Safety Engineering for Railway Control & Communications Systems

An introductory guide for candidates taking Module A of the IRSE Professional Examination

R Short

February 2021

Part 1: Safety Principles

This part should be treated as an addendum to the item in the Module A reading list entitled "Back to Basics - Principles of Railway Safety Engineering, IRSE News, Issue 267, June 2020“ which explains the identification and analysis of hazards and risks.

Hazard, Risk and Safety Requirements

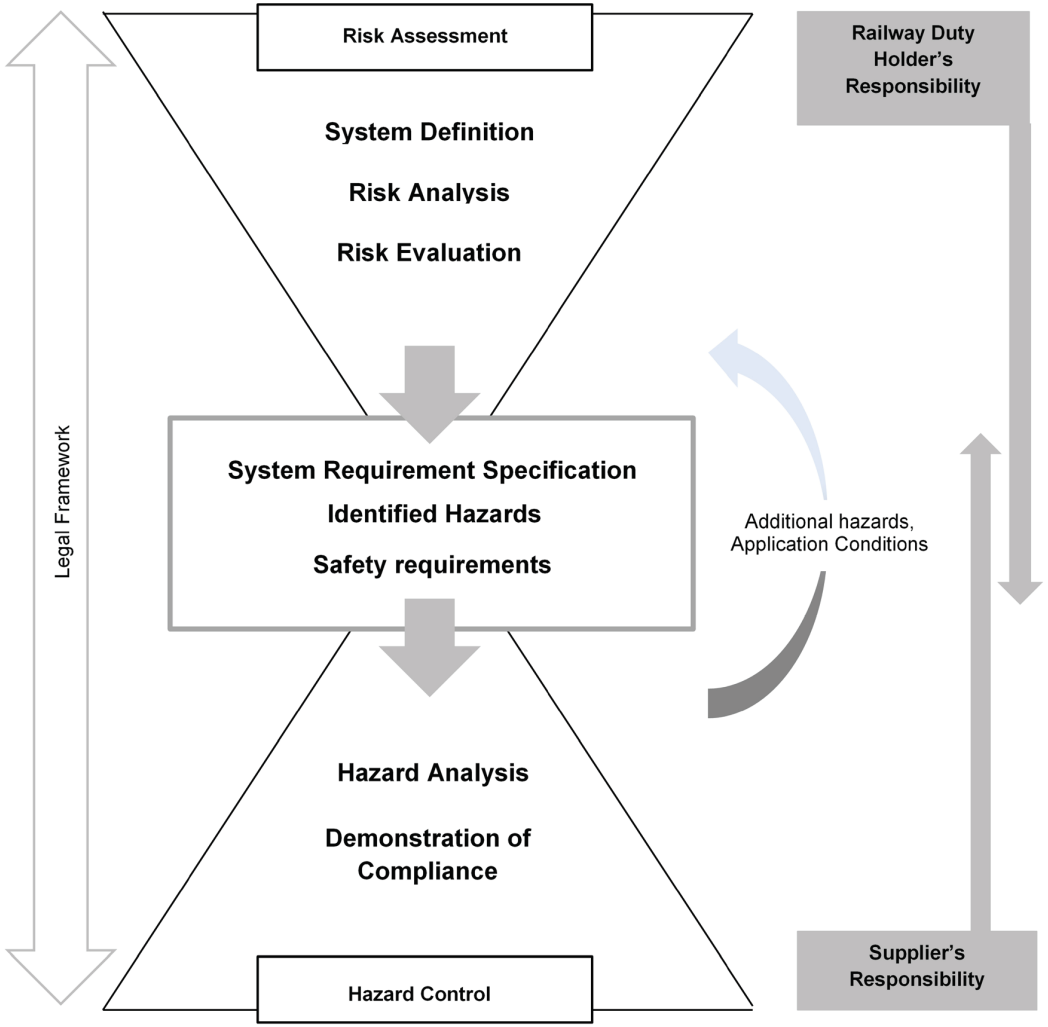
It is essential to derive a complete and correct specification of safety requirements as part of system development.

Systematic identification of hazards generally involves two phases:

- an empirical phase (exploiting past experience, e.g. checklists)
- a deductive phase (proactive forecasting, e.g. brain-storming, structured what-if studies, HAZOP, FMEA).

Hazard Control consists of a number of activities which can be summarized as follows:

- define the safety assumptions and system functions related to the defined hazards
- define the system architecture and allocate system functions within the architecture (technical solution) to meet the safety requirements including the defined THRs
- perform the hazard analysis (or causal analysis), to evaluate the possible causes of hazards
- determine the safety integrity requirements for the functions of the system
- complete the safety requirements specification
- identify potential new hazards arising out of the system design



Process Overview

Risk Acceptance

Risk acceptance criteria depend on national or international legislative requirements.

The Common Safety Method (CSM) promoted by the European Rail Agency (ERA) recognises three risk acceptance principles:

- use of a code of practice;
- use of a similar system as a reference;
- explicit risk estimation (here the ERA says “The acceptability of the estimated risks shall be evaluated using risk acceptance criteria either derived from or based on legal requirements stated in Community legislation or in notified national rules”).

In the UK the legal requirement (Health & Safety at Work Act) is that risk should be made as low as reasonably practicable (the ALARP principle – see next page).

In practice the CSM and ALARP principles are convergent, as use of a relevant industry code of practice or use of a system similar to one already in use in comparable applications may be accepted as meeting the ALARP principle by following industry best practice.

ALARP

The **ALARP** principle:

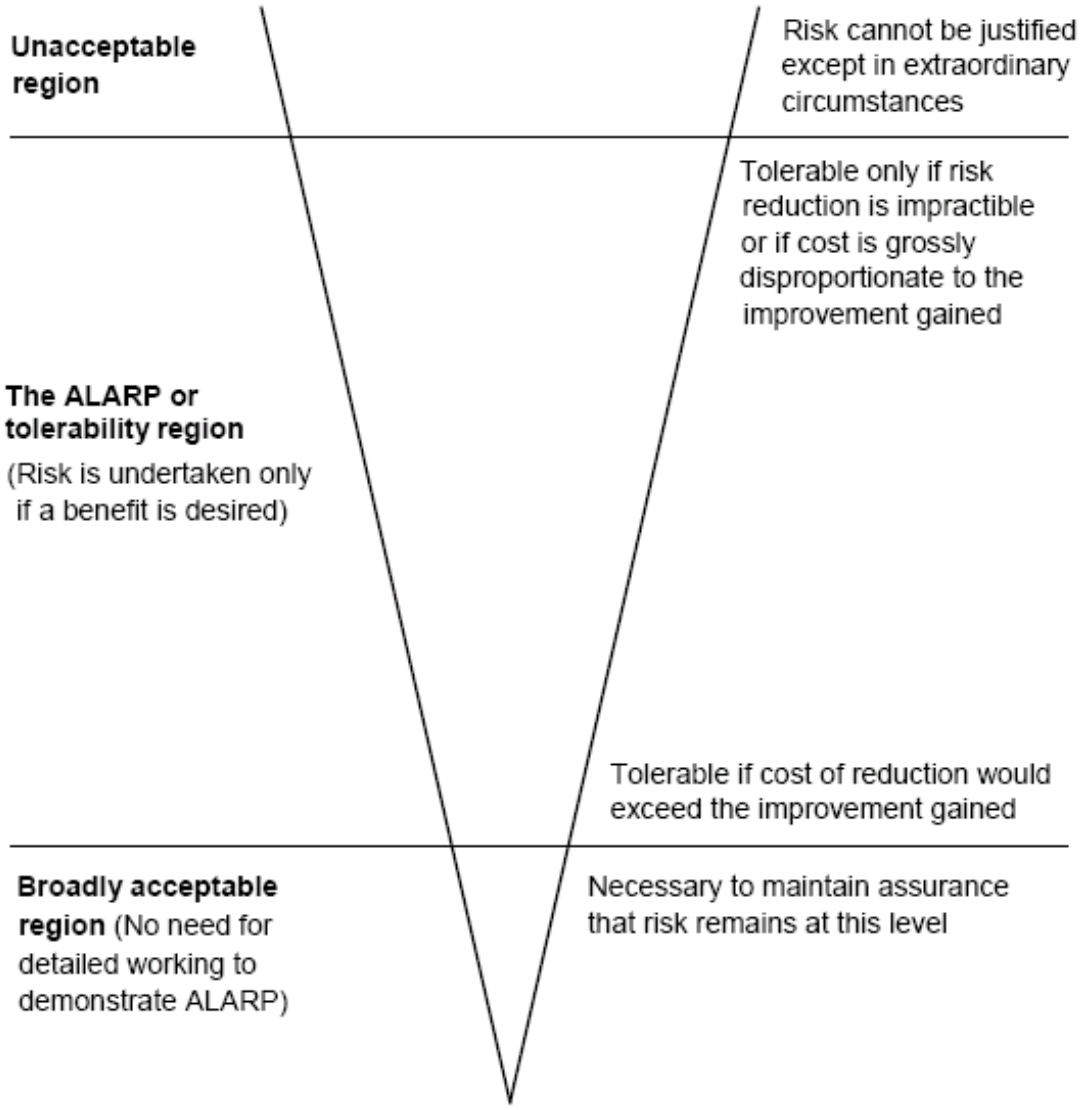
Risk should be made **A**s **L**ow **A**s **R**easonably **P**racticable

A safety measure is not ***reasonably practicable*** if its cost is ***grossly disproportionate*** to the safety benefit which it would provide

Ways of demonstrating ALARP:

Cost/benefit analysis – show that the cost of preventing a fatality is greater than the nominal value of life. UK has financial values for preventing fatalities based on surveys of people's willingness to pay for safety.

Best practice – show that best practice in the industry has been applied. It is not considered reasonably practicable to do more than the best that others in the same industry achieve. Compliance with ENs may be enough to demonstrate ALARP.



Engineering Safety Management

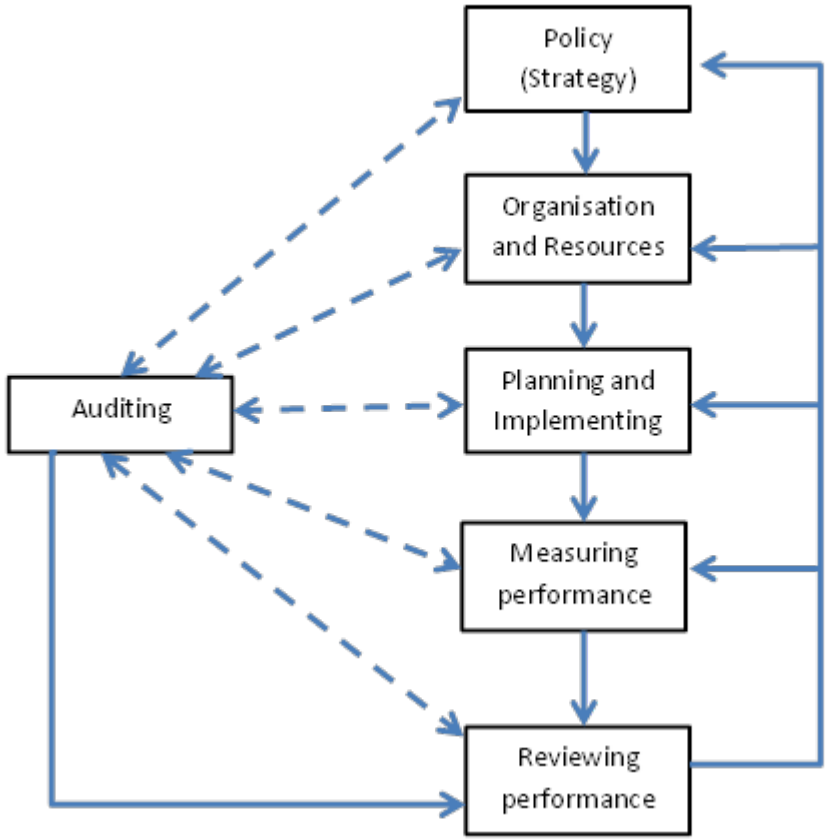
Safety Management can be defined as the organisational measures applied to ensure that an acceptable level of safety is maintained throughout the life of a system. It has much in common with Quality Management: both are concerned with the avoidance of loss.

What distinguishes Safety Management from Quality Management, or from the principles of good management in general, is that Safety Management must concern itself with events which are sufficiently improbable to be ignored by other aspects of management. For this reason hazard identification and risk assessment are prominent components of Safety Management.

The respective contributions of Quality Management and Safety Management to the safety of a system can be simply stated as follows: Quality Management ensures that the system does what was intended, while Safety Management ensures that what was intended was safe.

Safety Management as a Process

The safety management process, especially in high-hazard industry sectors, such as nuclear power, aviation or petro-chemicals, is often depicted as ‘Plan-Do-Check-Act’ and can be likened to a closed-loop feedback control system, as illustrated in the figure on the right, which is based on the model used by the Health and Safety Executive in their guidance.



Safety Management and Safety Integrity

The standards for safety-related electronic systems and software place particular emphasis on two aspects of engineering safety management: **INDEPENDENCE** and **DOCUMENTATION**.

Independence of Roles

Many roles within an organisation, such as verifier, tester, validator or assessor, are concerned with confirming the safety of what has been produced by other roles, such as designers and installers. Independence between such roles may be required in order to reduce the probability of people in different roles suffering from the same misconceptions or making the same mistakes.

It is also important that people in roles which involve making judgements about the acceptability of a product or process from the point of view of safety should not be influenced by pressure from their peers or supervisors, or by considerations of commercial gain.

Documentation

To engineer is essentially to generate or transform information, and engineering is a social activity involving collaboration and exchanges between individuals and organisations. Engineers work primarily with their brains, and documentation is the medium through which the product of this work is recorded and shared with others.

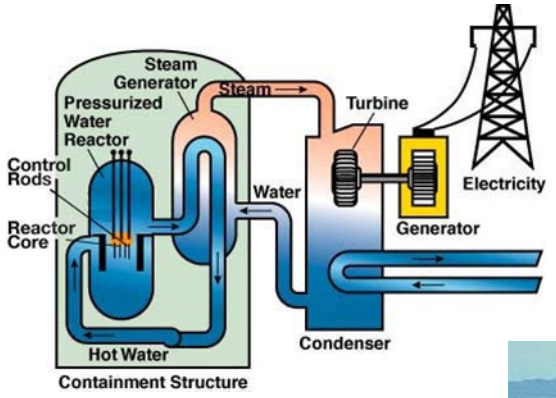
Ensuring the safety of complex systems is heavily dependent on large amounts of information being shared among all the parties concerned, including designers, operators, safety assessors, regulators and safety authorities. Documents form the principal medium of exchange of information, and there are established standards and guidelines for safety in systems engineering which set out requirements for what should be documented and by whom the documents should be reviewed and assessed

Safety Case: Origins and Definitions

safety case
the documented demonstration that the product complies with the specified safety requirements

"A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment"

In the term "Safety Case" the word "case" is used with the same meaning as in a law court – ***the evidence offered in court to support a claim***.

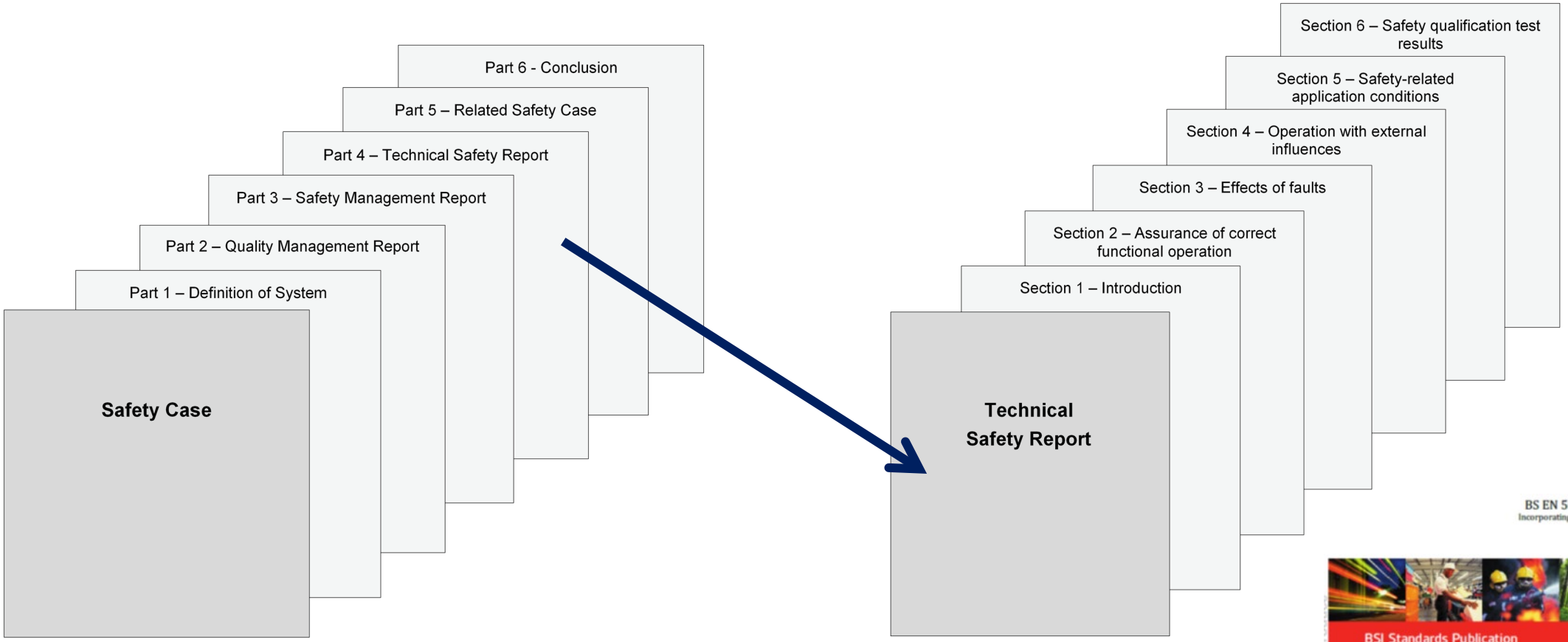


Safety cases were first used in the nuclear and off-shore oil industries to gain approval from their safety regulators

Why Safety Cases?

- In a Safety Case regime the Developer has to demonstrate that the system is safe.
- This is potentially more effective than relying on the Assessor or Approver investigating the system to find out if it is safe.
- With complex systems only the Developer has sufficient knowledge of the system to produce the evidence of safety

Structure and Content of a Safety Case



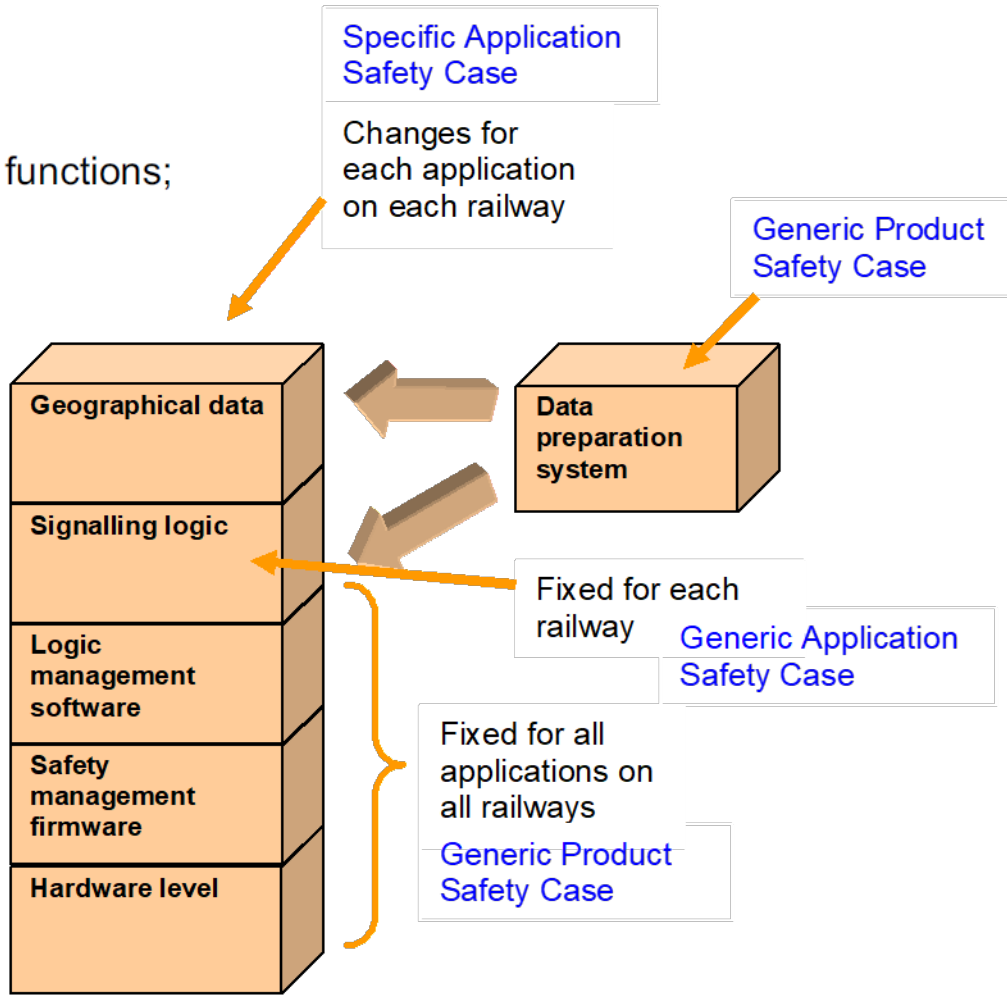
Types of Safety Case

Generic product Safety Case (independent of application)
A generic product can be re-used for different independent applications;

Generic application Safety Case (for a class of application)
A generic application can be re-used for a class/type of application with common functions;

Specific application Safety Case (for a specific application)
A specific application is used for only one particular installation.

The three types of safety case would apply to a programmable interlocking system as shown here. The signalling logic embodies the signalling principles of the railway network, while the geographical data configures each interlocking to its respective track and signal layout.



Part 2: Achieving Safety Integrity

What is Safety Integrity?

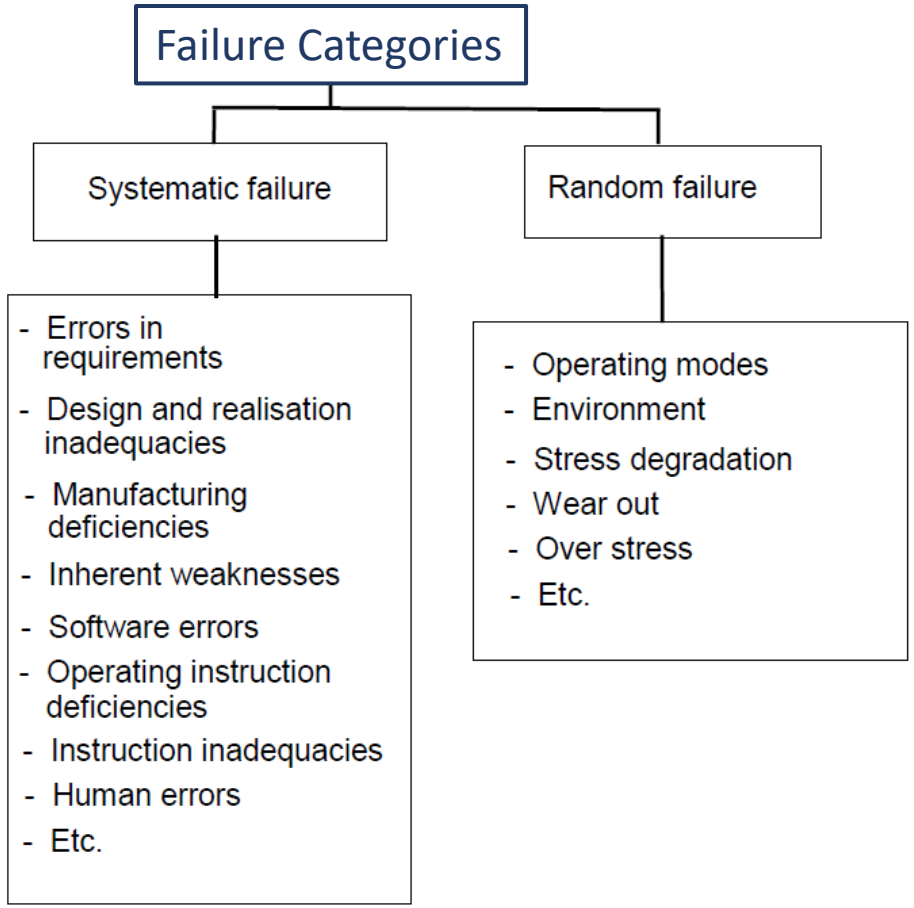
Safety Integrity is defined as the likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

The expression “required safety functions “ includes the function of reverting to a safe state in the event of a failure.

To achieve acceptable safety integrity we need to know why failures occur and how components and systems behave in the event of failure.

Failures relevant to safety are commonly classified as being either random or systematic.

Random and Systematic Failures



- From the point of view of the user, all failures are random. If it was known when they would occur they could be prevented or avoided.
- The failure of physical components is determined by the laws of physics. They appear to happen at random because we do not know enough about the precise physical condition of the component.
- The significant demarcation is between failures whose distribution is known and those whose distribution is unknown.
- Failures for which there is reliable statistical data, i.e. failures of well-established components, are treated as Random Failures
- Failures for which reliable statistics do not exist, e.g. design errors (especially software) or failures of new types of component, are treated as Systematic Failures.

Designing to Take Account of Failure

In general, failures classified as “random” are those whose rate of occurrence cannot be made low enough to provide to provide sufficient assurance of safety. For such failures safety is assured by means of the fail-safe principle, which can be defined as “a design property of signalling equipment, and of the system within which it is used, that under failure conditions will provide safety for traffic”.

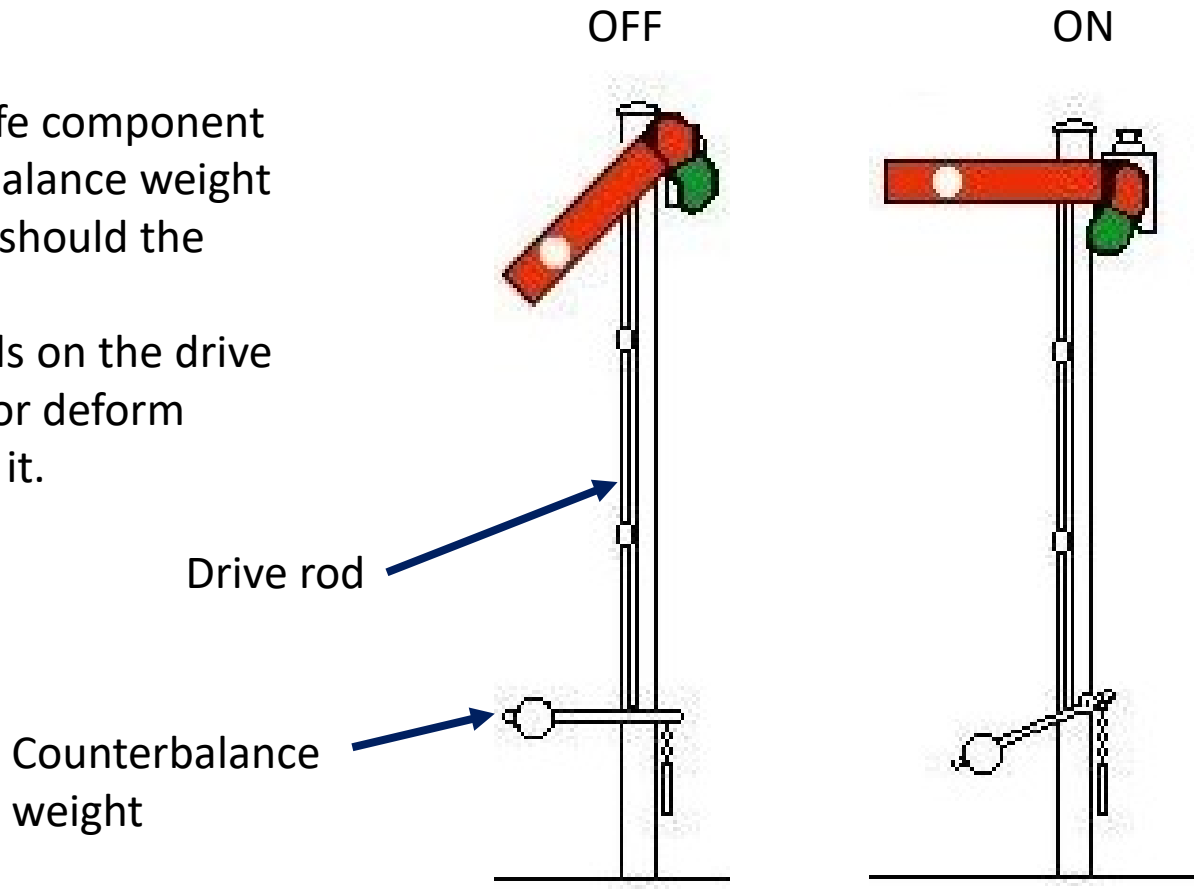
In practice this is achieved by constructing signalling systems from subsystems or components having well-defined predictable failure modes and ensuring that failure states correspond to restrictive traffic conditions.

Fail-safety, can be achieved in three different ways:

- Inherent fail-safety, where the system or subsystem is designed so that any credible failure mode of any of its component parts will result in a restrictive state.
- Composite fail-safety. With this technique, each safety-related function is performed by at least two items. Each of these items shall be independent from all others, to avoid common-cause failures. Non-restrictive activities can progress only if the necessary numbers of items agree.
- Reactive fail-safety. This technique allows a safety-related function to be performed by a single item, provided its safe operation is ensured by rapid detection and negation of any hazardous fault by another item.

Inherent Fail-Safety: The Semaphore signal

Perhaps the simplest example of a fail-safe component is the semaphore signal with its counterbalance weight to restore the signal to the “on” position should the operating wire break.
Note that fail-safe behaviour also depends on the drive rod being sufficiently strong not to beak or deform under any force which may be applied to it.



Inherent Fail-Safety: The Signalling Relay

The fail-safe characteristics of the signalling relay are at the heart of almost all classical electrical signalling safety. In British signal engineering practice the principal relay safety characteristics are an armature and contact operating mechanism with sufficient restoring forces from gravity and spring pressure to ensure that it will release when the coil is de-energised, and non-weldable contacts formed from mating and silver-impregnated carbon pairs.

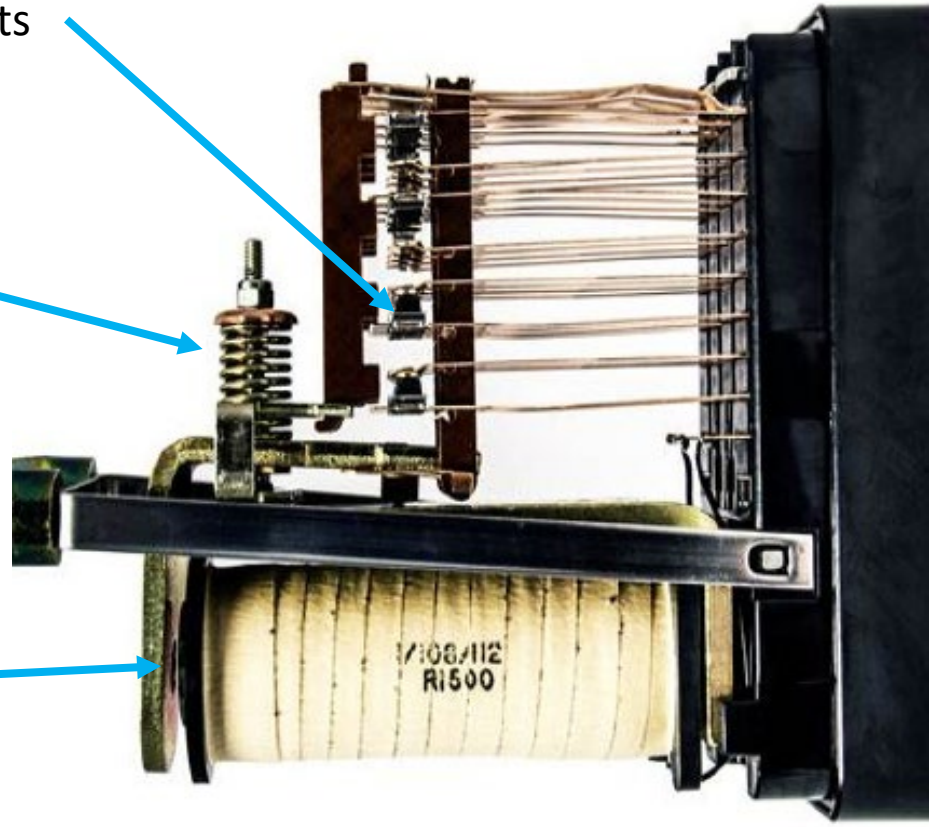
Signalling circuitry using such relays is designed so that relays are required to be energised to enable a "proceed" signal aspect to be given. Any failure, such as a broken wire or high-resistance contact, will cause one or more relays in the circuit concerned to de-energise, in which case a restrictive signal aspect will be displayed.

Safety features of Signalling relay

Non-weldable contacts

Restoring spring

Non-magnetic stud to prevent armature being held by residual magnetism when relay de-energised



Composite and Reactive Fail-Safety

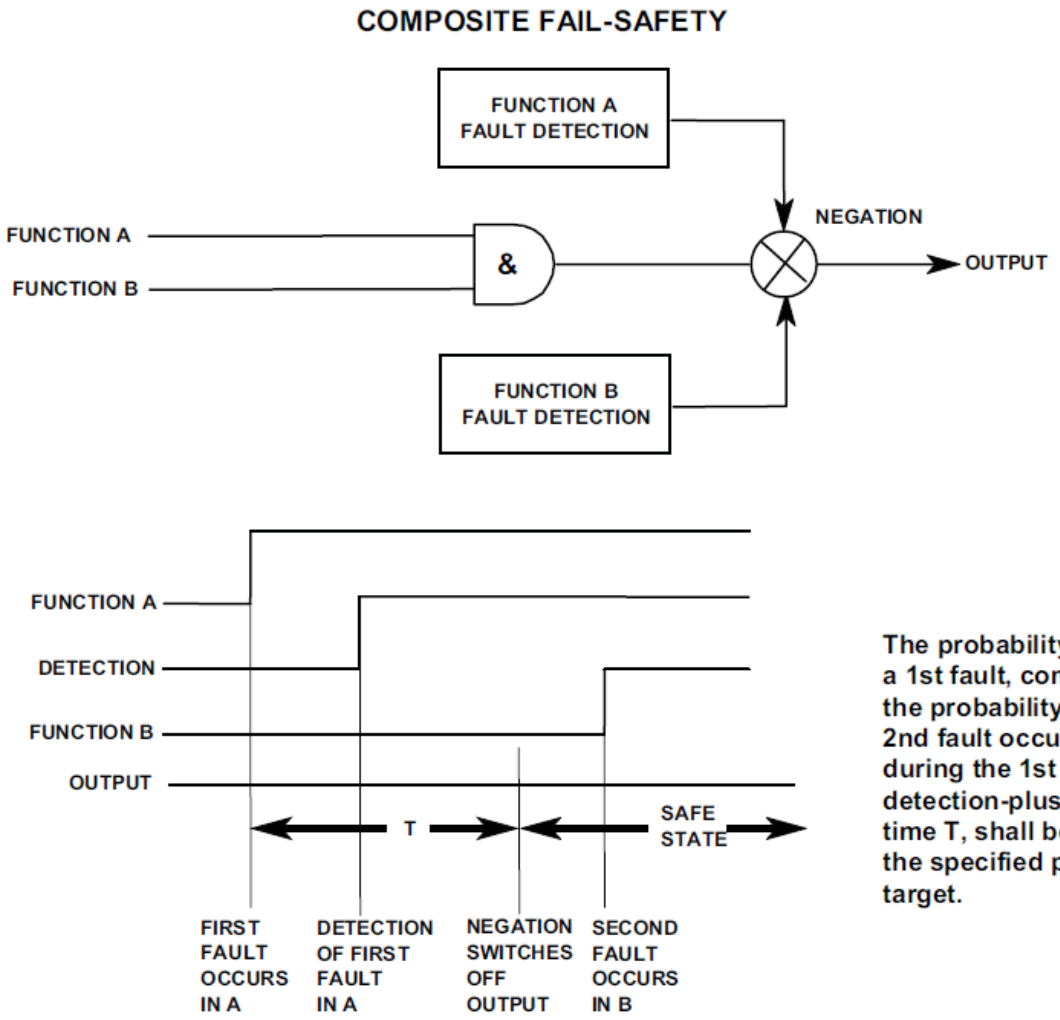
Inherent fail-safety is difficult to achieve in electronic systems because they generally comprise a large number of electronic components with a wide variety of possible failure modes, so that it is not feasible to design so that no credible failure mode of any component will result in an unsafe state.

Inherent fail-safety has been achieved for relatively simple electronic devices, such as the transmitter and receiver units of audio frequency track circuits, but for more complex applications based on microprocessors and other large-scale integrated electronic components, for example signal interlockings, composite or reactive fail-safety, or often a blend of the two, is almost always the preferred solution.

Both techniques depend on there being a very low probability of simultaneous failures in independent parts of the overall system. This calls for the system design to ensure that the time to detect and react to individual failures is sufficiently short. It is also necessary to ensure that inherent fail-safety will be achieved with regard to common-cause failures which might result in multiple simultaneous failures.

Composite Fail-Safety

Composite fail-safety not only requires two independent functional channels to agree in order to produce and output but also requires that neither channel will have detected a fault, typically by means of internal self-testing routines.
The ability to detect a first fault and isolate the faulty channel makes a significant contribution to safety. If the first fault were to remain undetected indefinitely, the probability of a similar fault occurring in the second channel during the life of the equipment would be far from negligible.

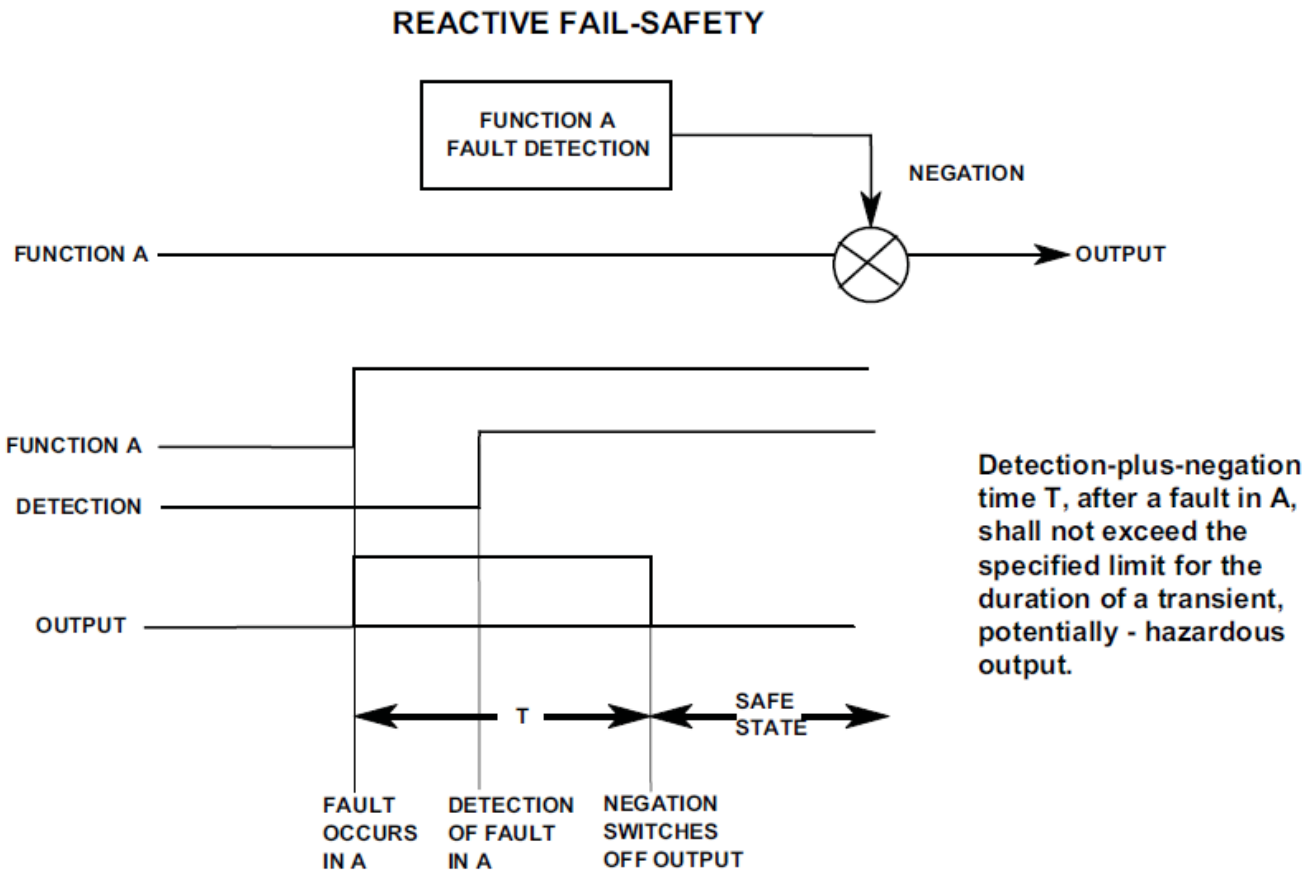


The probability of a 1st fault, combined with the probability of a 2nd fault occurring during the 1st fault detection-plus-negation time T, shall be less than the specified probabilistic target.

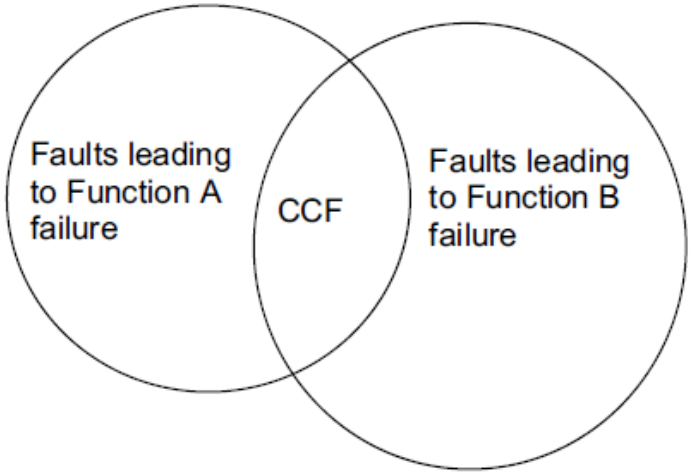
Reactive Fail-Safety

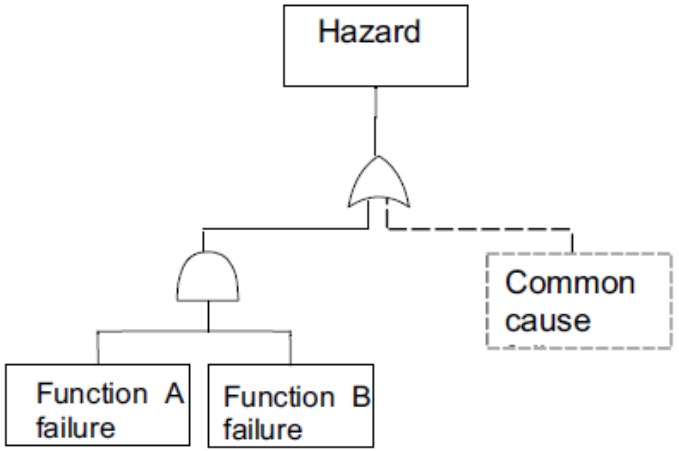
In the event of a failure of Function A an unsafe output can be present until negated by the fault detection. Hence the value of T for reactive fail-safety is much shorter than the value for composite fail-safety.

Reactive fail-safety is to be found in relay interlocking, where failure of signal lamps, which are not inherently fail-safe, is protected by lamp-proving circuits which restrict the aspects of relevant signals when a lamp failure is detected.



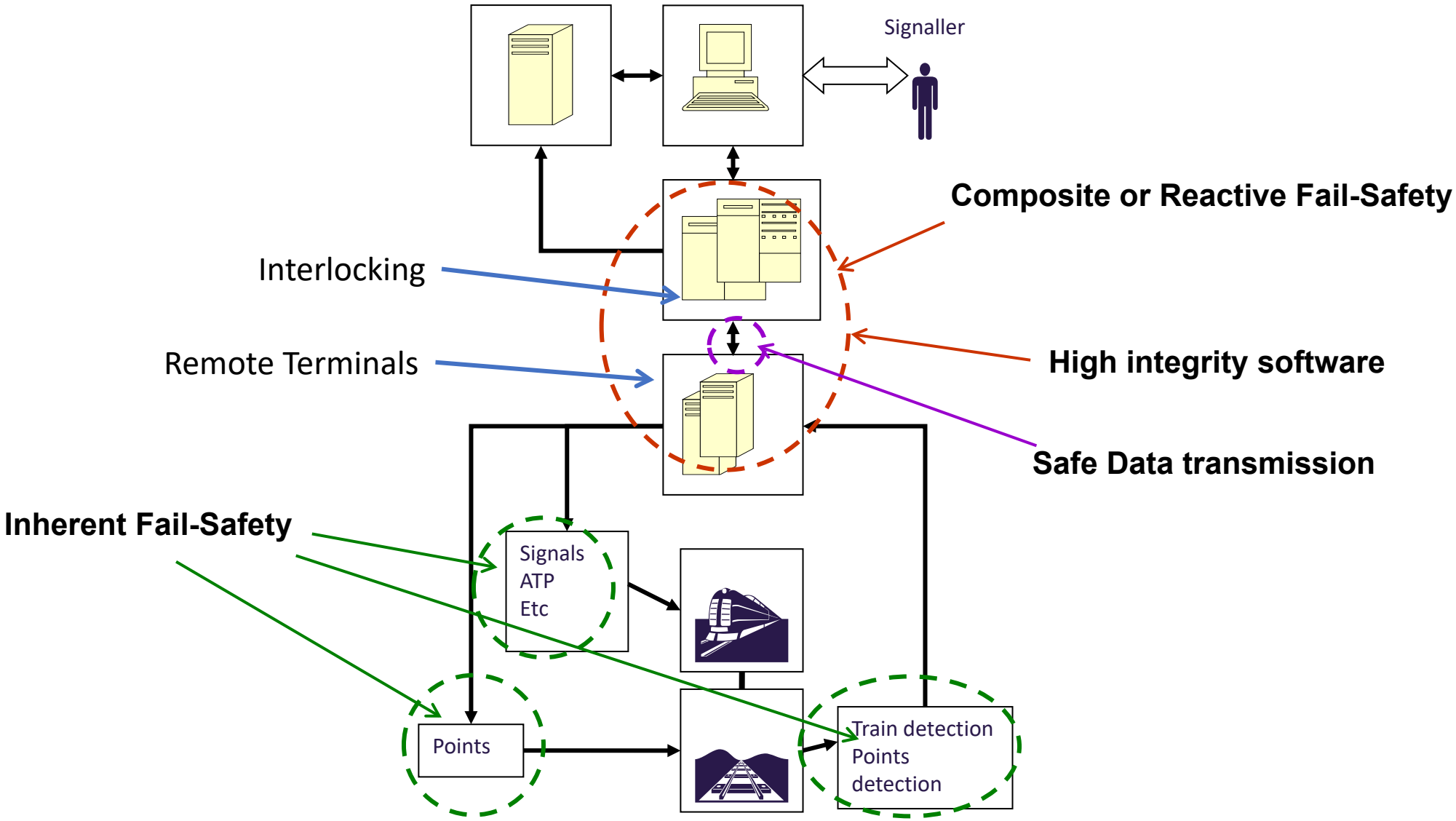
Common-Cause Failures





The Venn diagram and simple fault tree show how a common-cause failure (CCF) can undermine the protection given by composite fail-safety. A common-cause failure between function and fault detection would have a similar effect on reactive fail-safety.

Example of Combination of Safety Techniques within a Signalling System

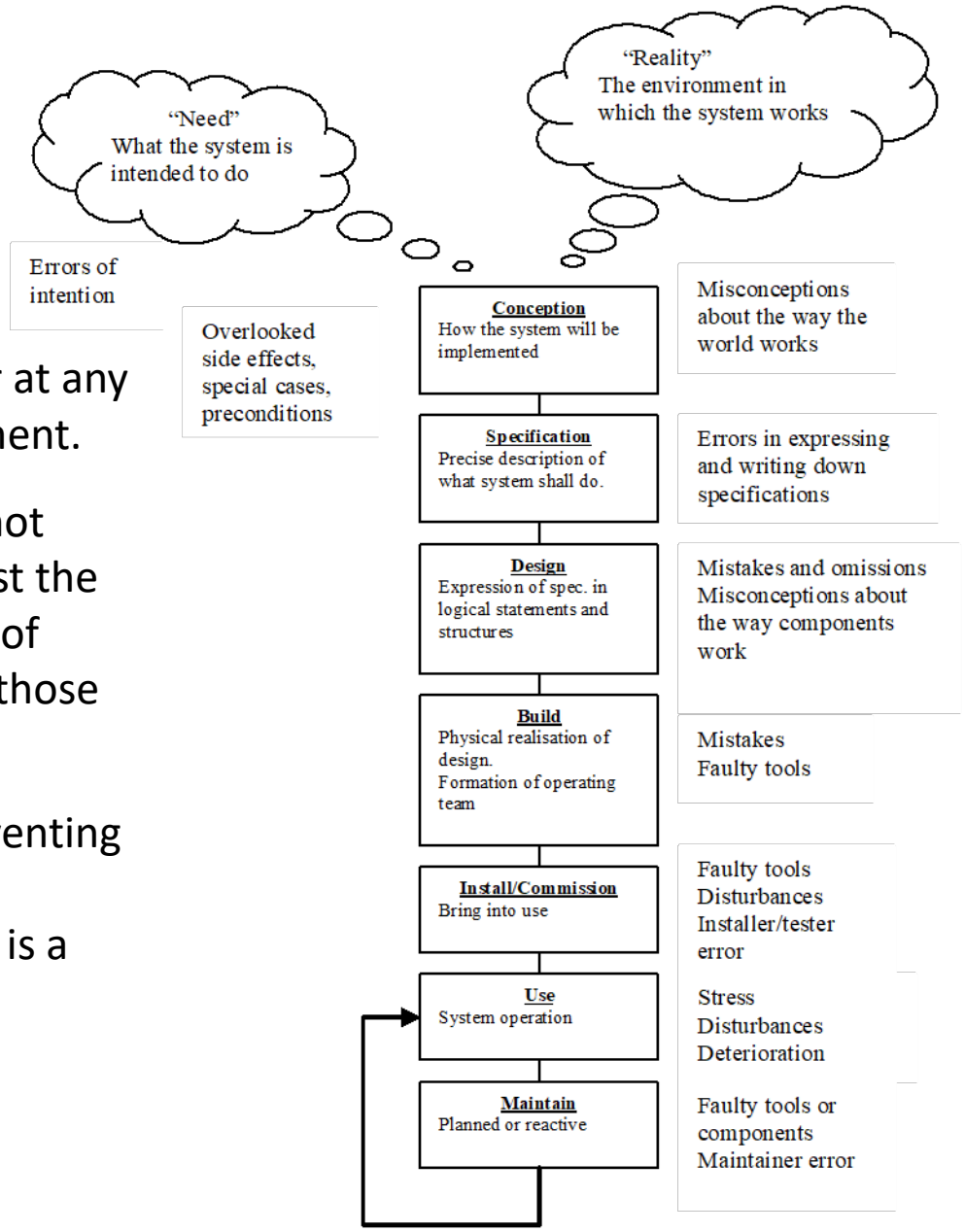


Systematic Failures

Systematic failures result from errors which can occur at any point in the lifecycle of a system or an item of equipment.

Examples of such errors are shown on the right. It is not possible to use the fail-safe principle to protect against the effects of systematic failures because there is no way of ensuring that the only errors which can occur will be those which result in a restrictive state.

Protection against systematic failure depends on preventing or detecting and removing errors at each stage of the lifecycle. The development of safety-related software is a prime example of this approach.



The Advent of Software

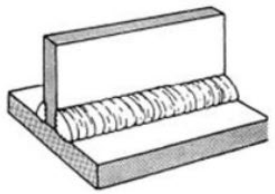
The development of processor based systems in the 1980s brought the problem of software, which cannot be fully tested.

The focus of safety assurance then shifted from product to process.

The Welding Analogy

You can't fully test software, so you rely on the production process and the competence of the software engineers

You can't test every weld, so you rely on the welding process and the competence of the welder



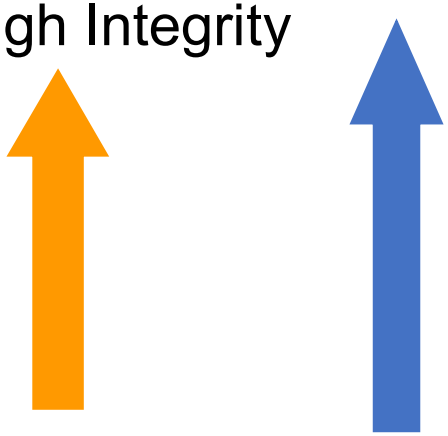
Solid State Interlocking

The SIL Concept

- The concept of **SIL** (**S**afety **I**ntegrity **L**evel) was introduced early in the development of standards for safety related software because there was no way of measuring the probability of unsafe failure of software.
- There is still no way of measuring this probability.
- Although it is not possible to determine a numerical value for the probability of failure, it is reasonable to believe that if more effective design and Verification & Validation methods are used, the probability will be lower.
- If the best possible methods are used, the software will have the highest possible safety integrity. It was decided to have four categories of method, so that SIL 4 is the highest possible.
- The SIL concept has been extended from software to cover all types of systematic failure, such as errors in requirements, design errors and manufacturing errors.

The SIL Concept Illustrated

Safety integrity level	Description of safety integrity
4	Very High Integrity
3	
2	
1	
0	Basic Integrity



Increasing rigour and effectiveness of methods

Definitions of SIL

- The following definitions are shared by standards BS EN 50126, 50128 and 50129

safety integrity
ability of a safety-related system to achieve its required safety functions under all the stated conditions within a stated operational environment and within a stated duration

safety integrity level
one of a number of defined discrete levels for specifying the safety integrity requirements of safety-related functions to be allocated to the safety-related systems

software safety integrity level
classification number which determines the techniques and measures that have to be applied to software

system safety integrity level
classification number which indicates the required degree of confidence that an integrated system comprising hardware and software will meet its specified safety requirements

Principles of Development for SIL

The principles applied in developing high integrity systems and software include, but are not restricted to:

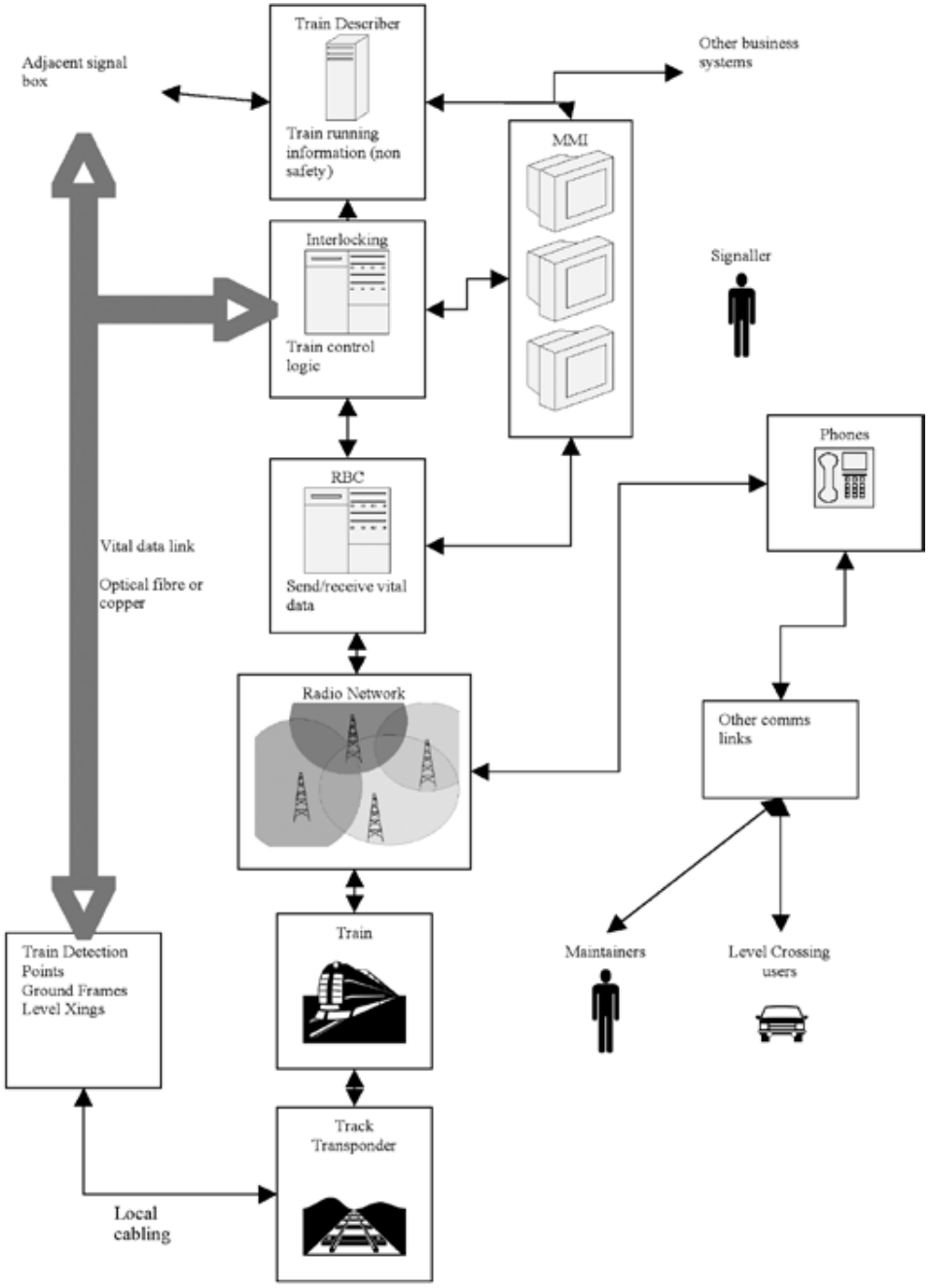
- top-down design methods
- modularity
- verified components and component libraries (mainly for software)
- verification of each phase of the development lifecycle,
- clear documentation and traceability
- auditable documents
- validation
- assessment
- configuration management and change control
- appropriate consideration of organisation and personnel competency issues

The standards EN 50129 (electronic systems) and EN 50128 (software) include tables of techniques and measures for implementing these principles to meet the required SIL

Part 3: Safety of Data Transmission

Railway Signalling and Data Transmission

The diagram shows a state-of-the-art signalling system where there are no lineside signals and vital data giving authority for train movements is transmitted to the train by radio. A fixed data link, which may use optical fibres or copper conductors for its transmission medium, transmits command and status data between lineside equipment and the control centre, and a speech link is also provided by radio between the signaller and the train driver. This system architecture is typical of that adopted for the European Train Control System (ETCS)

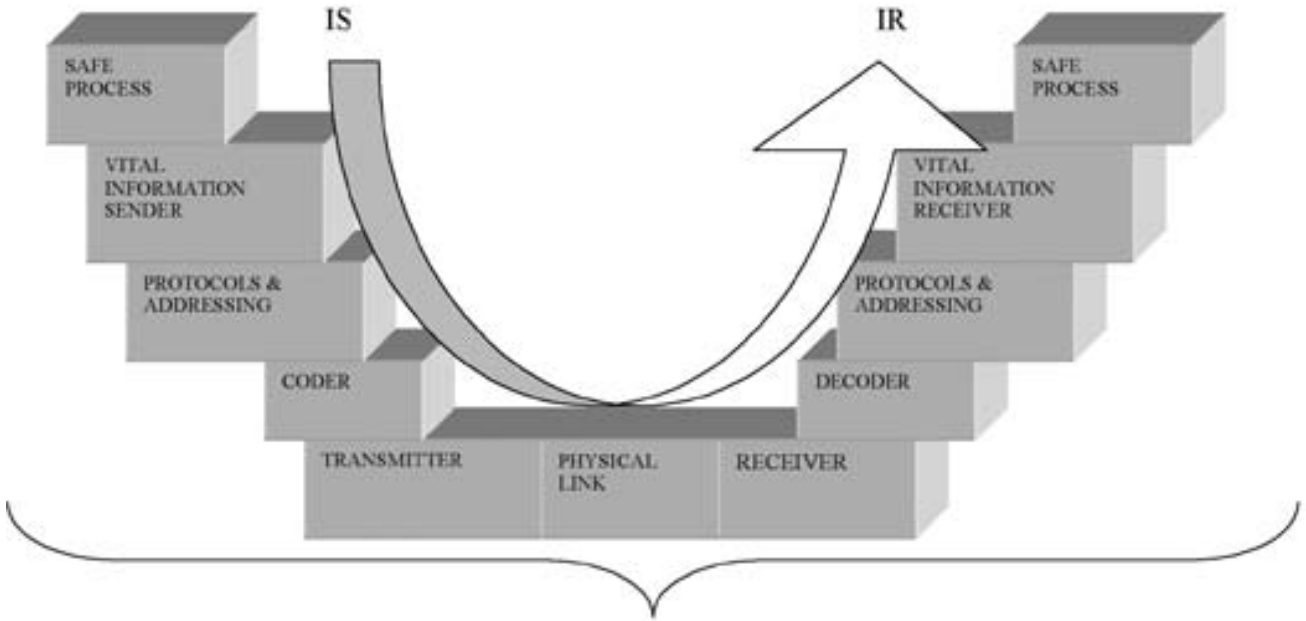


Conceptual Model of Data Transmission System

Information may be transmitted through a hierarchy of electronic systems which may store, forward or otherwise manipulate the information. Hardware or software faults in any of these systems might corrupt the information in unpredictable ways. The vital information receiver and the safe process must be capable of distinguishing between valid and corrupt information. Ways of making this distinction include:

- All physical signals above a certain amplitude or within a certain frequency band
- Digital data which satisfies particular coding rules
- Messages which satisfy certain protocols, e.g. have correct addresses or valid time stamps

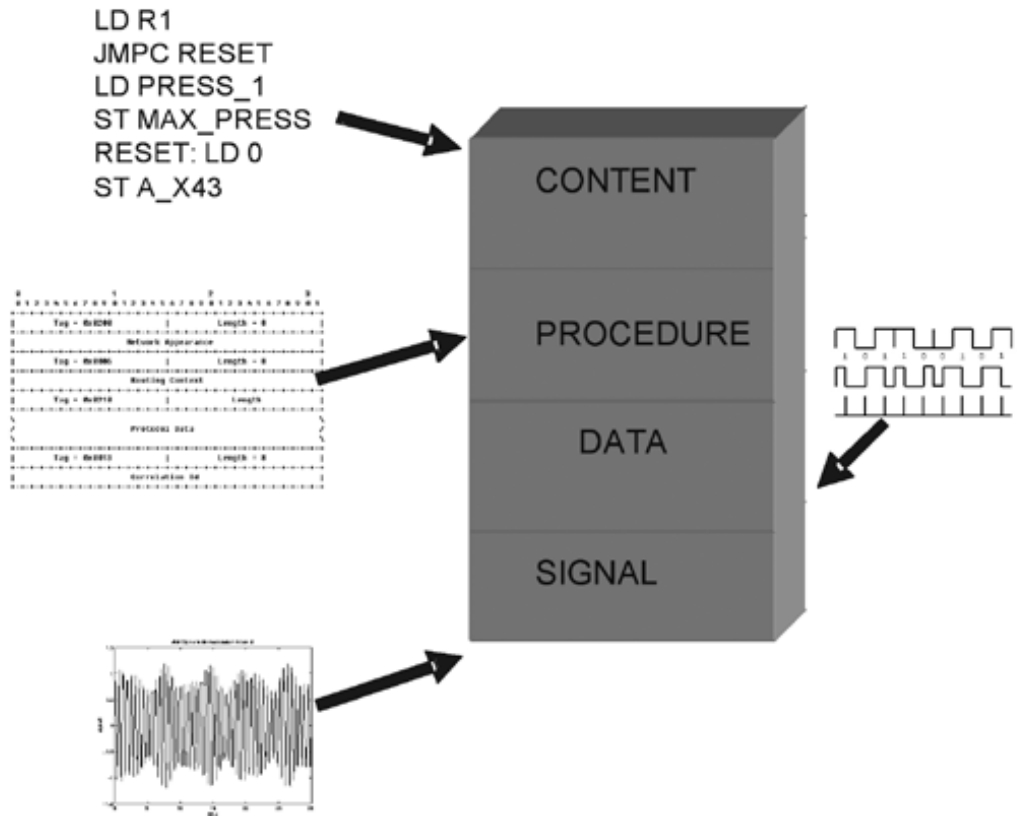
Based on the OSI model of open transmission systems



Failures, errors and noise may affect any component in the model

Multidimensional View of Information

- Physical signal – within this dimension only the analogue value of the physical signal is considered.
- Data – in this dimension information is generally considered as strings of binary digits, and the relevant information protection techniques focus attention on the patterns of digits, without any consideration of useful content or meaning.
- Procedures – the information units considered are words consisting of groups of digits, but checks refer to protocol or syntax rather than meaning.
- Content – in this dimension the meaning of transmitted information is taken into account in checking its correctness.



Sources of Error

- Inherent characteristics, error generated by sources within the transmission system (e.g. thermal noise in resistors)
- External influences (the electromagnetic environment), errors injected from sources outside the system, generally referred to as electromagnetic interference (EMI)
- Equipment failure, errors which are solely the result of equipment failure within the system.

Methods of Protecting Information Transmission

Protection in the Physical Signal Dimension

- Screening of cables and equipment housings
- The use of balanced twisted conductors in copper cables
- Suppression of interference at source
- Use of optical fibres as a transmission medium

The Data Dimension – Coding

- Repeat messages
- Block coding
- Convolution or cyclic block coding

Fail-Safe

The fail-safe principle is applied in the transmission of safety information by designing the receiving safe process to adopt a restrictive state in the event of errors being detected or loss of transmission

Protection in the procedural dimension

- Closed-loop protocols: receiver repeats message back to sender and awaits confirmation from sender before acting on message
- Time stamping: message contains time of origin – receiver will reject information which is too old
- Sender's address included in message – receiver will reject information from wrong sender, e.g. in the event of message routing errors or cross-talk