KU LEUVEN

PETER

PETER - Pan European Training network on Electromagnetic Risk management

Prof. D. Pissoort
KU Leuven, Campus Brugge

PLOT Showcase 2017

Overview

- Some definitions: EMC? FS?
- Why immunity testing is not sufficient
- EMC & FS: how to combine?
- MCSA European Training PETER
- Conclusions

KU LEUVEN

Overview

- **Some definitions: EMC? FS?**
- Why immunity testing is not sufficient
- EMC & FS: how to combine?
- MCSA European Training PETER
- Conclusions

Some definitions…

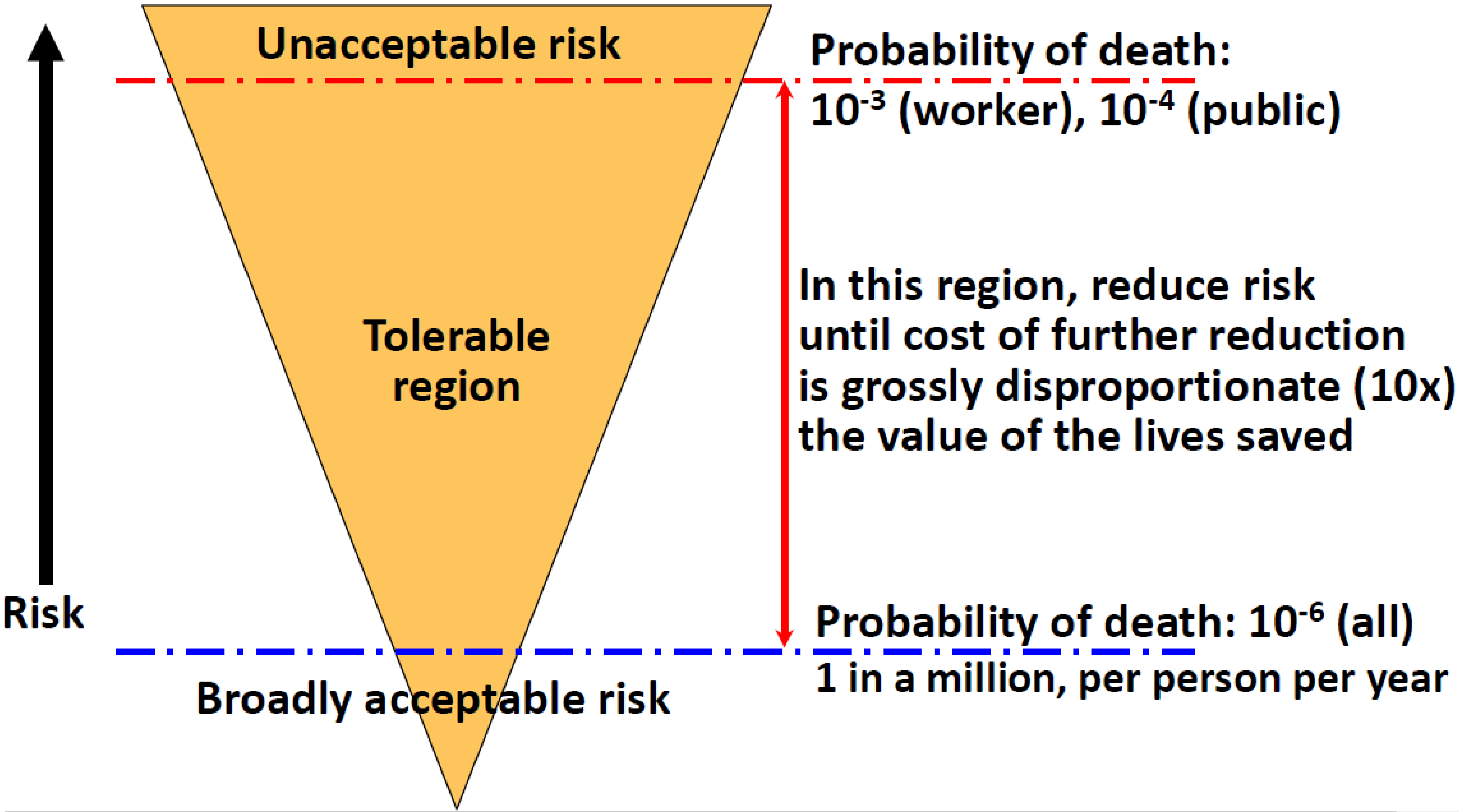
- EMC = ElectroMagnetic Compatibility
  - *the ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment*
  - *the engineering discipline of managing electromagnetic emissions and immunity to ensure that the occurrence of electromagnetic interference is acceptable given the application*

Some definitions…

- FS = Functional Safety
    - *the part of the overall safety that depends on an (electronic/electrical) system or equipment operating correctly in response to its inputs. FS ensures that errors, malfunctions or faults do not cause unacceptable safety risks to people or the environment*

KU LEUVEN

Acceptable Levels of Risk of Death, Per Person, Per Year



Safety Integrity Levels (SIL)

Safety Integrity Level (SIL)	Average probability of a dangerous failure, "on demand" or "in a year*"	Equivalent mean time to dangerous failure, in years*	Equivalent confidence factor required for each "demand" on the function
4	$\geq 10^{-5}$ to $<10^{-4}$	$>10^{4}$ to $\leq 10^{5}$	99.99 to 99.999%
3	$\geq 10^{-4}$ to $<10^{-3}$	$>10^{3}$ to $\leq 10^{4}$	99.9 to 99.99%
2	$\geq 10^{-3}$ to $<10^{-2}$	$>10^{2}$ to $\leq 10^{3}$	99% to 99.9%
1	$\geq 10^{-2}$ to $<10^{-1}$	>10 to $\leq 10^{2}$	90 to 99%

"Failure" is any error, malfunction or fault in a safety function

* Approximating 1 year = 10,000 hrs of operation

"On Demand"

"Continuous"

Safety Integrity Level (SIL)	Average dangerous failure rate, per hour	Equivalent mean time to dangerous failure, in hours	Equivalent confidence factor required for every 10,000 hours of continuous operation
4	$\geq 10^{-9}$ to $<10^{-8}$	$>10^{8}$ to $\leq 10^{9}$	99.99 to 99.999%
3	$\geq 10^{-8}$ to $<10^{-7}$	$>10^{7}$ to $\leq 10^{8}$	99.9 to 99.99%
2	$\geq 10^{-7}$ to $<10^{-6}$	$>10^{6}$ to $\leq 10^{7}$	99% to 99.9%
1	$\geq 10^{-6}$ to $<10^{-5}$	$>10^{4}$ to $\leq 10^{5}$	90 to 99%

"Failure" is any error, malfunction or fault in a safety function

EMC is becoming more important!

- All electronic devices are becoming more vulnerable for electromagnetic disturbances:
  - ***Lower intrinsic immunity of electronic devices*****:** Continuous miniaturization, demands for less power consuming products together with constant technological improvements of the manufacturing process result in die/mask shrinking and lower operating voltages. These developments make the internal electronic signals ‘weaker’ and more easily corrupted by EMI.

KU LEUVEN

EMC is becoming more important!

- All electronic devices are becoming more vulnerable for electromagnetic disturbances:
  - ***A more severe and complex electromagnetic environment*****:** Due to the rapidly increasing use of wireless data communications, faster switching power-devices, variable speed motor drives, the typical environment in which an electronic device is used becomes more ‘polluted’ with EMI of diverse nature and covering a very wide frequency range from the kHz-range up to GHz-range

KU LEUVEN

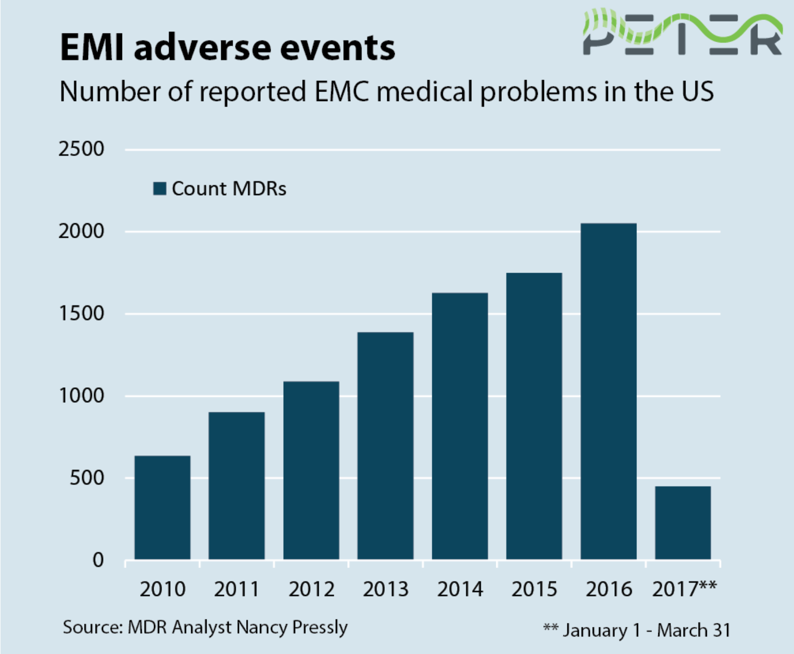
Failures due to EMI

- MAUDE (Manufacturer and User Facility Device Experience)
- Only medical device reports submitted to the FDA (U.S. Food and Drug Administration)
- Suspected device-associated deaths, serious injuries and malfunctions

What level of failures in 2017?

What level of failures in 2020?

What level of failures in 2025?



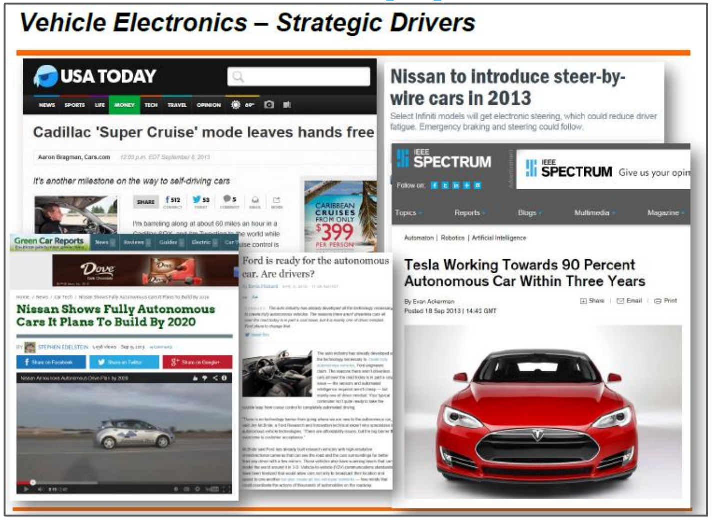
KU LEUVEN

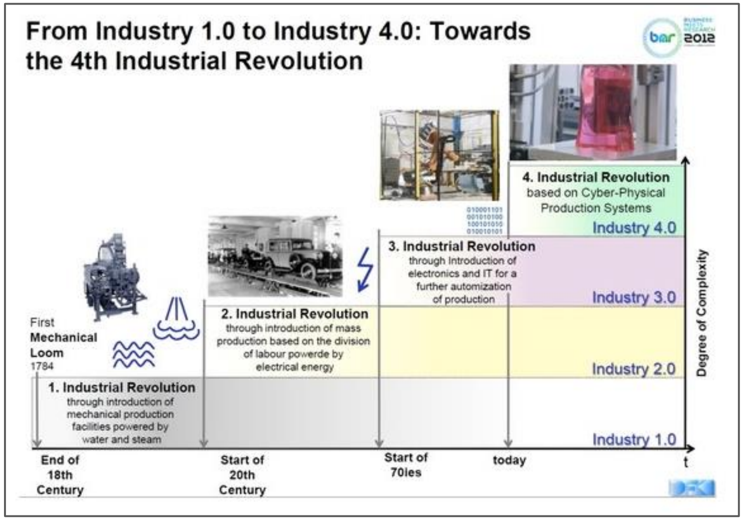
FS is becoming more important!

- Electronics is being used more and more in and for applications with stringent safety demands:

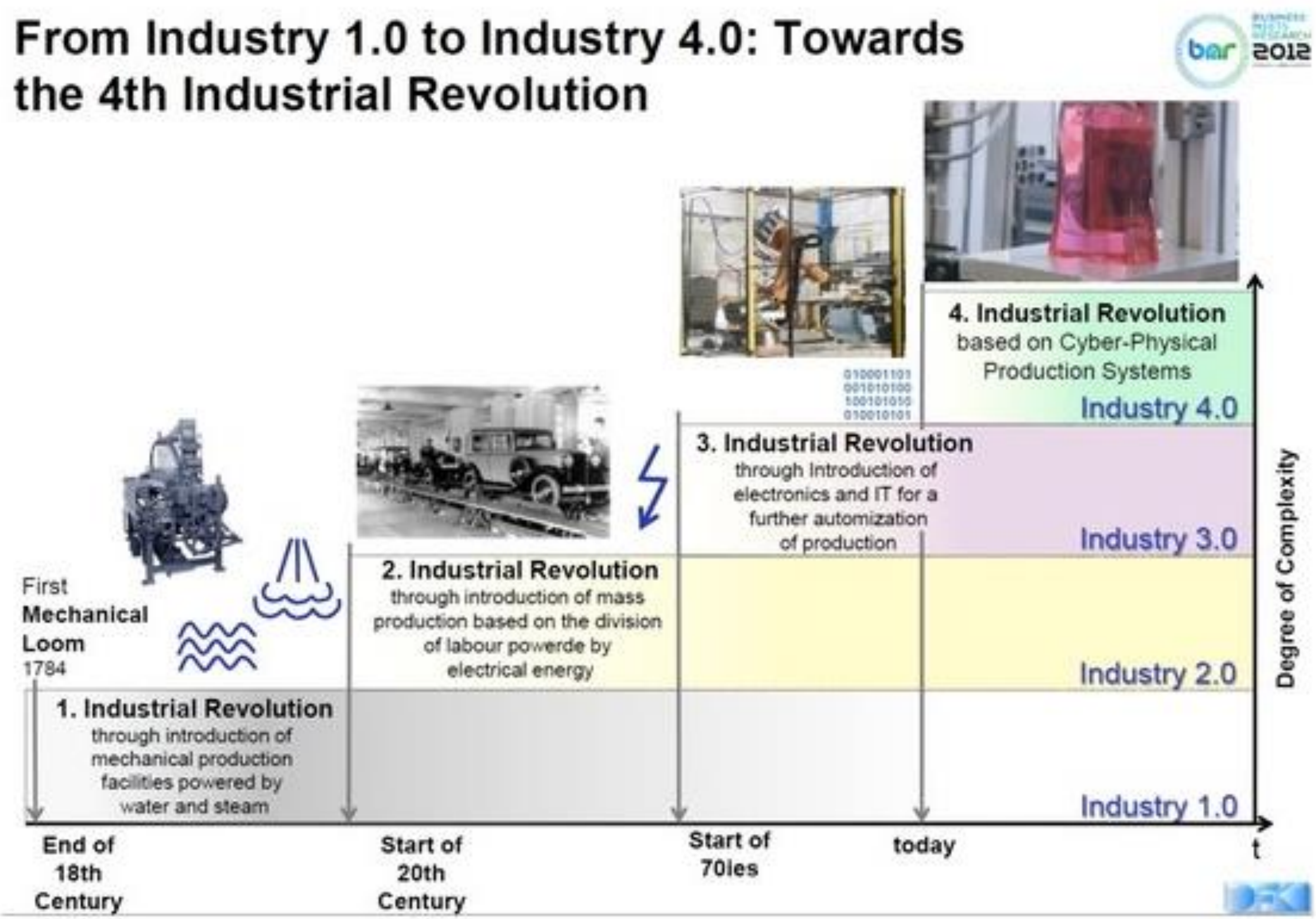
KU LEUVEN

Electronic Applications of the Near-Future

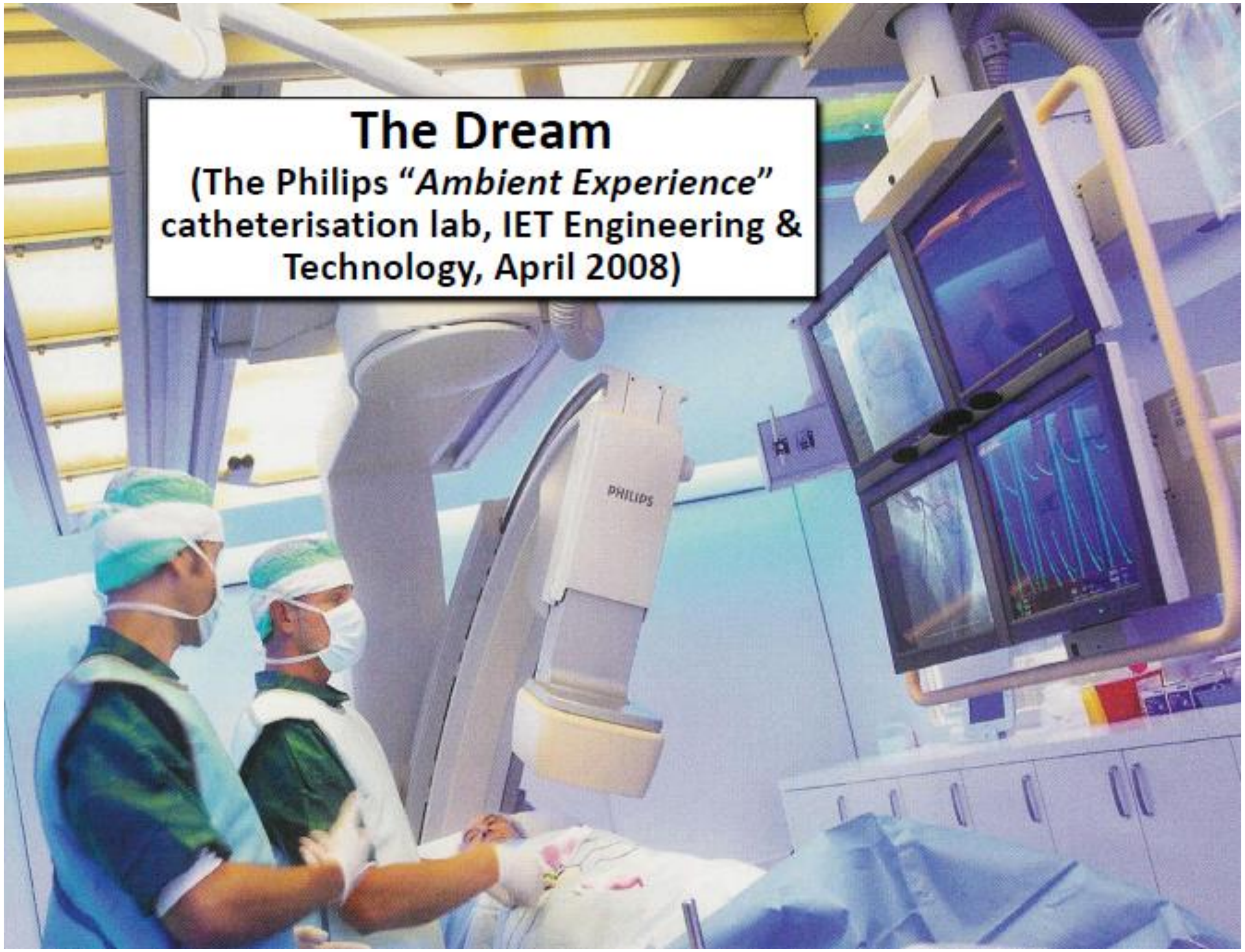




Industry 4.0

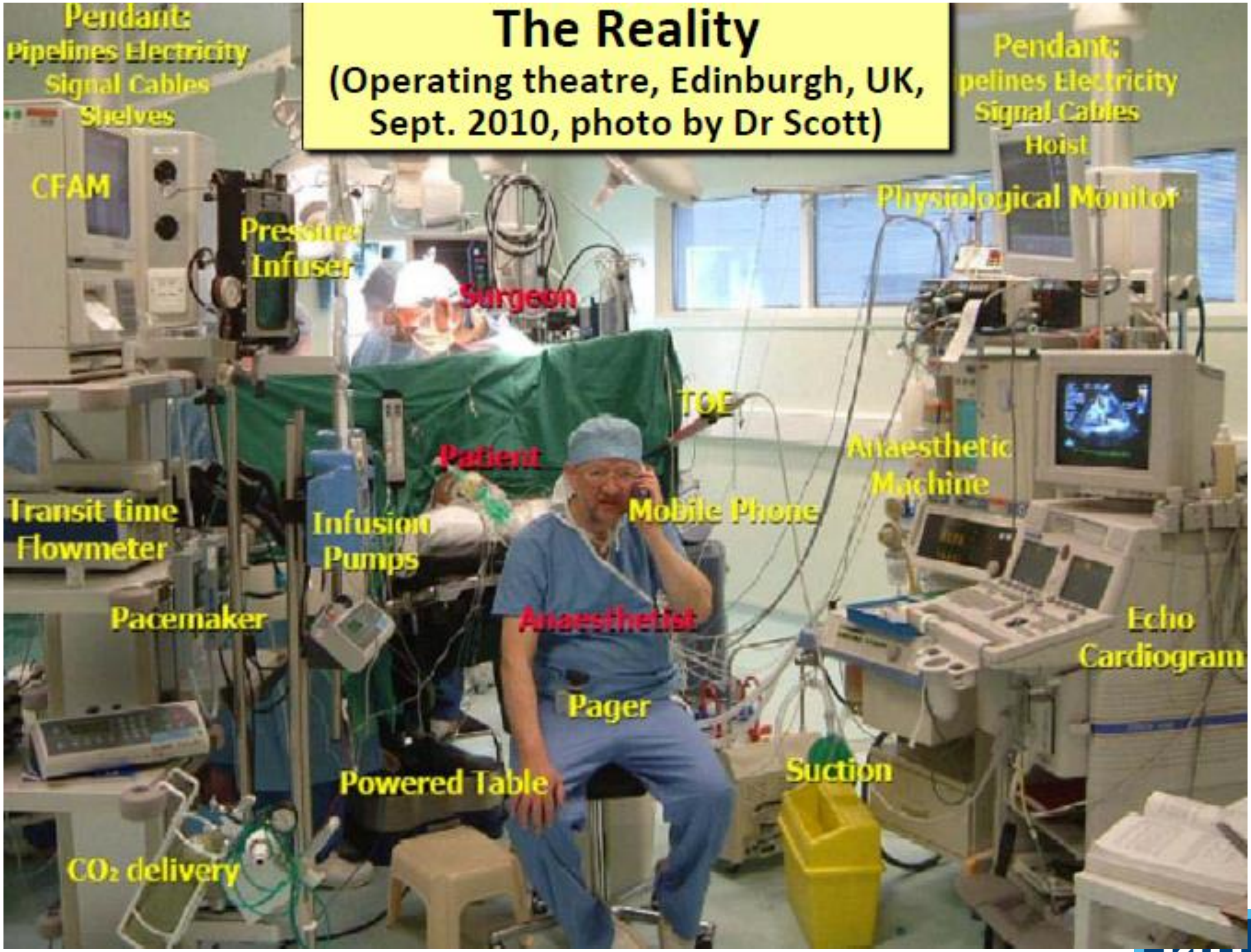

From Industry 1.0 to Industry 4.0: Towards the 4th Industrial Revolution
4. Industrial Revolution
based on Cyber-Physical Production Systems
Industry 4.0
3. Industrial Revolution
through Introduction of electronics and IT for a further automization of production
Industry 3.0
2. Industrial Revolution
through introduction of mass production based on the division of labour powerde by electrical energy
Industry 2.0
First
Mechanical
Loom
1784
1. Industrial Revolution
through introduction of mechanical production facilities powered by water and steam
Industry 1.0
Degree of Complexity
End of 18th Century
Start of 20th Century
Start of 70ies
today
t

Medical & Healthcare



KU LEUVEN

Medical & Healthcare



KU LEUVEN

Overview

- Some definitions: EMC? FS?
- **Why immunity testing is not sufficient**
- EMC & FS: how to combine?
- MCSA European Training PETER
- Conclusions

EMC and FS

- Traditionally two completely different areas of expertise
- So EMC experts and FS experts don’t speak the same language…
- This is seen in e.g. IEC 61508, the “mother” of all FS standards

KU LEUVEN

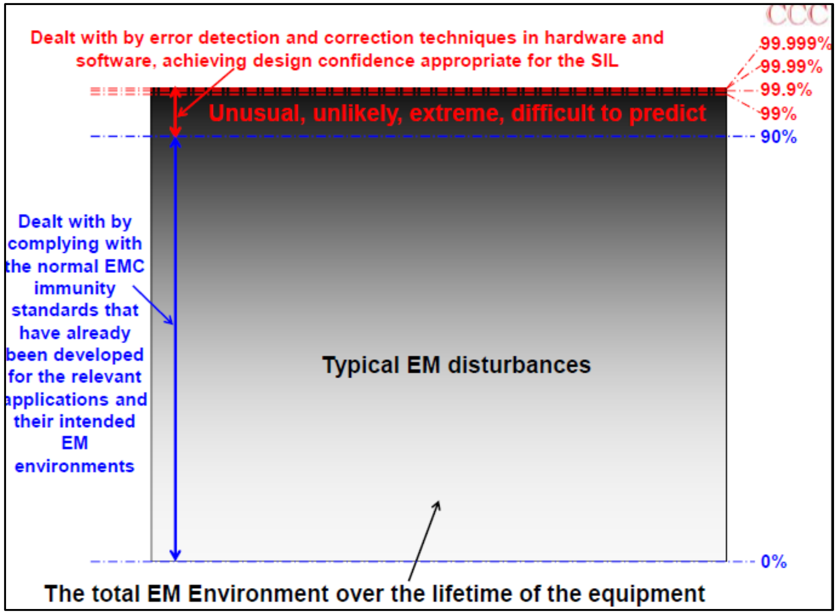
IEC 61508 and EMC?

- IEC 61508 mentions that EMC had to be taken into account, but does not clearly say how:
  - It referres to "normal" EMC standards which, however, state themselves not to be intended for functional safety…
  - It requires to "increase" the immunity test levels, but already mentions that this could not guarantee that EMC could not lead to a failure in practice...
- And immunity tests focus on whether EMI causes functional performance to degrade by too much…
  - but Functional Safety engineering cares nothing for functionality! *(however, see "availability" later)*…
  - *even if EMI causes permanent damage…*
  - as long as safety risks remain low enough!

KU LEUVEN

Why Immunity Testing is Not Sufficient

- Only meant to have about 90% confidence level



- Rather outdated: take not into account modern modulation types, take not into account close proximity of RF transmitters, LF EM disturbances below 150kHz,…

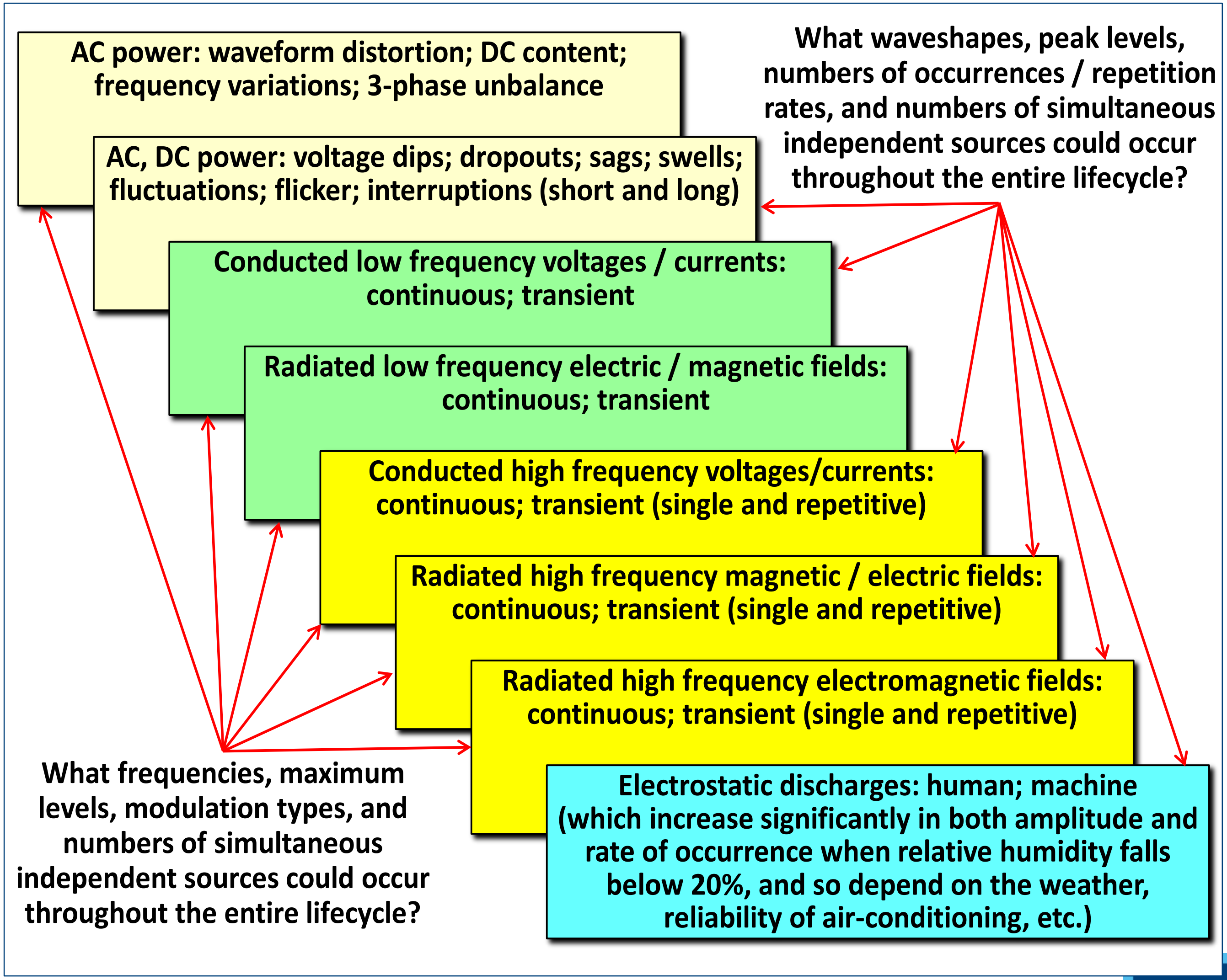
KU LEUVEN

Why Immunity Testing is Not Sufficient

- Just as for microprocessors and software, no practicable test plan could prove risks caused by EMI were acceptably low, because it would need to cover all reasonably foreseeable…
  - maximum EM disturbances over the entire lifecycle (normal tests aim for 80-90% of typical)…
  - physical and climatic stresses, aging, etc.…
  - degradations/faults in EM mitigation and circuits, simulated individually, and foreseeable combinations…
  - angles of incidence, polarisations, modulation types/frequencies, transient waveshapes and rates, etc.
  - combinations of any/all of the above!

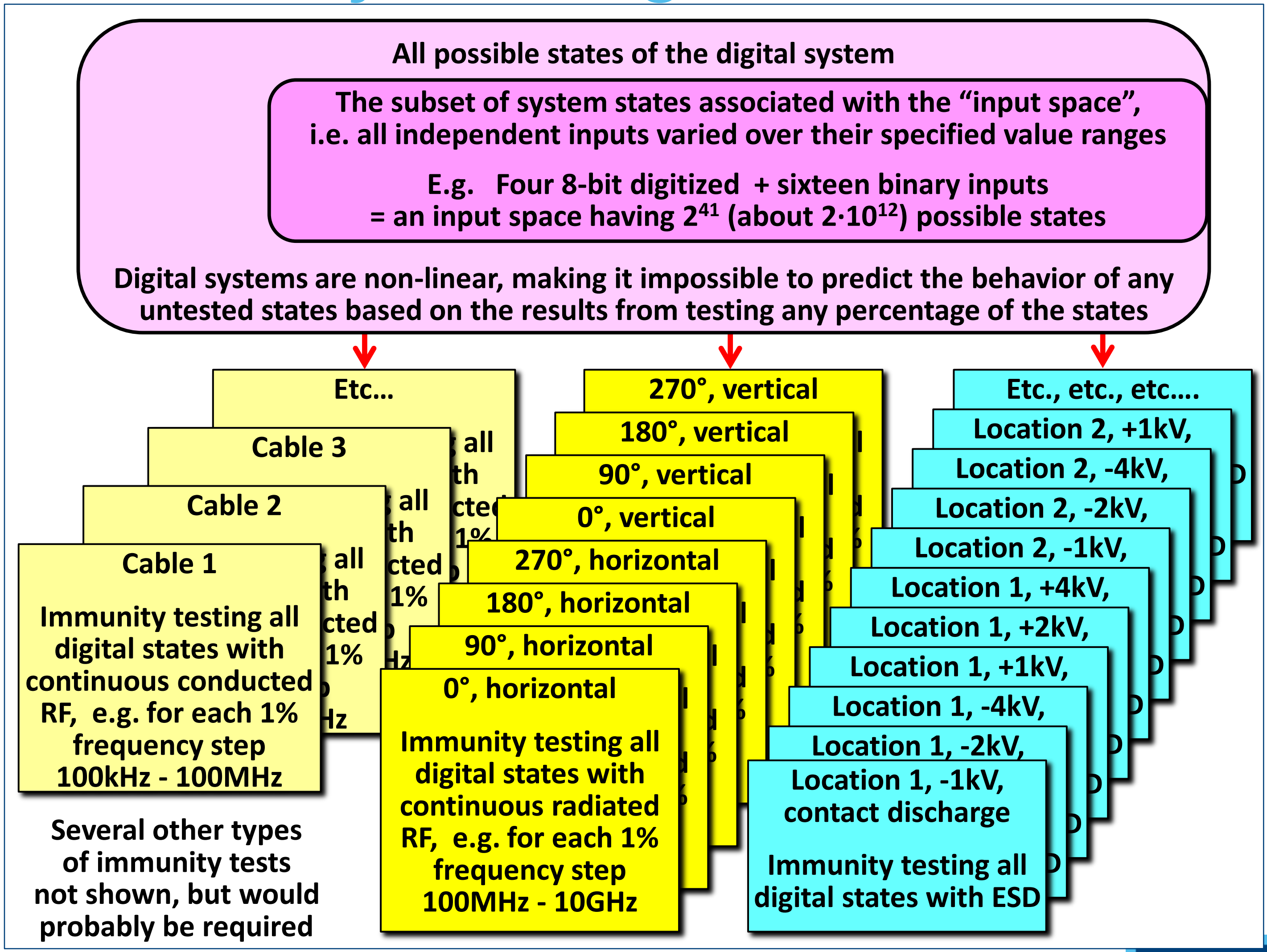
KU LEUVEN

Why Immunity Testing is Not Sufficient



KU LEUVEN

Why Immunity Testing is Not Sufficient



Overview

- Some definitions: EMC? FS?
- Why immunity testing is not sufficient
- **EMC & FS: how to combine?**
- MCSA European Training PETER
- Conclusions

KU LEUVEN

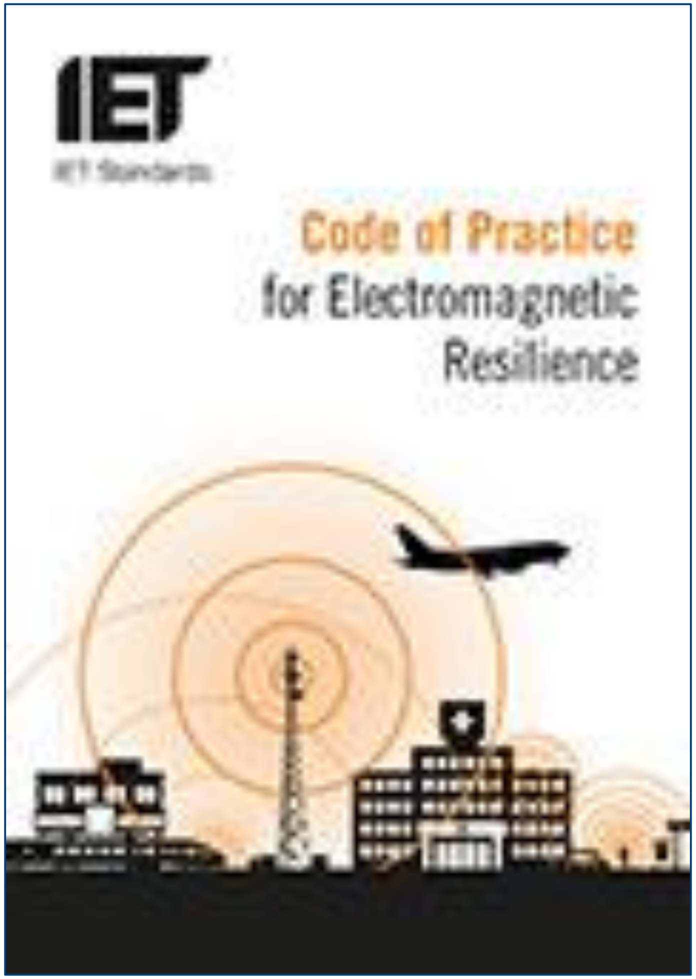
Big Grey Box Approach?

- The traditional way of achieving functional safety despite an unknown EM environment…
  - is to use over-specified and ruggedized EM mitigation (shielding, filtering, surge protection, etc.)… which is sure to maintain very high levels of EM mitigation over it's lifecycle despite anything/everything that might happen
  - We call this the 'Big Grey Box' (BGB) approach…
  - It works very well, but can be too large, heavy or costly for many modern safety-related systems…
    - e.g. domestic appliances, power tools, automobiles, medical devices, etc.

KU LEUVEN

Big Grey Box: Examples

IET CoP in EMI Risk Management



KU LEUVEN

IET CoP in EMI Risk Management

- Was developed by the IEE/IET Working Group on EMC for Functional Safety…
- First published in 2017... after a considerable amount of (all positive!) input from very many Functional Safety and EMC experts…
- Currently being "transformed" into an IEEE Standard

- It is the first truly *practical* alternative to BGBs…
- And it doesn't require anyone to learn very much that is new

KU LEUVEN

Solution

Comply with the usual, relevant EMC standards for functionality, *over the complete lifecycle*

Apply IEC 61508 design Techniques & Measures (T&Ms) appropriate for EMI (improved where necessary) to reduce residual risks

Overall result: EMI Resilience

Functional Safety should not be compromised by EMI, over the complete lifecycle

Use good EMC engineering at all levels of design

KU LEUVEN

Examples of IEC 61508 T&Ms

- Physically separating safety functions from non-safety functions

- Specification of system requirements and design approaches, including (for example):
  - redundancy and diversity
  - error detection and error correction
  - static and dynamic self testing

- Integration of subsystems, power supplies and communication links

- Fault monitoring and recording (to help identify causes of malfunctions and improve future designs)

Redundancy?

- Use of redundant paths is a often used technique in FS
- However, redundancy is most often applied by a n identical paths
- Such redundant systems can only cope with random failures (e.g. broken components)
- However, EMI is a **systematic common cause failure**:
    - Systematic: a given system design will always behave in the same way when a given EMI is applied
    - Common cause: EMI influences many different components in the same way at the same time

Examples of Redundancy and Diversity

- multiple sensors sense the same parameters
- multiple copies of data are stored…
- multiple communications carry the same data…
- multiple processors process the same data…
- with comparison (error detection) or voting e.g. any two that agree out of three (error correction)

- All these can benefit from a wide range of diverse technologies/techniques to improve their effectiveness against the common-cause failures typically caused by EMI

KU LEUVEN

Examples of Error Correction/Detection

- Error Detection Coding (EDC)…
  - means detecting corrupt data by adding sufficient redundant data bits…
  - designed to make a sufficient number of simultaneous bit errors detectable
- Error Correction Coding (ECC)…
  - means adding enough redundant data to EDC, designed to restore data to the degree required

- The modern world (GSM, Internet, CDs, DVDs, TV, etc.) relies totally on EDC and ECC

KU LEUVEN

Overview

- Some definitions: EMC? FS?
- Why immunity testing is not sufficient
- EMC & FS: how to combine?
- **MCSA European Training PETER**
- Conclusions

KU LEUVEN

European Training Network?

Goal: train a new generation of creative entrepreneurial and innovative Early-Stage Researchers (ESRs)

Consortium: min. 3 partners from different countries, 2 levels of partners, stronger focus on innovation and industrial participation

Fellows: Possibility for 15 ESRs. Max. 540 researcher-month (15 times 36 months)

Proposal: 3 main parts: excellence, impact, implementation (30 pages only: every sentence is important!)

Evaluation: criteria according to proposal structure, stronger focus on Impact

- on the fellows' careers
- on structuring (doctoral) training at the European level / strengthening European innovation capacity
- proposed measures for communication and dissemination of results

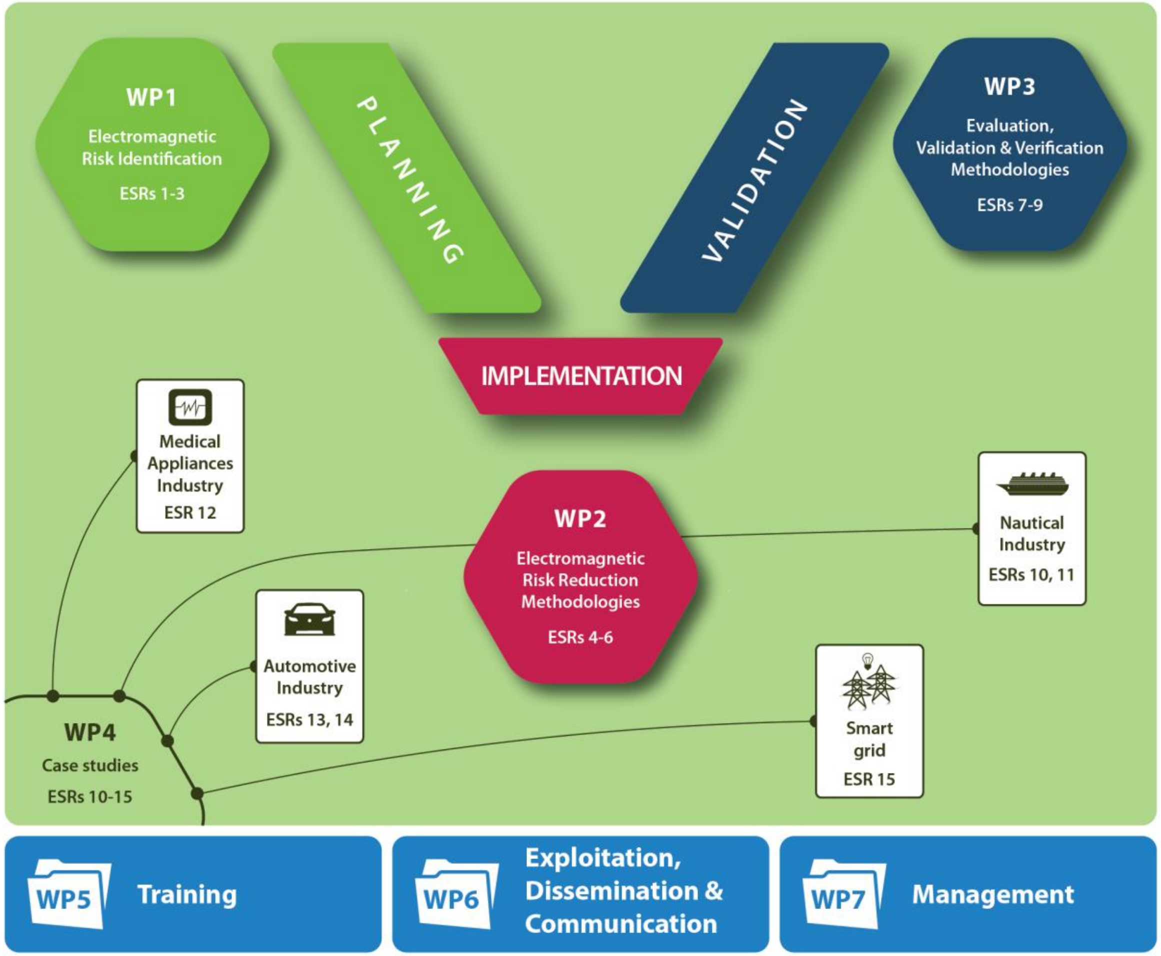
KU LEUVEN

PETER: Objectives

- PETER = Pan-European Training, research and education network on ElectroMagnetic Risk management
- 4 S/T objectives:
  - To develop EMI-dedicated risk-and-hazard analysis techniques
  - To develop effective EMI risk-reduction techniques in hardware and software
  - To improve EMI verification-and-validation methods
  - To apply a practical, industry-driven EMI risk-management methodology during 4 case studies

KU LEUVEN

PETER: Work-Packages



PETER: Overview Consortium

KU LEUVEN

PETER: Overview Topics

ESR No.	Recruiting Participant	Title	Seconded at	Start (Month)	Duration (months)
Work Package 1: Electromagnetic Risk Identification					
ESR1	LUH	Statistical Electromagnetic Risk Analysis of Large and Complex Systems, Development of Theoretical Description of Risk Assessment Methodologies	FHG, MIRA, RHM	7	36
ESR2	WIS	Statistical Electromagnetic Risk Analysis of Large and Complex Systems, Experimental Analysis and Model Verification	Barco, FHG, UTwente	7	36
ESR3	MIRA	Risk-Based Automotive Electromagnetic Engineering Approach aligned with the ISO26262 Functional Safety Approach	LUH, Nedap, Valeo	7	36
Work Package 2: Electromagnetic Risk Reduction Methodologies					
ESR4	UTwente	Risk-Based EMI-Aware Design of Complex Systems	Barco, WIS, LR	7	36
ESR5	KU Leuven	IEC 61508 Techniques & Measures for EMI Risk Reduction, Hardware-based Techniques & Measures	ESEO, Thales, MST	7	36
ESR6	KU Leuven	IEC 61508 Techniques & Measures for EMI Risk Reduction, Software-based Techniques & Measures	UoY, Nedap, MST	7	36
Work Package 3: Evaluation, Validation and Verification Methodologies					
ESR7	ESEO	Evaluation of Electromagnetic Hazards due to Environmental Stresses, Obsolescence and/or Ageing, Evaluation at the Integrated Circuit Level	KU Leuven, Melexis, UoY	7	36
ESR8	Valeo	Evaluation of Electromagnetic Hazards due to Environmental Stresses, Obsolescence and/or Ageing, Evaluation at the System Level	KU Leuven, UoY	7	36
ESR9	UoY	Statistical Verification and Validation of Immunity and Enclosure Shielding Effectiveness – Risk of Susceptibility	Melexis, LUH	7	36
Work Package 4: Application Case Studies					
ESR10	RHM	From Rule-Based Standards to Risk-Based, Cost-Effective, Up-to-Date, Maritime EMC Standards	LUH, LR	7	36
ESR11	UoY	Modelling and Reasoning about Electromagnetic Interactions in Autonomous and Complex Vessels	RHM, LR	7	36
ESR12	Barco	EMI-Resilient Medical Display Systems for Surgical-, Diagnostic Imaging- and Modality Applications	WIS, UTwente, MST	7	36
ESR13	Nedap	EMI Risk Management Applied to the Next Generation Vehicular Communication Devices	LUH, MIRA, Valeo	7	36
ESR14	Melexis	Risk-Based EMI-Aware Design of an Automotive Integrated Circuit	UTwente, ESEO	7	36
ESR15	FHG	EMI Risk Management on the Scale of the Smart Grid as a Network of Systems	KU Leuven, UoY, UTwente	7	36

KU LEUVEN

Overview

- Some definitions: EMC? FS?
- Why immunity testing is not sufficient
- EMC & FS: how to combine?
- MCSA European Training PETER
- **Conclusions**

Conclusion

- Both EMC and FS are becoming increasingly important!
- Radiant future for EMC engineers!
- Secure future for FS engineers!
- But both disciplines have to be brought together…

- EMC engineers need to understand what FS is and how it differs from “normal” EMC
- FS engineers need to understand that “EMC for CE marking” is not sufficient for FS and that EMI should be adequately taken into account