Railway Control & Communications Systems Management Version 6

A selection of fundamental concepts and methodologies

(This document is intended for candidates taking Module A of the IRSE Professional Examination. It is based on an extract from the 2018 Study Guide v1.3 for Module 7 of the IRSE Professional Examination)

1 Introduction

A railway is a complex system. All parts of the system must work well together to deliver safe and efficient outputs. This means that all sub-systems and their interfaces with each other (and with human operators) need to be carefully designed. Thinking about this should start at the beginning of any project because once equipment is being installed, or is in use, it is usually impractical or expensive to make changes.

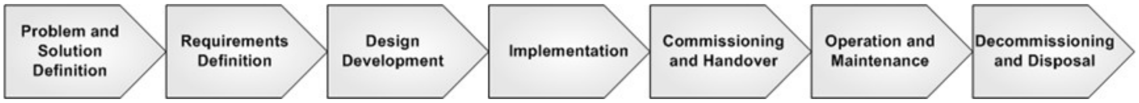
This document outlines some of the principles and tools of systems management and their application to the entire life cycle of assets.

2 Project Life Cycle & Stage Gates

2.1 Life Cycle for the Project

Good systems do not just happen, they are designed and planned; and they achieve this when their projects follow a disciplined procedure. This is often called a life-cycle and the ‘V’ life-cycle in particular will be discussed in the next section. This will look at the generic steps that a project should go through in order to deliver a well-engineered solution.

A typical project breakdown is shown in the figure below. It divides the whole project process from start to finish into a number of discrete steps or phases


Problem and Solution Definition
Requirements Definition
Design Development
Implementation
Commissioning and Handover
Operation and Maintenance
Decommissioning and Disposal

Each phase:

- Has a defined start point
- Can be described in terms of its characteristics
- Provides clear boundaries between its neighbouring phases
- Defines the transition to the next phase
- Has a clearly defined end point

2.2 Problem Solution and Definition

The problem to be solved should be clearly defined and articulated. The feasibility of the potential solutions should be confirmed. The potential solution(s) to be pursued should be selected on the basis of a systematic assessment and comparison of the proposals.

2.3 Requirements Definition

2.3.1 There are 2 parts to this:

- The business requirements describing the change that is needed. It is often expressed in performance or monetary terms. The business sponsor would define these with major input from operators and maintainers.
- The system requirements which are a technical response to the business requirements. These describe in clear engineering terms what the system will do.

2.3.2 As requirements are captured, there are certain items which the project knows to be true and upon which it relies in order to deliver its solution. There are other items about which it is not certain or is dependent on others to deliver, either as part of the project, or once the solution has been put into service. These are called Domain Knowledge, Assumptions, Dependencies and Caveats which are defined as:

- Domain Knowledge: Things known to be true: e.g. characteristics of signalling relays, typical adhesion values for steel wheels on steel rail;
- Assumptions are statements made about items outside the scope of the system under consideration, but are relied upon to be true in order for the system to operate as expected. Once the facts are known an assumption will either be deleted, or changed to become domain knowledge, a dependency or a caveat;
- A dependency is a requirement for someone or something else to act before a task can be completed, e.g. if a project is delivering new rolling stock, it would be reasonable to depend upon any necessary depot alterations to be made;
- Caveats are conditions that must be delivered after a system is put into operation, e.g. for the same rolling stock project a caveat is that the vehicle is maintained to design standards.

2.4 Design Development

This phase includes all the design activities that need to be carried out before the system can be realised. The phase results in a design baseline – a design set of documents and drawings. The level of detail in the design is very dependent upon the disciplines involved and the contractual strategy adopted.

2.5 Implementation/Migration

The Implementation phase includes all activities that are involved in realising the design, including all construction works as well as the integration of electronic and mechanical subsystems and delivering software and data. The output will be a physical system baseline and as-built documentation. Technical requirements need to be communicated to detailed designers and manufacturers in the form of engineering specifications and technical standards.

2.6 Verification, Validation and Testing

2.6.1 Verification and validation should be done at the appropriate level. See section 3 for an explanation of these terms. For example, validation of a signalling system should be undertaken at the system level, whereas individual components would be validated at the subsystem level.

2.6.2 The products will normally undergo a comprehensive regime of testing, comprising tests in the laboratory and factory environment and latterly in their target environment. The tests will seek to provide evidence to verify and validate that the products meet their requirements and are fit for purpose and that the safety functionality has been correctly implemented. This may include a set of routine tests for ‘proven’ products and more comprehensive tests for newly developed items of equipment. Testing may comprise the following:

- Unit testing – test carried out by the software developer to verify compliance of units of software with their requirements. The depth and extent of test coverage will depend on the safety integrity level (SIL) of the item under test.;
- Qualification testing – carried out by the hardware developer to prove correct functionality of the hardware, and non-functional requirements, such as shock and vibration, temperature and humidity, reliability.
- Software functional testing – carried out by the software developer to prove correct functionality of the software and that it does not exhibit any unexpected behaviour or hidden faults;
- Safety functional testing – carried out at all levels of the system assembly to prove the correct functionality of the safety functions under normal and failure conditions;
- Installation testing – a set of tests conducted on equipment installed in its intended location and environment to confirm correct installation;
- Integration test – carried out at a number of test stages to confirm that sub-assemblies, products, subsystems and systems are correctly integrated to ensure that they operate correctly together;
- Interface testing – used to prove correct functioning of the interface between two or more interfacing pieces of equipment;
- Test and commissioning – testing on the installed system to ensure that it performs the correct functions and does not have any hidden faults. This phase of testing may also include testing to ensure that the principles of safe railway operation have been adhered to (‘principles testing’). The final stage confirms that the system will operate as expected with the surrounding railway equipment with which it will interface.

2.7 Commissioning & Handover

2.7.1 This phase includes all activities required to bring the system into full service, including testing and commissioning for signalling and trial running of trains.

2.7.2 There are two linked but separate objectives:

- To demonstrate that the system is ready to be put into service;
- To demonstrate that the railway organisation is ready to accept the system into service. This includes:
    - Training
    - Maintenance manuals
    - Operation manuals
    - Correct organisation
    - Spares
    - Planning

2.7.3 Acceptance and handover of the tested and commissioned system to the operator/user will normally require the satisfactory completion of a number of activities:

- Safety approvals of the system including its operation and maintenance systems by the necessary approval bodies;
- Audit of test records;
- User acceptance tests – acceptance through testing or trials that the system meets its stated requirements and can be operated by the user;
- Processes for checking the competence of staff who have worked on the project;
- Handover operations and maintenance (O&M) systems to the operator and maintainer, including training, O&M manuals, relevant safety case information and accurate "as built" records of the design (including version details for traceability purposes).

2.8 Operations & Maintenance

This phase includes all activities involved with the normal operation of the system. The maintainer is responsible for the safe, whole life performance of the system. This includes replacement of components and subsystems within the system. This phase only ends when the system is removed from service.

Maintenance testing is needed to ensure that the equipment remains in a safe and reliable state. This includes testing after items of equipment are replaced by similar units. Test plans are needed to define the tests required. Technicians doing these tests should be monitored periodically to prevent bad practice or short cuts that omit vital parts of the test. A record should be kept of all maintenance tests.

2.9 Decommissioning & Disposal

2.9.1 The Decommissioning and Disposal phase includes all activities involved in removing the system from the railway. For most signalling systems, decommissioning coincides with or overlaps the commissioning of a new system.

2.9.3 The decommissioning or disposal of a system is as much a change to the railway as the introduction or commissioning of a new system and should be planned and executed with care. These activities must be planned and implemented so as to ensure the safety of any train operations that continue through the period of transition.

2.10 Stage Gates or Decision Gates

The division of a project into discrete steps or stages, permits those working on the project to stop and check that as a whole the project will deliver what is expected of it. It is all too easy for individual disciplines to become separated from the rest of the project (particularly where a project is delivered from multiple locations) and develop their designs without consideration of how it must integrate with others. It is also possible for projects to forget the original problem being solved and begin to move towards offering something that does not meet the client's requirements.

2.11 Uses of Stage Gates

Consider the following when using stage gates:

- Review the requirements that must be satisfied;
- Provide objective evidence that these requirements are being met;
- Confirm that designs comply (or will comply) with relevant legislation, consents, agreements etc.
- Look for opportunities to approve products or systems that are approved for use on other administrations (with similar functions, environment and interfaces) without the need to examine evidence from first principles.
- Determine that all applicable standards have been identified and any necessary derogations applied for and if possible, granted;
- Ensure that technical risks have been adequately captured, assigned to an owner, appropriate mitigations identified and implemented;
- Review the proposed design against the project costs of the project;
- Be assured that interfaces have been identified and properly designed so that individual design elements will integrate and work together as intended;
- Confirm that the proposed design can be constructed given limitations of technology, available equipment and site conditions;
- Review assurance evidence for each individual item of design;
- Review the programme timescales and apply any remedial action should delays be identified.

2.12 Engineering Approvals

Engineering approvals of designs, documents and products take place throughout a project's life cycle, but stage gates are an opportunity to check that all engineering controls are in place. Project engineering controls are an essential tool to ensure the delivery of safe and efficient outcomes.

2.13 Cross-acceptance

The process of approving a new product or system can be more efficient if it is already in use elsewhere (typically on another railway system). This cross-acceptance approach for a product will need to examine whether it is being used for the same function in a similar environment and with similar interfaces to the remainder of the system. The quality and scope of the acceptance process of the other administration is also relevant.

3. Verification, Validation and the V Model

3.1 Verification and Validation

These are key concepts in the process of ensuring that a project is delivering a system that meets the client’s requirements and is also fit for purpose.

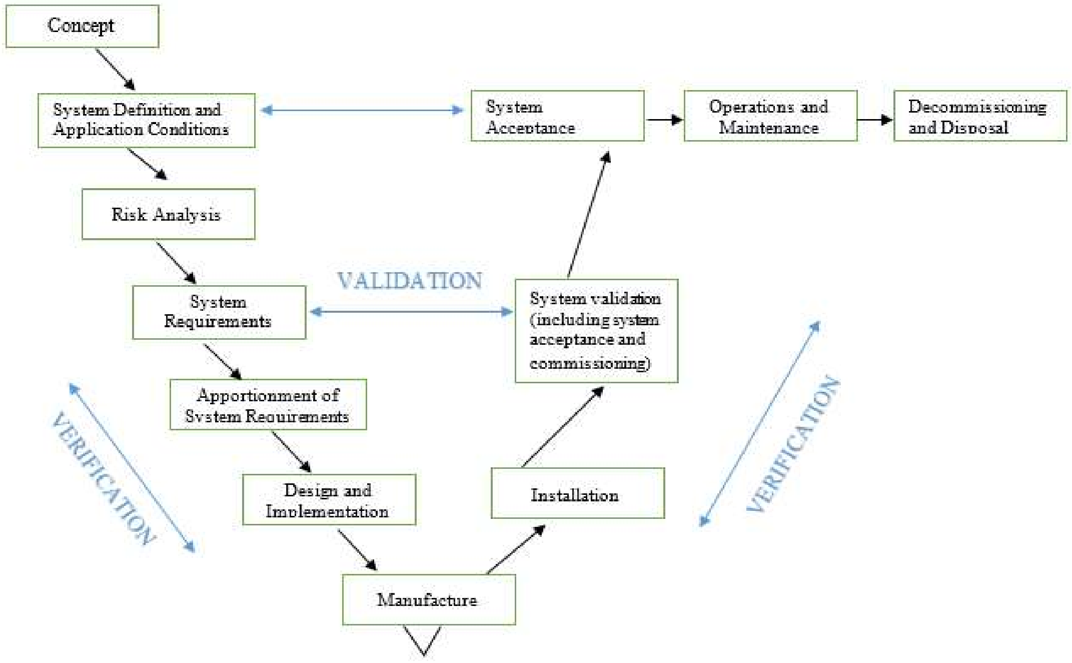
- Validation. The objective of validation is to provide confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.
- Verification. The objective of verification is to demonstrate that the requirements of each life cycle phase have been fulfilled.

3.2 The V-Model

3.2.1. A V-model is a common graphical representation (as shown in Fig. 1 below) of the system engineering life cycle. The left side of the V represents concept development and the decomposition of requirements into function and physical entities that can be designed, and developed. The right side of the V represents integration of these entities (including appropriate testing to verify that they satisfy the requirements) and their ultimate transition into the field, where they are operated and maintained. The V-model can be viewed as a time-line in the form of a "V". The product moves sequentially from the first phase, "Concept", to the next phase, "System definition and application conditions", etc.

3.2.2. Throughout the process, evidence will be gathered from a variety of sources including the review of specifications and the results of actual tests.

Fig. 1


Concept
System Definition and Application Conditions
System Acceptance
Operations and Maintenance
Decommissioning and Disposal
Risk Analysis
VALIDATION
System Requirements
System validation (including system acceptance and commissioning)
Apportionment of System Requirements
VERIFICATION
VERIFICATION
Design and Implementation
Installation
Manufacture

3.2.3. The principal advantage of the V-model is that it shows the relation of verification and validation to the activities in the lifecycle and makes clear their role in finding defects at an early stage and preventing the propagation of defects through the lifecycle.

For projects incorporating a high degree of novelty or innovation the life-cycle may have to be modified to include prototype testing or proof of concept.

4. Reliability, Availability, Maintainability and Safety (RAMS).

4.1 Definitions

- Reliability is the probability that an item can perform a required function under given conditions for a given time period
- Availability is the ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given interval
- Maintainability is the ability of a system to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance. Given conditions would include aspects such as: location for maintenance, accessibility, maintenance procedures and maintenance resources"
- Safety is freedom from unacceptable risk of harm.

The goal of a railway system is to achieve a defined level of rail traffic in a given time, safely. For the demonstration of RAMS, a RAM Programme and Safety plan needs to be developed for the project, so that during the system requirements phase, the following analysis needs to be considered within the RAMS programme:

- Failure Modes Effects Analysis (FMEA), fault tree analysis, for reliability;
- Data analysis for availability improvement and prediction for availability;
- Maintenance task analysis, personal safety procedures for maintainability;
- Defining safety related functional requirements, establish safety management processes.

4.2 Systematic and Random Failures

4.2.1 The RAMS of a railway system is influenced in three ways:

- by sources of failure introduced internally within the system at any phase of the system lifecycle (**system conditions**),
- by sources of failure imposed on the system during operation (**operating conditions**) and
- by sources of failure imposed on the system during maintenance activities (**maintenance conditions**).

4.2.2 Failures occurring due to internal disturbances in the system at any phase of system lifecycle are **systematic** failures or **random** failures. Systematic failures occur due to errors in requirements, design inadequacies, manufacturing deficiencies, software errors, human errors in installation or maintenance, etc. Random failures occur due to wear out, over stress, stress degradation, environment, etc, beyond that which could have reasonably been foreseen during the specification and design phases or due to failure of components which do not match their intended specification because of deficiencies in manufacture or quality control.

5. Security

5.1 Protection against Cyber Attacks

5.1.1 From the point of view of cybersecurity, railway signalling and communication systems have much in common with Industrial Control Systems (ICS, also known as Industrial Automation and Control Systems, IACS). They comprise a combination of both cyber and physical components, such as sensors and actuators and they incorporate networking devices and communication protocols; they commonly have long service lives, and comprise multiple generations of equipment from a wide range of suppliers; their software is often custom-written, using bespoke or older, unsupported operating systems. They are both potential targets of cyber-attacks from sources such as viruses, hackers, organised criminals, terrorists and state-sponsored groups. Consequently, cybersecurity for railway signalling and control applications can benefit from study of good practice and standards in ICS.

5.1.2 For ICT (Information Communication Technology) system, increasing use of IP (Internet Protocol) technology and commercial off-the-shelf operating systems in railway systems makes it important to understand the architecture and specific functions of those systems. Consider whether part of the system is networked, or whether there are interfaces with other systems that are. Understand how these systems share data, and what level of security is in place (passwords, encryption, firewalls, etc.). A system is only as secure as its weakest line of defence. Where systems that have been designed separately are connected together (such as railway ICS) a cyber analysis of the whole system should be carried out. Examples of cyber threats include web application attacks, phishing through email, denial of service, malware. Consider whether important passwords are secure, review the use of USB flash drives, and establish an incident response plan in case of an attack. The objectives of a cyber-attack may not be obvious, and can range from causing injury or disruption, to undetected data theft and reputational damage.

5.2 Cybersecurity Design Principles

5.2.1 The cybersecurity design principles listed below have been derived from the review of best practice and existing sources and standards undertaken in the course of developing a European Technical specification addressing cybersecurity within the railway sector.

- Secure the weakest link. This design principle aims to push the designer to consider the security of all the components of the system and not only the most obvious, such as the protocols or the interfaces.
- Defence-in-depth (several diverse protections in sequence)
- Fail secure (comparable to fail safe, but sometimes these two principles can be in conflict).
- Grant least privilege (each component should have only those privileges to accomplish its specified functions, but no more).
- Economise mechanism (avoid redundancies and overlapping of functionalities)
- Authenticate requests (check identity of users, human or devices)
- Control access (grant access only to authorised entities (users, programs, processes or other systems).
- Assume secrets not safe (assume an attacker knows the details of the system)
- Make security usable (avoid annoying and painful mechanisms)
- Audit and monitor

5.3 Safety and Security

5.3.1 Safety and security have complementary goals but are sometimes in conflict over the means to achieve their respective goals.

- In safety, frequent changes should be avoided because of the cost of safety demonstration. In security, update should be easy in order to be able to patch the system in a timely manner.
- From the safety perspective an emergency message (e. g. to immediately shut down or stop a system) should be transmitted as fast as possible and the reaction should be executed immediately. From a security perspective the message should be authenticated to prevent masquerade which might lead at least to denial of service, but the calculation and checking of cryptographic codes consumes time and leads to a delay of the emergency message and the reaction.

5.3.2 Trade-off between safe and secure design is not easy and it can be hard to find an optimal solution. Safety and security are different and cannot easily be merged: security cannot simply be regarded as an add-on to safety or vice versa. The following principles are aimed at achieving a harmonious relationship between security and safety.

- Safety and security are different and should be treated as such
- The security environment should protect essential functions, including safety
- Cybersecurity Threat & Risk Analysis is the main interface with Safety Analysis.
- Separate security and safety as far as possible but coordinate them effectively
- Security should be evaluated on the basis of international standards, e.g. IEC 62443
- It is infeasible to evaluate the Security Risk probabilistically.
- Safety and Security Target measures should not be coupled.
- Security is a collaborative continuous effort.

5.4 Protection against Physical Attacks, Theft & Vandalism

Physical attacks, theft and vandalism are all potential threats to the safety and availability of railway signalling and communications systems. For defence in depth to ensure cybersecurity the first barrier should be physical protection; with no trust on who can access the hardware, there is no trust on the data. Vandalism incidents include malicious damage and arson. Theft normally targets high value lineside equipment such as copper cables. Both vandalism and theft can adversely affect safety by damaging equipment in ways not seen as credible in the normal design process, e.g. by causing multiple simultaneous failures.

Measures to reduce risk include:

- Fencing
- CCTV
- Cable alarms
- Buried or secure cable routes
- Fibre cable instead of metal
- Security of equipment housings and rooms
- Lighting
- Movement detection

6. Obsolescence Management

6.1 Introduction

Items become obsolete when they can no longer adequately perform the function for which they were created, or when there is a clear advantage in changing to a new product or technology. Three types of obsolescence are described below.

6.1.1 Obsolescence affects all products and it impacts upon all stages of their life. The term includes:

- Capital equipment;
- Infrastructure;
- Consumer durables;
- Consumables;
- Software products.

6.1.2 Obsolescence is inevitable and it cannot be avoided, but forethought and careful planning can minimise its impact and its potential high costs. The objective of obsolescence management is to ensure that obsolescence is managed as an integral part of design, development, production and in-service support in order to minimise cost and detrimental impact throughout the product life cycle.

6.1.3 Obsolescence presents itself in three ways:

- The item is no longer suitable for current demands; or
- The item is no longer available from the original manufacturer; or
- The item can no longer be maintained because people with the necessary skills are no longer available.

6.2 Product Suitability

6.2.1 A system or product is designed to meet the requirements of the project at a specific moment in time. Additional functionality can be added to meet a future need. This is only a good idea if that future need is clear and/or the extra functionality does not add too much cost or complexity. Otherwise it can add design complexity, add cost (including design effort, manufacture and ongoing maintenance), reduce reliability and in the end, may not be what is actually required.

6.2.2 There is a need for products and systems to be 'future-proof' by which is meant minimal changes are required to enable the product or system to continue in operation for as long as possible.

6.2.3 A good approach for 'future-proofing' is to take time at the start of the project understanding what the user's needs are and how these might realistically change over time. This is not a perfect science, but careful consideration will ensure that all reasonable options can be considered and costed, enabling the design to progress. Issues that will need to be considered include:

- Increases or decreases in demand;
- Changes in supporting technology;
- Changes in customer behaviour and expectations;
- Legislation changes;

6.3 Item Availability

6.3.1 The availability of product parts reduces over time as manufacturers cease to make them. Mechanical items can be remade if the drawings are available (or can be re-drawn). And depending on the application, the advent of 3D printing may ease the supply of old parts.

6.3.2 Electronic components, particularly semi-conductor circuits, are very likely to be hard to source as time moves on. Manufacturers move on to the next iteration of the item and may cease its manufacturing altogether and make something new. It is also possible that the manufacturer can cease trading.

6.3.3 In these cases, an alternative part must be found if the project or system is to remain in operation. This requires as full an understanding as possible of the functions and interfaces of the obsolescent item concerned so that a replacement can be properly specified. For legacy items, this is often hard to capture due to lack of appropriate documentation and loss of staff knowledge (see below). Designers today, should ensure that each item is properly documented to enable its replacement by something suitable in the future should the need arise.

6.3.4 The key functions include:

- Operating environmental conditions (e.g. temperature, humidity, pressure, power supply resilience);
- Input timing considerations, particularly for microprocessor and memory chips;
- Storage requirements (e.g. temperature, shelf time - especially for batteries, humidity)
- Earthing arrangements;
- Operating sequence, where the receipt of some information before other information may be critical but undocumented;

6.4 Staff Knowledge

6.4.1 The failure to maintain sufficient corporate knowledge of a product (e.g. its history of development, experience of in-service operation and failures, frequent faults and their remedies) can lead to a loss of knowledge about that product. The result can be a reduction in reliability, poorly installed products, poor maintenance and badly applied modifications.

6.4.2 This can be particularly relevant to software modifications, especially if it has been poorly documented.

6.4.3 The skills of staff need to be maintained because some will retire or move to another job. Training, comprehensive documentation and succession planning are tools to address this.

7. Configuration Management

7.1 Configuration management follows four main principles:

- Each piece of information or product is uniquely identified, not just by type, but as a unique item in its own right.
- Each piece of information or product can have a status associated with it, and a record of its history.
- The component parts that make up a product or system can be listed, and associated together. Documents can also be similarly related. Examples are a set of requirements documents for a system, or plans for related sub-projects.
- Associations between elements of a wider system can be captured, so that if one item changes, then it is known that another must also change.

7.2 Configuration management consists of four basic elements

- Identification.
- Change Management
- Status Accounting
- Audit and review

7.3 **Identification**. Set the identification system for each configured item. This will not necessarily be the same for each item. Documents will almost certainly need a different method from products for example. Thought should be given to the creation of a document tree, and product list.

7.4 **Change Management.** Changes have to be managed, otherwise people will be working from different sets of uncontrolled information, resulting in costly delays later on in the project. There needs to be a change control process that ALL changes go through. A system of version control is needed for both hardware and software. But the change process should also take into account the different needs of major and minor changes, so that changes are given the appropriate scrutiny and then authorisation. Baselines provide a useful means of controlling the issue of information, particularly where there are several pieces of information that are related (e.g. various different product specifications for one system). This enables others to work from a common set of information, and all changes and their impacts to be compared against a known position. Finally, any information that is out of date, must be withdrawn, and the change management process should enable this to take place and to demonstrate that is has occurred.

7.5 **Status Accounting.** This provides a view of the current status of configuration items (number of changes, those pending, actioned etc.). People can see what changes have occurred, and when they occurred. They can also see which proposed changes have been rejected.

7.6 **Audit and review** There is often pressure to deliver the job now and update the documents later. In the long term, this attitude can be costly to a project. Performing audits and reviews challenges people to adhere to the process. It also provides a record that the process has been followed.

8. Use of DRACAS and FRACAS

8.1 Introduction

- The terms DRACAS (Defect Recording, Analysis and Corrective Action System) and FRACAS (Fault Reporting, Analysis and Corrective Action System) are often used interchangeably. While they overlap, they are different.

- FRACAS specifically addresses faults and failures, i.e. when something is no longer performing its intended function. Such a system would typically be used by a maintenance organisation to manage and record in-service failures. Analysis of these failures can lead to quicker repair times as common faults can be highlighted and appropriate repair mechanisms or preventative measures put in place.

- DRACAS has a wider remit, embracing not only faults, but other incidents and observations which, combined with faults, provides a richer picture of equipment performance and can lead to a significant improvement in reliability. Such a system would typically be used by a design organisation as the item under consideration is developed for in-service operation. It may also be used by a maintenance organisation. It is good to start using a DRACAS as early in the lifecycle as possible to capture defects as they occur throughout design.

8.2 Defect Recording / Fault Reporting

8.2.1 The first step in the process is to record the defect (or record the fault). The initial details necessary are:

- Observed defect / fault
- The effect of the default/fault on the operation of the equipment and, if relevant, the safe operation of the railway;
- Date, time and location of where and when the defect was first observed;
- Details of what was happening at the time;
- Details of the equipment involved (type, model, manufacturer, serial number, software version)
- Details of personnel involved;
- Details of the person making the report;

8.2.2 The report record then needs to be stored. Supporting this should be a process that takes the recorded information and makes it available for relevant personnel. Such personnel could include:

- Designers;
- Maintainers;
- Operators;
- Safety engineer.

8.2.3. The information should then be used (alongside data from previous faults) for analysis and corrective actions to improve future performance.