



# *Functional Safety #2:* *Verifying the SIL of a Transport Braking System*

Presented by Marcus Punch  
Hatch Associates Pty Ltd. (Newcastle)  
7 Warabrook Bld, Warabrook NSW 2304  
PO Box 5000, Hunter Mail Centre NSW 2310  
Phone : +61 (0)2 4968 6879, Fax: +61 (0)2 4968 6800, Mobile +61 (0)434 603720,  
Email : [mpunch@hatch.com.au](mailto:mpunch@hatch.com.au)

## The Requirement



### SAFETY ALERT

#### Maintenance of Safety Critical Systems - Braking, Steering & Warning Systems

3. All safety critical systems have been assessed and the appropriate integrity level applied in accordance with AS 4024, AS 62061, AS 61508 or other similar standards.
4. A Failure Modes and Effects Analysis (FMEA) or other similar risk assessment method has been carried out to confirm the integrity of all safety critical systems.



# Summary of Findings – Part

1

System	CAT	SIL
Service / Emergency Brake	CAT3	SIL3 (high demand) PFH < 0.0000001
Retarder	CAT2/3	SIL2 (low demand) PFD < 0.01

Safety Systems

## AS/IEC61508 Process

### PRE-DESIGN

(Phases 1 to 5)

1. Concept
2. Scope
3. Risk Analysis
4. Overall safety requirements
5. Allocate safety requirements

### DESIGN AND INSTALLATION

(Phases 6 to 13)

- 6-8. Plan
- 9-11. Design
12. Install & Commission
13. Validate

### OPERATION

(Phases 14 to 16)

14. Operate & Maintain
15. Modify & Retrofit
16. Decommission

# AS/IEC61508 SIL3 Verification

**Depending on the SIL allocated, there are specific requirements for:**

## Architecture (configuration)

- Hardware Fault Tolerance (HWFT) (eg. redundancy, single points of failure), and
- Safe Failure Fraction (SFF) (ie. % of failures that are not dangerous and undetected)

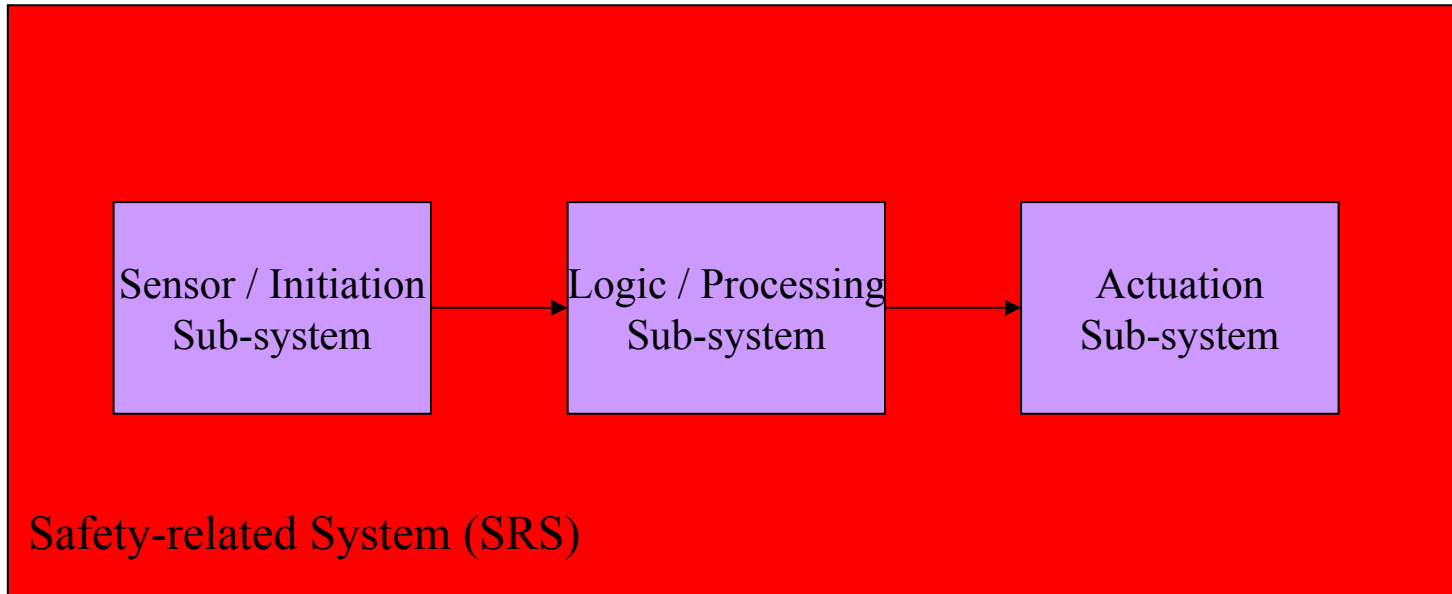
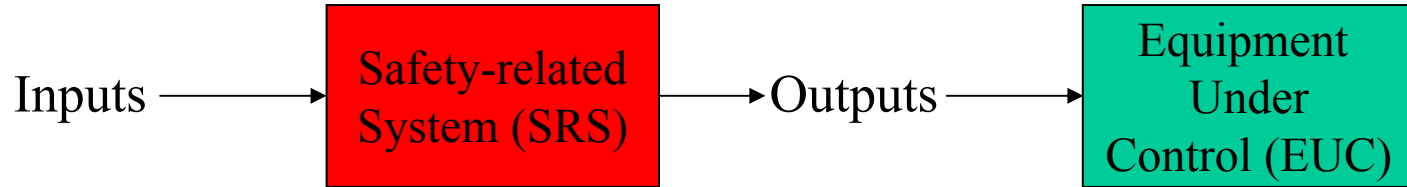
## Reliability

- Probability of Failure on Demand (PFD), or
- Probability of Dangerous Failure Per Hour (PFH),

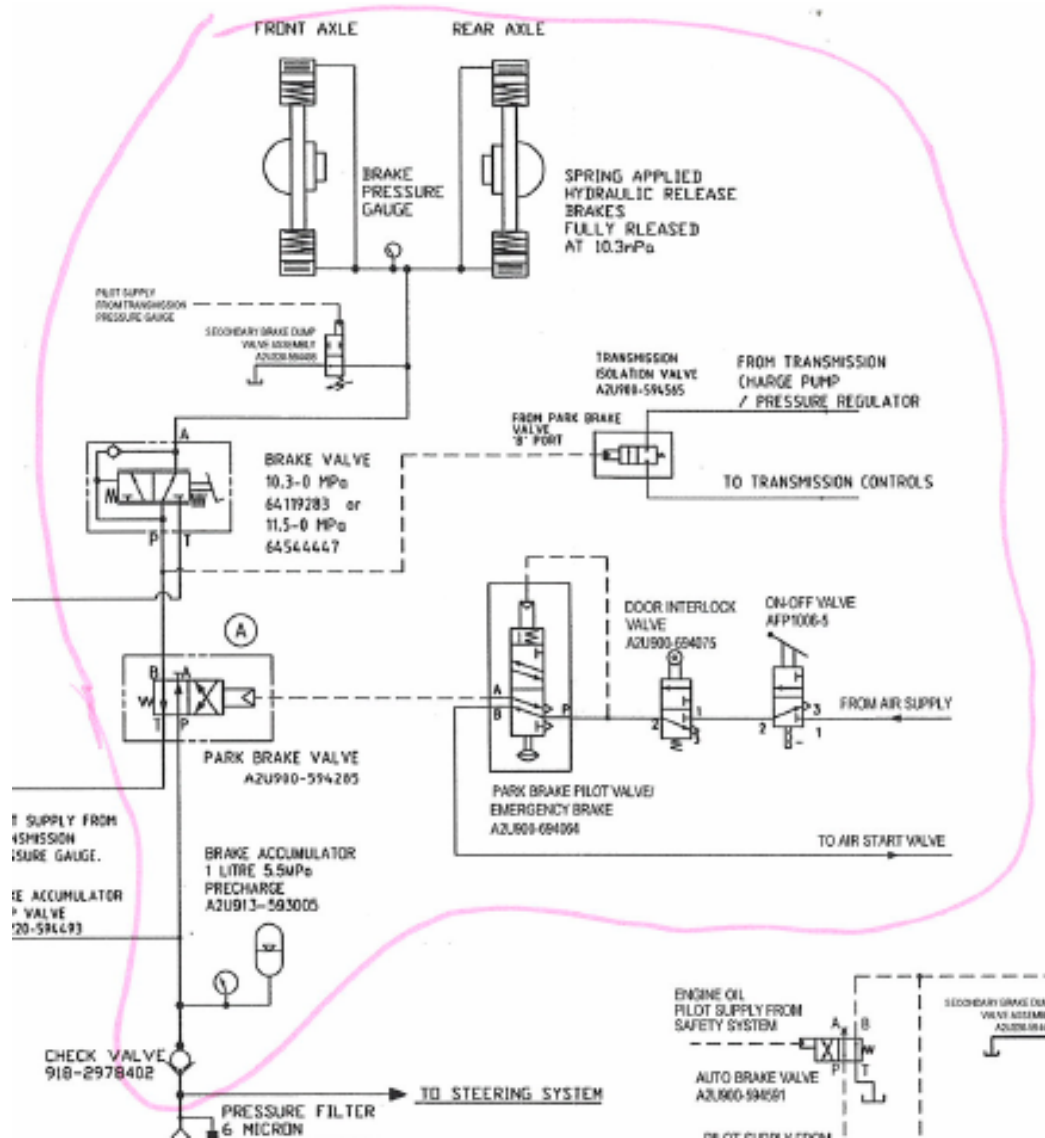
## Measures and Techniques to Avoid Systematic Failures

1. Hardware, and
2. Software.

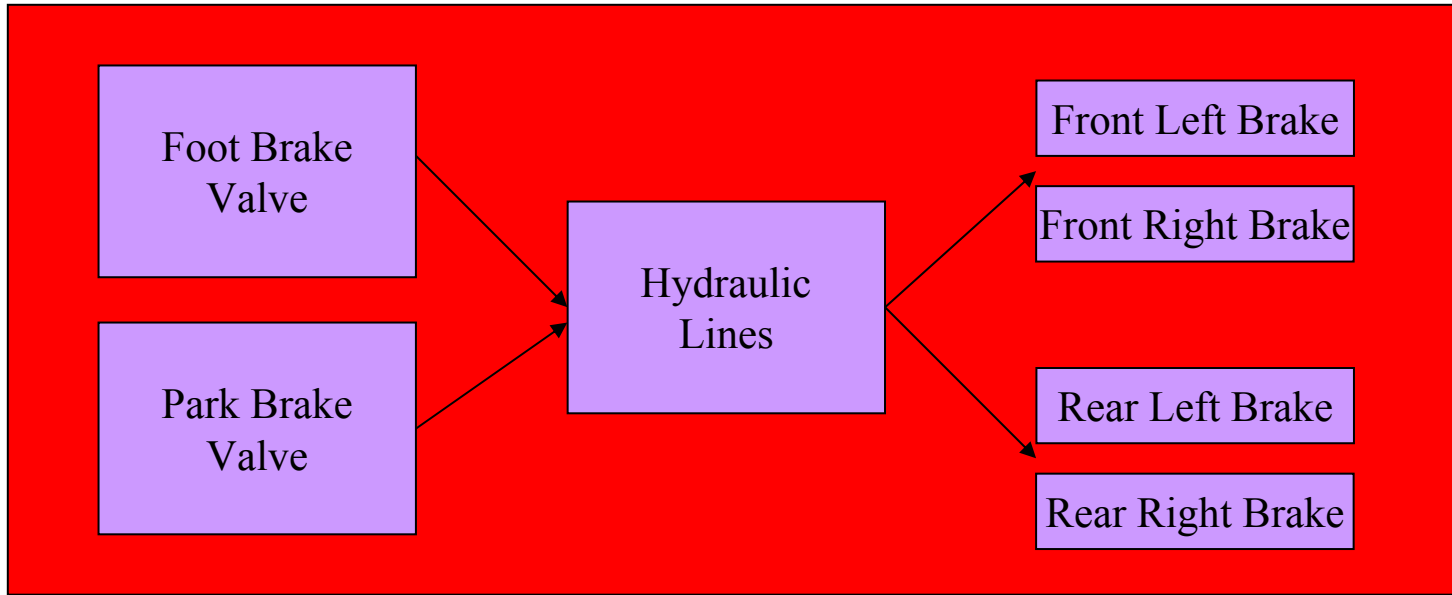
# Safety System Architecture



## Safety System Architecture



# Safety System Architecture



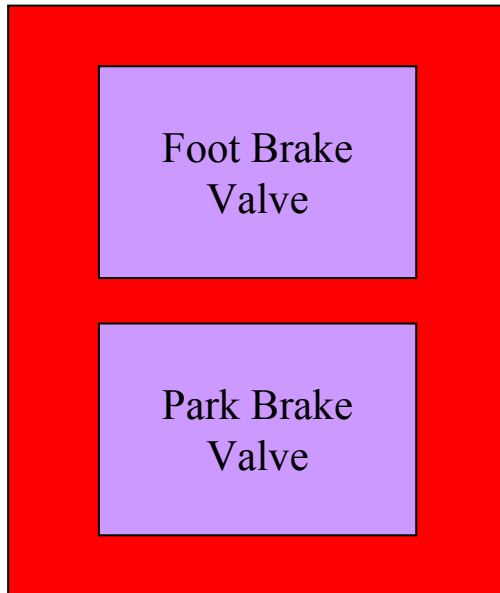
**Sensor/Initiation**

**Logic/Processing**

**Actuation**

## Safety System Architecture

Safe failure fraction	Hardware fault tolerance (see note 2)		
	0	1	2
< 60 %	Not allowed	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL4
≥ 99 %	SIL3	SIL4	SIL4



Eg. Initiation Sub-system

HWFT = 1 (redundant means of initiation)

For SIL3, SFF of each 'channel' must be ≥ 90%

(SFF is calculated during the reliability analysis)

## Safety System Architecture

### Initiation Sub-system

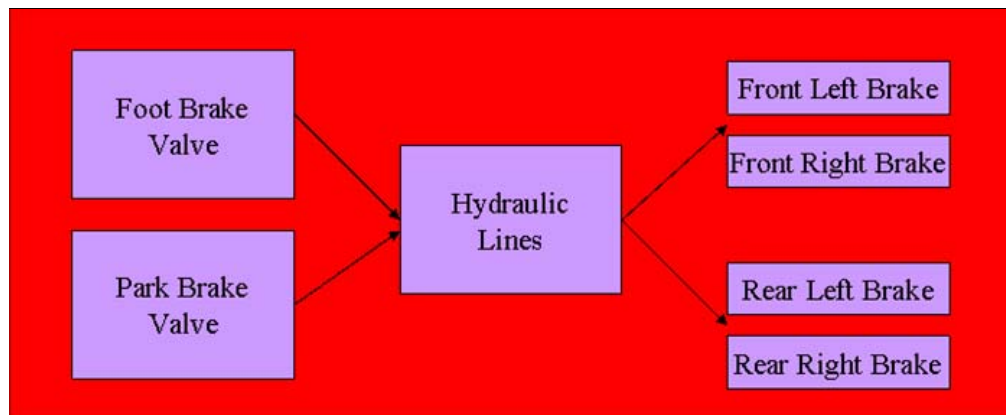
HWFT = 1, for SIL3, SFF of each 'channel' must be  $\geq 90\%$ .

### Logic / Processing Sub-system

HWFT = 0, for SIL3, SFF must be  $\geq 99\%$

### Actuation Sub-system

HWFT = 2, for SIL3, SFF of each 'channel' must be  $\geq 60\%$ .



# Safety System Reliability

## “High Demand” Mode

The frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof test frequency.

<u>SIL</u>	<u>Probability of Dangerous Failure per Hour (PFH)</u>
4	$PFH < 10^{-08}$
3	$10^{-08} \leq PFH < 10^{-07}$
2	$10^{-07} \leq PFH < 10^{-06}$
1	$10^{-06} \leq PFH < 10^{-05}$

For a single component, generally  $PFH \approx \lambda (1 - SFF)$   
(from AS/IEC61508, Part 6)

Where:

$\lambda$  = total failure rate of the component (per hour)

SFF = Safe Failure Fraction

(the % of failures that are not dangerous undetected)

## Safety System Reliability

- Total failure rate of a component,  $\lambda$ , is determined from failure records, supplier data, industry databases or from staff knowledge.
- For mechanical components,  $\lambda$  may be dependent on the inspection interval applied.
- Safe Failure Fraction, SFF, is usually determined via an Failure Modes, Effects & Diagnostic Analysis (FMEDA)
- The overall PFH of the safety system is determined via a reliability analysis, taking account of all component failure rates, SFF's, redundancies, inspection intervals, common-cause failures etc... → this is usually determined via a Fault Tree Analysis (FTA).

## Failure Modes, Effects & Diagnostic Analysis (FMEDA)

### Purpose

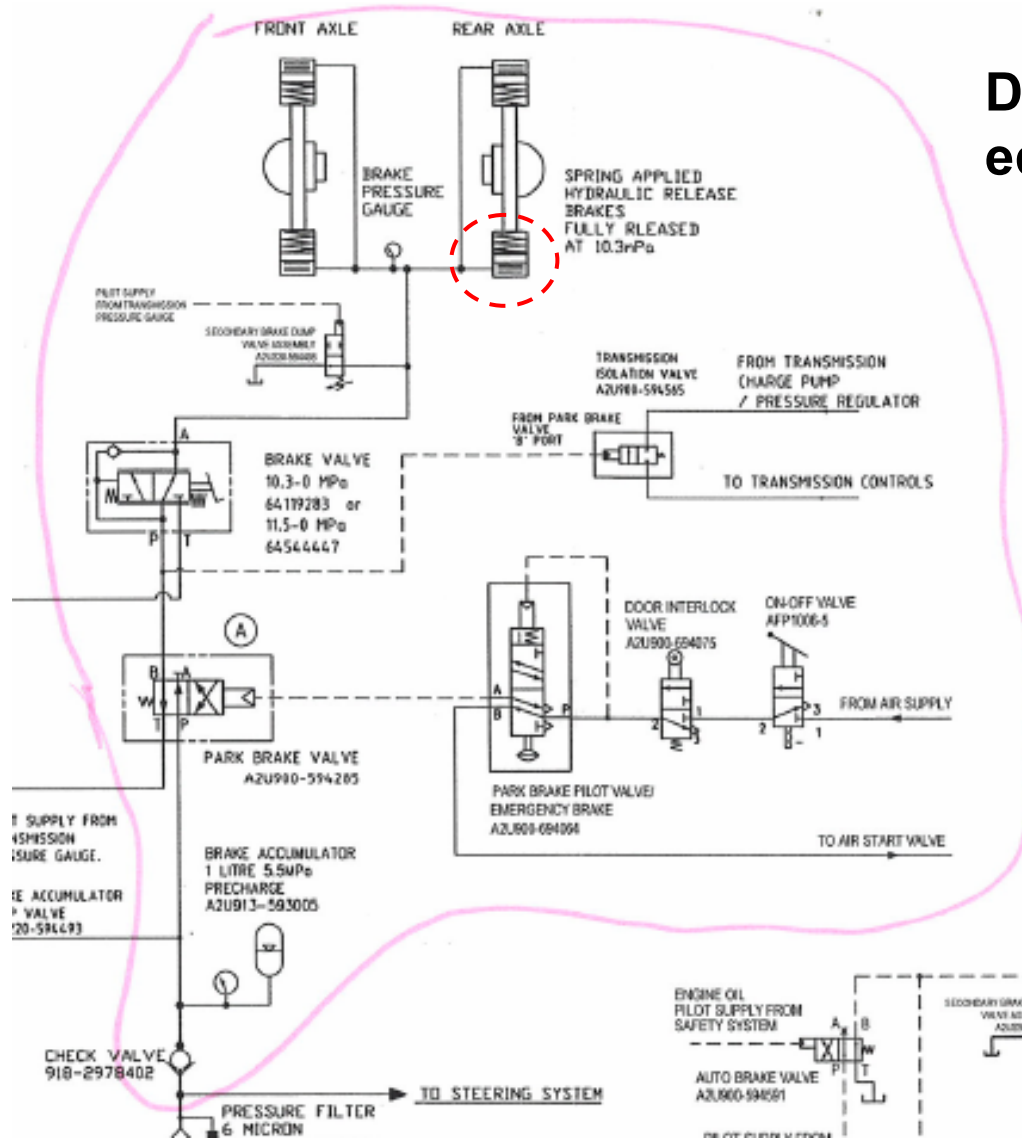
- Identifies the possible ways a safety system can fail to perform its designed function/s and the consequences of those failures.
- Identifies measures that can be taken to detect or prevent the failures or reduce the severity of the consequences.
- Incorporates information to allow the Safe Failure Fraction (SFF) to be calculated.
- Very similar process to FMEA, but includes numerical calculations.

### Guidance on FMEDA & SFF Calculation:

AS/IEC61508 Part 6

AS/IEC61508 Part 2, Annex C.

## Braking System FMEDA



Define functions and equipment breakdown

# Braking System FMEDA

## Hub mounted brake unit

Failure Mode	Failure Mode Apportionment of Failure Rate	Effect on Safety Function	Safe Failures (%)	Detection Method / Diagnostics	Detectable Failures (%)
Broken Spring	5%	Braking force reduced	50%	Inspection/testing	0%
Incorrect Oil	10%	Loss of braking	0%	Inspection/testing	0%
Worn Linings	80%	Braking force reduced	50%	Onset detectable by brake lining indicators	100%
Stuck Piston	5%	Loss of braking	0%	Inspection/testing	0%

**Results of FMEDA: SFF = 83%**

Note: previous slide on architectural constraints requires  $SFF \geq 60\%$  for brake system actuators.

# Safety System Reliability

## Hub mounted brake unit

- Manufacturer quotes an MTBF figure for each brake unit of 2,000,000 operations.
- MTTR assumed to be 10 hrs.
- In Part 1 the LOPA assumed 350,400 brake operations per year.
- So,  $MTBF = 2,000,000 / 350,400 = 5.71 \text{ years} = 50,000 \text{ hrs.}$
- So, the failure rate,  $\lambda = 1 / 50,000 \text{ hrs} = 0.00002 / \text{hr}$
- From AS61508, Part 6:  $\lambda_{\text{dangerous-undetected}} = \lambda \times (1 - SFF)$
- The FMEDA yielded an  $SFF = 83\%$ .
- $\lambda_{\text{dangerous-undetected}} = 0.00002 \times (1-0.83) = \underline{0.0000034 / \text{hr}}$

# Safety System Reliability

## Hub mounted brake unit

$$\lambda_{\text{dangerous-undetected}} = 0.00002 \times (1-0.83) = \underline{0.0000034 / \text{hr}}$$

- Brake inspections are carried out every 12 months (8760 hrs).
- **NB:** If a dangerous undetected failure occurs (or is occurring) it may not be found for up to 12 months.
- For a single brake unit, the probability of a dangerous undetected failure occurring between inspections:
  - If annual inspections is = 2.93%.
  - If quarterly inspections = 0.74%.
  - If monthly inspections = 0.25%.
  - If weekly inspections = 0.06%.
  - If daily inspections = 0.01%
  - If never inspected = 100%.

# Safety System Reliability

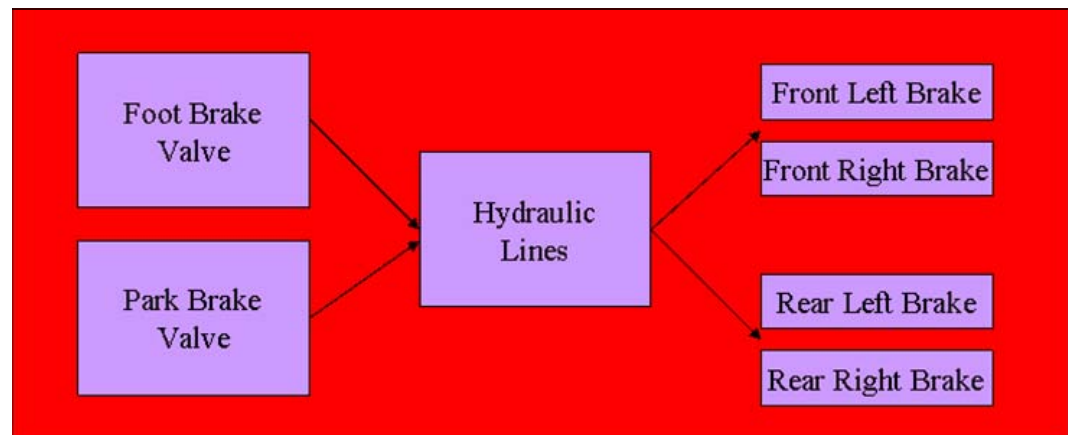
## Hub mounted brake unit

$$\lambda_{\text{dangerous-undetected}} = 0.00002 \times (1-0.83) = \underline{0.0000034 / \text{hr}}$$

- Brake inspections are carried out every 12 months (8760 hrs).

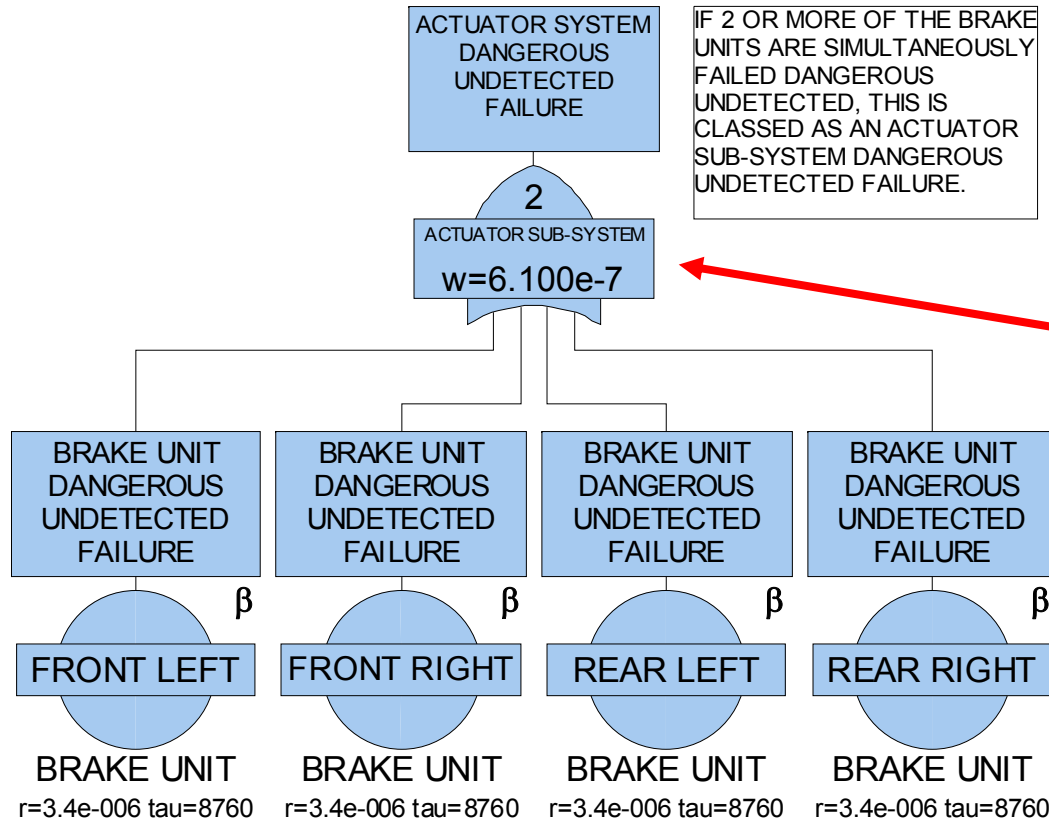
But what is the PFH for a 2-out-of-4 configuration of brake units?

And does it meet SIL3?



## Safety System Reliability

### Eg. Actuation Sub-system (with annual inspections)



PFH is in SIL2 range

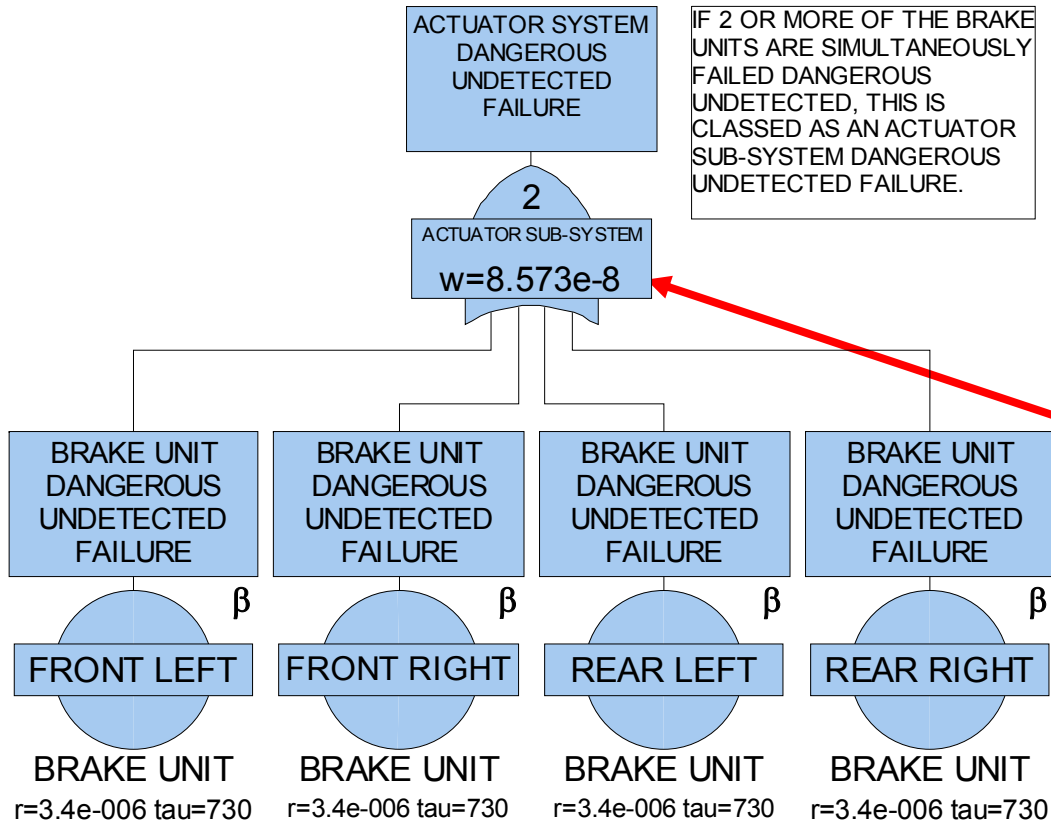
ie.  $< 0.000001$

But not much allowance for failure in other parts – brake valves and hydraulic lines etc...

THESE ARE IDENTICAL BRAKE UNITS AND ARE THEREFORE SUBJECT TO COMMON CAUSE FAILURES (CCF) THROUGH THEIR DESIGN AND THROUGH OPERATION AND MAINTENANCE. A CCF BETA FACTOR MUST BE APPLIED TO CORRECTLY CALCULATE THE PFH.

## Safety System Reliability

### Eg. Actuation Sub-system (monthly inspections)



THESE ARE IDENTICAL BRAKE UNITS AND ARE THEREFORE SUBJECT TO COMMON CAUSE FAILURES (CCF) THROUGH THEIR DESIGN AND THROUGH OPERATION AND MAINTENANCE. A CCF BETA FACTOR MUST BE APPLIED TO CORRECTLY CALCULATE THE PFH.

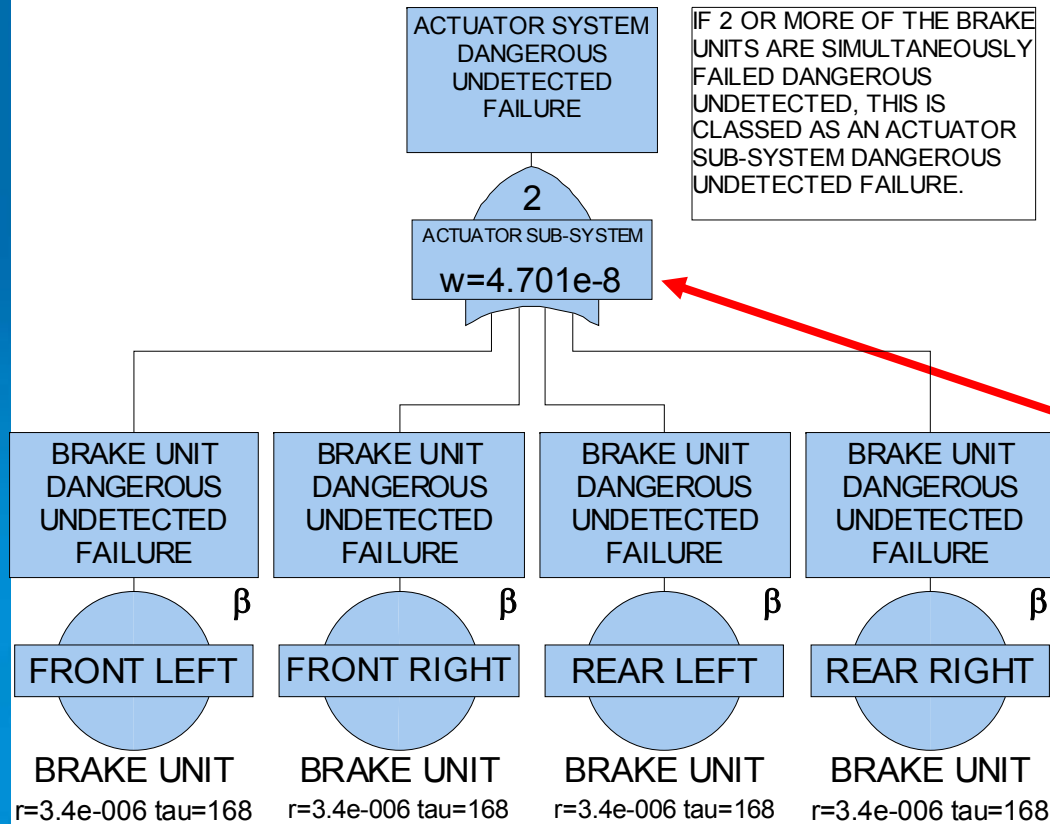
PFH is in SIL3 range

ie.  $< 0.0000001$

But not much allowance for failure in other parts – brake valves and hydraulic lines etc...

## Safety System Reliability

### Eg. Actuation Sub-system (weekly inspections)



THESE ARE IDENTICAL BRAKE UNITS AND ARE THEREFORE SUBJECT TO COMMON CAUSE FAILURES (CCF) THROUGH THEIR DESIGN AND THROUGH OPERATION AND MAINTENANCE. A CCF BETA FACTOR MUST BE APPLIED TO CORRECTLY CALCULATE THE PFH.

PFH is in SIL3 range

ie.  $< 0.0000001$

Better allowance for other failures, but what is the effect on availability of the vehicle, manpower, costs etc...

## Systematic Failure Avoidance

- Systematic failures are usually only found when something goes wrong, eg...
  1. Intended use misunderstood,
  2. Incorrectly specified,
  3. Imprecise drawings or documentation to designer,
  4. Residual faults in the design of hardware or software,
  5. Environmental stresses,
  6. Operator/maintainer error,
- These failures are avoided by good design practices, using competent people, operating equipment within design parameters, suitable levels of testing, checking etc..
- AS/IEC61508 Part 2 and 3 has a number of techniques that can be adopted to assist in the avoidance of systematic errors.

# Systematic Failure Avoidance

For mechanical systems, suggested guidance is:

- Use AS61508, Part 2, Annex B for general measures against systematic failures introduced via specification, design, integration, etc...
- Apply the basic and well-tried safety principles of AS4024 Part 1502, Appendices A, B and C for mechanical, pneumatic and hydraulic systems.

## Systematic Failure Avoidance

Use AS61508, Part 2, Annex B for general measures against systematic failures introduced via specification, design, integration, etc.

**Table B.2 – Recommendations to Avoid Introducing Faults During Design and Development**

Technique / Measure Utilised	SIL3 Requirement
Observance of guidelines and standards	HR Mandatory
Project Management	HR Medium
Documentation	HR Medium
Structured Design	HR Medium
Modularisation	HR Medium
Use of well-tried components	R Medium

# AS/IEC61508 SIL3 Verification

## Key Points:

- Functional safety design is focussed on eliminating / preventing dangerous undetected failures.
- Never underestimate the effect of appropriate and timely maintenance on safety system PFH.
- Never underestimate the effect of using high reliability parts to simultaneously achieve conflicting targets on plant availability, cost and safety.
- For new equipment / modifications, ensure suppliers provide reliability information.
- Keep records on in-service failures and confirm the SIL achieved.

Next.....

Functional Safety #3:

Verifying the CAT of a Transport Braking System