SIEMENS

Transportation Systems

Rail Automation

On a Formal Definition of Risk in Standards for Safety-related Computer Systems

Jens Braband
München, April 6, 2005

SIEMENS

Transportation Systems

Rail Automation

Introduction

- The risk-based approach towards safety seems to have become widely accepted and several standards have been established
- The concepts of 'risk' and 'target safety measure' as they appear in many standards are very unstructured and unsystematic
- Although even worldwide standards for terminology exist, terminology is the starting point for confusion
- N.B.: The focus of this paper is restricted to standards which are applicable to safety-related computer systems in transport applications

SIEMENS

Transportation Systems

Rail Automation

Risk: Some Definitions (1)

- An expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence

  (MIL-STD-882-D, IEEE 1483)

- A combination of the probability of an event and its consequence

  (ISO/IEC Guide 73)

- A combination of the probability of occurrence of harm and the severity of that harm

  (ISO/IEC Guide 51/IEC 61508)

SIEMENS

Transportation Systems

Rail Automation

Risk: Some Definitions (2)

- The probable rate of occurrence of a hazard causing harm and the degree of severity of that harm

  (EN 50126/IEC 62278)

- The combination of the frequency, or probability, and the consequence of a specified hazardous event

  (IEC 60300-3-9, EN 50128/50129)

- The frequency (probability) of an occurrence and the associated level of hazard

  (SAE ARP 4754)

SIEMENS

Transportation Systems

Rail Automation

Some Observations (1)

- At first glance, the discrepancies may merely seem to be annoying
  - Note that even within the same standardisation body different definitions of risk are used
- The definitions are all quite fuzzy and vague, e.g. it is not clear
  - what “combination” means or
  - why sometimes probabilities, sometimes frequencies and sometimes rates are included

SIEMENS

Transportation Systems

Rail Automation

Some Observations (2)

- In some definitions, even mathematically incorrect concepts are introduced
  - e.g. “probable rate”
- Matters get worse when we realise that standards usually do not prescribe a particular method of risk analysis
- In the end, it is up to the user to derive a quantitative target safety measure
- But this concept is also confusing

SIEMENS

Transportation Systems

Rail Automation

Target Safety Measures: Some Definitions

- Residual mishap risk
  (MIL-STD-882-D)
- Average probability of failure on demand
  (PFD, IEC 61508)
- Probability of a dangerous failure per hour
  (PDFH, IEC 61508)
- Hazard rate
  (HR, EN 50126/EN 50129)
- Mean time between hazardous events
  (MTBHE, IEEE 1483)

SIEMENS

Transportation Systems

Rail Automation

Further Observations

- None of the cited standards provide either a formal mathematical definition of or appropriate background information on the concepts, giving no more than a verbal description of the target safety measures
- Thus, the puzzled user of the standard is left alone with his own interpretation of the terminology and the standards
- This presentation seeks to supply the missing background information on the terminology and concepts behind the standards, as well as a more solid mathematical definition, particularly of the relationships between the concepts

SIEMENS

Transportation Systems

Rail Automation

A Practical Definition of Risk (1)

- The appropriate definition of risk for a particular application depends to a large extent on the scope and purpose of the analysis
- While in the discussion of the societal risk of e.g. nuclear plants or nuclear waste management, the Farmer curve (FN curve) may be very appropriate, it is usually not suitable for the risk analysis of a safety-related computer system
- Usually, only the frequency of accidents can be influenced and not the severity
- Often an assessment of the average risk is sufficient

SIEMENS

Transportation Systems

Rail Automation

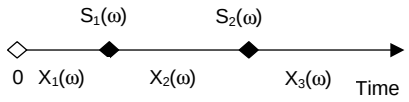
A Practical Definition of Risk (2)

- Thus, we can regard risk as being a product of
  - the expected severity and
  - frequency of an accident

$$R = E(S) \times E(F)$$

Basic Hazard Model

- By means of consequence analysis (e.g. Event Tree Analysis), the expected frequency E(F) is transformed into the expected frequency of hazards as the basic target safety measure (this step is neglected here)
- Thus, the basic model applied in renewal theory can also be used for the modelling of system hazards



- Applying Blackwell's renewal theorem, it follows that on average

$$E(F) = 1/MTBHE \quad MTBHE = E(X_1) = \int_0^\infty R_H(t)dt$$

SIEMENS
Transportation Systems
Rail Automation

Relationship to Hazard Rates

- For constant hazard rates, the following relation holds

$$\lambda_H = \frac{1}{MTBHE} \qquad \lambda_H(t) = \frac{-R_H'(t)}{R_H(t)}$$

- But, in general, this relation is not valid, only

$$\lambda_H(\infty) \le \frac{1}{MTBHE}$$

- However, in the author's experience, for all practical applications the error introduced only amounts to a few percent and can therefore be neglected in a safety context

Relationship to Probability of Failure (1)

- We are now considering the probability that a hazard will occur in an interval of length T, say [t,t+T]
- We can then define $P_n(T)$ as the probability that exactly n hazards will occur within the time interval [t,t+T] and express the expected frequencies in terms of probabilities (often called PdFH), as follows

$$E(F) = \frac{\sum_{n=1}^{\infty} nP_n(T)}{T} \xrightarrow{T \to \infty} \frac{1}{MTBHE}$$

- For large T, the basic renewal theory yields the same result as before

SIEMENS
Transportation Systems
Rail Automation

Relationship to Probability of Failure (2)

- If the probability of multiple hazards occurring within [t,t+T] is very small or T is very small, then

$$E(F) \xrightarrow{T=t} -R'_H(t)$$

- This result can be related to the hazard intensity, NOT the hazard rate

A Simple Application Example

- We consider finite, time-homogeneous Markov processes with constant transition rates which seem to be the standard technique in the context of IEC 61508
- This process is completely characterised by the transition rates matrix $Q=[q_{ij}]$ and the initial conditions at $t = 0$
- For simplicity, we shall assume that, among the states $\{1,2,3,\ldots,n\}$, there is only one hazardous state, say n, and that the process starts in state 0 with the probability 1
- We shall define $MTBHE_i$ as being the MTBHE when the process is in state i at time 0. Thus MTBHE= $MTBHE_0$

SIEMENS
Transportation Systems
Rail Automation

Calculation of MTBHE vs. HR

- $MTBHE_0$ can then be found as the solution of a set of linear equations

$$MTBHE_i = \frac{1}{q_i} + \sum_{\substack{j=0,\ldots n-1 \\ j\neq i}} \frac{q_{ij}}{q_i} MTBHE_j, \qquad q_i = \sum_{\substack{j=0 \\ j\neq i}}^{n} q_{ij}$$

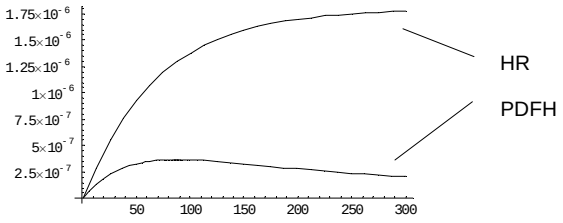
- If the Markov process is solved for the time-dependent state probabilities $p_j(t)$ (which requires the solution of an ordinary linear differential equation), then

$$\lambda_H(t) = \frac{\sum_{i=0}^{n-1} p_i(t) q_{in}}{1 - p_n(t)}$$

- By comparison, the calculation of MTBHE is much simpler than the calculation of HR or failure probabilities (both need to calculate $p_j(t)$ first)

Numerical Example (1)

- A very simple example of a 1oo2-model with two identical components is used to demonstrate that even the assumptions behind the different target safety measures play an important role in a safety assessment



HR	hazard rate
PDFH	probability of a dangerous failure per hour

SIEMENS

Transportation Systems

Rail Automation

Numerical Example (2)

- It should be noted that neither of the results is wrong, they are just different
- They each have a particular purpose and meaning, but depending on whether the assumptions behind, and limitations of, the models used are correctly understood or not, either correct or false conclusions can be drawn

SIEMENS

Transportation Systems

Rail Automation

Summary and Conclusions (1)

- All standards related to safety-related computer systems in different application sectors should use the same definition of risk
- A concise definition of terminology and a clear relationship between the definition of risk and the target safety measures is necessary
- Otherwise, it is very likely that incorrect safety requirements will be derived or false conclusions drawn from safety analyses

SIEMENS

Transportation Systems

Rail Automation

Summary and Conclusions (2)

- A definition of risk in terms of frequency seems more natural than one based on probability as the latter requires the consideration of additional parameters (e.g. the time T) and assumptions
- Thus, the author's proposal is to use either MTBHE or HR as target safety measures for safety-related computer systems
- However, it should be noted that MTBHE is the more general concept