APCRMS2005
December 1, 2005

Accident Sequence Analysis of Railway Accidents Based on Safety Control Functions

Takehisa Kohda
Kyoto University, Kyoto, Japan
&
Hiroshi Fujihara
Railway Technical Research Institute, Kokubunji, Japan

Contents of Presentation

Backgrounds

In the Japanese railway history, most of **the safety measures were devised <u>after suffering severe railway accidents</u>**, resulting in multilayered protective systems. **Currently**, we still have **accidents due to human errors**, and all the accidents in the system cannot vanish completely.

Due to their **depressed economical condition**, the Japanese railway companies must **accomplish the safety mission efficiently without keeping the safety level of the overall railway system down**. The railway system should be considered **as a total system**, and thus **a <u>proactive system approach</u>** to the safety problems is to be desired; firstly the **identification of possible accident sequences**, and then an **appropriate measure.**

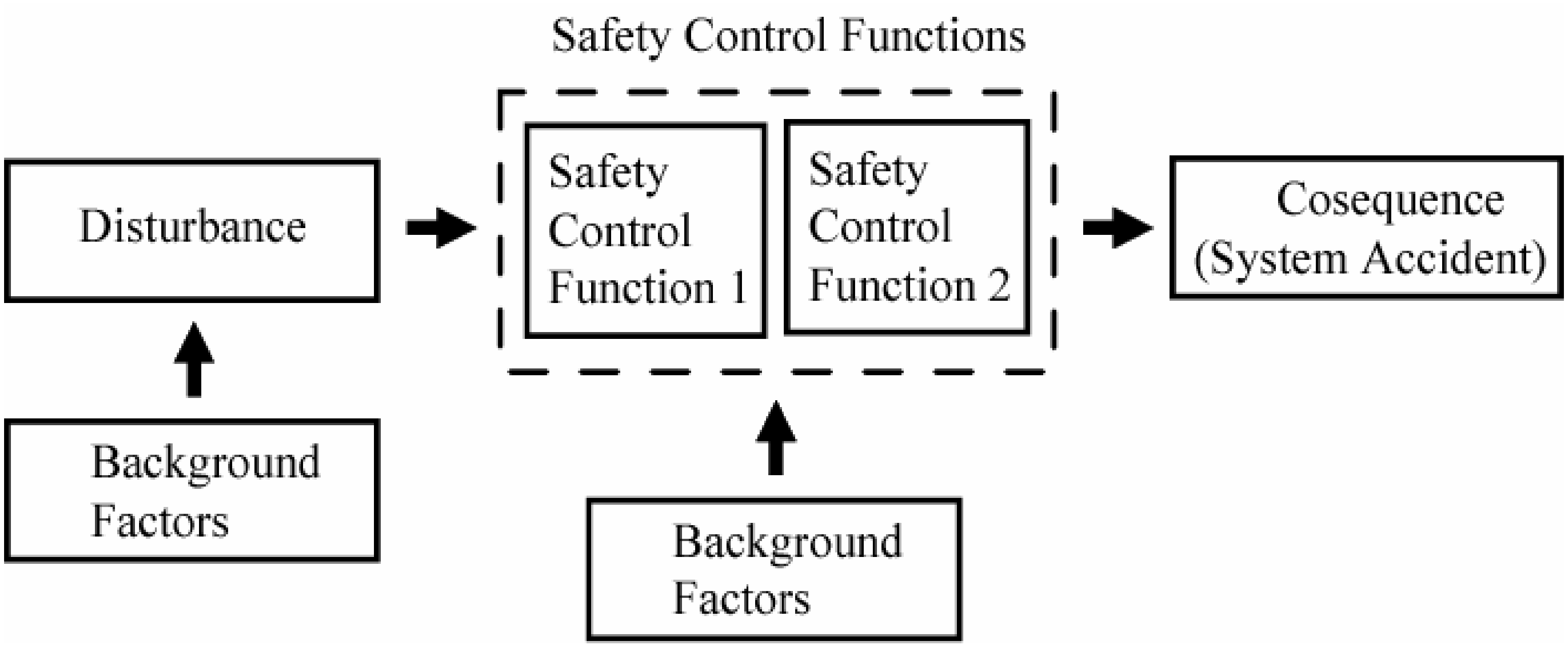
This paper tries to apply the concept of **<u>"safety control functions"</u>** to the **<u>derivation of accident sequences</u>** in an event tree model for a specific disturbance or initiating event.

Accident Sequence Conditions Based On Safety Control Functions

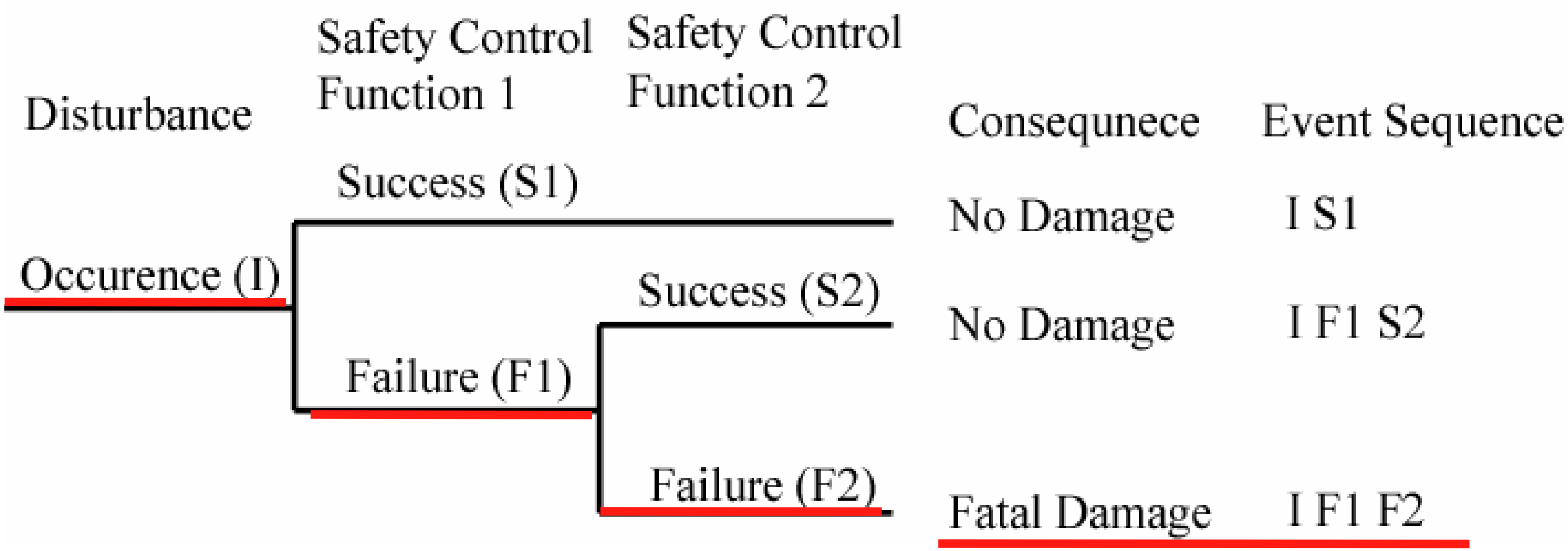
For a **system accident** to occur:

(C1) A **disturbance** can cause a deviation leading to the system accident.

(C2) **Safety control systems** must be **failed**.



Accident Sequence Conditions



Accident sequence conditions = **logical AND** combination of the **occurrence condition of a disturbance** and **failure conditions of safety control functions**.

<u>To identify a disturbance</u>:

Bottom-up: FMEA (Failure Mode and Effect Analysis): component failure, human erroneous action, or external event

Top-down: FTA (Fault Tree Approach)

Safety Control Function

<u>**Safety control functions**</u> :

Detection, Diagnosis, and Execution.

<u>**Safety control system**</u>

Sensing part, Controlling part, and Executing part

For a safety control function to work successfully, all three basic functions must work successfully. Thus, the **failure condition** is obtained as a <u>**logical OR combination of failure conditions of sensing, controlling, and executing parts**</u>.

Ex. <u>**Operator recovery action issued by alarms:**</u>

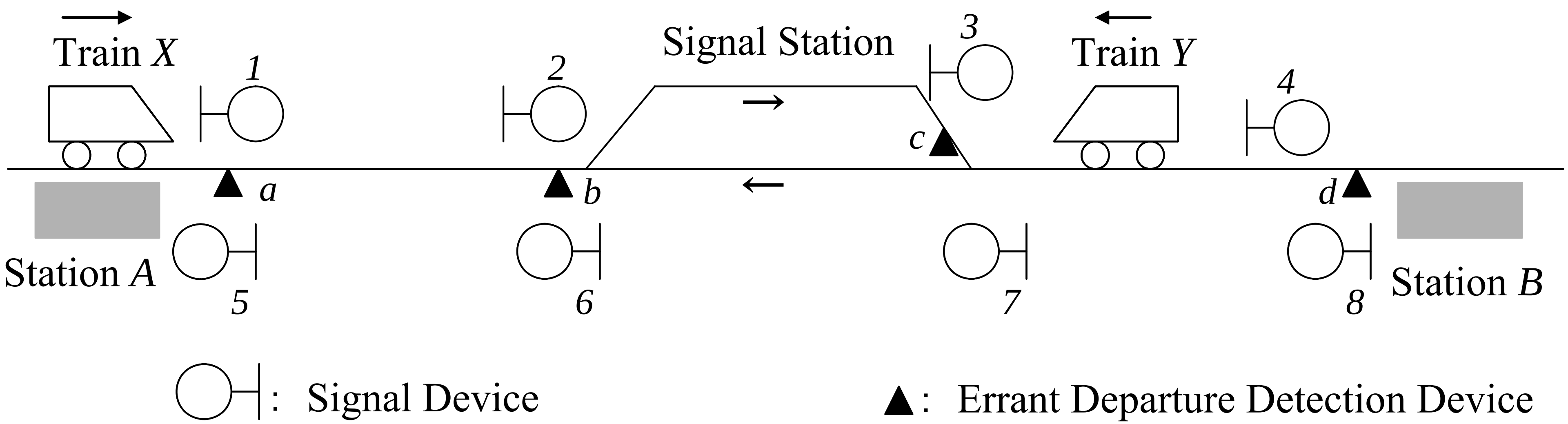
Alarm: Detection Operator: Diagnosis and Execution

Human errors such as perceptional errors and mistakes

By examining whether the <u>**sensing part can detect the effect**</u> of the disturbance, the **related safety control functions** can be identified.

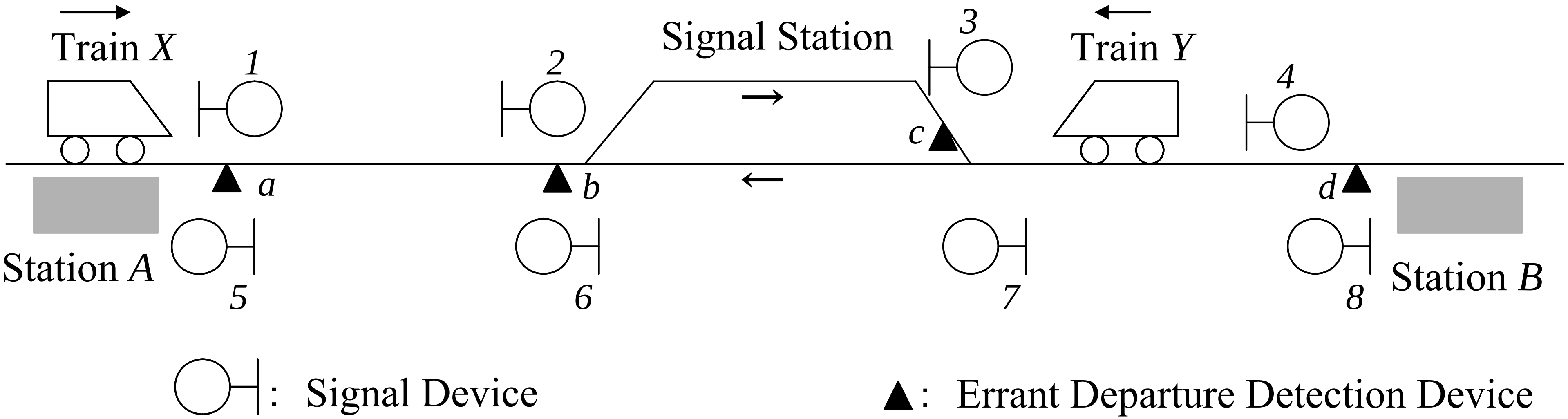
Illustrative Example: Collision Accident

<u>Safety Principle</u>: Only one train is allowed to run **in a block section**.
Three block sections: (1) Between station A and the signal station
(2) Section including the signal station
(3) Between the signal station and station B



controlled by
"special automatic block"

Safety Control Function



Safety Control Functions:

(S1) Signal system with Driver,

(S2) Errant departure detection device, Signal & Driver,

(S3) Driver by himself

(a1) Errant departure of train *X*: train *X* from station *A* accidentally departs with signal *1* being red **after train *Y* leaves** form station *B* for station *A*

Accident Sequences

<u>Position of train *Y* when train *X* makes a false departure:</u>

(A1) Train *Y* is **entering the signal station** with a consistent signal condition, where at least signals *6* & *7* are green (to go) and signals *1* & *2* are red (to stop).

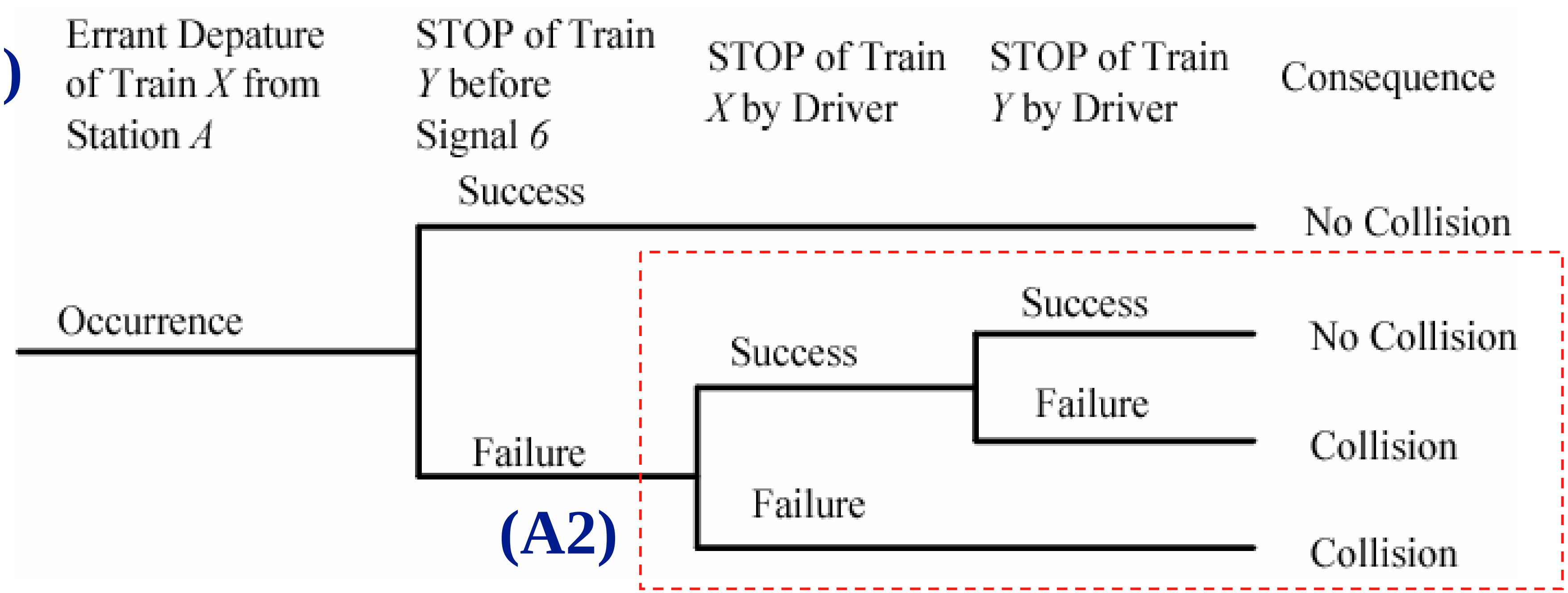
(A2) Train *Y* is leaving for station *A* **after passing by signal 6.**

<u>Available safety control functions</u> depending on the position of train *Y*

(A1): (S2) Signal *6* with driver action and **(S3**) Driver actions at trains *X* & *Y*.

(A2): (S3) Driver actions at trains *X* & *Y*.

(A1)



(A2)

Failure Conditions

<u>**Accident occurrence conditions:**</u> **logical AND** combination of a **disturbance condition** and **failure conditions of its effective safety control functions**

<u>**Stop/go operation depending on the signal:**</u> a kind of **stimulus-response action** of the driver

<u>**[Failure condition of (S2)]:**</u> **logical OR** combination of

(b1) the failed-dangerous failure of **errant departure detection device *a***,
(b2) the communication failure of **signal *6***,
(b3) the **perception error of the driver at train *Y***,
(b4) the **execution error of the driver at train *Y***.

<u>**[Failure conditions of (S3)]:**</u> **logical OR** combination of

(c1) the driver at train *X* failed to **detect** train *Y* coming near,
(c2) the driver at train *X* failed to **stop** his train
(c3) the driver at train *Y* failed to **detect** train *X* coming near,
(c4) the driver at train *Y* failed to **stop** his train

Accident Sequence Conditions

Accident sequence conditions for (A1):

{a1} **AND** {b1 **OR** b2 **OR** b3 **OR** b4} **AND** {c1 **OR** c2 **OR** c3 **OR** c4}

16 minimal cut sets of **size 3**

Accident sequence conditions for (A1):

{a1} **AND** {c1 **OR** c2 **OR** c3 **OR** c4}

4 minimal cut sets of **size 2**

The size of minimal cut sets is less in **(A2)**, which means the situation is **more dangerous** and **drivers' control actions are more serious**.

Conclusions

- This paper applies the concept of **"safety control function"** to the derivation of accident sequence conditions of **railway systems** in the event tree analysis.
- The **decomposition** of a safety control function into **detection, diagnosis and execution** can simplify not only the **identification of safety control functions**, but also the **derivation of their failure conditions** including hardware and human actions.
- From the viewpoint of taking an effective countermeasure, the proposed method can clarify not only the **cognitive aspects of human action**, but also the **role of each component** in the overall system safety control function.
- **Depending on the initial condition**, the event tree expression can be easily modified.
- The **quantitative** analysis is our next step: **time dependency** and the **dynamical** system failure probability.

Accident Sequence Conditions

Accident sequence conditions for (A1):

{a1} **AND** {b1 **OR** b2 **OR** b3 **OR** b4} **AND** {c1 **OR** c2 **OR** c3 **OR** c4}

16 minimal cut sets of **size 3**

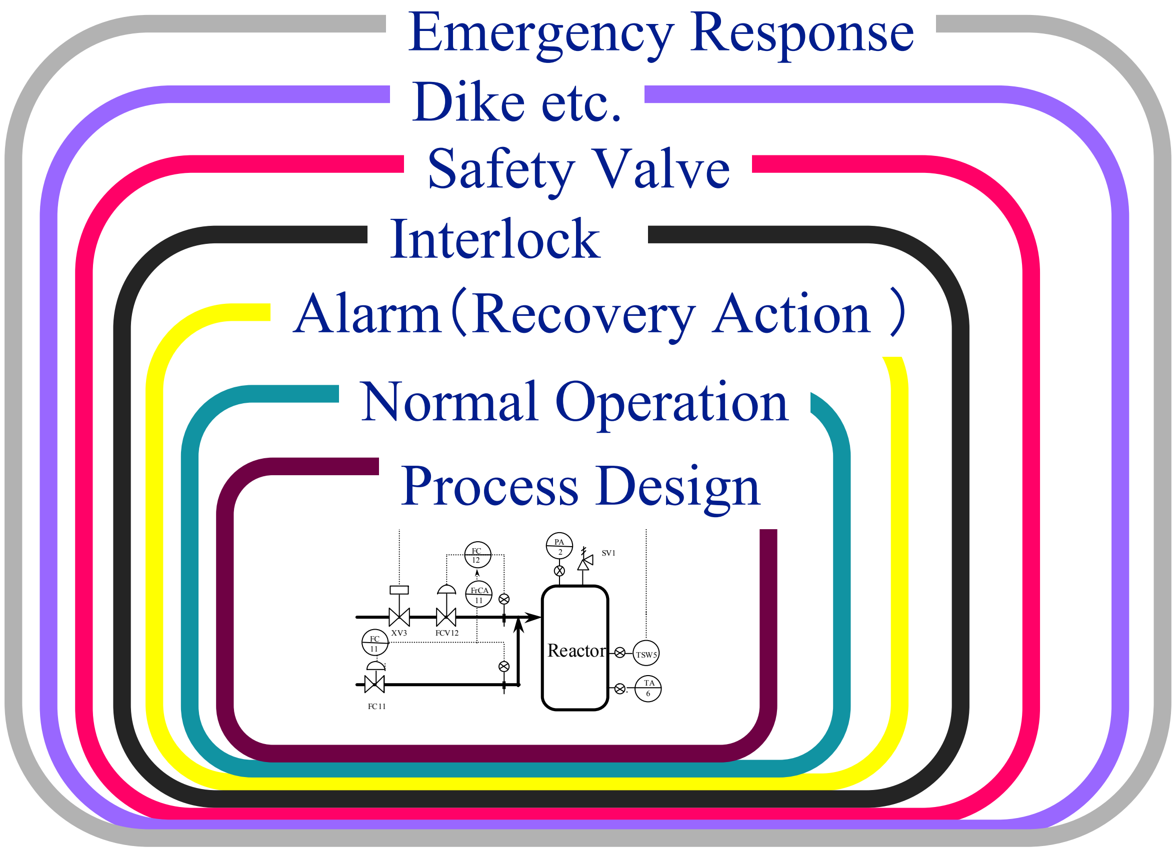
Accident sequence conditions for (A1):

{a1} **AND** {c1 **OR** c2 **OR** c3 **OR** c4}

4 minimal cut sets of **size 2**

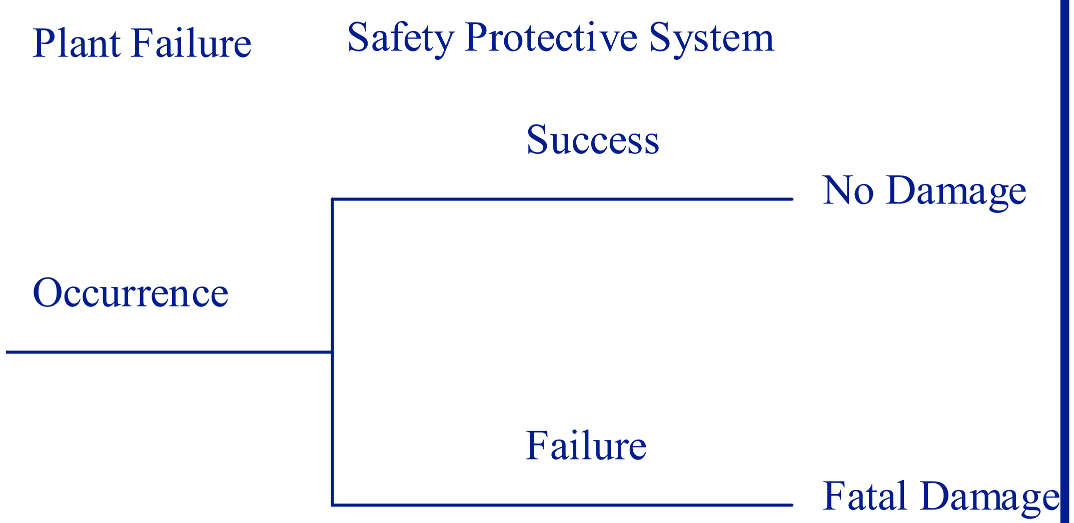
The size of minimal cut sets is less in **(A2)**, which means the situation is **more dangerous** and **drivers' control actions are more serious**.

Protective Systems:
“Defence in Depth” Approach



To prevent the occurrence of a system accident, several types of protective systems are installed in nuclear and chemical plants based on the concept of **“defence in depth”**.

Risk Reduction
by Safety Protective System



Accident Occurrence probability until overhaul maintenance time T:

$$F(T)=\int_0^T \boxed{\frac{dF^P(t)}{dt}F^S(t)}dt$$

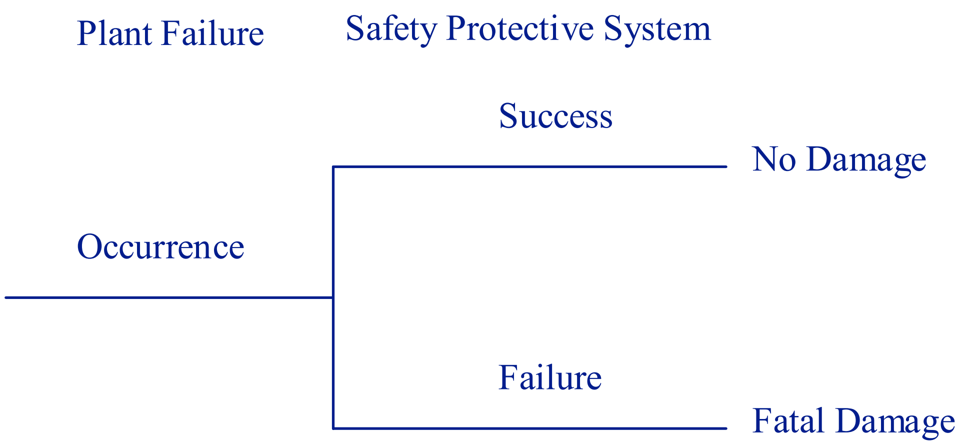
(Product of Time Average Value)

$$F^*(T) = \frac{F^P(T)\int_0^T F^S(t)dt}{T}$$

(Exponential Distribution)

$$F(T)=1- e^{-\lambda^P T} - \frac{\lambda^P}{\lambda^P+\lambda^S}\left(1-e^{-(\lambda^P+\lambda^S)T}\right) \qquad F^*(T) = \left(1-e^{-\lambda^P T}\right)\left(1-\frac{1-e^{-\lambda^S T}}{\lambda^S T}\right)$$

Risk Reduction
by Safety Protective System



Accident Occurrence probability until overhaul maintenance time T:

$$F(T)=\int_0^T \frac{dF^P(t)}{dt} F^S(t)dt$$

(Product of Time Average Value)

$$F^*(T) = \frac{F^P(T)\int_0^T F^S(t)dt}{T}$$

(Exponential Distribution)

$$F(T)=1- e^{-\lambda^P T} - \frac{\lambda^P}{\lambda^P+\lambda^S}(1-e^{-(\lambda^P+\lambda^S)T})$$

$$F^*(T) = (1-e^{-\lambda^P T})(1-\frac{1-e^{-\lambda^S T}}{\lambda^S T})$$

$T=8760(hr)$ $\lambda^P=0.00005(/hr)$
$\lambda^S=0.00005(/hr)$
$F^P(T)=0.043$
$F(T)=0.00091$
$F^*(T)=0.00092$

Risk Reduction Evaluation of Safety Protective Systems

Accident Occurrence Probability per Unit Time at Each Time Instant**:**

$$\frac{dF^{P}(t)}{dt}F^{S}(t)$$

(In Case of Exponential Distribution)

For $t<1/(\lambda^{P}+\lambda^{S})$, it is a monotonically increasing and becomes the largest at the end of the operation period.

For T=8760(hr) λ^{P}=0.00005(/hr) λ^{S}=0.00005(/hr)

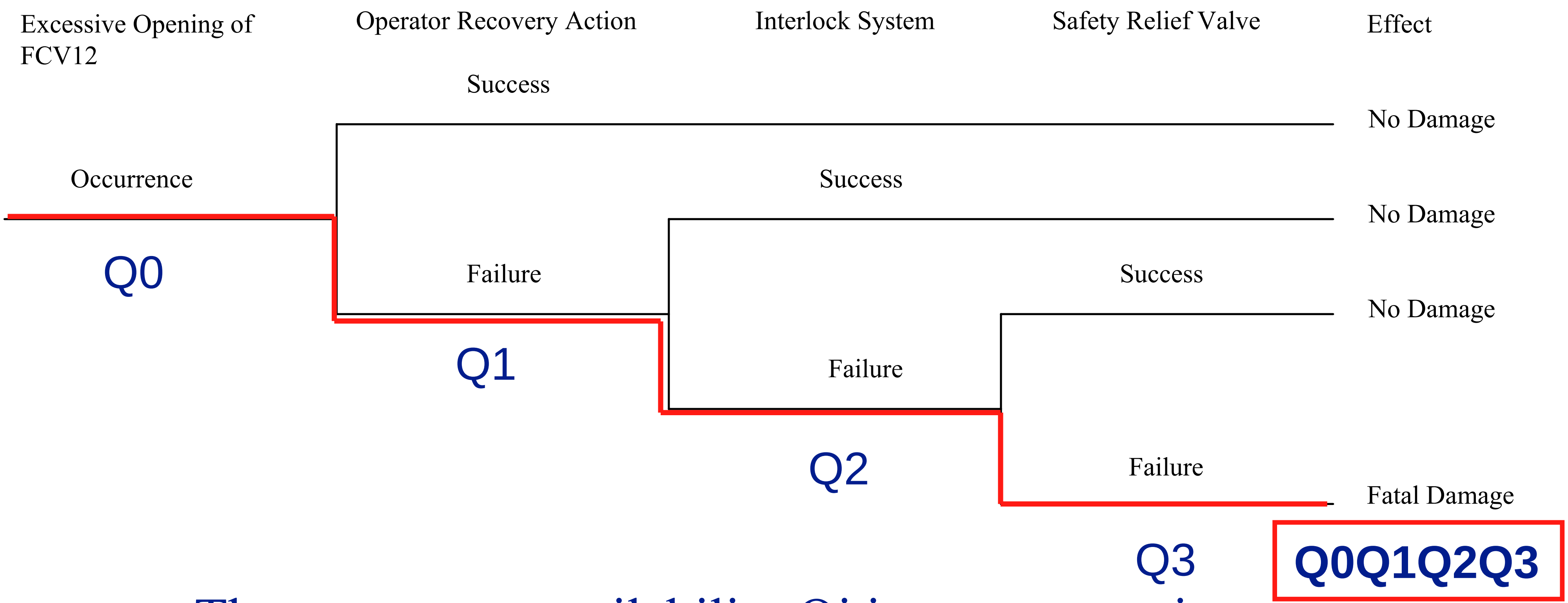
The maximum: 2.1×10^{-7} (/hr)

The average value: 1.0×10^{-7} (/hr)

Change of the accident occurrence probability during the operation period must be considered.

Accident Sequence Evaluation:

Event Tree Approach



The <u>average unavailability Qi</u> is not appropriate for the failure evaluation of the protective system.

This paper proposes **a dynamic evaluation** method of the accident occurrence probability..

On-Demand Failure Condition of Protective System

For a protective system to perform its function, the protective system must satisfy the following requirements:

(1) the **detection** of a plant failure

(2) the **selection** of an appropriate protective action

(3) the **performance** of the specified protective action

If any one of the requirements is not satisfied, the protective system gets failed: **On-Demand Failure Condition** is evaluated in terms of

(1) the **detection failure:** unavailability, active failure

(2) the **selection (diagnosis) failure:** unavailability, active failure

(3) the **performance (action) failure:** unavailability, active failure

Unavailability Condition

A plant failure occurring in the **unavailable state of a protective system** leads to a system accident.

(UA-1) the component is **failed** and its fault **cannot be detected**

(UA-2) the component is **under its inspection**

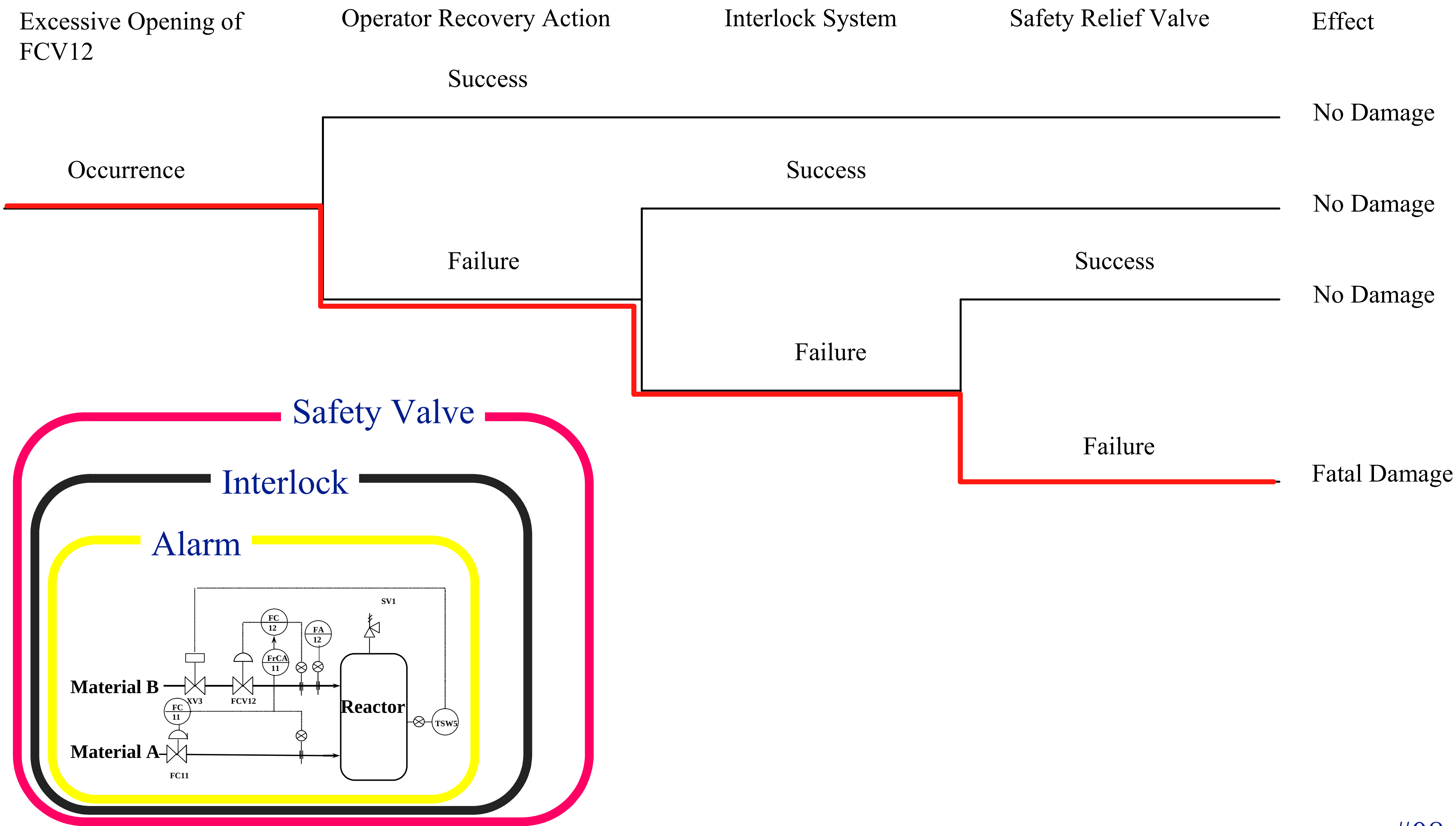
(UA-3) the component is **under its repair/maintenance**.

The **inspection and repair/maintenance** actions have much effect on the availability.

After the repair or maintenance, the system can resume **as good as new**.

The system state after the inspection depends on its result.
If the system is judged **as failed**, the system is **under repair**.
Otherwise, the system maintains the **status quo**.

Reactor System with Multiple Protective Systems



Occurrence Conditions for On-Demand Failure of Protective Systems and Initiating Event

Initiating Event: **Excessive Opening of FCV12**

{Failure of FCV12($\mathbf{X}^{FCV12}$)} {Failure of FC12($\mathbf{X}^{FC12}$)} {Failure of FS ($\mathbf{X}^{FS}$)}

Operator Recovery Action

{Failed-Dangerous Failure of Alarm System($\mathbf{X}^{FD}$)}
{Operator Failure to Detect the Alarm ($\mathbf{X}^{DE}$)}
{Operator Failure to Complete the Protective Action ($\mathbf{X}^{AE}$)}

Interlock System

{Failure of TSW5($\mathbf{X}^{TSW5}$)} {Failure of the Relay Circuit($\mathbf{X}^{RC}$)}
{Failure of XV3($\mathbf{X}^{XV3}$)}

Safety Relief Valve

{Failure of Safety Relief Valve($\mathbf{X}^{RV}$)}

Accident Occurrence Condition

Accident Occurrence:

All three protective systems fail against the excessive opening of FV12

$$\begin{pmatrix} X^{FCV12} \\ X^{FC} \\ X^{FS} \end{pmatrix}\begin{pmatrix} X^{FD} \\ X^{DE} \\ X^{AE} \end{pmatrix}\begin{pmatrix} X^{TSW5} \\ X^{RC} \\ X^{XV3} \end{pmatrix}\left(X^{RV}\right)$$

No common condition appears in all parentheses,
the accident occurrence probability can be evaluated as
the product of the occurrence probability of initiating event and on-demand failure probabilities of protective systems.

$$Q^{PSA}(t)=Q^{EIF}(t)Q^{ORA}(t)Q^{IL}(t)Q^{RV}(t)$$

On-Demand Failure of Operator Recovery Action

Operator recovery action fails if (1) the alarm system is unavailable, (2) operators are absent, (3) operators do not notice the alarm, or (4) operators fail to complete the recovery action.

$$\boxed{\begin{aligned} Q^{ORA}(t) &= Q^{UA}(t) + (1-Q^{UA}(t))Q^{UO} + (1-Q^{UA}(t))(1-Q^{UO}(t))Q^{PE}(t) \\ &\quad + (1-Q^{UA}(t))(1-Q^{UO}(t))(1-Q^{PE}(t))Q^{DE}(t) \\ &\approx Q^{UA}(t) + Q^{UO}(t) + Q^{PE}(t) + Q^{DE}(t) \qquad \text{if } Q^{UA}(t), Q^{UO}(t), Q^{PE}(t) \ll 1 \end{aligned}}$$

Unavailability of Alarm System: Periodic Inspection

$$Q^{UA}(t) = 1-(1-Q^{UFD}(t))(1-Q^{UAA}(t))$$

$$Q_i^{UFD}(t') = \begin{cases} 1-A_i^{FD}(t'), & \text{if } 0 \le t' < T^{FD} \\ 1, & \text{if } T^{FD} \le t' < T^{FD} + \tau^{FD} \end{cases}$$

$$Q_i^{UAA}(t') = 1-A_i^{AA}(t'), \qquad \mathit{for} \quad 0 \le t' < T^{AA}$$

$$\boxed{\begin{aligned} & A_0(t') = R(t') \\ & A_i(t') = R(t'+iT_i) + \sum_{j=1}^{i} FR_j A_{i-j}(t') \\ & \qquad\qquad\qquad\qquad \mathit{for} \quad i \ge 1 \\ & FR_j = R((j-1)T) - R(jT) \end{aligned}}$$

On-Demand Failure of Interlock System

The interlock system can be considered as a **series structure** of temperature switch TSW5, the relay circuit and shut-down valve XV3. All components can be inspected and repaired **only at the overhaul maintenance**.

$$\boxed{Q^{IL}(t) = 1 - (1 - Q^{UTS}(t))(1 - Q^{URC}(t))(1 - Q^{USV}(t))}$$

Unavailability: Failure Probability

$$Q^{UTS}(t) = F^{TS}(t) \qquad for\ 0 \le t < T^{OM}$$

$$Q^{URC}(t) = F^{RC}(t) \qquad for\ 0 \le t < T^{OM}$$

$$Q^{USV}(t) = F^{SV}(t) \qquad for\ 0 \le t < T^{OM}$$

On-Demand Failure of Safety Relief Valve & Initiating Event

The protective system is composed of **only the safety relief valve**, which can be maintained **only at the time of over-haul maintenance**.

$$\boxed{Q^{RV}(t) = F^{RV}(t) \qquad\qquad for \quad 0 \le t < T^{OM}}$$

The excessive input flow from FCV12 is caused by **the failure of the control loop composed of FCV12, flow controller, and flow sensor.** All these components are maintained **only at the time of overhaul maintenance.**

$$\boxed{Q^{EIF}(t) = \frac{d}{dt}\{1-(1-F^{FCV12}(t))(1-F^{FC}(t))(1-F^{FS}(t))\}dt}$$

Numerical Example

The time of each component failure follows the exponential distribution.

$$F^i(t) = 1 - \exp(-\lambda^i t)$$

$$A_i(t') = R(t'), \qquad for \quad i \geq 0$$

Q^{UO}	Q^{PE}	Q^{DE}	
0	0.0001	0.3	
T^{OM}	T^{FD}	τ^{FD}	T^{AA}
8640 (hrs.)	719.917 (hrs.)	0.083 (hrs.)	24 (hrs.)
λ^{FD}	λ^{AA}	λ^{RV}	
0.000118 (/hr.)	0.00000077 (/hr.)	0.00000168 (/hr.)	
λ^{TS}	λ^{RC}	λ^{SV}	
0.000097 (/hr.)	0.00000191 (/hr.)	0.0000487 (/hr.)	
λ^{FCV12}	λ^{FC}	λ^{FS}	
0.00000359 (/hr.)	0.0000012 (/hr.)	0.000118 (/hr.)	

System failure probability Q during the operation period:

Q = 0.000663

System failure probability Q’ **without protective systems**:

Q’ = 0.654

System failure probability Q” **without inspections**:

Q” = 0.00129

Numerical Example

The time of each component failure follows the **exponential distribution**.

$$F^i(t) = 1 - \exp(-\lambda^i t)$$

$$A_i(t') = R(t'), \quad for \quad i \geq 0$$

Q^{PE} 0.0001 Q^{AE} 0.3 T^{OM} 8640

T^{FD} 719.917 τ^{FD} 0.083 T^{AA} 719.917

τ^{AA} 0.083 λ^{FD} 0.000118

λ^{AA} 0.00000077 λ^{RV} 0.00000168

λ^{TS} 0.000097 λ^{RC} 0.00000191

λ^{SV} 0.0000487 λ^{FCV12} 0.00000359

λ^{FC} 0.0000012 λ^{FS} 0.000118

Accident Occurrence Probability per Unit Time:

Overall Average: 7.99×10^{-8} (1/hr)

Average During Operation Period
2.60×10^{-7} (1/hr)

Just Before Overhaul Maintenance
4.22×10^{-7} (1/hr)

Accident Occurrence Probability During Operational Period

Without Protection: 0.654

With Inspection 0.000691

Without Inspection 0.00129

Conclusions

- The accident occurrence condition can be obtained as the plant failure occurrence condition multiplied by **on-demand failure** (or **failure to respond the demand**) conditions of all protective systems.
- This paper proposes a **dynamic evaluation** of system accident occurrence probability.
- On-demand failure of a protective system is evaluated in terms of (1) its detection failure, (2) its selection (diagnosis) failure, and (3) its performance (action) failure.
  - **Analytic formula for availability** evaluation of a component **with periodic inspection** is given, whose result depends on its repair action,.
- We are now extending the proposed framework to a more practical situation.

Component Availability with Periodic Maintenance

Assumptions

(1) The entire system composed of plant and protective systems is as good as ne w at time 0 when it begins to operate.

(2) After the overhaul maintenance, the entire system resumes as good as new.

(3) The entire system is maintained as good as new if a system accident is preven ted without fatal damage.

(4) Components fail statistically independently.

(5) An inspection of some component is performed periodically to confirm its no rmal condition. If the inspection result shows some fault, it is repaired with t he entire system halted and resumes as good as new while other components maintain their status quo. Otherwise, it maintains the status quo, i.e., it is as g ood as before the inspection.

(6) Any component without periodic inspections is repaired at the overhaul mainte nance and resumes as good as new.

(7) Any component of a protective system can achieve its role, if it succeeds in a