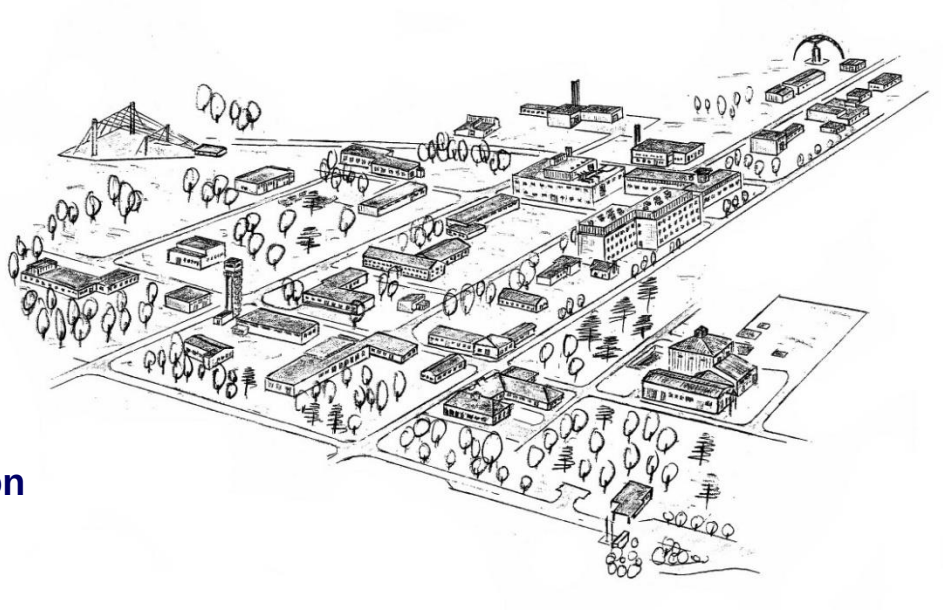
Analysis of documented IEMI attacks and Classification of IEMI caused effects



F. Sabath

Bundeswehr Research Institute for Protective Technologies and NBC Protection (WIS)

Overview

Introduction

A. Analysis of documented IEMI attacks
   1. Documented criminal Usage of EM
   2. Analysis of documented IEMI Attacks
   3. Lessons Learned

B. Classification of IEMI caused effects
   1. Observed Effects
   2. Classification of EMI Effects
   3. Conclusion

Electrical and electronic systems are important in modern day life

- Security Systems
- Medical science
- Economy
- Transportation
- Communication
- Defense

Trends in system design

Military Systems

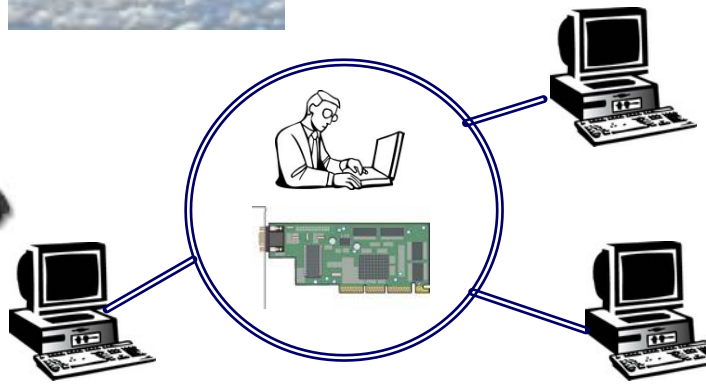








Civil Systems



- increasing portion of electronic components and subsystems
- increasing ration of commercial components in safety critical systems
- control of safety critical functions by electronic systems
- waving of mechanical redundancy / back up
- networked architecture / design
- short reaction cycles of critical functions

Technological Trend

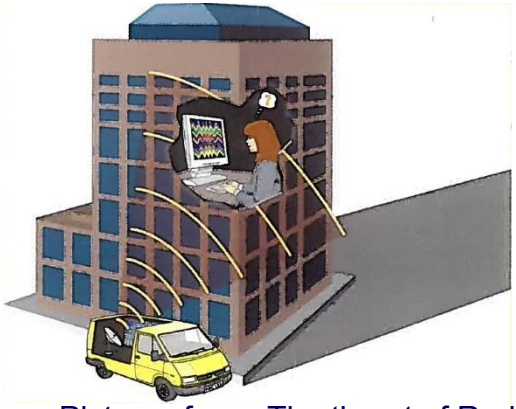
1) Technological development enabled the design of high-power EMI sources and components (e.g. antennas)
   - ⇨ Availability of EMI sources
   - ⇨ Proliferation of EMI technologies
   - ⇨ Increase of potential threat

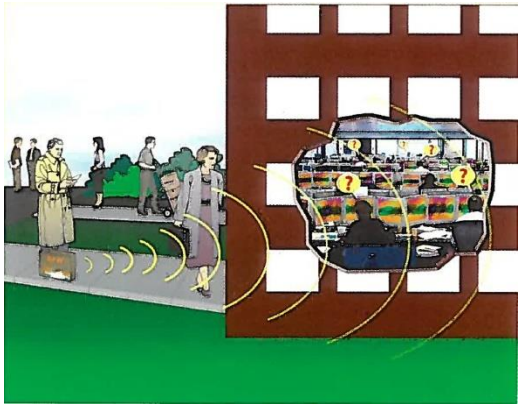
2) Increasing dependency of all parts of modern society on IT-technology
   - ⇨ Decreasing susceptibility levels
   - ⇨ Classical EMC protection measures are ineffective against IEMI disturbances
   - ⇨ Increasing vulnerability

Potential criminal threat

3) Worldwide rise of criminal and terrorist (asymmetric) threats;

4) The use of electromagnetic sources to generate Intentional Electromagnetic Interference (IEMI) is becoming an increasing concern.
   - ⇨ EM fields can penetrate physical boundaries such as fences and walls
   - ⇨ IEMI attacks can be undertaken covertly and anonymously
   - ⇨ Potential to disable or disrupt functionality of critical systems and infrastructure





Pictures from „The threat of Radio Frequency Weapons to critical infrastructure facilities“

A.
Analysis of documented IEMI attacks

1. Documented criminal Usage of EM
2. Analysis of documented IEMI Attacks
3. Lessons Learned

Key questions

a) Have IEMI attacks been observed and documented?

b) How large is the possibility that a critical electronic system becomes a target of an IEMI attack?

c) How dangerous are the possible and observed consequences of an IEMI attack?

Introduction

A. Analysis of documented IEMI attacks

1. Documented criminal Usage of EM

2. Analysis of documented IEMI Attacks

3. Lessons Learned

B. Classification of IEMI caused effects

1. Observed Effects

2. Classification of EMI Effects

3. Conclusion

EMI Events with IEMI potential

1. On a ferryboat the spurious emission of energy saving lamps disturbed the frequency band used by the Automatic Identification System (AIS). As a result the AIS was unable to acquire targets which were farther away than 8 NM.

2. The S-band radar of a ferryboat caused disturbances and short-time dropouts in its TV-system.

3. At a new build vessel an incorrect grounding of the air condition system caused interferences with the Differential GPS (DGPS) system. As a consequent the navigation system was unable to determine the accurate position.

4. In November 1999, San Diego San Diego Gas and Electric company experienced severe electromagnetic interference to its SCADA wireless network. It was unable to actuate critical valve openings and closings under remote control of the SCADA electronic systems. The source of the SCADA failure was later determined to be radar operated on a ship 25 miles off the coast of San Diego.

⇒ EMI has the potential to cause serious damage and hazardous situations!

⇒ Can EMI intentionally be employed for criminal activities?

⇒ Has that happened?

Documented Criminal Usage of EM (1)

1. In Japan, criminals used an EM disruptor on a gaming machine to trigger a false win
2. In St. Petersburg, a criminal used an EM disruptor to disable a security system an a Jeweler store
3. In Kizlyar, Dagestan, Russia Chechen rebel command disabled police radio communication using RF jammer during a raid.
4. In multiple European cities (e.g. Berlin) criminals used GSM-Jammern to disable the security system of limousines.
5. In Russia, Chechen rebels used an EM disruptor to defeat a security system and gain access to a controlled area.

Documented Criminal Usage of EM (2)

6. In London, UK, a city bank was the target of blackmail attempt whereby the use of EM disruptors was threatened to be used against the banks IT-system.

7. In the Netherlands an individual disrupted a local bank IT network because he was refused loan. He constructed a briefcase-size EM disruptor, which he learned how to build from the internet.

8. In Moscow, the normal work of one automatic telephone station has been stopped as a result of remote injection of a voltage in to a telephone line. As a result 200 thousand people had no phone connection for one day

Introduction

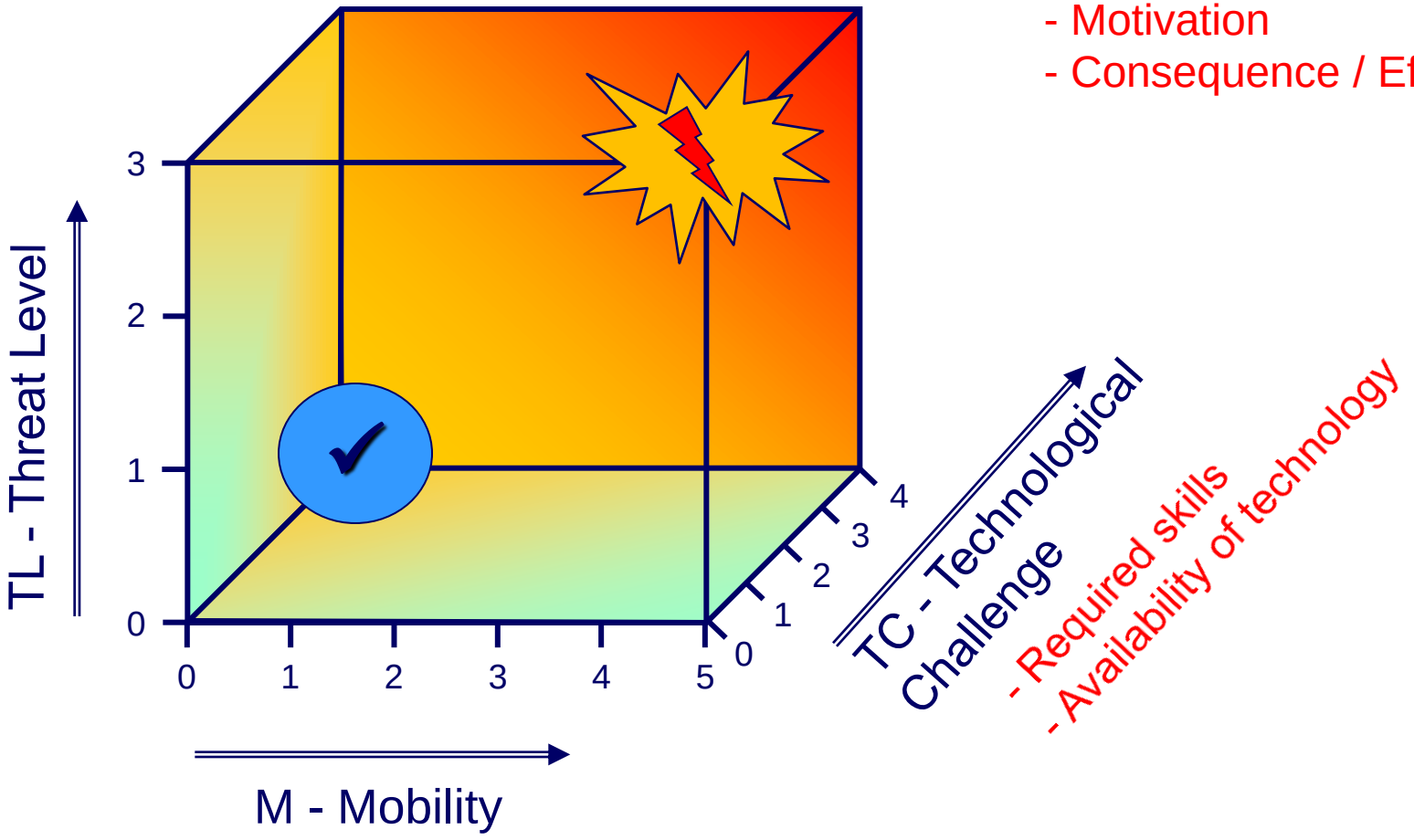
A. Analysis of documented IEMI attacks

1. Documented criminal Usage of EM
2. **Analysis of documented IEMI Attacks**
3. Lessons Learned

B. Classification of IEMI caused effects

1. Observed Effects
2. Classification of EMI Effects
3. Conclusion

IEMI Risk Analysis



Additional Aspects:
- Motivation
- Consequence / Effect

- Distance source target

Offender - Motivation

Case		Motivation
1	Gaming machine	Money
2	Jeweler store	Robbery → Money
3	Police radio communication	Obstruction of police
4	Car security system	Robbery → Money
5	Russian security system	Suppression / Denial of service & Robbery → Money
6	UK Bank	Blackmail / robbery → Money
7	NL Bank	Payback
8	Telephone Moscow	?

TC – Technological Challenge

Case		Technology	Availability	Skills	Technological Challenge
1	Gaming machine	RF Gun (EM Disruptor)	Commercial / Internet	1 - Amateur/ Internet	1 - Low tech system (Amateur)
2	Jeweler store	EM Disruptor	Commercial components	2 - Technician	1.5 - Medium tech system (Technician)
3	Police radio communication	Jammer	Commercial / Commercial components	2 - Technician	1.5 - Medium tech system (Technician)
4	Car security system	GSM Jammer	Commercial	1 - Amateur/ Internet	1 - Low tech system (Internet)
5	Russian security system	unknown	Commercial components	2 - Technician	No information available
6	UK Bank	unknown	unknown	1.5 - Amateur - Technician	1.5 - Medium tech system (Technician)
7	NL Bank	HPM-Source	Commercial / Commercial	1 - Amateur/ Internet	1 - Low tech system (Internet)
8	Telephone Moscow	Direct Injection	unknown	unknown	No information available

M - Mobility

Case		Distance Source-Target	Mobility
1	Gaming machine	RF Gun (EM Disruptor)	4 - Very mobile
2	Jeweler store	EM Disruptor	3.5 – (Very) mobile
3	Police radio communication	Jammer	3.5 – (Very) mobile
4	Car security system	GSM Jammer	5 - Highly mobile
5	Russian security system	unknown	5 - Highly mobile
6	UK Bank	unknown	unknown
7	NL Bank	HPM-Source	4 - Very mobile
8	Telephone Moscow	Direct Injection	?

CO - Consequence

Case		Effect	Criticality	Consequence
1	Gaming machine	malfunction	interference	Unjustified win/ economic loss
2	Jeweler store	suppression of main function	degradation/ loss of main function	economic loss
3	Police radio communication	suppression of main function	degradation	unknown
4	Car security system	suppression of main function	loss of main function	economic loss
5	Russian security system	suppression of main function	degradation	unknown
6	UK Bank	unknown	unknown	economic loss
7	NL Bank	malfunction/ destruction of components	degradation/ loss of main function	defect → lack of confidence & economic damage
8	Telephone Moscow	Shut-down	loss of main function	economic damage

Introduction

A. Analysis of documented IEMI attacks

1. Documented criminal Usage of EM
2. Analysis of documented IEMI Attacks
3. **Lessons Learned**

B. Classification of IEMI caused effects

1. Observed Effects
2. Classification of EMI Effects
3. Conclusion

Lessons Learned (1)

- The threat by (criminal) Intentional Electromagnetic Interference Attacks on electronic systems already exists today
  - IEMI sources and their components are available on the free market
  - Needed knowledge needed can be gained from open literature and the internet
  - Available IEMI sources are small and highly mobile

- IEMI attack has the potential to cause major accidents or economic disasters.
  - Used IEMI sources need to be operate in the close ambient of the target system

Challenges of an IEMI Scenario

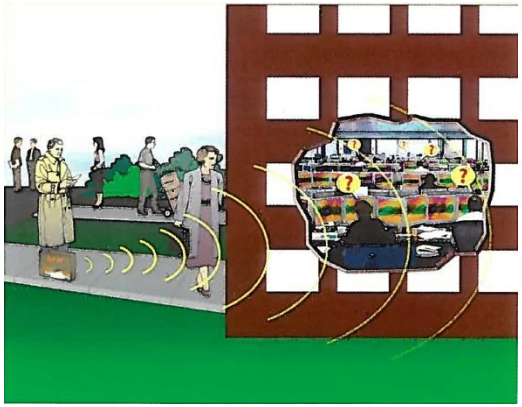
No information on caused effects

Offender

The Effect (malfunction) is observed

User / Operator

Information on the operation of the IEMI source



No information on external EM fields

Pictures from „The threat of Radio Frequency Weapons to critical infrastructure facilities“

Lessons Learned (2)

- IEMI attacks barely leave useful and provable traces
- user of a system under IEMI attack is unlikely to have any sensation or perception of the (external) electromagnetic stress
- IEMI counterattack measure depends on a monitoring of the (external) electromagnetic fields

- Offender has limited information on the susceptibility of the target system ($\rightarrow$ multiple attempts)
- In most scenarios the offender can not observe the caused effects ($\rightarrow$ no information on success)

B.
Classification of IEMI caused Effects

1. Observed Effects
2. Classification of EMI Effects
3. Conclusion

Introduction

A. Analysis of documented IEMI attacks

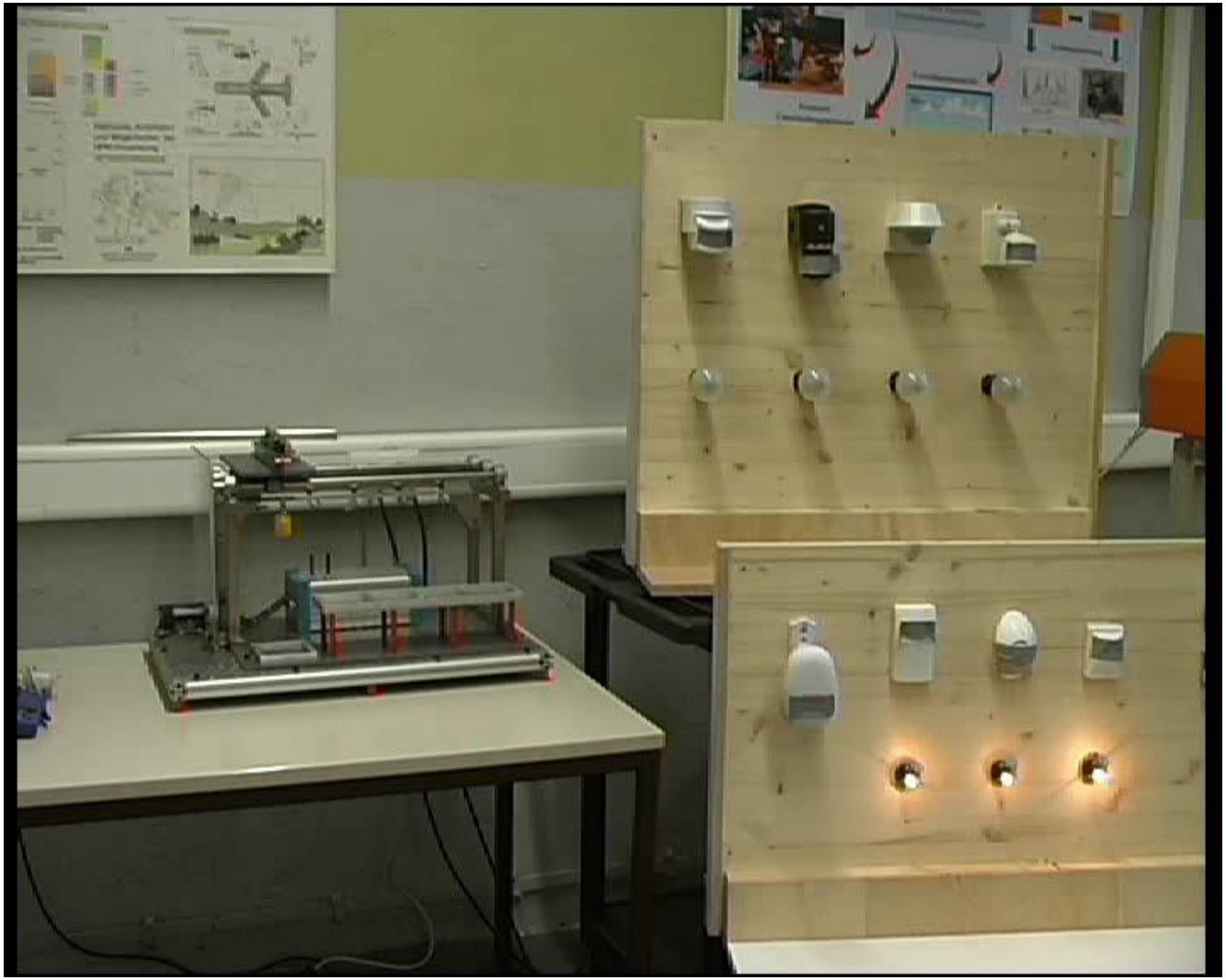
1. Documented criminal Usage of EM
2. Analysis of documented IEMI Attacks
3. Lessons Learned

B. Classification of IEMI caused effects

1. Observed Effects

2. Classification of EMI Effects
3. Conclusion

Observed Effects



Source: Diehl VA

Observed Effects

- Flickering of screens / distorted meter or display
- Black screen
- Display of wrong data
- Corruption of data
- Response of sensors
- Reduction of computational performance / data transfer
- Hang up of software
- Reboot of computer, controller, processor
- Failure / destruction

Observed Effects

- Observed effects differ significantly from each other due to
  - employed HPEM test environment
  - set up of susceptibility tests
  - design and the functionality of system under test

- Manufacturers of electronic systems are reluctant to have the susceptibility data of their systems be published and discussed in public.

Observed Effects

⇒ A scientific discussion needs a categorization of HPEM effects that

1. summarizes the essential information without giving away too much detail on the system and
2. enables a comparison of different manifestations of HPEM effects in different systems.

Introduction

A. Analysis of documented IEMI attacks

1. Documented criminal Usage of EM
2. Analysis of documented IEMI Attacks
3. Lessons Learned

B. Classification of IEMI caused effects

1. Observed Effects
2. **Classification of EMI Effects**
3. Conclusion

Classification of EMI Effects

Effects caused by an HPEM environment can be characterized by:

1. attributes of the physical mechanism
2. duration of the effect
3. the need of human intervention
4. Consequences
   (e.g. implication on the main (or critical) function)

Classification by Mechanism (I)

Category		Effect	Description
	U	Unknown	Unable to determine due to effects on another component or not observed.
	N	no effect	No effect occurs.
Interference	**I.1**	noise	Raised noise level on signal and power lines, which results in flashing of displays or reduced data rates.
	I.2	bit flip	Injected signals alternate bits of a datastream.
	I.3	failure	Malfunction of the system / component due EM interference.
	I.4	break down	Hang-up or crashing of software.

Classification by Mechanism (D)

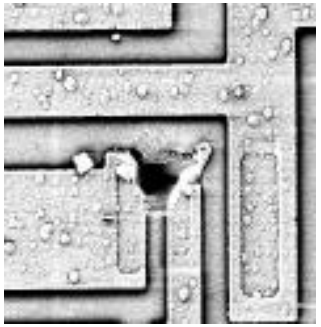
Category		Effect	Description
Destruction	**D.1**	latch up	Injected signal causes latch up in semiconductor components.
	D.2	flashover	On chip flashover / flashover in components.
	D.3	on chip wire melting	Wires on chip are melted by injected energy.
	D.4	bond wire destruction / wire melting on PCB	Wires on PCB and/or bond wires in semiconductor devices are melted by injected HPEM energy.

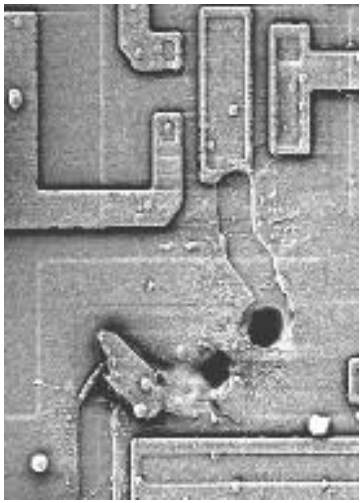
Example D.2: Flashover

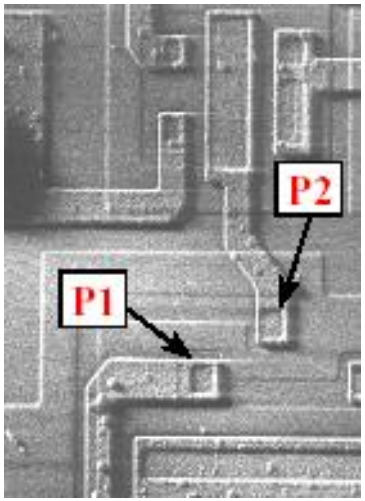
High differences in the electric potential can cause flashover between of conducting parts as

- GND und VCC layers / lines
- signal traces

The high currents during flashover yield to thermal destruction of components.

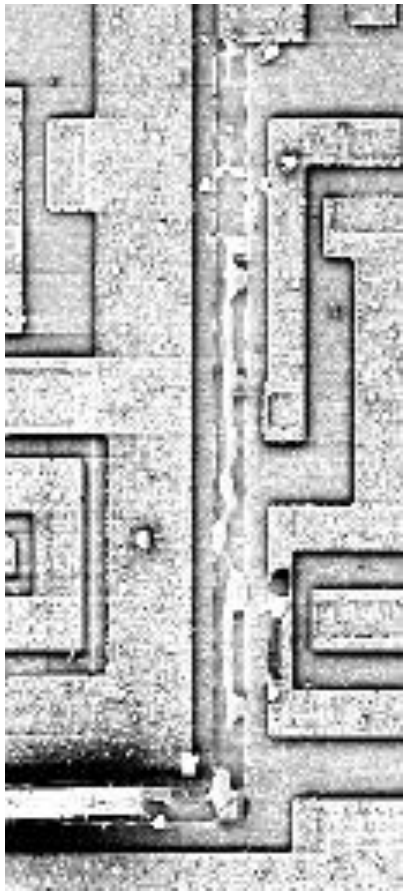






Example D.3 / D.4: Wire Melting

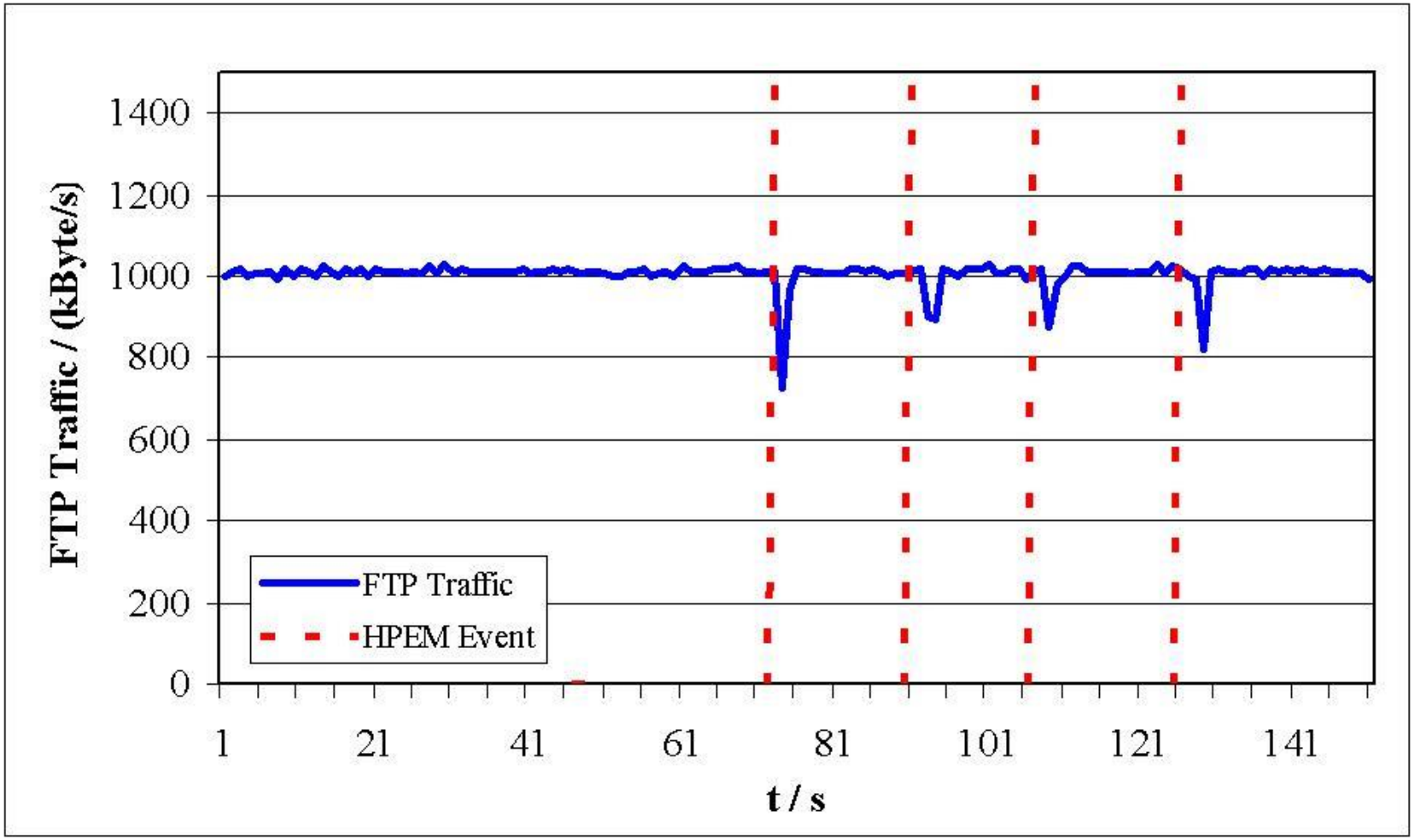
High currents on signal lines (on chip) as well as on bond wires (chip / PCB) can result to the thermal melting of wires.



Classification by Duration

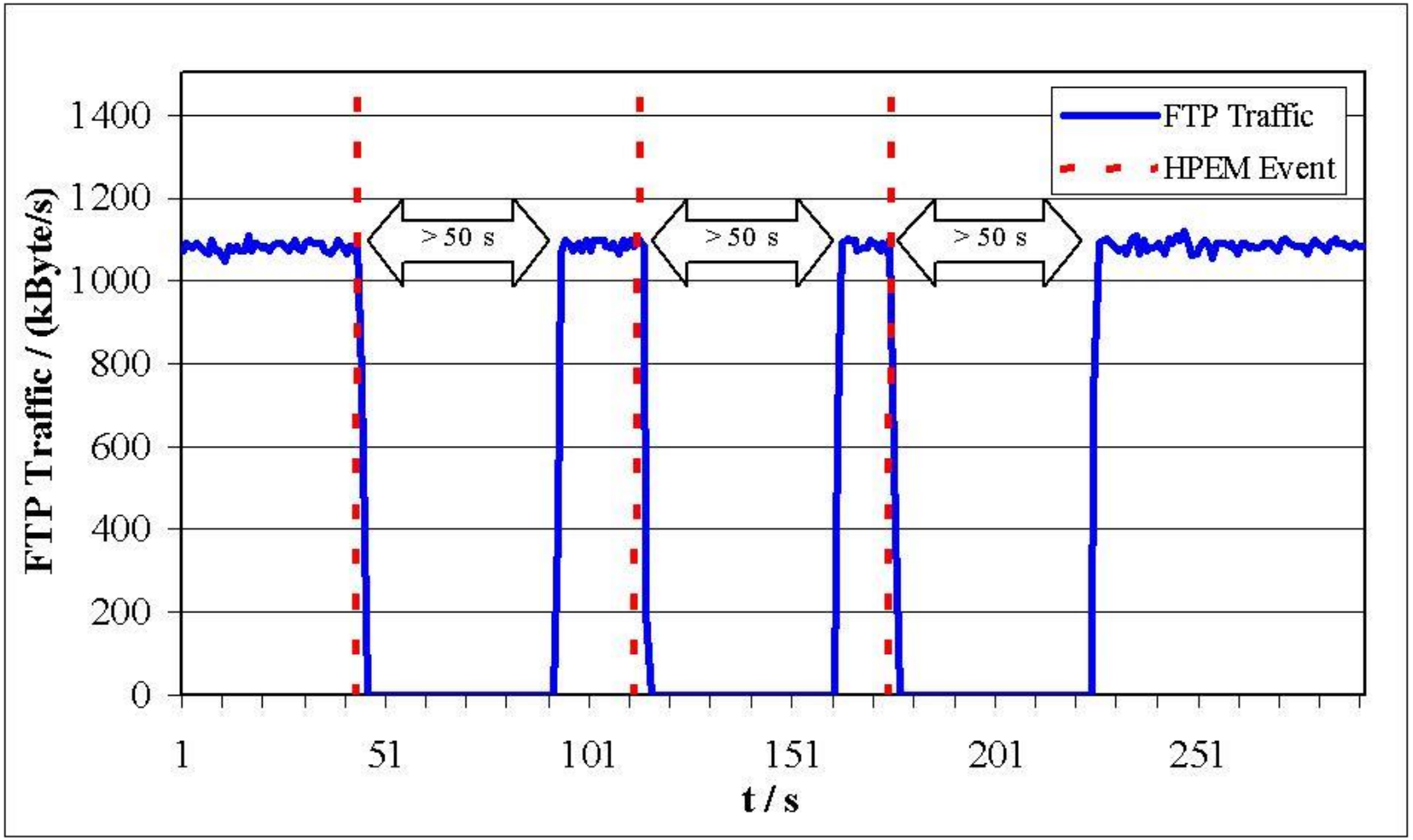
Level	Duration	Description
U	**u**nknown	Unable to determine due to effects on another component or not observed.
N	**n**o effect	No effect occurs.
E	during **e**xposure only	Observed effect is present only during exposure to HPEM environment; system functionality is completely available after HPEM environment has vanished .
T	**t**emporary	Effect is present some time after HPEM environment has vanished, but system recovers without human intervention.
H	resistant till **h**uman intervention	Follow-up time is shorter or equal to typical reaction/ operation cycle of the system.
P	**p**ermanent or till replacement of HW / SW	Effect is present till human intervention (e.g. reset, restart of function). Due to the effect the system is not able to recover to normal operation within an acceptable period.

Example E Effect



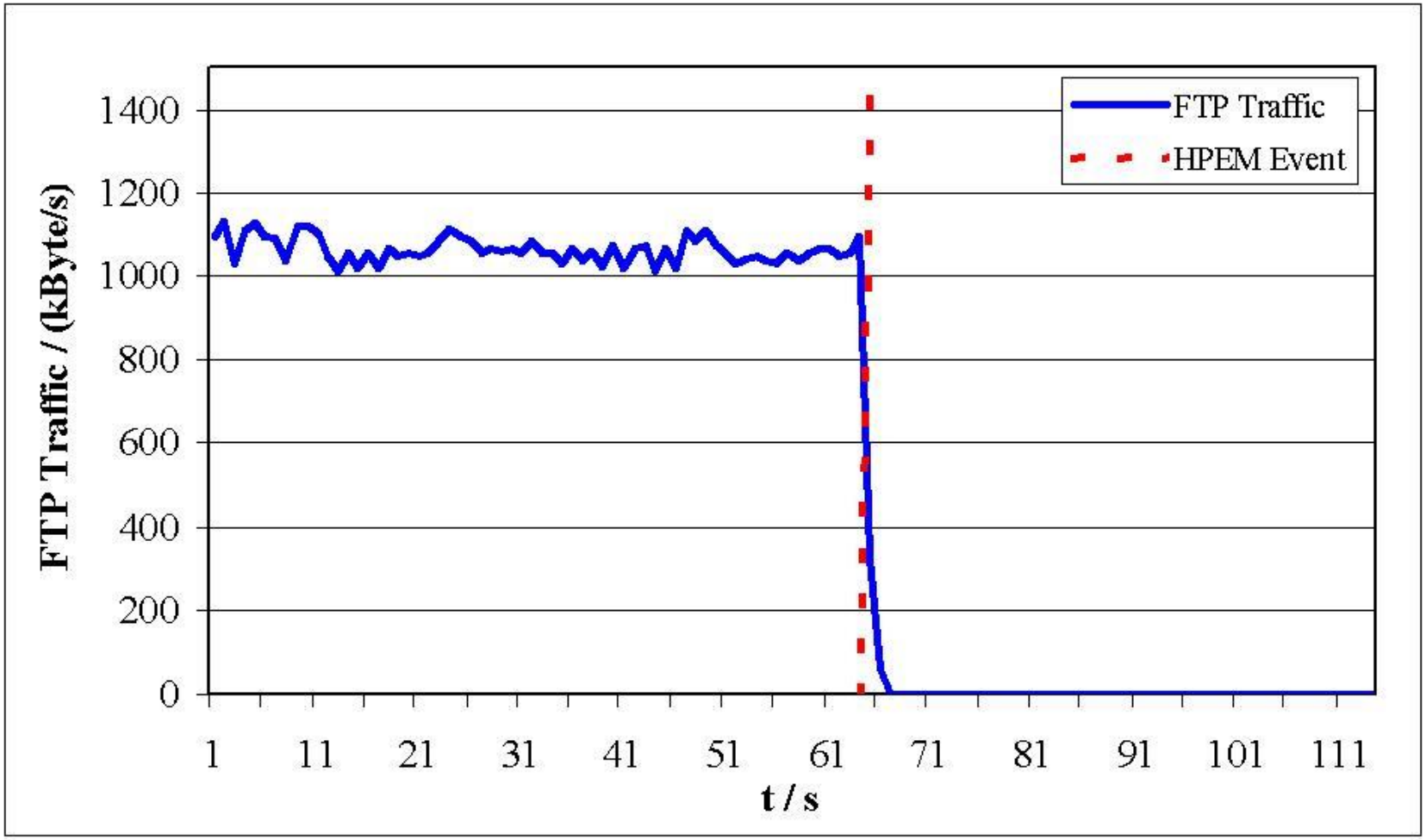
Source: WIS

Example T Effect



Source: WIS

Example H Effect

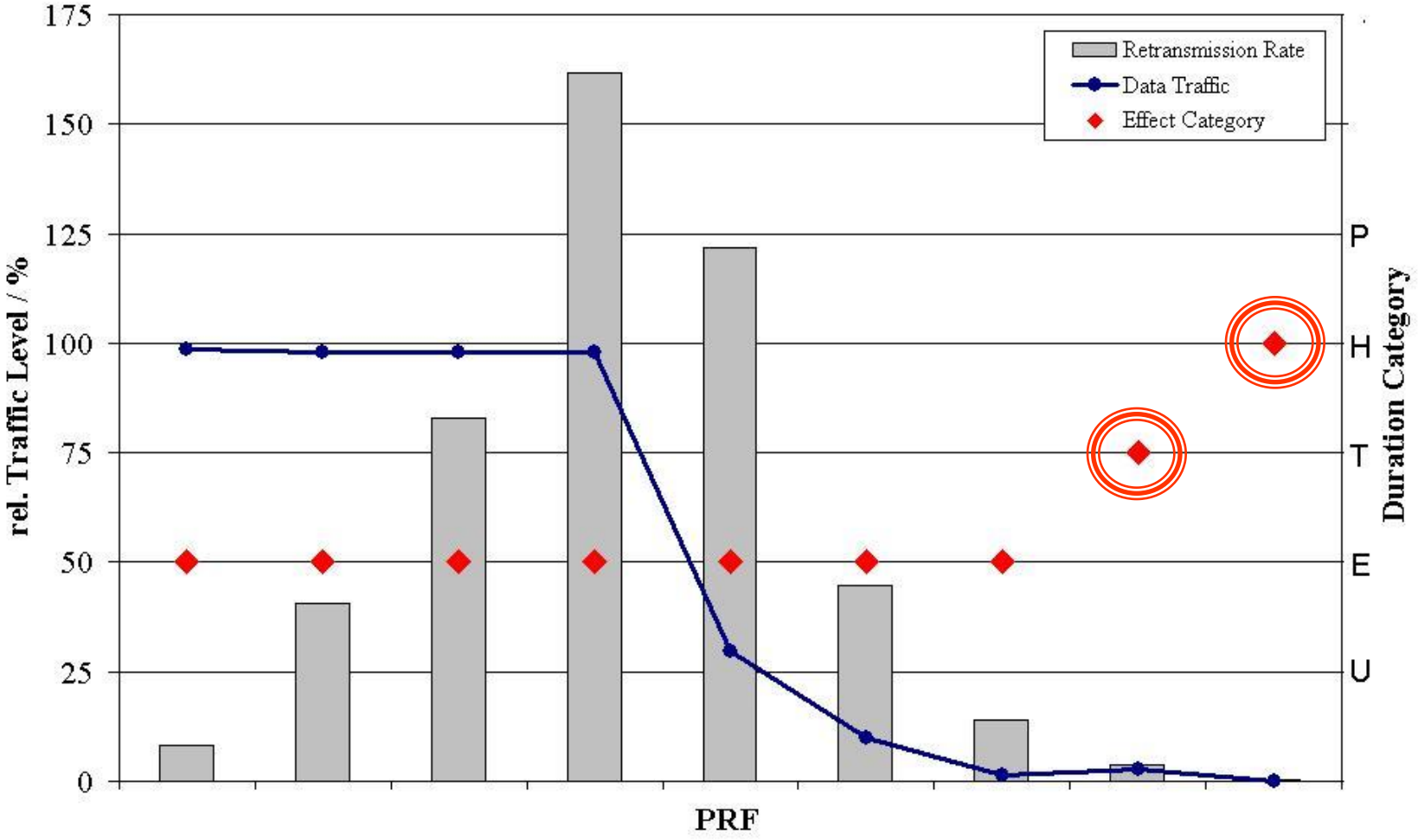


Source: WIS

Classification by Criticality

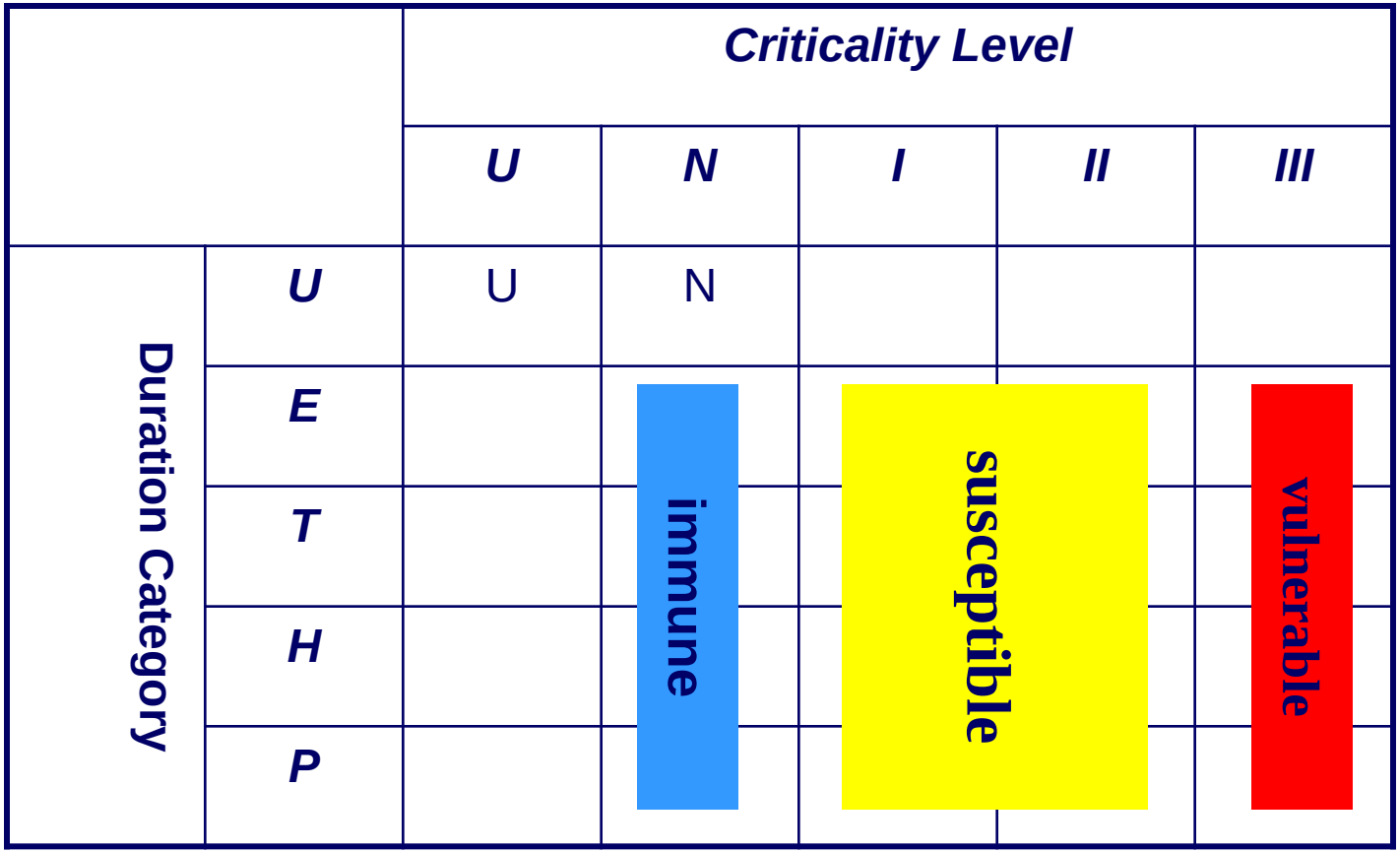
Level	Criticality	Description
U	unknown	Unable to determine due to effects on another component or not observed.
N	no effect	No effect occurs or the system can fulfill his mission without disturbances.
I	interference	The appearing disturbance does not influence the main mission.
II	degradation	The appearing disturbance reduces the efficiency and capability of the system.
III	loss of main function (mission kill)	The appearing disturbance prevents that the system is able to fulfill its main function or mission.

Example IT-Network



Source: WIS

Classification



Introduction

A. Analysis of documented IEMI attacks

1. Documented criminal Usage of EM
2. Analysis of documented IEMI Attacks
3. Lessons Learned

B. Classification of IEMI caused effects

1. Observed Effects
2. Classification of EMI Effects
3. **Conclusion**

Conclusion

- need of a scientific discussion for a categorization of HPEM effects, which
  - provides the essential information
  - enables a comparison of different manifestations
- Three classifications
  - by physical mechanism
  - by duration
  - by criticality
- combination of duration and criticality might be of best value

Thank you for your attention

Questions ?