

Inhärente Sicherheit: Wie wichtig ist das für die Zukunft?

Inherent Safety: How important is it for the future?

Hans Tschürtz, VISSE

Agenda

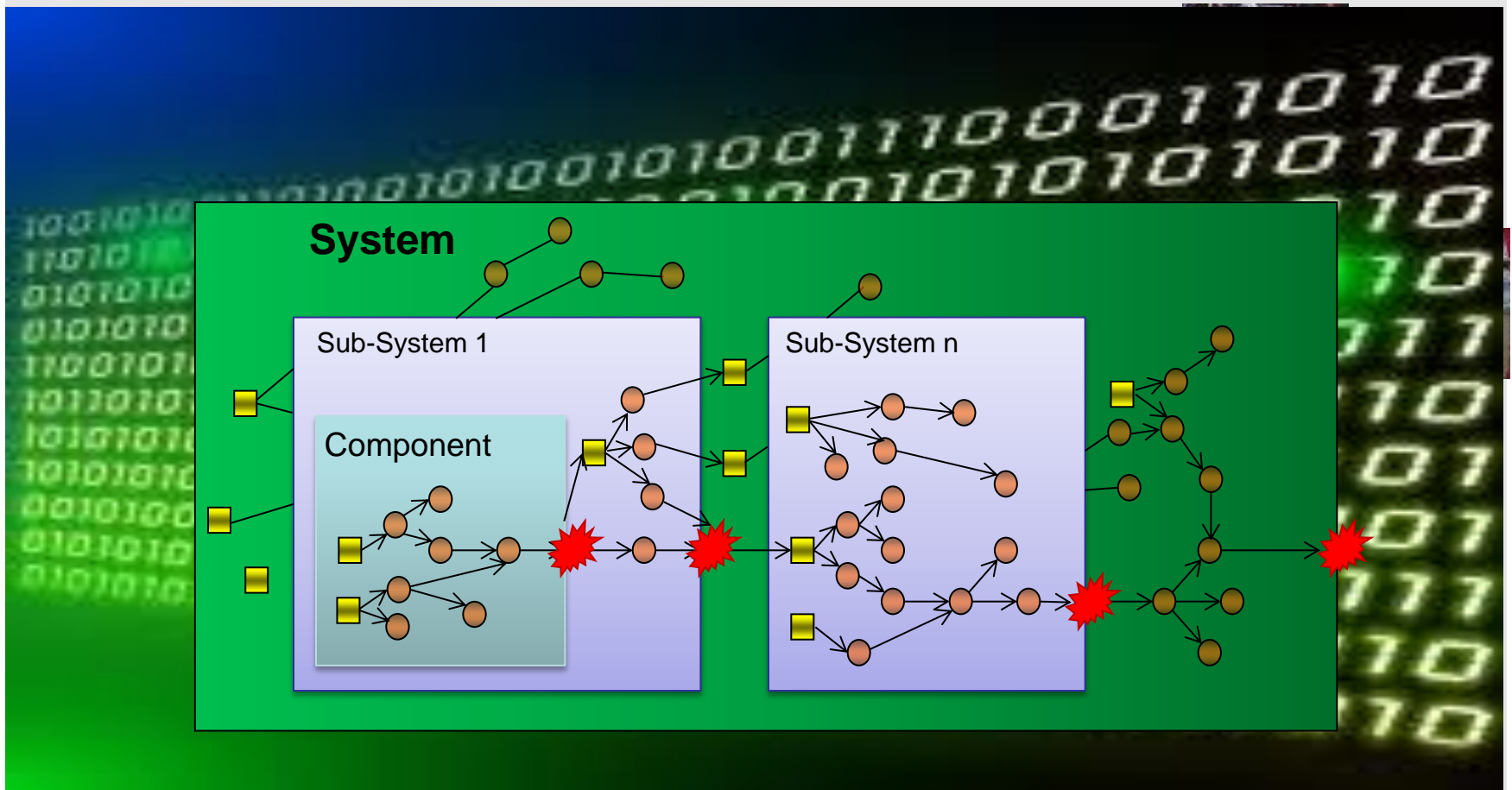
- > Technological Revolution
- > Problem Statement
- > What is Inherent Safety?
- > Inherent System Safety Approach
- > Conclusion

Technological Revolution



- > New technology has sprinted forward
- > Time to market has greatly decreased
- > We have to utilize opportunities and control the risks





Problem Statement

- > „Seldom does a single hazard cause an accident. More often, an accident occurs as the result of a sequence of causes termed initiating and contributory hazards.”
[FAA_00]
 - > “[...] the probability of any one specific combination of failures will be extremely low, but as experience shows, this is precisely what leads to major accidents.”
[Hol_07]
 - > “System failure can come from the interaction of sub-systems deficiencies which individually do not produce an end system failure but may do in combination.”
[GMS_12]
- Increasing system complexity and tight coupling leads to non-predictable system states that can lead to

System Accidents

[Lev_11]

What do we need?

- > Designing and managing complex technological systems requires not only traditional engineering skills
- > Especially safety engineers and safety manager have to have this holistic picture of the whole system on organisational and on engineering level
- > New broad approaches, frameworks, and theories will be needed to analyse, design, deploy and manage complex systems
 - » We need to identify hazards in early stages
 - » We need to preventively avoid hazards, instead of controlling them
 - » Safe operation should not be dependent on its external safety functions or on his electronic control system

→ We need an Inherent System Safety Approach

What is Inherent Safety?

- > Concept of inherently safer design was developed by Trevor Kletz et. al. in the late 1970s as a fundamental approach to hazard management which emphasised avoiding or limiting the hazard at source, rather than relying on „add-on“ safety features or management systems and procedures to control them.

[HSE_07]

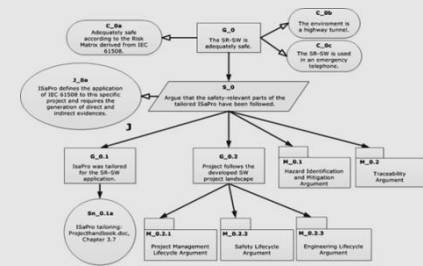
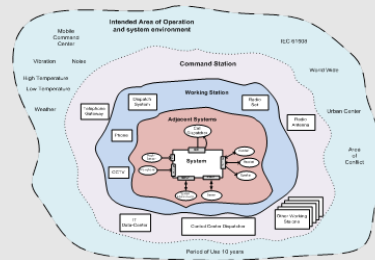
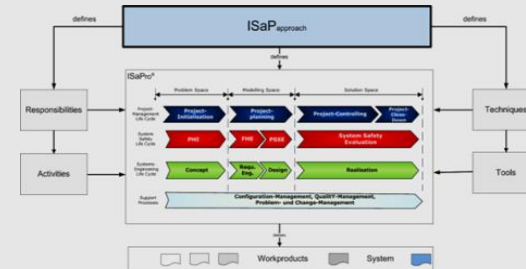
- > Objectives of a safer design:
 - » Hazard avoidance
 - » Hazard prevention
 - » Risk minimisation
 - » Good engineering

What is Inherent System Safety?

Inherent System Safety is a systematic engineering and management approach for developing inherent safer systems, sub-systems and modules, where safety is intentionally designed into them under all environmental conditions.

Our objective is an inherent safer system:

- > Framework (ISaPro®)
- > Systematic approach (ISaPapp)
- > Safety analysis methods (Shell-Model)
- > Good requirements engineering
- > Inherent safer design
- > Safety case model based on the used framework



Conclusion

- > New technology introduces unknowns into our systems and creates new paths to losses
- > Learning from the past accidents and incidents over centuries is still an important part of practising inherent system safety
- > There is a need to see the overall context
- > Preventing requirement flaws
- > Safer design for easy inspections
- > Safety culture

References

- > [FAA_00] FFA System Safety Handbook, Federal Aviation Authority, Principles of System Safety, December 30, 2000
- > [GMS_12] Sundaram P., Hartfelder D.: Rigor in Automotive Safety Critical System Development, CTI-Conference ISO 26262, Detroit, June 2012
- > [Hol_07] Holzmann G. J.: Conquering Complexity, NASA/JPL for Reliable Software, 2007
- > [HSE_07] HSE-Offshore Technology Report OTH 96 521: Improving Inherent Safety, Health and Safety Executive, 1996
- > [Lev_11] Leveson N.G.: Engineering a Safer World: System Thinking Applied to Safety, 2011, Massachusetts Institute of Technology

Safe Systems for a Safer World!