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

鉄道ピクトリアルから引用

Fail safe

keeps safe state even in malfunction

Definition of safety is possible (standstill)

鉄道ピクトリアルから引用

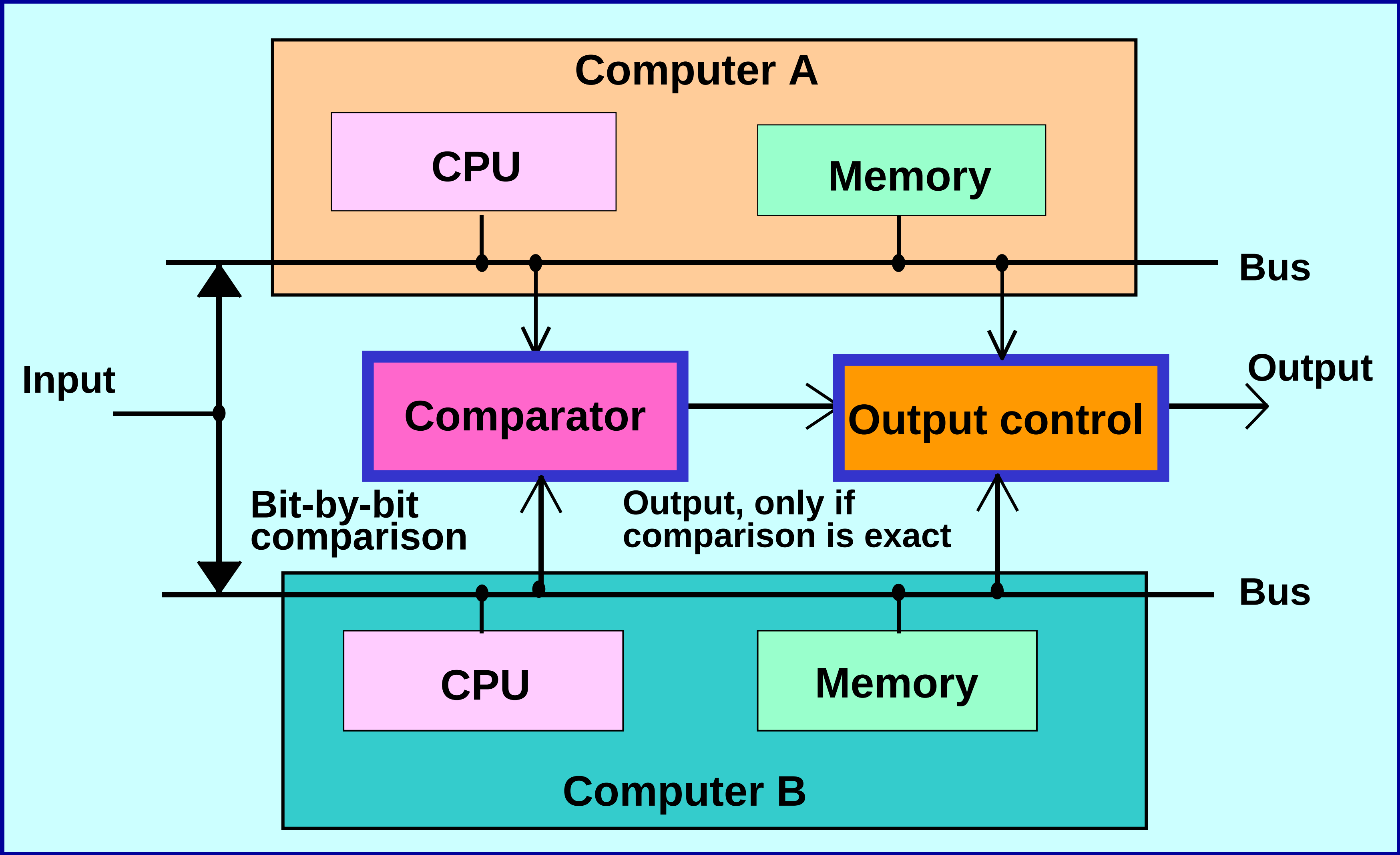
relay

Micro-computer

Technical Principles for Safety

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

Redundant CPU Architecture

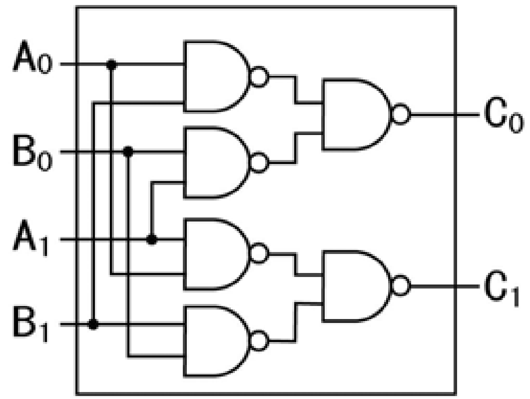


Comparator with 2-pair 2-bit comparison

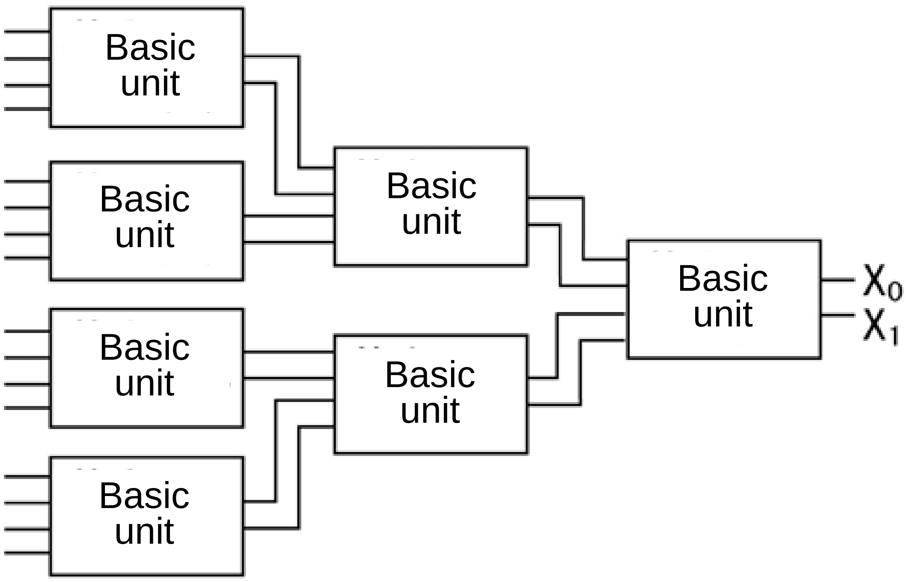
Comparator with 2-pair 2-bit comparison

Input of 2 pair of 2 bits					Output of 1 pair of 2 bits	
(A_0	B_0	A_1	B_1)	→	(C_0	C_1)
(0	1	0	1)	→	(0	1)
(0	1	1	0)	→	(1	0)
(1	0	0	1)	→	(1	0)
(1	0	1	0)	→	(0	1)

Basic unit



Basic concept



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

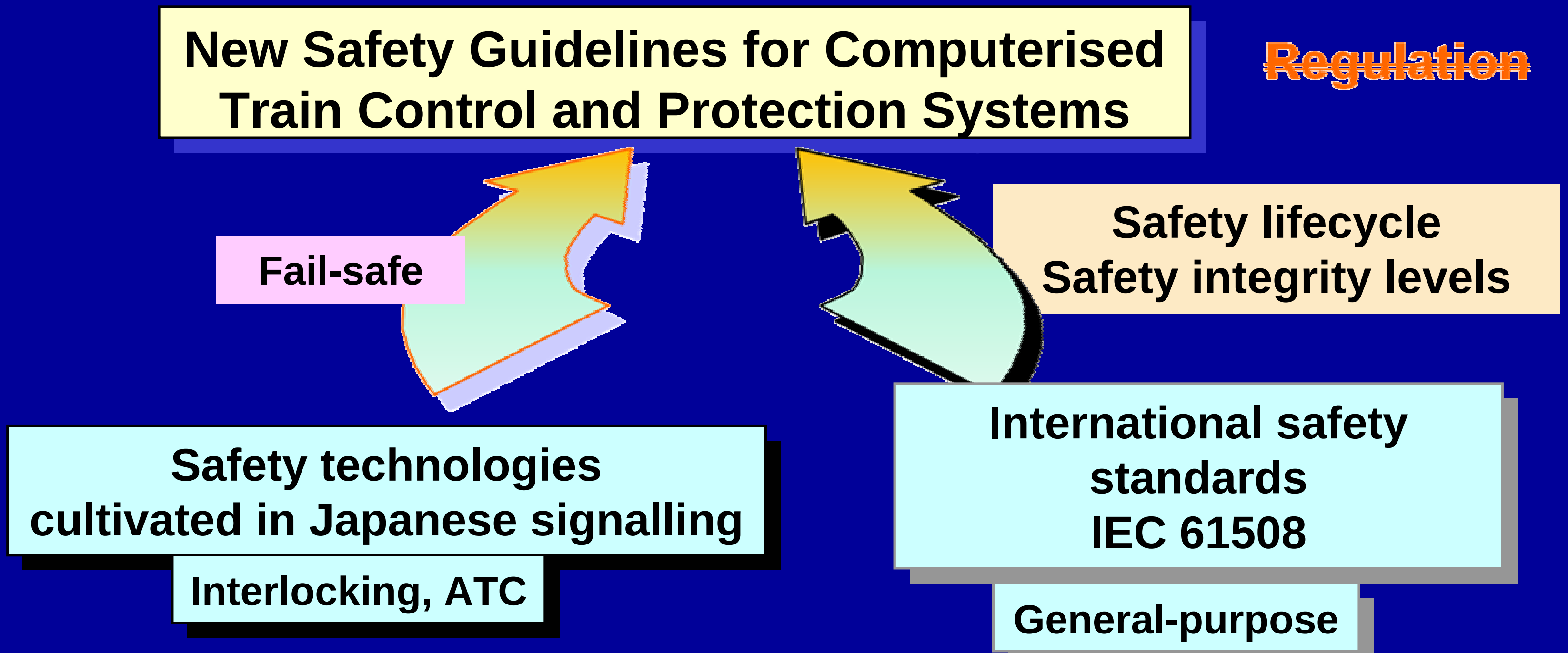
Software Techniques

(1) OS	(2) Common subroutine, firmware
(a) interruption • prohibition of interruption	**(a) common subroutine** • common programs for quasi synchronisation
(3) Application	**(4) Input/output, interface**
(a) system • continuation of conventional system design • control cancellation in the case of field equipment dysfunction • safety processing when transmission disconnected • information refreshment • guarantee of continuity during changeovers • procedures at error detection and resumption **(b) program** • separation of safety-related processing from non-safety processing • simplification of program structure • prohibition of "GO TO" sentence • consistent allocation of safe and unsafe position	**(a) input/output** • combination of input data • multiple input agreement (avoidance of transient values) • checking of input data (average value and range) • measures for incorrigible dangerous output • diagnosis of input hardware • feedback check of output **(b) transmission** • measures for serial data transmission **(c) CPU** • transmission check between CPUs **(d) man-machine** • rejection of mistaken control • protection mechanism for mistaken operation • consistency check for operation input data • guidance for protection against mistaken operation • guaranteed correctness of VDU information
(5) Interface	**(6) Other**
(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	**(a) other** • independence of design and checking • layer system for checking common functions

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



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

Functional Safety Standards

◆ IEC 61508

- An umbrella safety standard for conputerised 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 (Europe)
for railway signalling

EN 50126 (RAMS)
EN 50128 (Software)
EN 50129 (Safety Cases)
EN 50159 (Transmission)

Fast Track Procedures

IEC (International)

CDV (Committee Draft for Voting)

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)

Tolerable Hazard Rate and Safety Integrity Level (IEC 62425)

THR (h^{-1} / Function)	SIL
$10^{-9} \leqq THR < 10^{-8}$	4
$10^{-8} \leqq THR < 10^{-7}$	3
$10^{-7} \leqq THR < 10^{-6}$	2
$10^{-6} \leqq THR < 10^{-5}$	1

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

Absolute Value	Comparative Value
Final Confirmation	Identification of More Dangerous Hazards
(absolutely the same or better)	(by comparison)

◆Necessity of a Prudent Approach

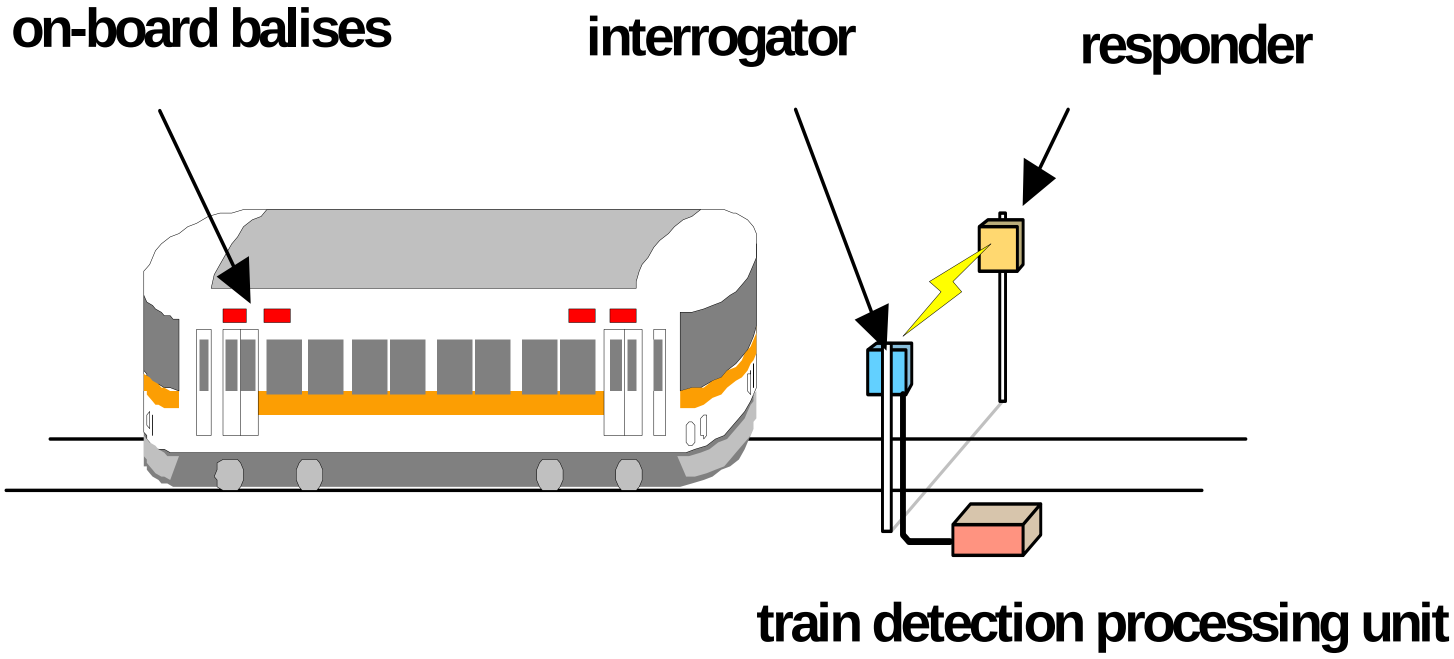
- the lack of a database
- the inherent danger of new systems
- the limits of modelling

An Example of Hazard Analysis

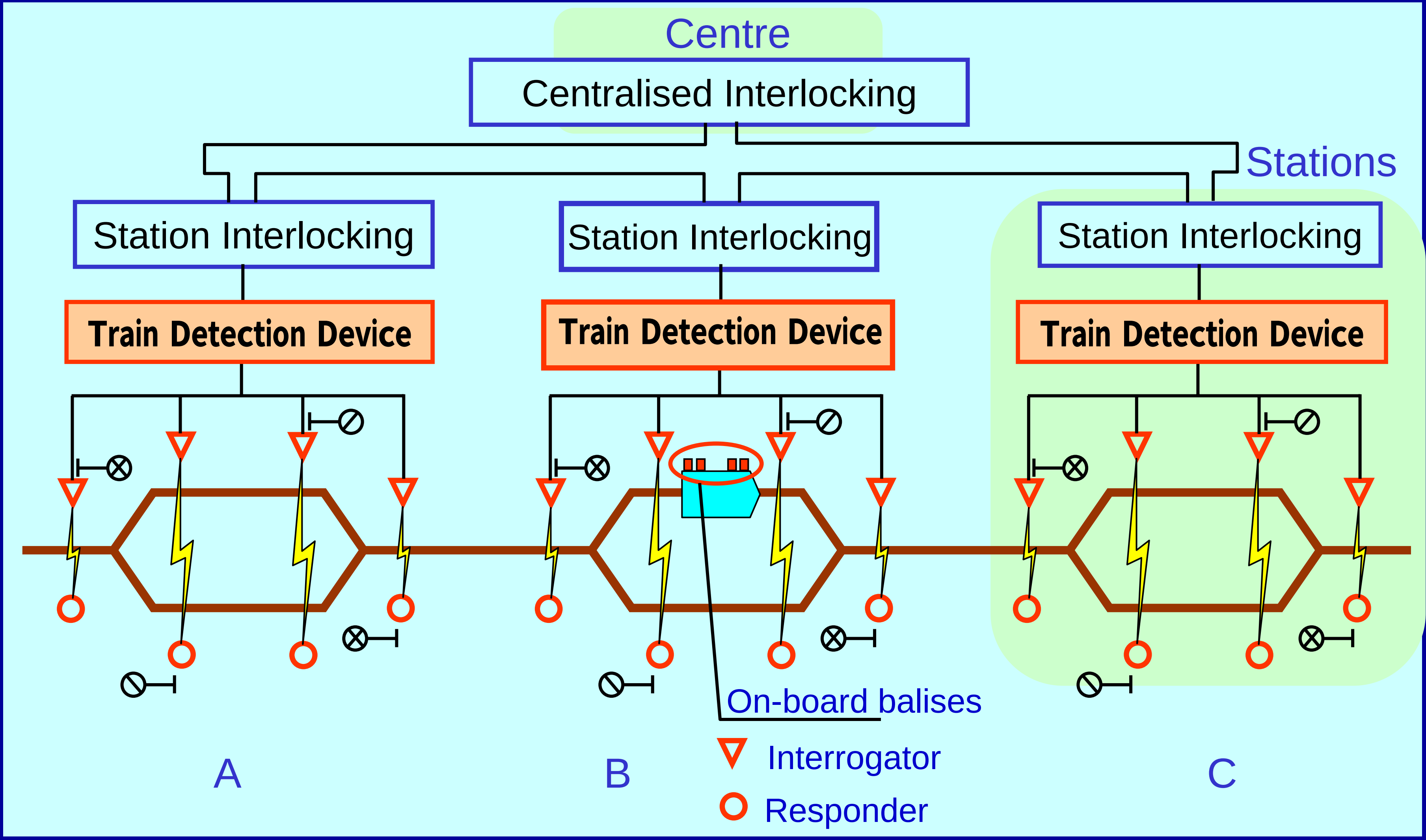
COMBAT = a blocking system

a new train detection by microwave balises

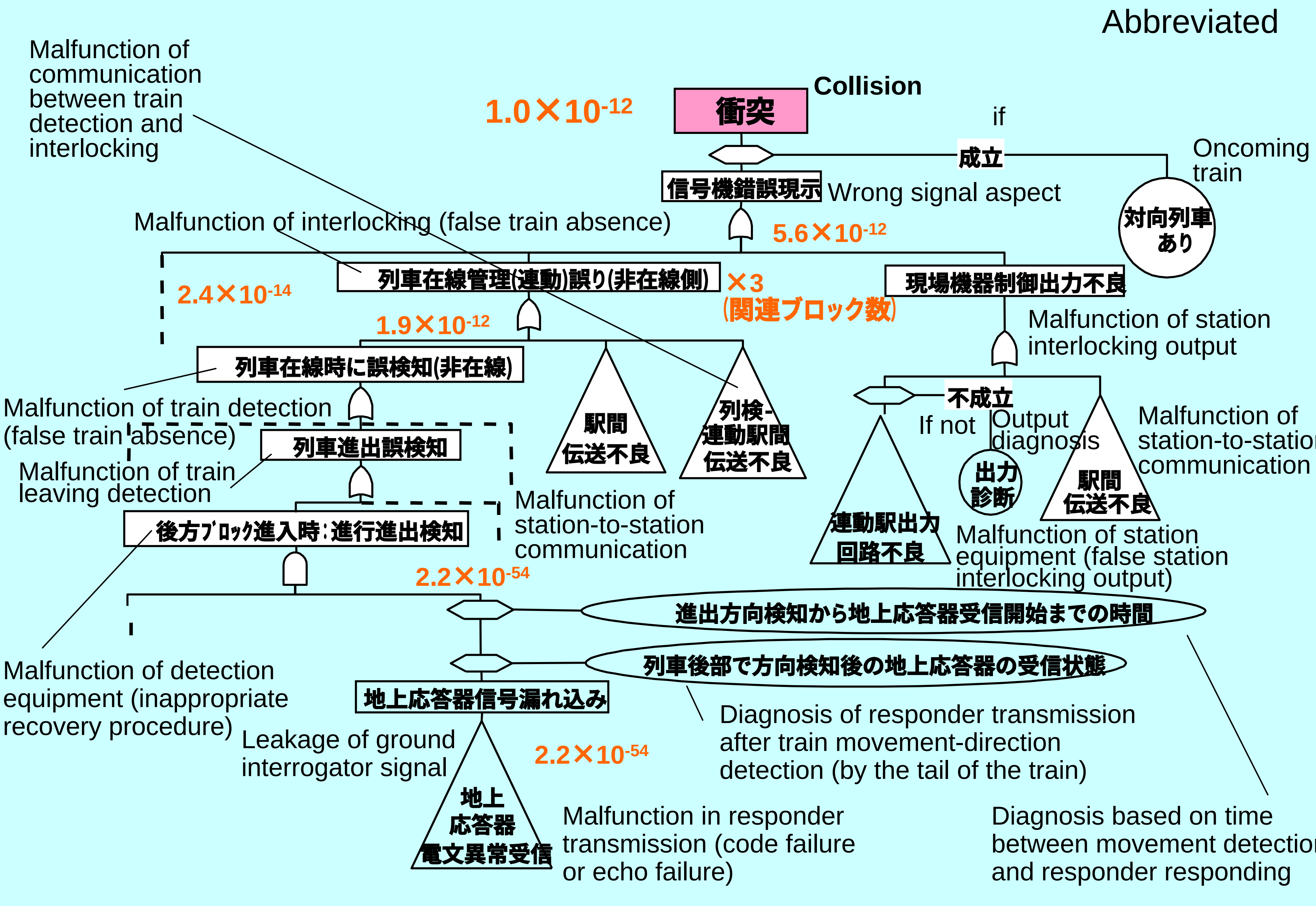
+ centralised electronic interlocking (blocking function)



COMBAT Configuration



An Example of the Results of Safety Analysis



An Example of the Results of Safety Analysis

Abbreviated

Subsystem	Function block	Failure mode	Anticipated causes of failure ① Hardware ② Electric source ③ Human	Failure	Influence: Range (scope)	Influence: Situations	Hazard level
Baise train detection	Interrogator	Oscillation	① ②	Ground repeater information receipt	a) The two blocks, one each side of the interrogator b) The block between the interrogator and the next station	Non-detection of train entry	IV
		Inappropriate installation position	① ③ Disasters, etc.	No shut-down between interrogator and responder but with train direction detection	Block section recently vacated	False block-is-empty signal	IV

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

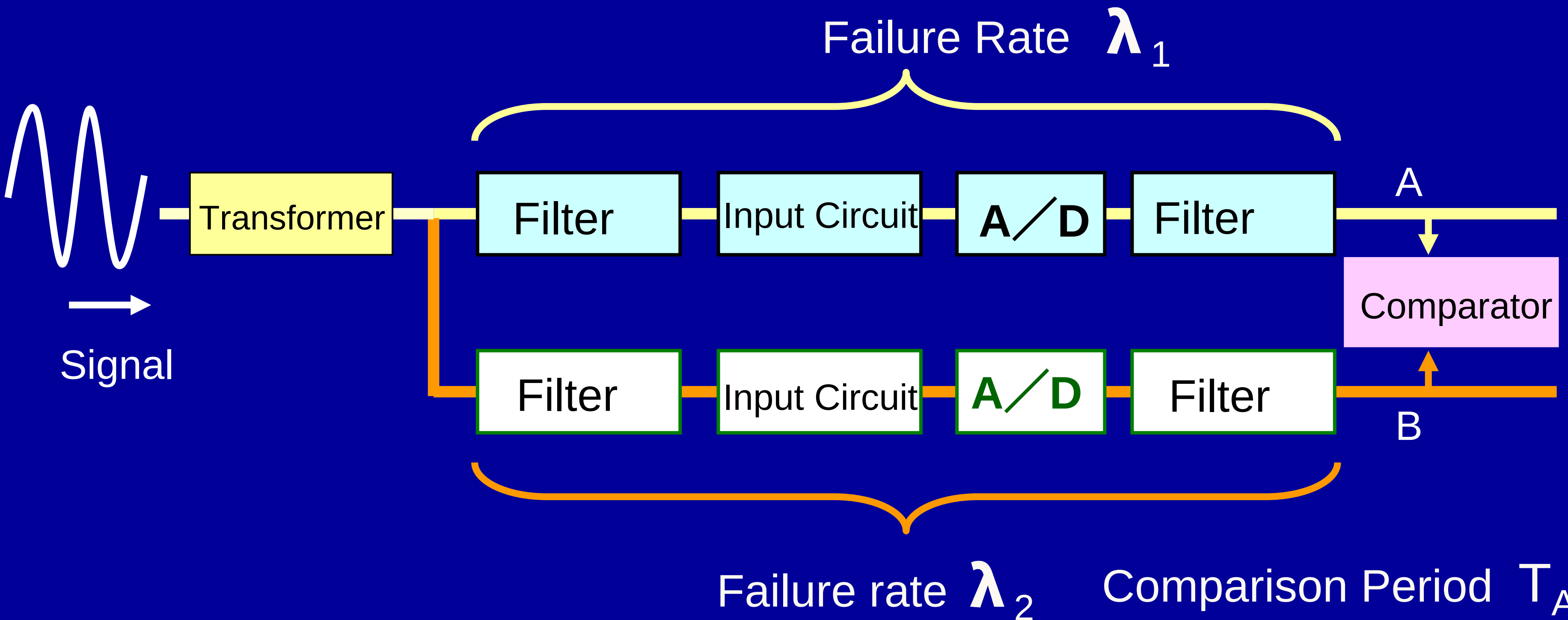
<= Many individual effects interact in unclear ways

Quantitative Evaluation of Effects and Interactions

=> Simpler (and cheaper) singalling 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

$$\lambda_2 T_A = 1.1 \times 10^{-9}$$

(λ_2 : Failure Rate 10^{-5} [/h]

T_A : Comparison Period 1.1×10^{-4} [h] (0.4 sec))

Framework for Evaluation of Safety Measures

System Analysis

- Function analyses
- Function correlation analyses
- Malfunction influence analyses

Function failure rate setting → **Failure rate vector (column) A construction**

↓

Correlation matrix P_M construction → **Malfunction occurrence vector (column) G construction**

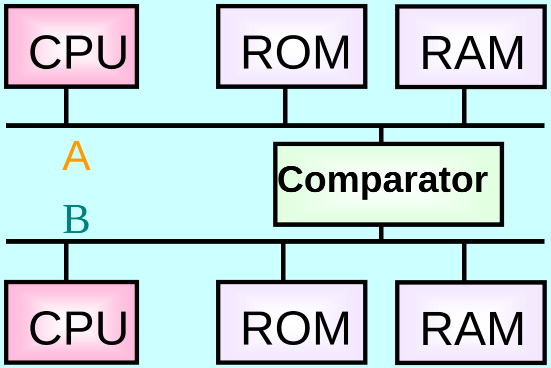
$$G = P_M \cdot A$$

Evaluation of Safety Measures

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

Risk	$R = f\{CM \cdot G\}$
System dangerous failure occurrence probability	$D = E \cdot G$
Residual failure probability	$L = M_M \cdot A$
System residual failure probability	$S = M \cdot A$
Dangerous failure probability despite safety measures	$Q = \underbrace{E \cdot P_M \cdot M'}_{G'} \cdot A$

An Example of Safety Analysis of a Fail-safe CPU Board



Malfunction occurrence vector (without safety measures) *G*

G_1	Non-code output	1.48×10^{-6}[/h]
G_2	Wrong code output	7.48×10^{-7}[/h]
G_3	Zero output	1.25×10^{-6}[/h]
G_4	One output	4.49×10^{-7}[/h]
G_5	Output ceases	8.00×10^{-7}[/h]

Correlation matrix *PM*

$$\begin{pmatrix} \cdot & \cdot & 1 & 0.5 & 1 \\ \cdot & \cdot & 1 & 0.5 & 10^{-5} \\ \cdot & \cdot & 0 & 0.5 & 1 \\ \cdot & \cdot & 1 & 0.5 & 10^{-3} \\ \cdot & \cdot & 0 & 0 & 1 \end{pmatrix} \circ$$

Failure rate vector *A*

A_1	Input circuit 0-stick	3×10^{-8} [/h]
A_2	Input circuit 1-stick	3×10^{-8} [/h]
A_3	Input circuit intermittent failure	1×10^{-8} [/h]
A_4	Bus 0-stick	3×10^{-9} [/h]
A_5	Bus 1-stick	3×10^{-9} [/h]
A_6	Bus intermittent failure	3×10^{-8} [/h]

$\therefore D = G_2 + G_4 = 1.2\times10^{-6}$

Effects of safety measures

Malfunction occurrence vecto
(with safety measures) *G*

Safety measures *M*

M_1	Pulse input checking
M_2	Front and back contact checking
M_3	Masking of uncertain input
M_4	Logical checking of input data
M_5	Fail-safe comparator
M_6	Software self-diagnosis

Safety Measures Matrix *MM*

$$\begin{pmatrix} 0.05 & 0.001 & 0.05 & 0.5 & \cdot & \cdot \\ 0.001 & 0.001 & 0.05 & 0.5 & \cdot & \cdot \\ 0.5 & 0.5 & 0.05 & 1 & \cdot & \cdot \\ 0.05 & 0.005 & 0.05 & 0.5 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

False output (danger

$G_2' = 7.8\times10^{-11}$

$G_4' = 1.1\times10^{-10}$

$\therefore Q = G'_2 + G'_4$
$= 1.9\times10^{-10}$

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

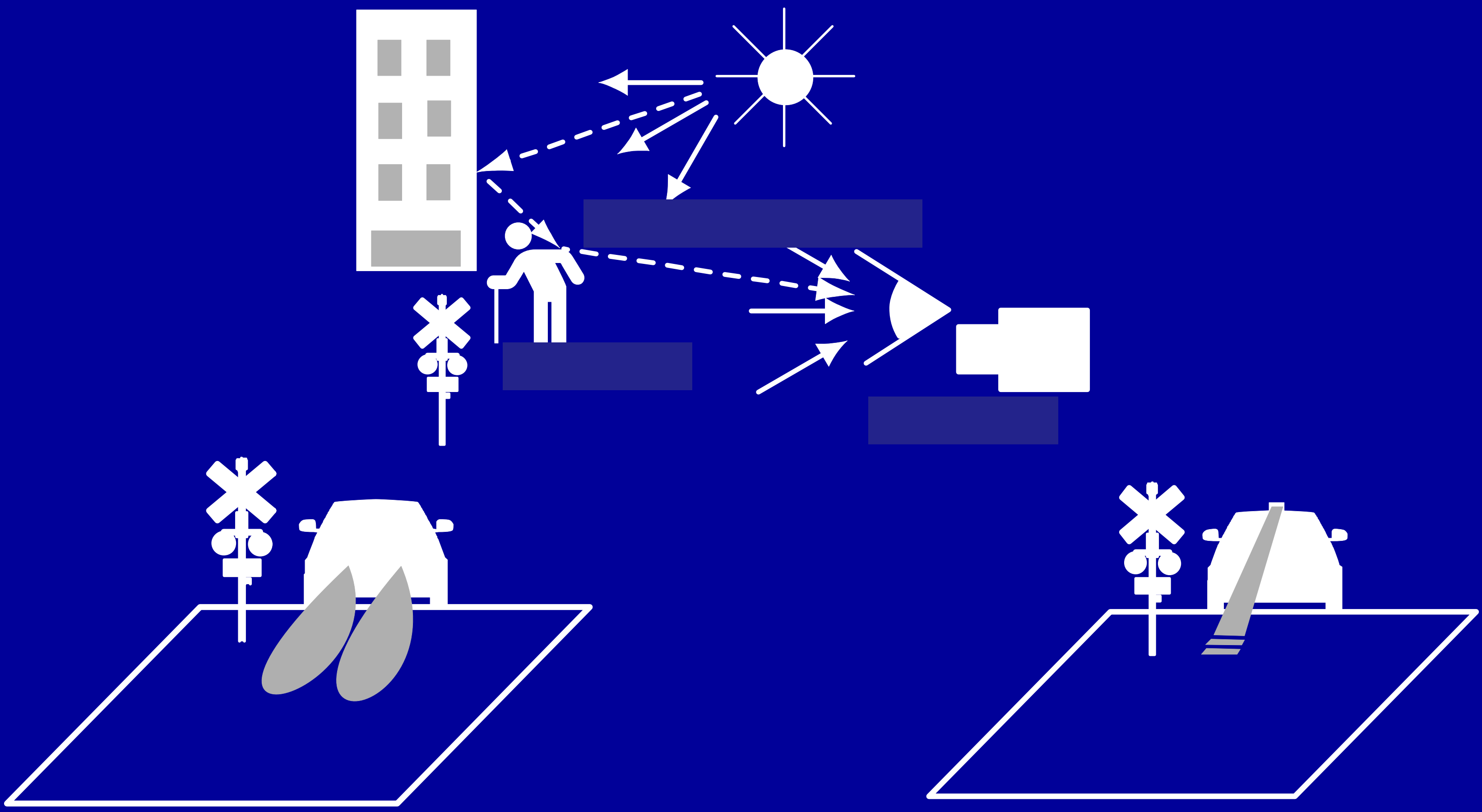
Safety-related Functions

- 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

Reliability
Availability
Maintainability
Safety

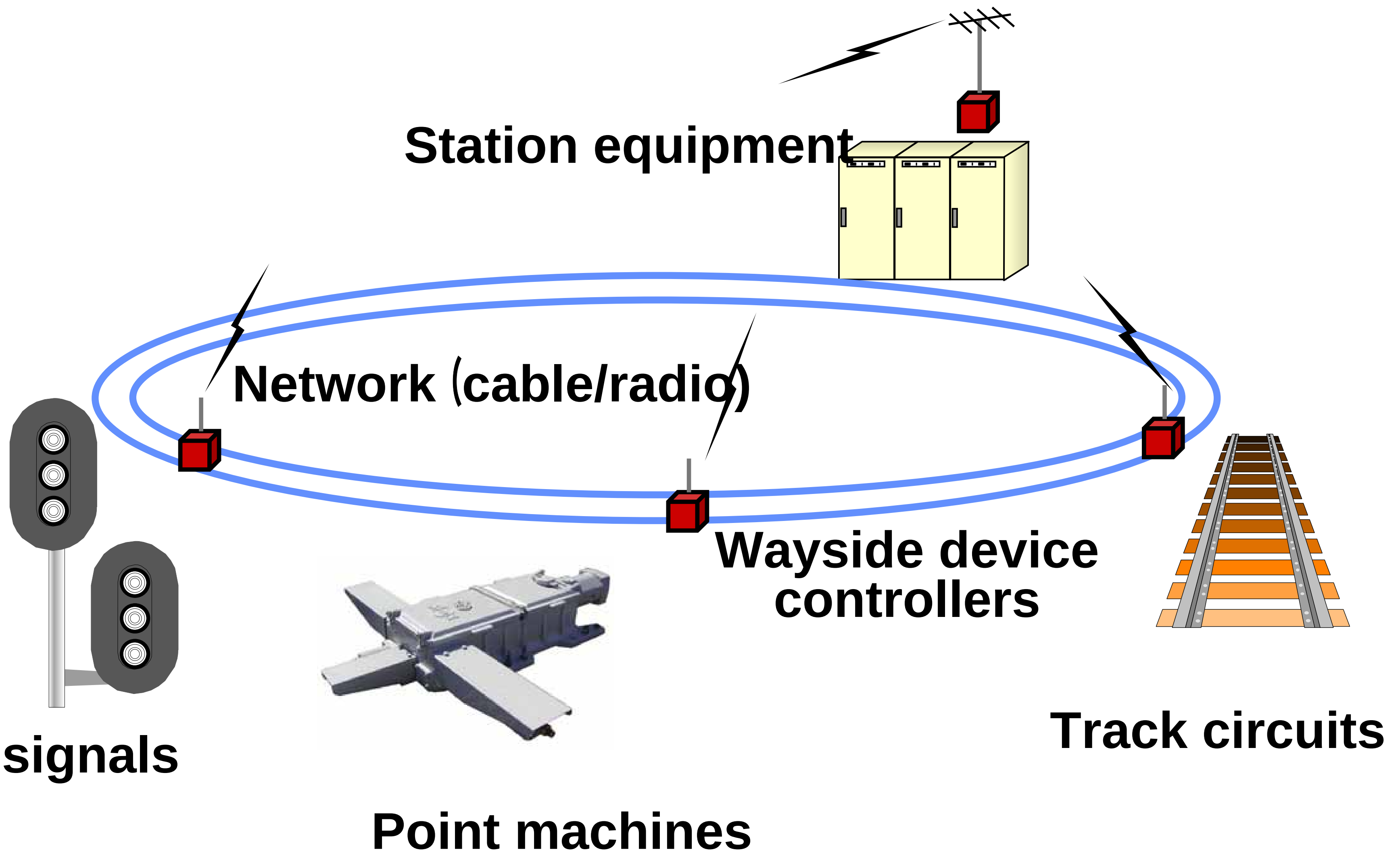
Each signalling system shows constant improvement (viewed separately)

↓

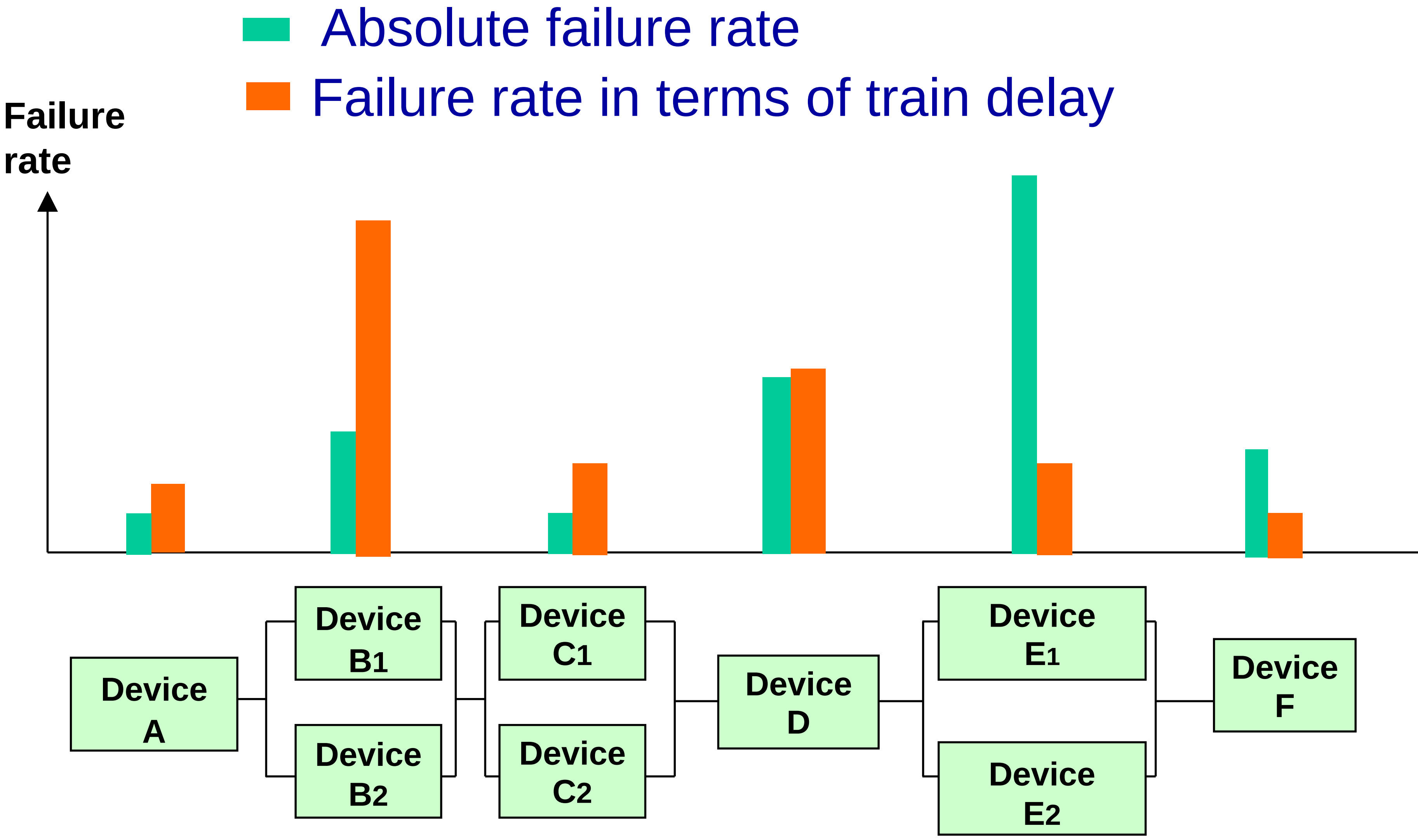
The influence on overall train operation (delay time)

- Harmonisation of reliability and cost-effectiveness
- Quick recovery from and small influence of malfunctions

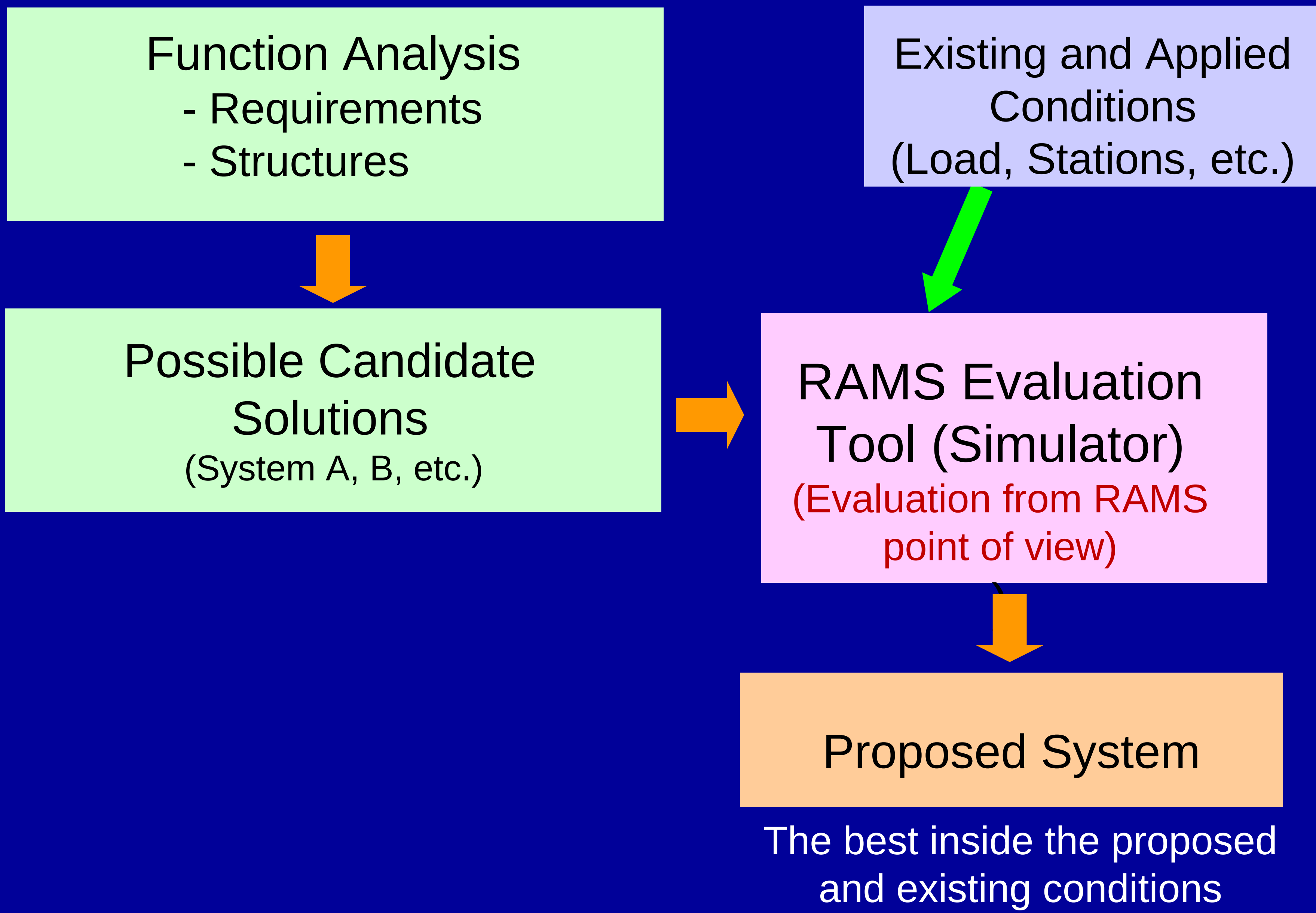
Signalling System Reconstruction



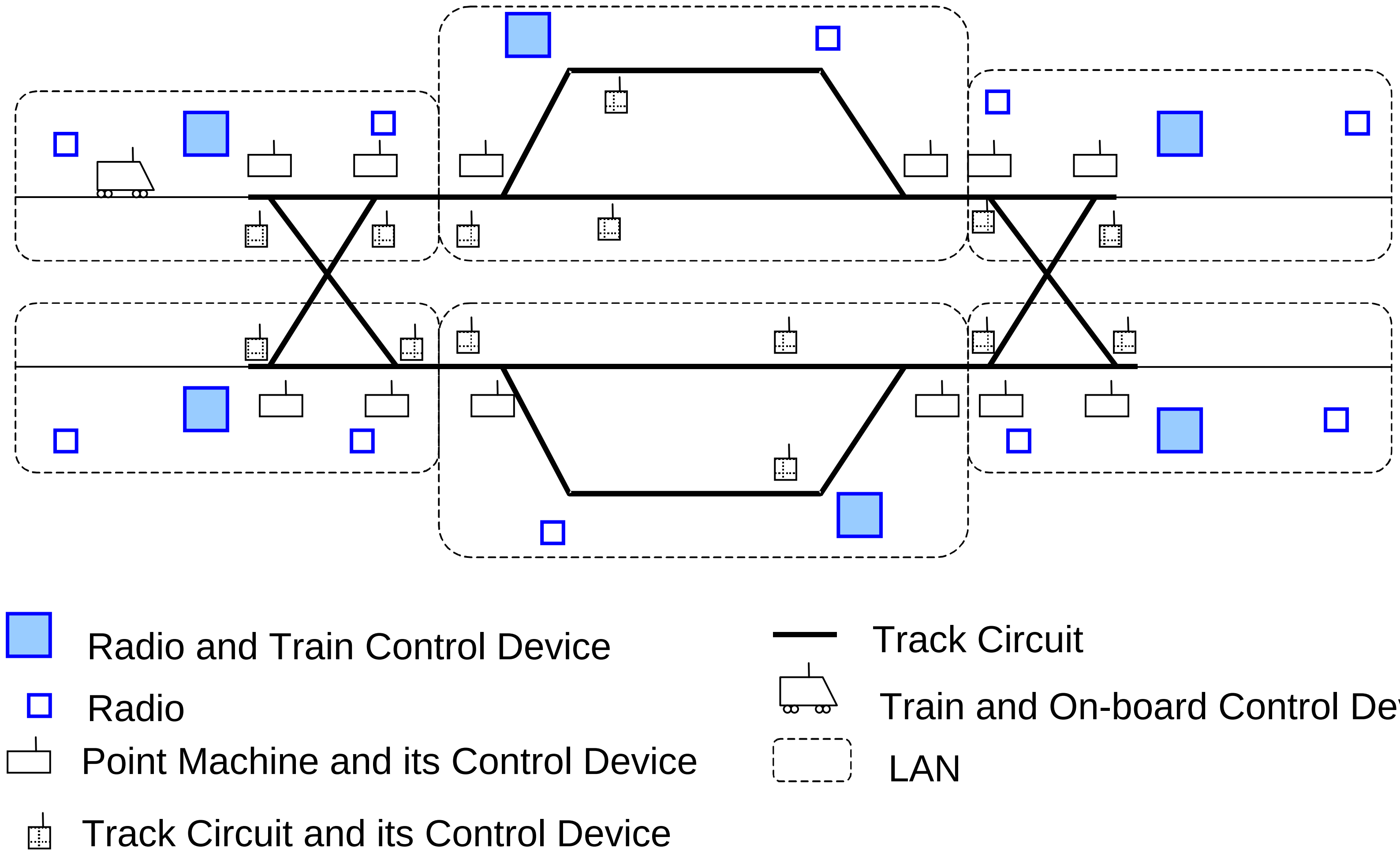
Example of Failure Rate Analysis



Proposed Signalling System Processes



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

Outstanding Questions

1. Increasing Integration of Hardware

   $\Rightarrow$ Uncertainties in diagnosis

2. Safety Assessment

   - Documentation

     How many documents are documents enough?

     cost

   - Safety

     How safe is safe enough?

   $\Leftarrow$ Appropriate Safety Assessment Criteria

3. Software