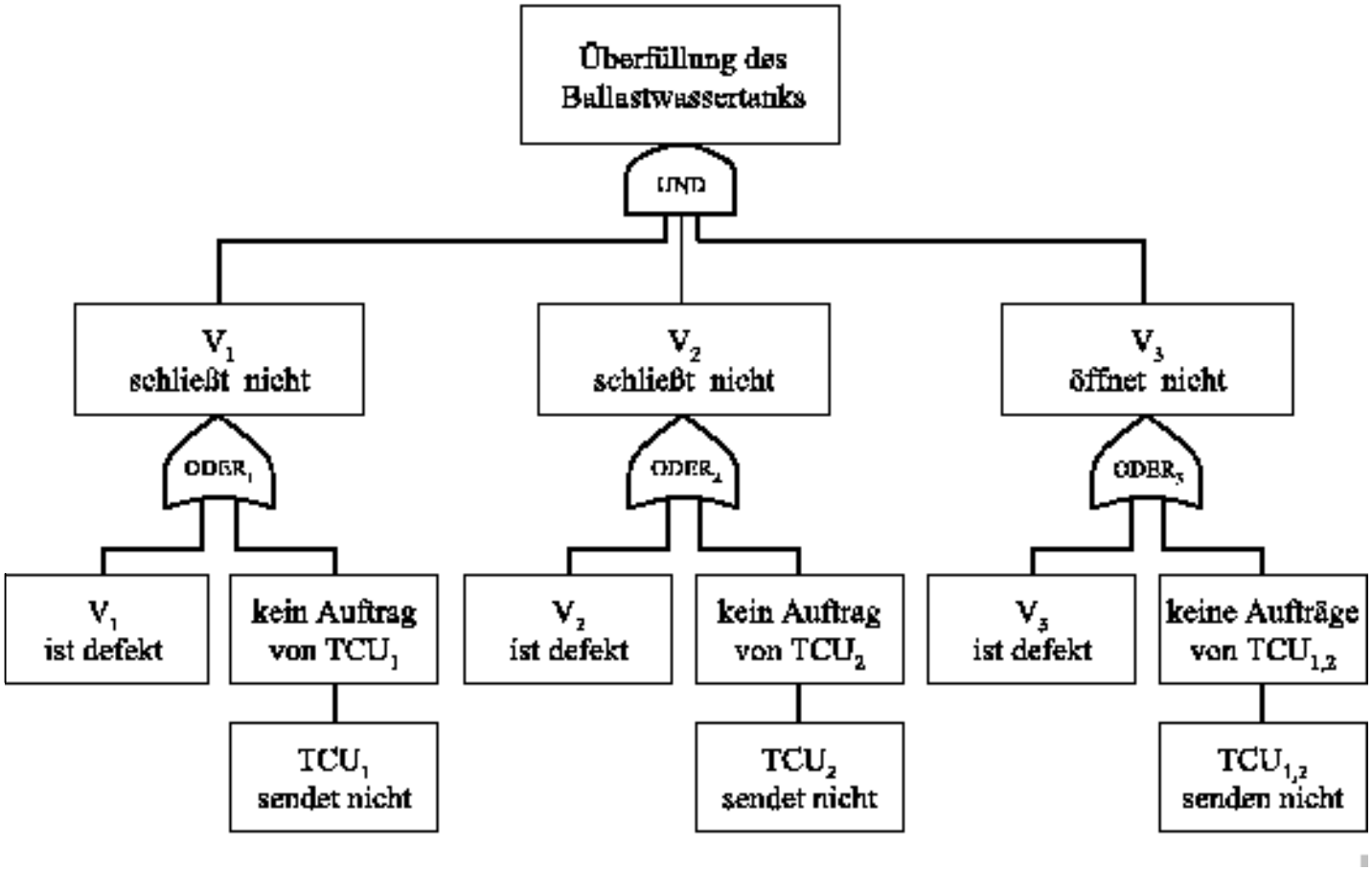
- ***Example #1:*** **Fault Tree Analysis (FTA)**



FCU = Flight Control Unit

3. *Safety & Security Hazard Analysis Techniques (2)*

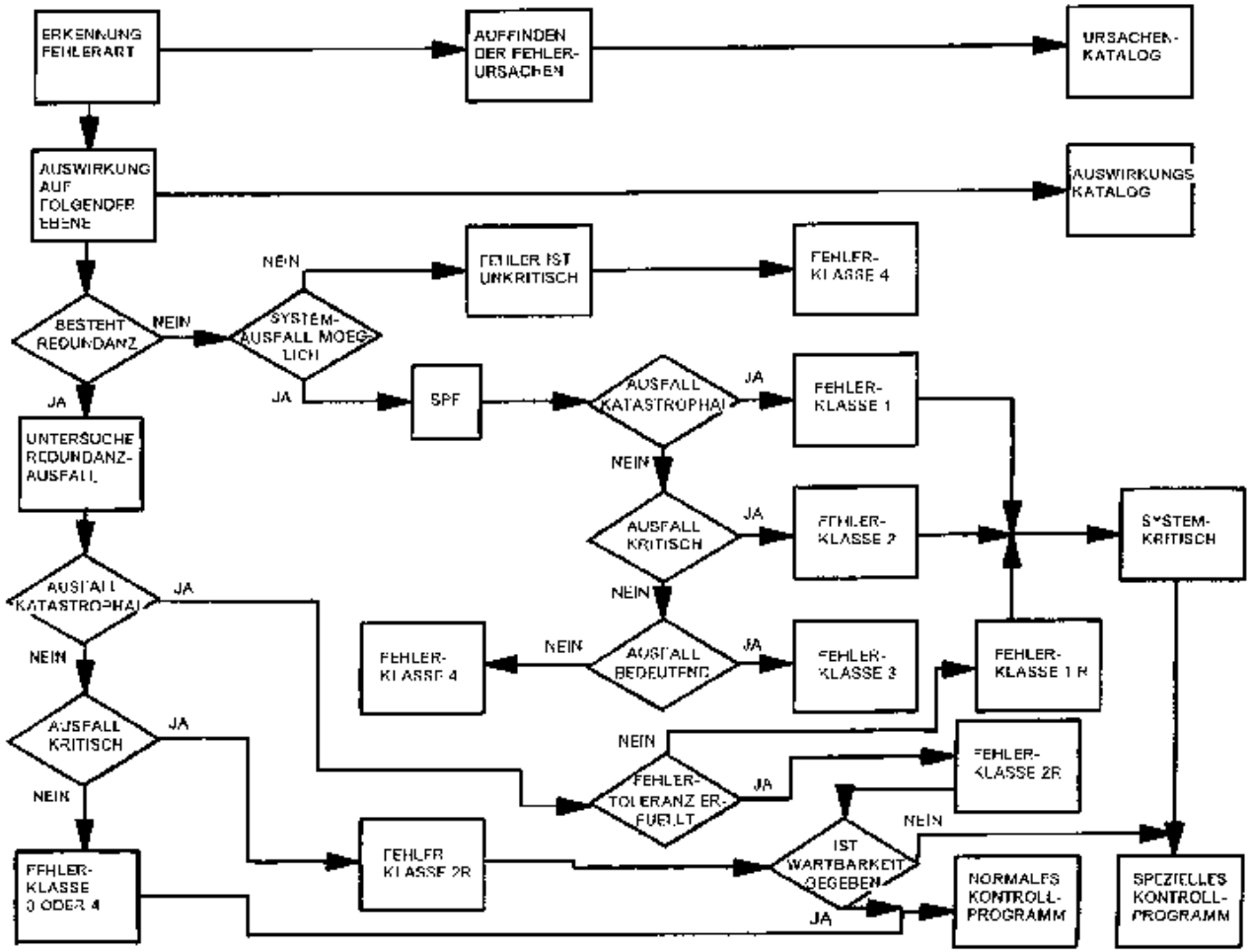
- ***Example #2:*** **Fault Tree Analysis (FTA)**



TCU = Trim Control Unit

3. *Safety & Security Hazard Analysis Techniques (3)*

- ***Example #3:*** **Failure Modes, Effects, and Criticality Analysis (FMECA)**



3. *Safety & Security Hazard Analysis Techniques (4)*

- **More possible single/joint hazard analysis techniques:**
  - **Attack Tree Analysis (ATA)**
  - **Attack Modes, Effect, and Criticality Analysis (AMECA)**
  - **Fault/Attack Tree Analysis (F/ATA)**
  - **Failure/Attack Modes Effect, and Criticality Analysis (F/AMECA)**

4. Summary and Conclusions

In this talk the idea of extended safety hazards to

- **safety & security hazards**

has been presented.

Classical hazard analysis techniques could be adapted for the usage within special aspects of security risk analysis, e.g.

- **Fault/Attack Tree Analysis (F/ATA)**
- **Failure/Attack Modes, Effects and Criticality Analysis (F/AMECA)**

A joint nomenclature could be partially derived from the usage of similar methods and techniques for hazard analysis.