



Functional Safety #3: Verifying the CAT 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

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.



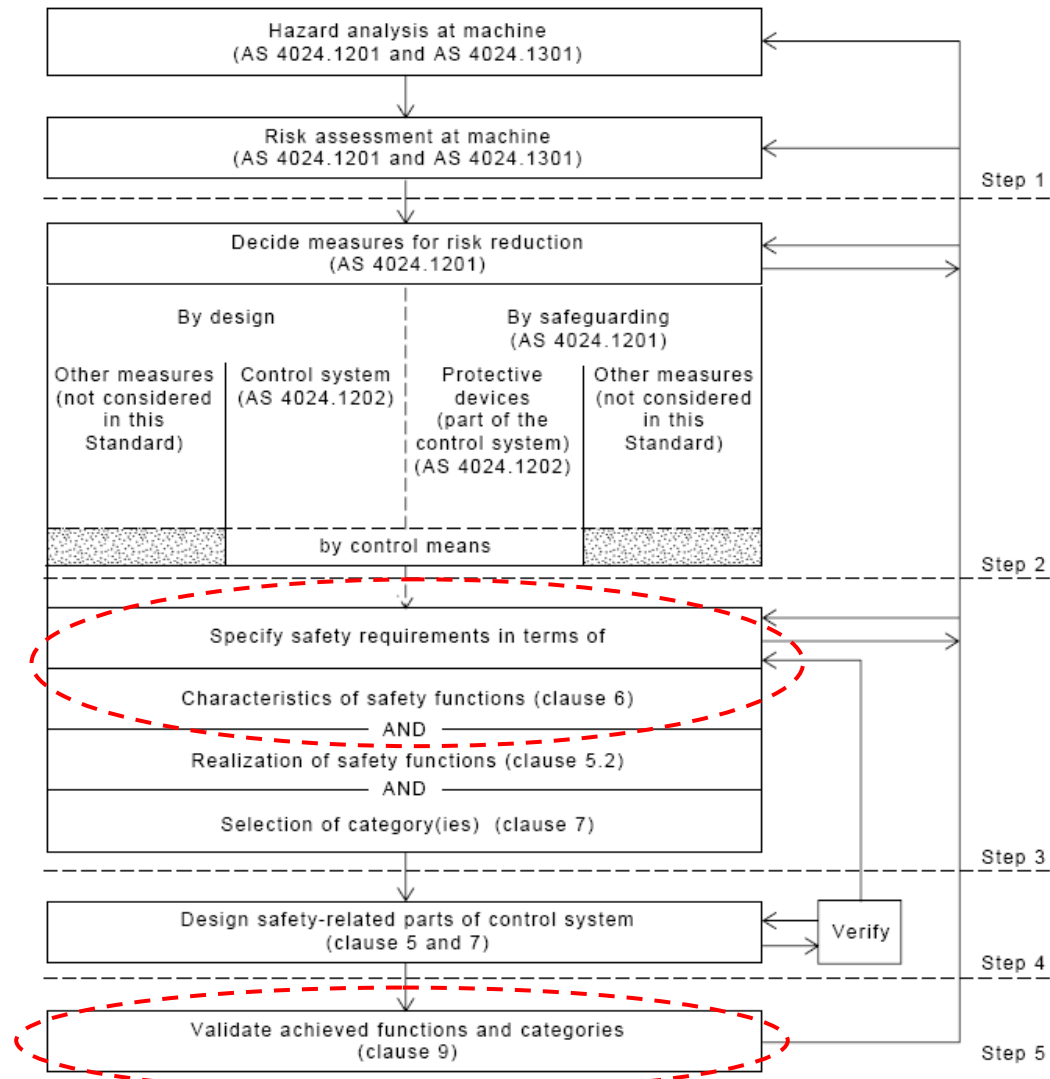
Summary of Findings – Part

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

AS4024 Process



AS4024 CAT3 Design Requirements

See AS4024.1501, Clause 7.

Category 3

The requirements of Category B, the use of well-trying safety principles and the following requirements shall apply:

- (a) Safety-related parts of control systems to Category 3 requirements shall be designed so that **a single fault in any of these parts does not lead to loss of the safety function.***
- (b) Common-mode faults shall be taken into account when the probability of such a fault occurring is significant.*
- (c) Whenever reasonably practicable, **the single fault shall be detected at or before the next demand upon the safety function.***

Category 3 system behaviour allows that:

- (i) when a single fault occurs, the safety function is always performed;*
- (ii) some but not all faults will be detected; and*
- (iii) accumulation of undetected faults can lead to loss of the safety function.*

AS4024 CAT3 Validation Requirements

- Validation consists of applying analysis and, if necessary, executing tests (see AS4024.1502, Clause 4.1).
- Validation by analysis rather than testing requires the formulation of 'deterministic arguments' (see AS4024.1502, Clause 5.1).
- Deterministic arguments show that the required properties of a system follow logically from a model of the system.
- Analysis usually involves either a top-down technique such as Fault Tree Analysis (FTA), or a bottom-up technique, such as Failure Modes and Effects Analysis (FMEA) (see AS4024.1502, Clause 5.2).
- When validation by analysis is not sufficient, testing shall be carried out. Testing is complementary to analysis (see AS4024.1502, Clause 6.1).
- Validation should be carried out by independent persons – the degree of independence should reflect the integrity required of the safety system.

AS4024 CAT3 Validation Requirements

CAT3 safety systems shall be validated by demonstrating the following (See AS4024.1502 Clause 8.2.4):

1. Meets requirements of CAT B,
2. Well-trying safety principles have been implemented correctly,
3. A single fault does not lead to the loss of the safety function,
4. Single faults shall be detected at or before the next demand on the safety function, where reasonably practicable.

AS4024 CAT3 Validation

Requirements

Item1 - Requirements of CAT B

(see AS40234.1501, Clause 7.2.1)

The safety-related parts of control systems shall, as a minimum, be designed, constructed, selected, assembled and combined, in accordance with the relevant Standards, using **basic safety principles** for the specific application so that they can withstand:

- (a) expected operating stresses, e.g. force and frequency of braking;
- (b) influence of the processed material, e.g. resistance of a braking system to coal dust; and
- (c) other relevant external influences, e.g. mechanical vibration, heat, power supply interruptions etc....

Basic Safety Principles

(see AS4024.1502, Appendix A, Table A1).

Eg. de-energisation principle, proper fastening, simplification, separation from other machine functions,

AS4024 CAT3 Validation Requirements

**Item 2 - Well tried safety principles
(see AS4024.1502 Appendix 2, Table A2)**

Eg.

Over-dimensioning,

Carefully selected materials and manufacturing,

Positive mechanical action,

Multiple redundant parts,

AS4024 CAT3 Validation Requirements

Items 3 & 4 - Single Faults

1. Must not affect operation of the safety function,
2. Must be detected, where reasonably practicable, before or at the next demand.

These qualities may be confirmed via a **Failure Modes and Effects Analysis (FMEA)** of the proposed braking circuit.

Failure Modes and Effects Analysis (FMEA)

Purpose

- Identifies the possible ways equipment or systems can fail to perform their designed functions 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.
- Identifies issues for the purpose of improving design.
- If criticality (risk) is to be considered, then it is called a FMECA – Failure Modes, Effects and Criticality Analysis)

Standards for FMEA / FMECA:

IEC60812

BS5760

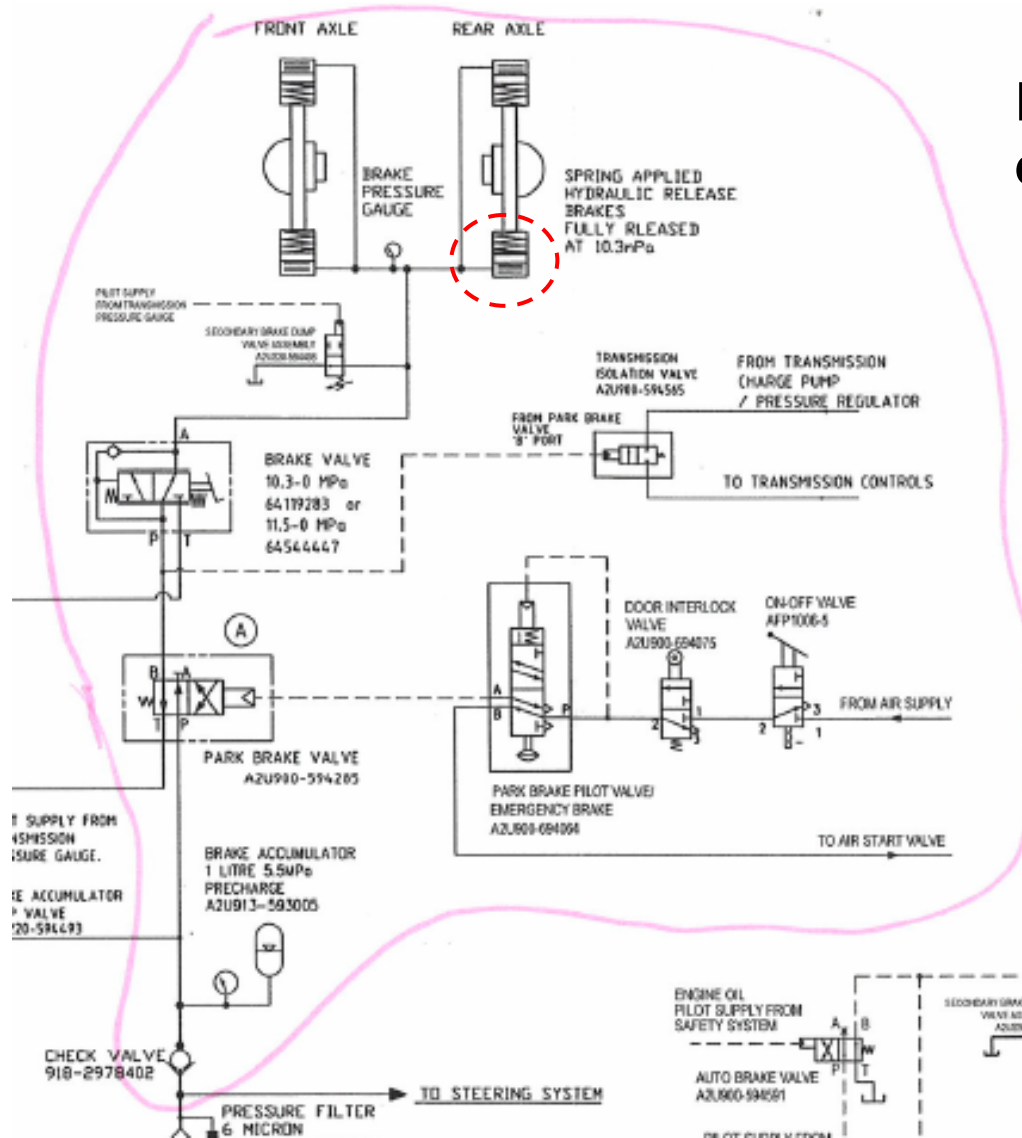
MIL-STD-1629A

FMEA Process

1. Functions:
 - Define the system to be analysed and its functions.
 - Define what constitutes a failure of those functions.
 - Break the system down into a functional or hardware hierarchy.
 - Construct 'functional block diagrams' (FBD's) for the system.
2. Failure Modes: Identify the causes of failure at equipment or component level or at interfaces which lead to failure of functions.
3. Effects: Determine the effects of those failure modes at component, equipment / sub-system and system level.
4. Compensating Provisions: Document existing compensating provisions (risk controls). Identify additional compensating provisions and/or corrective actions required.
5. Detection: Document how each failure mode can be detected.
6. Recommendations / Conclusions:
 - Make an overall judgment on whether the requirement/s have been met.
 - Create a system improvement action list.

Braking System FMEA

Define functions and equipment breakdown



Braking System FMEA

Hub mounted brake unit

Failure Mode	Effect on Safety Function	Compensating Provisions	Detection Method
Broken Spring	Braking force reduced	4 brake units installed. Routine testing.	Inspection.
Incorrect Oil	Loss of braking	Use only OEM recommended lubricants. Routine testing and replacement.	Inspection.
Worn Linings	Braking force reduced	Routine testing. Wear indicators installed.	Indicating device.
Stuck Piston	Loss of braking	4 brake units installed. Routine testing and lubrication.	Inspection.

Braking System FMEA (FMECA)

Criticality Analysis (not essential) allows prioritisation of actions.

Risk	Item	Component	Failure Mode
3	5.2	Brake Dump Valve	Stick closed
3	5.7	Brake Dump Valve	Tank line blocked
3	12.6	Brake valve (foot)	Check valve in valve fails open
3	12.7	Brake valve (foot)	Check valve in valve fails closed
4	5.4	Brake Dump Valve	Failure of pilot signal - pilot pressure always maintained
4	7.2	Park Brake Valve	Spool stuck in brake release position
4	7.4	Park Brake Valve	Pilot fails to apply brakes
4	7.7	Park Brake Valve	Tank line crimped or blocked
4	8.11	Park Brake Pilot Valve	Latch circuit hose crimped or blocked
4	8.8	Park Brake Pilot Valve	Hose attached to A port crimped or blocked
4	9.4	Door Interlock Valve	Door latch works loose and allows door to open.

Braking System FMEA

Actions / Recommendations

Add test for application on engine shutdown to Brake test procedure

Consider moving brake dump valve to between service brake valve and brake units to provide parallel path, should simultaneous failure of park brake valve and check valve in service brake valve occur.

Fit mechanical latch that operator must engage to allow brake to be released. 2. Move valve to hinge area, put additional valve in series mounted on door operated by latch.

Consider moving brake dump valve to between service brake valve and brake units to provide parallel path, allowing automatic brake on engine shutoff to work.

Consider engine shutdown on low hydraulic oil level.

Next.....?

Obtain a judgement:

1. Meets requirements of CAT B,
2. Well-tried safety principles have been implemented correctly,
3. A *single fault does not lead to the loss of the safety function*,
4. Single faults *shall be detected at or before the next demand* on the safety function, where *reasonably practicable*.

