4th INTERNATIONAL CONFERENCE
TRANSPORT SYSTEMS TELEMATICS TST'04

ZESZYTY NAUKOWE
POLITECHNIKI ŚLĄSKIEJ 2004
TRANSPORT z.55, nr kol. 1657

safety-related systems,
hazard control, safety analysis

Jerzy M. SKRYPKO[1]

HAZARD CONTROL

Author presents process of risk analysis and hazard control. In the second part author presents sequence of events leading to accident and control ways of the sequence in such a way that hazard rate should less then THR (tolerable hazard rate). The designer has some ways to reduce hazard rate.

STEROWANIE ZAGROŻENIAMI

Autor przedstawia proces analizy ryzyka i sterowanie zagrożeniami. W drugiej części autor pokazuje sekwencje zdarzeń prowadzących do wypadku i sposoby sterowania tą sekwencją tak, żeby intensywność zagrożeń była niższa niż THR (dopuszczalna intensywność zagrożeń). Konstruktor ma kilka sposobów by zmniejszyć intensywność zagrożeń

1. INTRODUCTION

Author wants to present process of risk analysis and hazard control which are talked over in standard Safety-related electronic systems for signalling [9]. The standard Risk analysis of technological systems [11] describes risk analysis, too.

In the second part author presents sequence of events leading to accident and control ways of the sequence in such a way that hazard rate should less then THR.

2. GLOBAL PROCESS OVERVIEW

Global process consists of risk analysis and hazard control. Railway Authority has responsibility for risk analysis. System supplier has responsibility for risk analysis. The Safety Authority shall approve both, the risk analysis and hazard control.

[1] Bombardier Transportation (ZWUS) Polska, Modelarska 12, 40-019 Katowice, Poland
jerzy.skrypko@pl.transport.bombardier.com

2.1. RISK ANALYSIS

Data input for the risk analysis is:

- specification of system functions

The risk analysis includes:

- hazard identification for each function
- accidents, as consequences of hazards
  - hazard severity - consequences to persons or environment
  - frequency of occurrence hazardous events
- risk evaluation - hazard categorization
- risk acceptance

Data output of the risk analysis is:

- THR for functions

I described this process in my work *Lista zagrożeń, jako podstawa do specyfikacji wymagań* [13]

2.2. HAZARD CONTROL

Data input for the hazard control is:

- Safety specification:
  - THR for functions
  - safety states

The hazard control include:

- causal analysis
  - translated THR for function to SIL (Safety Integrity level) (SIL will be safety requirement for system)
  - THR apportionment e.g. FTA (Fault Tree Analysis)
- CCF (common cause failure) analysis
  - physical independence claims
  - functional independence claims
  - process independence claims

  The independence of items allow us to treat these items in gate AND during FTA.
- SIL allocation
- system architecture definition according to table E.4 EN 50 129 [9]
- safe function allocation
  - algorithm of fail-safe reaction
  - time of failure detection
  - time of achievement of safe state retention
  - safe states

- SIL specification for subsystems
- calculation of HR (hazard control). I described this process in my work *Przekształcanie drzewa zagrożeń metodą „Zofii"* [14]

Data output of the hazard control is:

- hazard rate for functions

3. WAYS OF HAZARD CONTROL

3.1. HAZARD SOURCES

The hazard sources can be:

- Systematic failures - software or design mistakes.
- Random failures – defects of hardware or transmission disturbance

We can avoid systematic failures, as hazard sources by techniques and measures.[8], [9]

We can avoid random failures, as hazard sources by hazard rate calculation and compare with THR for function. The random failures, as hazard sources are under consideration of my work.

3.2. ACCIDENT SCENARIO

The following figure present scenario of accident.

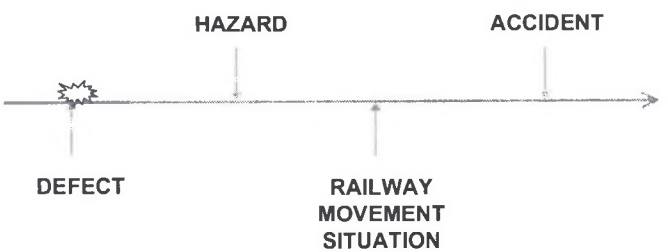

Fig.1. Accident scenario

Single defect leads to hazard. There is accident after the hazard and the railway movement situation.

The following figure presents scenario of hazard control.

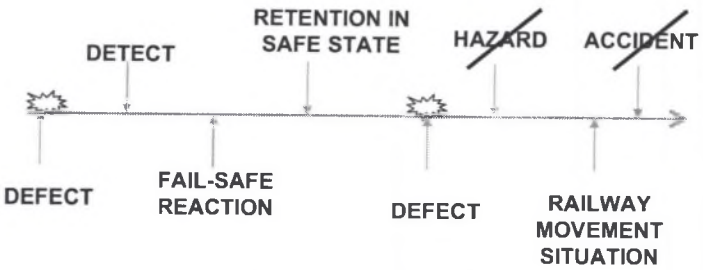

Fig.2. Fail-safe reaction scenario

Two defects lead to hazard. Our system reacts after first defect before second defect

- Detection of defect
- Fail-safe reaction
- Retention in safe state

There is not accident after two defects and the railway movement situation, because the second defect does not lead to hazard. The state of system is retention and it is safe-state.

3.3. HAZARD CONTROL

The state of system should be retention and it should be safe-state before second defect. How to control this process?

There are the following means to hazard control:

- The defects should be independent.
- The rate of defect should be low.
- The detection time and fail-safe reaction and shutting in retention in safe state should be short
- The transmission telegram should be suitably protected according to standard: Safety-related communication in closed transmission systems [10]

The sequence of events leading to accident and control ways of the sequence in such a way that hazard rate should less then THR (tolerable hazard rate). The designer has some ways to reduce hazard rate.

The designer has same ways to reduce hazard rate:

- change electronic elements for more reliable element
- diverse structure with fail-safe comparison
- remove common cause of failure
- decrease time of fault detection
- decrease time of fail-safe reaction
- increase safety code of transmission telegram
- increase safety redundancy (three, four defects lead to hazard, but this worsen reliability of system.

The software has the influence for the detection time and the reaction time against random failures. The retention in safe-state needs high efficacy, and any next defect can not move out system from safe-state and can not lead to any hazard.

We should use these same data to calculation of hazard rate and to calculation of reliability of system. We can take defect rate bigger than it is, but not less.

4. CONCLUSION

1. Hazard control needs high experience.
2. Theoretical hazard analysis needs confirmation by tests.
3. Hazard control needs iteration so long as hazard rate will be less than THR.
4. It is not possible to avoid random failure, but it is possible to control effects of the failure.

BIBLIOGRAPHY

[1] CICHOCKI T., SKRYPKO J., Wprowadzanie wiarygodności i bezpieczeństwa systemów stosowanych na kolei zgodnie z wymaganiami norm Wspólnoty Europejskiej, Systemy czasu rzeczywistego '96, Wrocław, 1996.

[2] IEC 61 508-1 Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 1:General requirements

[3] IEC 61 508-2 Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 2: Requirements for electrical / electronic / programmable electronic safety-related systems

[4] IEC 61 508-3 Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 3:Software requirements

[5] IEC 61 508-6 Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 6: Guide on the application of IEC 61 508-2 and IEC 61 508-3.

[6] IEC 61 508-7 Functional safety of electrical / electronic / programmable electronic safety-related systems – Part 7: Over view of techniques and measures.

[7] PN-EN 50 126: 2002 (U) Zastosowania kolejowe. Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (Railway application – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS))

[8] PN-EN 50 128: 2002 (U) Zastosowania kolejowe. Łączność sygnalizacja i systemy sterowania – Programy dla kolejowych systemów sterowania i zabezpieczenia (Railway application – Communication, signalling and processing systems – Software for railway control and protection systems)

[9] PN-EN 50 129: 2003 (U) Zastosowania kolejowe. Łączność sygnalizacja i systemy sterowania – Elektroniczne systemy sygnalizacji związane z bezpieczeństwem (Railway application – Communication, signalling and processing systems – Safety-related electronic systems for signalling)

[10] PN-EN 50 159-1: 2002 (U) Zastosowania kolejowe. Łączność sygnalizacja i systemy sterowania – Część 1: Łączność systemów bezpieczeństwa w układach zamkniętych (Railway application – Communication, signalling and processing systems – Part 1: Safety-related communication in closed transmission systems)

[11] PN-IEC 60 3000-3-9 Zarządzanie niezawodnością – Część 3: Przewodnik zastosowań – Sekcja 9: Analiza ryzyka w systemach technicznych (Dependability management – Part 3: Application guide Section 9: Risk analysis of technological systems)

[12] SKRYPKO J., Railway application - system dependability, Workshop Proceeding, Gliwice, 1996

[13] SKRYPKO J., Lista zagrożeń, jako podstawa do specyfikacji wymagań, Materiały VI Konferencji Naukowej - Problemy niezawodności transportu, Ustroń - Jaszowiec, 1997.

[14] SKRYPKO J., Przekształcanie drzewa zagrożeń metodą „Zofii", Metody i systemy komputerowe w badaniach naukowych i projektowaniu inżynierskim, CCATIE, Kraków, 1999

Reviewer: Ph. D. Jerzy Mikulski