Functional Safety Experience on Railway Signalling in Japan

Yuji Hirao
Nagaoka University of Technology
(Japan)
Functional Safety Experience on Railway Signalling in Japan

1. Application of computers to railway signalling in Japan
   - Technical breakthroughs
   - Safety guidelines

2. Functional safety experience: current situation
   - Functional Safety Standards
   - Quantitative Safety Evaluation and Hazard Analyses
   - Evaluation of Safety Measures
   - Risk Management

3. Outstanding questions to be addressed
1. Application of computers to railway signalling in Japan
   - Technical breakthroughs

Safety technologies for computerised control

Fail safe
keeps safe state even in malfunction

Definition of safety is possible (standstill)
Technical Principles for Safety

- Redundancy (e.g. CPUs, Software)
- Diagnosis
- Fixed safe output
Redundant CPU Architecture

Computer A
- CPU
- Memory

Comparator

Output control
- Output, only if comparison is exact

Computer B
- CPU
- Memory

Bus

Input

Output

Bit-by-bit comparison
Comparator with 2-pair 2-bit comparison

<table>
<thead>
<tr>
<th>Input of 2 pair of 2 bits</th>
<th>Output of 1 pair of 2 bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A₀, B₀, A₁, B₁)</td>
<td>(C₀, C₁)</td>
</tr>
<tr>
<td>(0, 1, 0, 1)</td>
<td>(0, 1)</td>
</tr>
<tr>
<td>(0, 1, 1, 0)</td>
<td>(1, 0)</td>
</tr>
<tr>
<td>(1, 0, 0, 1)</td>
<td>(1, 0)</td>
</tr>
<tr>
<td>(1, 0, 1, 0)</td>
<td>(0, 1)</td>
</tr>
</tbody>
</table>

Basic unit

Extension to n-bit pairs
## Hardware Techniques

### (1) System structure
- **(a) redundant configuration**
  - duplicate
  - stand-by double duplicate
  - TMR
- **(b) comparison**
  - computer-bus level by fail-safe comparator
  - comparison of results
- **(c) multiprocessor**
  - access to common memory
  - fault-tolerant connection of multiprocessors
  - avoidance of bus collision in the case of disturbance of common signals
- **(d) monitoring**
  - diagnosis functions by quasi-signals

### (2) Processing
- **(a) redundant configuration**
  - bus synchronisation
  - fail-safe comparator
  - timing for comparison
  - input of interruption signal
  - diagnosis of comparator
  - mask of intermittent error
  - segue from triple-redundancy to double
  - measures for electrical source fluctuation
  - compensation for timing difference
  - priority of dangerous-side input data in the case of disagreement
- **(b) error detection**
  - alternating output
  - processing of alternating signal
  - data processing by code checking data
  - diagnosis of RAM and ROM
- **(c) circuit design**
  - fail-safe frequency transformer
  - fail-safe watchdog timer
- **(d) other**
  - fixing of unused bits

### (3) Input/output
- **(a) redundant configuration**
  - priority of lower value
  - conjunction of 2 CPUs
  - cross-input of data
  - changeover of master and slave systems
  - synchronisation of input data
- **(b) error detection**
  - diagnosis by test input data
  - diagnosis of input data by opposite value input data

### (4) Interface
- **(a) redundant configuration**
  - transmission drive by conjunction of CPUs
- **(b) multiprocessor**
  - processing of common signals
  - measures for delay of bus arbiter
  - measures for electrical source switching in the module
<table>
<thead>
<tr>
<th>Software Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>(1) OS</strong></td>
</tr>
<tr>
<td>(a) interruption</td>
</tr>
<tr>
<td>• prohibition of interruption</td>
</tr>
<tr>
<td><strong>(2) Common subroutine, firmware</strong></td>
</tr>
<tr>
<td>(a) common subroutine</td>
</tr>
<tr>
<td>• common programs for quasi synchronisation</td>
</tr>
<tr>
<td><strong>(3) Application</strong></td>
</tr>
<tr>
<td>(a) system</td>
</tr>
<tr>
<td>• continuation of conventional system design</td>
</tr>
<tr>
<td>• control cancellation in the case of field equipment dysfunction</td>
</tr>
<tr>
<td>• safety processing when transmission disconnected</td>
</tr>
<tr>
<td>• information refreshment</td>
</tr>
<tr>
<td>• guarantee of continuity during changeovers</td>
</tr>
<tr>
<td>• procedures at error detection and resumption</td>
</tr>
<tr>
<td>(b) program</td>
</tr>
<tr>
<td>• separation of safety-related processing from non-safety processing</td>
</tr>
<tr>
<td>• simplification of program structure</td>
</tr>
<tr>
<td>• prohibition of “GO TO” sentence</td>
</tr>
<tr>
<td>• consistent allocation of safe and unsafe position</td>
</tr>
<tr>
<td><strong>(4) Input/output, interface</strong></td>
</tr>
<tr>
<td>(a) input/output</td>
</tr>
<tr>
<td>• combination of input data</td>
</tr>
<tr>
<td>• multiple input agreement (avoidance of transient values)</td>
</tr>
<tr>
<td>• checking of input data (average value and range)</td>
</tr>
<tr>
<td>• measures for incorrigible dangerous output</td>
</tr>
<tr>
<td>• diagnosis of input hardware</td>
</tr>
<tr>
<td>• feedback check of output</td>
</tr>
<tr>
<td>(b) transmission</td>
</tr>
<tr>
<td>• measures for serial data transmission</td>
</tr>
<tr>
<td>(c) CPU</td>
</tr>
<tr>
<td>• transmission check between CPUs</td>
</tr>
<tr>
<td>(d) man-machine</td>
</tr>
<tr>
<td>• rejection of mistaken control</td>
</tr>
<tr>
<td>• protection mechanism for mistaken operation</td>
</tr>
<tr>
<td>• consistency check for operation input data</td>
</tr>
<tr>
<td>• guidance for protection against mistaken operation</td>
</tr>
<tr>
<td>• guaranteed correctness of VDU information</td>
</tr>
<tr>
<td><strong>(5) Interface</strong></td>
</tr>
<tr>
<td>(a) redundant configuration</td>
</tr>
<tr>
<td>• transmission drive by conjunction of CPUs</td>
</tr>
<tr>
<td>(b) multiprocessor</td>
</tr>
<tr>
<td>• processing of common signals</td>
</tr>
<tr>
<td>• measures for delay of bus arbiter</td>
</tr>
<tr>
<td>• measures for electrical source switching in the module</td>
</tr>
<tr>
<td><strong>(6) Other</strong></td>
</tr>
<tr>
<td>(a) other</td>
</tr>
<tr>
<td>• independence of design and checking</td>
</tr>
<tr>
<td>• layer system for checking common functions</td>
</tr>
</tbody>
</table>
1. Application of computers to railway signalling in Japan
- Safety Guidelines

Safety Guidelines for introduction of microelectronics to railway signalling in Japan (1996)

- the first electronic interlocking (1985) (>1,000 stations)
- safety guidelines in 1980s (within-department-purpose)
- specialists’ committee (1994-1996)
- IEC 61508

New Safety Guidelines for Computerised Train Control and Protection Systems

- Safety lifecycle
  - Safety integrity levels
- International safety standards
  - IEC 61508
- General-purpose

Safety technologies cultivated in Japanese signalling
- Interlocking, ATC

Fail-safe

Regulation
Functional Safety Experience on Railway Signalling in Japan

1. Application of computers to railway signalling in Japan
   - Technical breakthroughs
   - Safety guidelines

2. Functional safety experience: current situation
   - Functional Safety Standards
   - Quantitative Safety Evaluation and Hazard Analyses
   - Evaluation of Safety Measures
   - Risk Management

3. Outstanding questions to be addressed
2. Functional safety experience: current situation
   - Functional Safety Standards

   Functional Safety Standards

   ◆ IEC 61508
      • An umbrella safety standard for computerised control
      • Two concepts:
         Safety lifecycle and Safety integrity

   ◆ Railway Signalling Situations
      (almost the same as IEC 61508; no conflict)
      • Sector-specific situations
      • Driving force for introduction
IEC / TC9 standards for railway applications

**CENELEC** for railway signalling
- EN 50126 (RAMS)
- EN 50128 (Software)
- EN 50129 (Safety Cases)
- EN 50159 (Transmission)

**IEC** International
- IEC 62278 (RAMS)
- IEC 62279 (Software)
- IEC 62425 (Safety Cases)
- IEC 62280 (Transmission)

Driving force in the background:
EU unification

Interoperability = ERTMS
(European Railway Traffic Management System)
2. Functional safety experience: current situation
   - Quantitative Safety Evaluation and Hazard Analyses

Tolerable Hazard Rate and Safety Integrity Level
(IEC 62425)

<table>
<thead>
<tr>
<th>THR (h^{-1} / Function)</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^{-9}$ &lt; THR $&lt; 10^{-8}$</td>
<td>4</td>
</tr>
<tr>
<td>$10^{-8}$ &lt; THR $&lt; 10^{-7}$</td>
<td>3</td>
</tr>
<tr>
<td>$10^{-7}$ &lt; THR $&lt; 10^{-6}$</td>
<td>2</td>
</tr>
<tr>
<td>$10^{-6}$ &lt; THR $&lt; 10^{-5}$</td>
<td>1</td>
</tr>
</tbody>
</table>
Application of Functional Safety Standards for Railways (1)

(almost the same as IEC 61508; no conflict)

- Uncertainty of quantitative risk analysis and allocation of safety integrity levels
  - Estimation of probability is not easy because of
  - Insufficiency of actual statistical data

- Emphasis on hazard analysis
  - Specifying failure causes is crucial (FTA)
Application of Functional Safety Standards for Railways (2)

◆ Absolute Value vs. Comparative Value

Final Confirmation
(absolute the same or better)

Identification of
More Dangerous Hazards
(by comparison)

◆ Necessity of a Prudent Approach
  - the lack of a database
  - the inherent danger of new systems
  - the limits of modelling
An Example of Hazard Analysis

**COMBAT** = a blocking system
- a new train detection by microwave balises
  + centralised electronic interlocking (blocking function)
COMBAT Configuration

Centre

Centralised Interlocking

Station Interlocking

Stations

A

Station Interlocking

B

Station Interlocking

C

On-board balises

Interrogator

Responder
An Example of the Results of Safety Analysis

Malfunction of communication between train detection and interlocking

1.0 $\times 10^{-12}$

Malfunction of interlocking (false train absence)

5.6 $\times 10^{-12}$

Malfunction of train detection (false train absence)

2.4 $\times 10^{-14}$

Malfunction of train leaving detection

1.9 $\times 10^{-12}$

Malfunction of detection equipment (inappropriate recovery procedure)

2.2 $\times 10^{-54}$

Leakage of ground interrogator signal

2.2 $\times 10^{-54}$

Diagnosis of responder transmission after train movement-direction detection (by the tail of the train)

Oncoming train

Collision

If

Wrong signal aspect

Malfunction of station interlocking output

Malfunction in responder transmission (code failure or echo failure)

Diagnosis based on time between movement detection and responder responding

Abbreviated
### An Example of the Results of Safety Analysis

#### Abbreviated

<table>
<thead>
<tr>
<th>Subsystem</th>
<th>Function block</th>
<th>Failure mode</th>
<th>Anticipated causes of failure</th>
<th>Failure</th>
<th>Range (scope)</th>
<th>Influence</th>
<th>Situations</th>
<th>Hazard level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baisetrain detection</td>
<td>Interrogator</td>
<td>Oscillation</td>
<td>Ground repeater information receipt</td>
<td>a) The two blocks, one each side of the interrogator</td>
<td>Non-detection of train entry</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>b) The block between the interrogator and the next station</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Inappropriate installation position</td>
<td>Disasters, etc.</td>
<td>No shut-down between interrogator and responder but with train direction detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Block section recently vacated</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

FMEA: Failure Mode and Effect Analysis
2. Functional safety experience: current situation
   - Evaluation of Safety Measures

for Micro-computerised Signalling Systems

Multiple Application of Safety Measures
  <= Many individual effects interact in unclear ways

Quantitative Evaluation of Effects and Interactions
  => Simpler (and cheaper) signalling systems

Formulation of the Effects of Each Safety Measure
and Integrated Framework for Evaluation
Formulation of the Effects of Each Safety Measure

The Effect of Double Input Architecture

\[ \frac{2 \cdot T_A}{2} = 1.1 \times 10^{-9} \]

\[ \frac{2}{2} : \text{Failure Rate } 10^{-5} [/h] \]

\[ T_A : \text{Comparison Period } 1.1 \times 10^{-4} [h] \]

(0.4 sec)
Framework for Evaluation of Safety Measures

System Analysis
- Function analyses
- Function correlation analyses
- Malfunction influence analyses

Evaluation of Safety Measures
- Fatality matrix $CM$ construction
- Fatal failure selection vector (row) $E$ construction
- Safety Measures Matrix (mitigation matrix) $MM$ construction
- Safety measures set vector (row) $M$ construction

Risk
- System dangerous failure occurrence probability $D = E \cdot G$
- Residual failure probability $L = MM \cdot A$
- System residual failure probability $S = M \cdot A$
- Dangerous failure probability despite safety measures $Q = E \cdot P_M \cdot M' \cdot A$
An Example of Safety Analysis of a Fail-safe CPU Board

Correlation matrix $PM$

Failure rate vector $A$

Malfunction occurrence vector $G$

Safety measures $M$

Safety Measures Matrix $MM$

Malfunction occurrence vector (without safety measures) $G$

Effects of safety measures

False output (danger)

$G'_2 = 7.8 \times 10^{-11}$

$G'_4 = 1.1 \times 10^{-10}$

$Q = G'_2 + G'_4 = 1.9 \times 10^{-10}$
2. Functional safety experience: current situation
  - Risk Management

Risk Management

1. Necessity of the Hazard List and its Methodical Assembly

2. Extension of Risk Analysis to Safety-related Systems

3. Railway Signalling System Reconstruction by RAMS Criteria
1. Necessity of the Hazard List and its Methodical Assembly

- Identification of Hazard is crucial
- Dangers may be hidden or latent
- Hazard lists specific to Railway Signalling
  - Circuit device failures
    - Circuit design inappropriate
    - Operation error
2. Extension of Risk Analysis to Safety-related Systems

Obstacle Detection by Image Processing
Safety-related Functions
- Hazard
- Risk

Necessity of Diagnosis
Identification of Hazard

Influence of Variable Lighting Conditions on Image Processing for Obstacle Detection
Risk Analysis of Image Processing for Level Crossing Obstacle Detection

FTA of Image Processing (Identification of Hazards) → Counter Measures/ Evaluation
3. Railway Signalling System Reconstruction by RAMS Criteria

Each signalling system shows constant improvement (viewed separately)

The influence on overall train operation (delay time)
- Harmonisation of reliability and cost-effectiveness
- Quick recovery from and small influence of malfunctions
Signalling System Reconstruction

- Signals
- Track circuits
- Station equipment
- Network (cable/radio)
- Wayside device controllers
- Point machines
Example of Failure Rate Analysis

- **Absolute failure rate**
- **Failure rate in terms of train delay**

Diagram showing failure rates for devices A, B1, B2, C1, C2, D, E1, E2, and F.
Proposed Signalling System Processes

Function Analysis
- Requirements
- Structures

Possible Candidate Solutions
(System A, B, etc.)

Existing and Applied Conditions
(Load, Stations, etc.)

RAMS Evaluation Tool (Simulator)
(Evaluation from RAMS point of view)

Proposed System
The best inside the proposed and existing conditions
An Example of a Proposed System

- Radio and Train Control Device
- Radio
- Point Machine and its Control Device
- Track Circuit and its Control Device

- Track Circuit
- Train and On-board Control Device
- LAN
Functional Safety Experience on Railway Signalling in Japan

1. Application of computers to railway signalling in Japan
   - Technical breakthroughs
   - Safety guidelines

2. Functional safety experience: current situation
   - Functional Safety Standards
   - Quantitative Safety Evaluation and Hazard Analyses
   - Evaluation of Safety Measures
   - Risk Management

3. Outstanding questions to be addressed
3. Outstanding questions to be addressed

Outstanding Questions

1. Increasing Integration of Hardware
   ⇒ Uncertainties in diagnosis

2. Safety Assessment
   - Documentation
     How many documents are documents enough?
     How safe is safe enough?

   - Safety
     How safe is safe enough?

⇐ Appropriate Safety Assessment Criteria

3. Software