

**Safety Analysis according to IEC 61508
Putting it into Practice**

Prof. Jens Braband
Stephan Griebel

Siemens Transportation Systems – Rail Automation

Rail automation systems for mass transit and main line:

- Operations control systems
- Interlockings
- Automatic train control systems
- Components
- Telecommunications systems for rail applications



Interlockings and operations control systems




Automatic train control systems



Components



Telecommunications systems for rail applications



SIEMENS


Transportation Systems

Objectives

Rail Automation

- State the need for a well-founded causal structure of a risk analysis
- Reveal ambiguities in the definition of the different modes of operation in IEC 61508
- Elucidate certain intricacies of the modes of operation using Markov modelling
- Model different strategies for repair and inspection

Prof. Braband, Griebel 2004-09-14 3




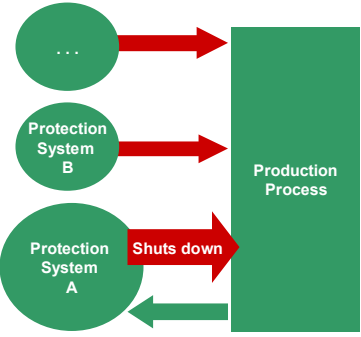
SIEMENS


Transportation Systems

Rail Automation

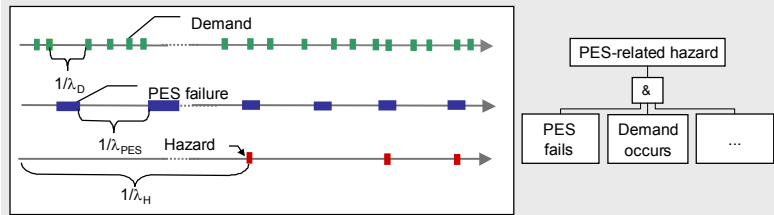
- I. Risk Analysis – Issues, Steps, Deviations and Observations**
- II. Definition of Modes of Operation
- III. Calculation of Target Failure Measures
- IV. Experience with Different Strategies for Repair and Inspection
- V. Conclusions

Prof. Braband, Griebel 2004-09-14 4

	SIEMENS
Transportation Systems	<h2 style="text-align: center;">Risk Analysis – Issues</h2>
Rail Automation	<ul style="list-style-type: none"> ■ Main object: protect people from harm ■ Measure of risk obtained from function of the probability or frequency of occurrence O and the severity S of an accident: $R=f(O, S)$. ■ System considered: protection system for a production facility, which shuts down the process when a certain threshold for safe process operation is approached ■ Top-level safety targets are apportioned to the individual protection systems taking account of their interoperation. (Outside scope of IEC 61508) <div style="text-align: right; margin-top: 20px;">  </div>
<small>Prof. Braband, Griebel 2004-09-14 5</small>	

	SIEMENS
Transportation Systems	<h2 style="text-align: center;">Risk Analysis – Steps</h2>
Rail Automation	<ul style="list-style-type: none"> ■ Step 1: Definition of overall safety target and selection of appropriate quantitative and qualitative figures <ul style="list-style-type: none"> • Determining the aim of our analysis • Weighing up different methods (FTA,...) • Taking the user into account ■ Step 2: Apportionment to PES considering other risk reduction factors <ul style="list-style-type: none"> • Taking risk reduction factors into account • Establishing a complete causal and time-related model
<small>Prof. Braband, Griebel 2004-09-14 6</small>	

Risk Analysis – Causal structure



$$\lambda_H = \lambda_D \times \lambda_{PES} \times \frac{1}{\mu_{PES}} \quad \text{PFD}$$

PdFH probability of dangerous failures per hour
 PES programmable electronic system
 PFD probability of failure on demand

Risk Analysis – Deviations and Observations

- Ambiguous definition of PdFH in IEC 61508
– same concept as instantaneous failure rate or hazard rate ?
- Strong dependence of the PFD on proof test intervals
- The advantage of the PdFH is that it depends only on the failure rates and test capability of the PES.

For this reasons we shall select the PdFH as our primary target measure

Transportation Systems

Rail Automation

Risk Analysis – Deviations and Observations

- Given a particular frequency for the PES-related hazard, an average demand frequency and a proof test interval, we obtain a **PdFH requirement** of 1.6×10^{-2} failures per year. Yet the corresponding **PFD requirement** would be 8×10^{-3} or 1 in 125 demands.
- Resulting contradictions:
 - requirement based on **PdFH** permits a PES designed according to **SIL 2**,
 - whereas requirement based on **PFD** demands a PES developed according to **SIL 3!**

SIL: safety integrity level

Prof. Braband, Griebel 2004-09-14 9

Transportation Systems

Rail Automation

Risk Analysis – Deviations and Observations

- I. Risk Analysis – Issues, Steps and Observations
- II. Definition of Modes of Operation**
- III. Calculation of Target Failure Measures
- IV. Experience with Different Strategies for Repair and Inspection
- V. Conclusions

Prof. Braband, Griebel 2004-09-14 10



Definition of Modes of Operation

- Distinction between modes is rather arbitrary
 - More than one demand per year
 - ⇒ high-demand or continuous-mode system (PdFH)
 - Otherwise
 - ⇒ demand-mode system (PFD)

There is no explanation for this definition in IEC 61508, except perhaps for the fact that at this particular boundary the SIL tables in IEC 61508 seem to coincide.

- The authors therefore
 - propose abandoning the concept of modes of operation and
 - would like a complete description of the causal and time-related model.



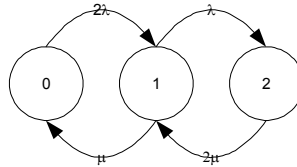
- I. Risk Analysis –
Issues, Steps and Observations
- II. Definition of Modes of Operation
- III. Calculation of Target Failure Measures**
- IV. Experience with Different Strategies
for Repair and Inspection
- V. Conclusions



Calculation of Target Failure Measures 1

1oo2 model for a logic subsystem made up of two identical components.
A failure of both components at the same time is considered a system failure.

Calculation of PFD:



The hazard rate is NOT given by:

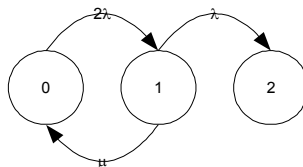
$$\frac{PFD'(t)}{1 - PFD(t)}$$

since state 2 is not an absorbing state
(see definition of failure rate!).



Calculation of Target Failure Measures 2

- Necessary adjustment for deriving PdFH:

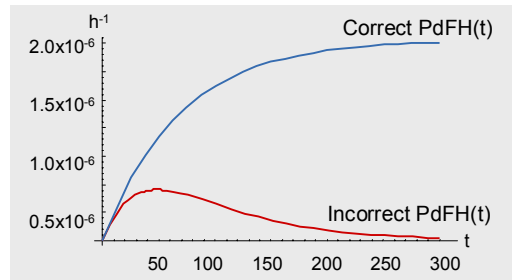


- This yields: $PdFH(T) = \frac{P_2'(t)}{1 - P_2(t)} \xrightarrow{t \rightarrow \infty} \frac{2\lambda^2}{\mu}$



Calculation of Target Failure Measures 3

- Comparison of correct PdFH (absorbing model) and incorrect PdFH (recovery model):



- I. Risk Analysis – Issues, Steps and Observations
- II. Definition of Modes of Operation
- III. Calculation of Target Failure Measures
- IV. Experience with Different Strategies for Repair and Inspection**
- V. Conclusions



Reflections on Modelling Repair and Inspection

- Another crucial point besides the correct calculation of the PdFH is the modelling of the repair or inspection behaviour in the Markov models presented.
- One has to take into account the underlying assumptions about the stochastic/deterministic nature of the repair/inspection process. The commonly used assumption of a constant repair/inspection rate has to be verified or at least proven conservative.
- In the following sections we wish to briefly compare this assumption of a constant rate with two different repair and inspection modes



Randomly Distributed Detection vs. Constant Rate Inspection

We assume that

- a channel is tested cyclically at least once every T hours.
- a particular failure is detected randomly in the period $[0, T]$ after its occurrence.

➡ detection on average after $T/2$ hours

Observation:

Using $1/T$ as a constant inspection rate in a Markov model, you can show that the constant rate inspection dominates the cyclical inspection time stochastically, i.e. it is conservative.



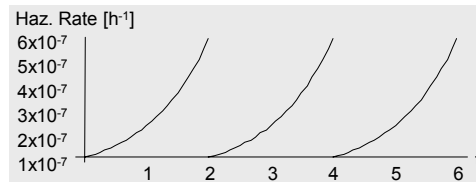
Deterministic Inspection Intervals vs. Constant Rate Inspection 1

We assume that

- the channel is tested cyclically at a fixed interval T ,
- without any stochastic nature,
- with 100% failure coverage and complete reinitiation.

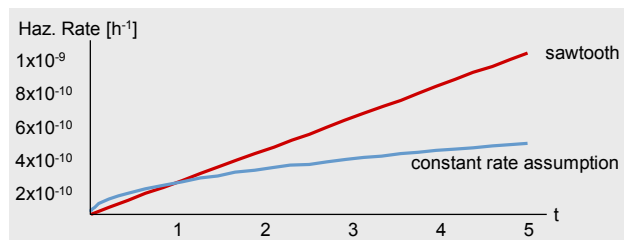
Question:

Is the resulting level reached by this sawtooth function higher or lower than the level which would be obtained had we used the repair rate of $1/T$ from the constant rate assumption?





Deterministic Inspection Intervals vs. Constant Rate Inspection 2

- Ongoing research underscores the conjecture that in cases where the quotient $1/T$ is two orders of magnitude greater than the failure rate λ the assumption of a constant repair rate $1/T$ is no longer conservative.



- A closed expression of this functional relationship has not yet been established and is subject to further research.





Transportation Systems

Rail Automation

- I. Risk Analysis – Issues, Steps and Observations
- II. Definition of Modes of Operation
- III. Calculation of Target Failure Measures
- IV. Experience with Different Strategies for Repair and Inspection
- V. Conclusions**

Prof. Braband, Griebel 2004-09-14 21



Transportation Systems

Rail Automation

Conclusions

- Some terminology does not follow international reliability standards and may confuse users, leading to incorrect results. Setting PFD or PdFH targets may lead to different requirements for the SIL for the same system.
- The concept of different modes of operation should be abandoned. It should be replaced by the requirement to specify a complete causal and time-related model.
- The assumption of a constant repair/inspection rate may lead to non-conservative results and has to be looked into thoroughly.

Prof. Braband, Griebel 2004-09-14 22



Thank you for your attention !