Environment Project FIS5-1999-00355 wp5_ade039

CEMSIS:
Cost Effective Modernisation of Systems Important to Safety

Public domain case study: An example application of the CEMSIS guidance

v1.0

26/3/2004

Authors

PG Bishop, Adelard
RE Bloomfield, Adelard
MJP van der Meulen, Adelard

Revisions

v0.1	Initial document (inc. comments from BE)	24/07/03
v0.2	Draft for CEMSIS review	25/09/03
v0.3	Draft for Adelard review	31/10/03
v0.4	Draft for CEMSIS review	12/12/03
v0.5	Include review comments and additional text	30/01/04
v0.6	Include material from wp5_ade049	23/03/04
v0.7	Issue for CEMSIS review	26/03/o4
v1.0	Issue final deliverable	06/04/04

Circulation

Unrestricted

Contents

Glossary

The following abbreviations will be used in the document.

CEMSIS	Cost effective Modernisation of Systems Important to Safety
EEPROM	Electrically erasable programmable read only memory
EMC	Electromagnetic compatibility
I&C	Instrumentation and Control
MHS	Materials Handling Systems
MTBF	Mean time between failure
MTTR	Mean time to repair
OTS	Off the shelf
OTSP	Off the shelf product
PC	Personal computer
PLC	Programmable logic controller
SIS	System Important the Safety
TUV	Technischer Überwachungs Verein

1. Overview

This document is one of a set of guidance documents produced in the EU-supported project on the "Cost Effective Modernisation of Systems Important to Safety" (CEMSIS). This document aims to provide a practical illustration of the application of use of the CEMSIS guidance for the replacement of I&C systems important to safety , giving examples of best practice techniques and methods that can be applied during the lifecycle phases. The guidance includes the experience of the project partners on actual modernisation projects document and also incorporates the experience gained in applying the guidance to the CEMSIS case studies.

1.1 Introduction to the CEMSIS project

CEMSIS is an EU supported project on the "Cost Effective Modernisation of Systems Important to Safety" in the nuclear industry. There are many nuclear power installations within the EU which require maintenance and modernisation. These installations contain I&C systems that are regarded as "systems important to safety" (SIS). In the past, SIS were specially developed for the nuclear industry in a particular country. These systems would often be implemented using simple analogue, relay or discrete logic technologies that were relatively easy to analyse and justify. In addition SIS tended to be developed to comply with the requirements of a single national regulatory body. This situation has changed dramatically, SIS are now becoming heavily reliant on computer-based systems. The current control system market is subject to increasing globalisation. These issues pose considerable additional problems in the justification and regulatory approval of SIS refurbishments for nuclear plants in the Member States.

The CEMSIS project seeks to *maximise safety* and *minimise costs* by developing common approaches within the EU to the development and approval of SIS refurbishments that use modern commercial technology. The project consortium comprised European nuclear utilities, SIS suppliers, regulators and safety specialists. The objective of the project were to:

- Develop a safety justification framework for the refurbishment of SIS that is acceptable to different stakeholders (licensing bodies, utilities) within the Member States.
- Develop approaches for establishing the safety requirements for control system refurbishment together with an associated engineering process.
- Develop justification approaches for widely used modern technologies, i.e., COTS products and graphical specification languages.
- Evaluate these developments on realistic examples taken from actual projects.
- Disseminate the results of our work to plant operators and regulators within the EU.

This document is part of the dissemination process, and applies the guidance to a simplified, but realistic nuclear materials handling control system. These systems are common in both nuclear power production and nuclear fuel reprocessing.

1.2 Intended Audience

This SIS refurbishment example should be relevant to the:

Utility	Who has to establish the cost effectiveness of the SIS replacement, the requirements for the SIS replacement, and justify the safety of the replacement.
SIS supplier	Who has to supply the SIS and information required to justify the safety of the SIS.
Regulator	Who has to assess whether the safety justification of the refurbished system is acceptable.

1.3 Scope of the document

This document is an illustration of the application of the guidance developed in the CEMSIS project and should be read in conjunction with the other CEMSIS guidance documents, namely:

[1] CEMSIS Deliverable D1.2, "A Dependability Justification Fra mework for NPP Digital Instrumentation and Control Systems"

[2] CEMSIS Deliverable D2.3, "Requirements Engineering Best Practice Guide for Refurbishment."

[3] CEMSIS Deliverable D3.4, "Assessment and analysis guidelines for Off-The-Shelf Product-based Systems Important for Safety."

All public CEMSIS documents are available on the project web site (http://www.cemsis.org/).

It should be noted that the CEMSIS documents do not cover the entire modernisation lifecycle, but focus on the early phases of the project and the safety justification of the SIS.

In the remainder of this document we will use this symbol to indicate to the reader that more detail will be provided in the other CEMSIS guidance documents.

1.4 Structure of the document

Section 2 describes the modernisation process and the relationship of the CEMSIS guidance to this process. Section 3 introduces the materials handling system (MHS) that will be used to illustrate the guidance. Sections 4 to 8 illustrate the application of the guidance during the modernisation process, and Section 9 summarises the main benefits of using this approach. Appendices A to C provide supporting material for the application of the guidance to the materials handling example.

The remaining appendices cover more generic issues that supplement the other CEMSIS guidance documents. Appendices D and E compare the CEMSIS justification approach against existing methods, Appendix F discusses the factors that affect the cost-effectiveness of modernisation projects.

2. The modernisation process

The modernisation process is illustrated in the Figure 1 below:

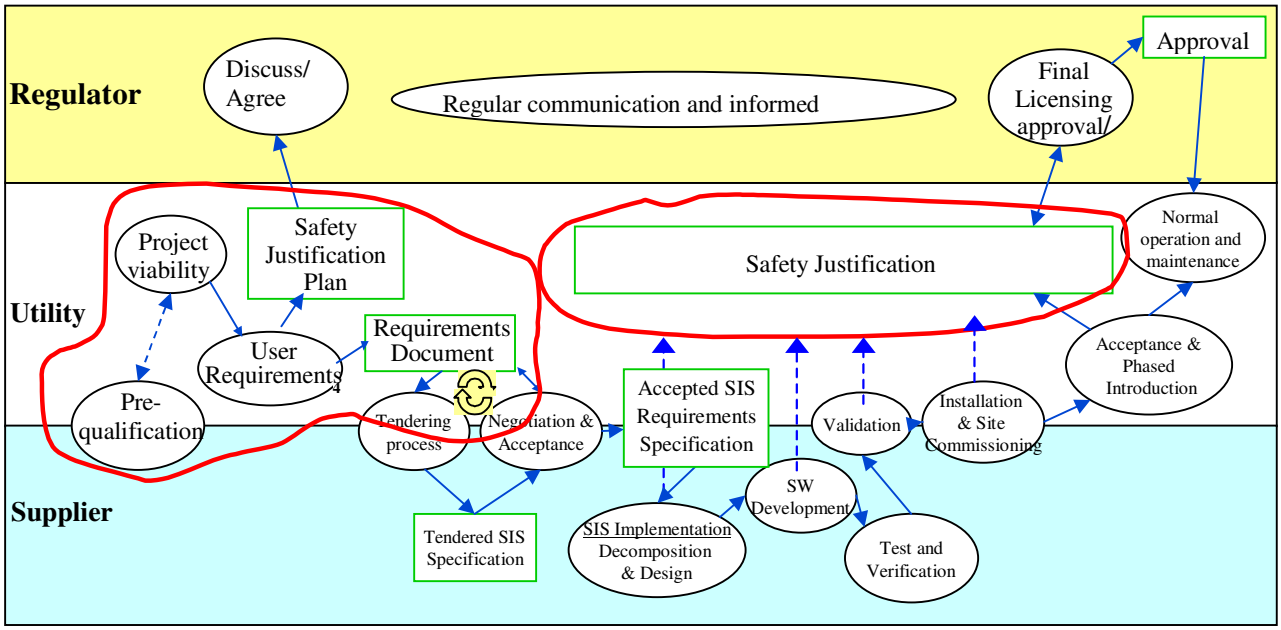


Figure 1: Modernisation process and CEMSIS guidance

The ringed portions of the process shows the phases that are addressed by the CEMSIS guidance, and the overall process activities are described below.

The diagram shows the activities undertaken by the three main "actors" in the modernisation process, namely:

- the utility
- the supplier
- the regulator

The detailed activities and interactions between the actors vary in different Member States but the main activities that can be undertaken in the modernisation process are:

- *Pre-qualification of COTS*. This activity can be shared between several projects and helps to minimise project risks by identifying and evaluating suitable COTS prior to project initiation.
- *Project viability*. The costs, benefits and feasibility of the proposed project are assessed to determine whether the project should be initiated.
- *User requirements*. The user requirements for the replacement SIS are established by the utility. The requirements for the existing SIS and the replacement SIS are captured and consolidated, and form the basis for tender by the I&C supplier.
- *Tendering and negotiation.* Tendered system design might not fit the utility's requirements exactly or may be too expensive. In addition, the supplier's tender typically includes more detail than the original user requirements, so there could be negotiations about alternative enhancements to the utility's original specification. Incompatibilities in the requirements may also be identified by the supplier. The negotiations could therefore result in a modified set of user requirements. These will be used to develop more detailed requirements for the SIS and its component parts.
- *Implementation.* The supplier develops the replacement system hardware and software.

- *Test and verification.* This would normally be undertaken by the supplier as part of the development process but, for more critical systems, additional test and verification might be performed by a separate organisation.
- *Validation.* This is undertaken jointly by the utility and the supplier. Typically there is some form of factory acceptance test where all user functional requirements are tested and the results are assessed by the utility.
- *Installation and commissioning*. The SIS is installed at the plant. This process could involve a repeat of earlier functional tests together with additional tests on the integrity of the plant interfaces. This is followed by progressive connection to the plant and commissioning tests up to full plant operation.
- *Acceptance and phased introduction.* The acceptance conditions could involve some "probationary period" where the use of the SIS is restricted and the restrictions gradually removed if satisfactory operation is observed.
- *Normal operation and maintenance*. In this phase, the SIS has to be operated in accordance with suitable operating procedures and the equipment has to be maintained to ensure that the SIS can perform its safety function.
- *Licensing activities.* For the SIS to be licensed, the utility has to produce a *safety justification* of the replacement SIS for the regulator, and this safety justification has to be accepted by the regulator.

The involvement of the regulator in the safety justification process tends to vary in the different Member States. The CEMSIS approach encourages a phased development of the safety justification in parallel with the development of the SIS and involvement of the regulator during the development. This allows the main safety justification arguments and evidence to be identified at an early stage (e.g. during the user requirements and tendering stages). This information can be used to ensure that suitable safety justification evidence is identified and made available by the SIS suppliers and it also makes it possible to gain early feedback from the regulator on the acceptability of the safety justification. This phased development of the safety justification should reduce the risk of licensing delays and economic losses if the plant cannot operate.

3. The materials handling system (MHS)

3.1 Plant context

The materials handling system (MHS) SIS is part of a processing system for radioactive material. Nuclear material, stored in cans, is transferred between processing units by a material transporter, as shown in Figure 2 below.

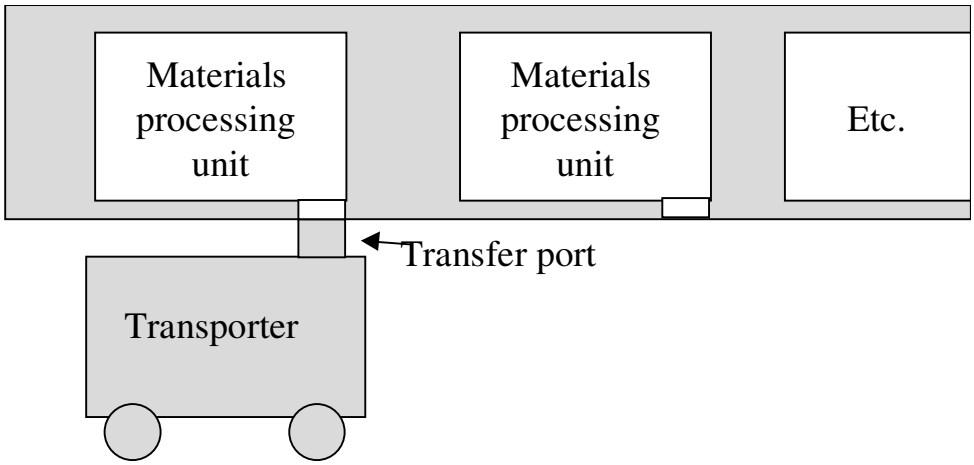


Figure 2: Materials Handling System

The material in the transporter is stored in individual vertical chambers in a shielded rotating assembly (the "carousel"). The carousel can be connected via a transfer port to a processing unit and, once connected,

radioactive material is either drawn into the carousel or discharged into the connected unit using a manually operated mechanical grab and hoist.

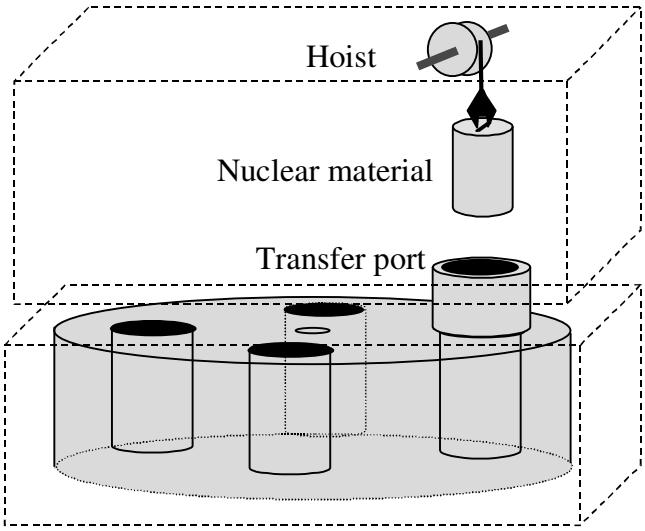


Figure 3: MHS: transfer post and carousel

The carousel is a buffer store and is filled by rotating the carousel and transferring the material into successive chambers until all the chambers are filled. To connect with a different processing unit, the transfer port is disconnected from one unit, then the transporter moves to a new unit and is reconnected via the transfer port, so the carousel can be emptied (and possibly refilled with material for the next location).

Clearly it is important that the carousel is only rotated when it is safe to do so. Some plant hazards related to the MHS are listed below:

Hazard	**Consequence**
Rotation of carousel while hoist active	Rupture of container Radioactive contamination within cell
Rotation of carousel past end-stops	Motor burn-out Operational delay
Carousel chamber not aligned with transfer port and hoist operation allowed	Rupture/jamming of container during transfer Radioactive contamination within cell of container on down hoist
Movement of transporter while hoist active	Rupture of container Radioactive contamination within cell Transfer port broken External radiation leak
Transfer port closed while hoist active	Rupture of container in transfer port Radioactive contamination within cell
Transporter moves without undocking	Transfer port broken External radiation leak

Table 1: MHS plant hazards

To prevent these hazards, the MHS logic implements a set of interlocks that only allow carousel movement, docking, undocking, hoist operation and transporter movement when the action is safe.

3.2 Legacy control system and interfaces

The legacy control system for the MHS has separate control logic units and control panels for:

- moving the transporter and locking the transporter
- controlling the docking of the transfer port
- controlling the carousel and aligning a chamber with the transfer port

The hoist is controlled separately from the materials handling cell and the hoist status is signalled to the MHS transporter via the transfer port when it is docked.

For simplicity, the illustrations used in this document will relate to only one of the MHS functions—the carousel control function, which is described in more detail below.

3.2.1 Carousel logic functions

The carousel control logic comprises:

- Interlock logic
  – to disable carousel movement (if transfer is in progress)
  – to disable hoist movement (if carousel is being rotated)
- Control logic – to implement operator controls to move the carousel and align the next chamber with the transfer port
- Indicator logic
  – current status of the carousel
  – current status of the transfer port

3.2.2 Carousel control panel

The operator interface is shown below.

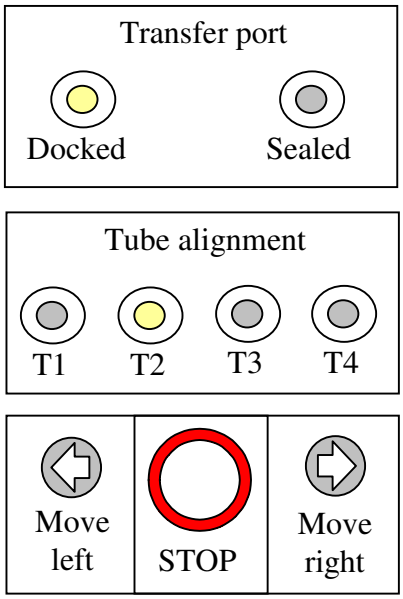


Figure 4: MHS operator control panel

3.2.3 Carousel logic implementation

The original carousel control system was implemented using discrete logic. The main type of logic used in the design is the 'Sum logic" unit. This logic sums two or more logic inputs and generates TRUE if the sum exceeds a specified limit. By changing the limit setting of the Sum logic, it is possible to implement AND gates, OR gates or more complex functions like 2 out of 3 voters.

Two independent sets of relay-based safety interlocks are used to prevent incorrect operation. The interlocks are also implemented within the control system.

Relays are used to interface the logic to the sensors and actuators. The type of relay (normally open or normally closed) is chosen to ensure fail-safe behaviour. For example, if power is lost to an interlock signal,

the input state of the relay disables the movement of the carousel. The same approach applies to failures of output relays.

Control system output signals are used to activate:

- the leftward carousel drive motor
- the rightward carousel drive motor
- high speed drive mode
- low speed drive mode
- carousel alignment position indicators (T1 to T4)
- transfer port status indicators

The carousel rotation outputs control two separate carousel drive motors. Two other outputs select fast and slow movement —slow movement is used when a chamber is close to alignment with the transfer port. It is also possible to 'hand-wind" the carousel to correct alignment problems.

The carousel cannot rotate more than 330° so there are end-stop sensors to detect when the carousel has reached the end of travel (left and right).

The inputs to the control unit comprise:

- Transfer port status signals (whether docked/undocked and sealed/unsealed).
- Hoist status and interlocking signals (via docking port).
- Chamber alignment status (coarse and fine alignment for each tube).
- Left and right end-stop sensors.
- Hand wind mode.
- Maintenance mode.
- Left and right movement pushbutton.
- Emergency stop pushbutton.

3.3 Operation and maintenance of the transporter

The transporter is subjected to periodic testing every few months. There are procedures for periodic checking of the safety interlocks.

In operation, the transporter has to be docked via the transfer port. Once connected, the transfer port is unsealed and once a chamber is aligned with the transfer port, a container of nuclear material can be transferred with the hoist. The carousel is then rotated until the next chamber is aligned so that another container can be transferred. This continues until all chambers are filled. The transfer port is then sealed and the transporter is disconnected from the processing unit. The transporter can then move to a new processing unit, be reconnected and unloaded. Hence the transporter has three main operational modes:

- Transporting
- Docking
- Handling

Carousel rotation and hoist operation is only allowed in the handling mode. This is enforced by only switching on the electrical supplies to the hoist and carousel drive motors in handling mode.

Carousel rotation is controlled by an operator using pushbuttons. Indicator lights show when the next chamber is precisely aligned with the transfer port. Indicators also show when the transfer port is docked and

whether it is sealed. To correct carousel positioning problems, the carousel can be "hand wound". Motor drive operations from the control panel are disabled while hand-winding takes place.

4. Project viability phase

A key phase in the whole process is the viability study of a SIS replacement. In some cases, the company has no choice in the replacement decision, e.g. it may be imposed by the regulator. However in the majority of cases the company would have to make a decision whether the system should be replaced. Typically there are budget restrictions, and some priority order is assigned to replacement projects.

The replacement decision has to balance the feasibility and cost of maintaining the existing system and the costs and benefits of a replacement. A major parameter in the cost would be project overruns beyond the planned plant outage time. This could be due to technical problems or licensing problems. While it is difficult to assess the risks accurately before tender, the risks of implementation and licensing delay may be reduced by imposing constraints on the tendered system.

As described in the CEMSIS requirements guidance [2], this phase has to consider:

- The purpose of the replacement.
- The advantages it provides.
- Whether the advantages exceed the costs and effort involved in replacing the SIS.
- An assessment of the project risks and feasibility of the replacement.
- Assessment of safety implications.
- Whether the replacement is optional or inevitable.

Based on these points, the stakeholders need to decide whether to go ahead with the project.

4.1 Project viability of MHS SIS replacement

In this instance, the motivation for replacing the MHS was impending obsolescence of the hardware and increasing unreliability. Using the approach outlined in [2], an assessment was performed that reviewed:

- the current maintenance difficulties
- the current operational performance
- the cost benefit implications of a replacement system
- the potential causes and costs of implementation overruns
- specific constraints on the implementation of the replacement

Table 2 below summarises the results of the project viability stage.

System boundary	MHS sensor, actuator and operator interfaces
Scope	Replacement of the control and interlock logic of the MHS (for movement, docking, operations)
Stakeholders	Plant safety department, I&C department, Maintenance department, Plant operations, regulator

Reason(s) for replacement	Obsolete components Spares stock likely to be exhausted in 5 years Unreliability increasing, 1 in 10 materials handling operations delayed by >10 minutes (requires manual override) Maintenance cost (24 hour): •180 000/year Cost of production delays: •750/day
Cost of replacement	Spec and tender: •85,000 Equipment: •75,000 System design: •120,000 Installation: •75,000 Safety Case: •180,000 Maintenance (12 hour): •75,000/year Excess outage cost: •15,000/day
Project risk(s)	Implementation delay. Functional complexity of the MHS logic is low - should be capable of implementation in any technology. Licensing delay. Might be hard to demonstrate adequate safety integrity if the safety interlocking is only implemented by a replacement programmable system. Programmable systems also have to meet new regulatory requirements.
Assessment	The equipment must be replaced within 5 years. Yearly savings should be around •240 000. Replacement costs recovered in around 2 years. Licensing delay could be expensive: a 36 day production delay could double the replacement costs. Recommend reducing licensing risk by either: • Retaining existing relay-based interlocks and replicating the safety interlocking function within the programmable system. • Updating entire system using modern fail-safe discrete logic components.
Decision	Priority 1 (proceed immediately) Replace MHS control logic and replicate the safety interlocking. Priority 2 (review yearly) Replace the external MHS safety interlocks by an alternative system.
Functional requirements	Must replicate the existing MHS control logic functionality and safety interlock logic.
Constraints	The existing relay-based safety interlocks must be retained. Programmable systems must demonstrate compliance with new regulatory requirements. Must be capable of installation and operation in the existing equipment bays on the transporter. Replacement budget: •600,000.

Table 2: Results of project viability study

On the basis of this study, a project was initiated to procure a replacement for the MHS logic.

5. MHS requirements

Once the replacement decision is made, it is necessary for the utility to prepare a requirements document for tender. The requirements document has to include any constraints identified in the project viability stage, e.g.:

- preferred technologies
- preferred suppliers
- regulatory requirements
- budget constraints
- safety constraints
- plant constraints

However the bulk of the requirements are established in the user requirements phase. The CEMSIS guidance outlined in [2] defines a two-stage requirements capture process:

1. Identify the requirements for the existing system, i.e. collect information about the existing system and its environment and to establish the design basis for the current SIS.
2. Identify potential new requirements, such as revised functionality, user interfaces, test support, etc.

The details of this process are outlined below, and illustrated in relation to the MHS SIS.

5.1 Establishing the design basis (requirements before modernisation)

5.1.1 Identification of the design basis

Following the process described in [2], the data gathering process for the existing MHS system comprised:

- Assembling information about the existing system:
  1. Establishing the existing safety claims for the logic from the plant safety case.
  2. Obtaining the original logic drawings.
  3. Obtaining design documentation.
  4. Obtaining plant interface documentation.
  5. Obtaining documentation on equipment and components.

- Assembling information about the system environment, including:
  1. Plant descriptions and schematics.
  2. Plant safety report.
  3. Operator interface drawings.
  4. Plant operating and maintenance modes.
  5. Operating procedures.
  6. Maintenance procedures.
  7. Operational safety and problem reports.

Some example design basis documents are shown in Appendix A.

Strictly speaking, a "clone" of the existing MHS logic should not need information about the system environment because the required logic should be unchanged. In practice, however, knowledge of the behaviour of external systems and support environment surrounding the MHS is helpful in understanding the existing logic and in assessing the impact of proposed changes.

The MHS design basis documentation was then reviewed for consistency and currency, i.e. that:

- all documents and drawings were up to date
- the documents were internally consistent (cross referencing, identification of inputs and outputs, etc.)

- the MHS logic drawings agreed with the logic wiring in the MHS control cabinets
- the MHS safety functions were consistent with the plant safety requirements
- the MHS safety function availability and integrity requirements were consistent with the plant safety requirements
- the design safety rules and principles were applicable
- the MHS operating and maintenance procedures were complete and consistent with actual practice

Any inconsistencies and problems were recorded and resolved. For example, the consistency of the MHS logic drawings relative to the implemented logic on the plant was verified by:

- checks of the master drawings against local maintenance copies
- checks for consistency of the interconnections between drawings
- checks of the drawings against the actual plant connections

Two discrepancies in the MHS design basis documents were detected during this stage:

- A simplified logic schematic diagram was used to show the interconnections between major functions but omitted some of the interconnection details present in the more detailed drawings.

- One of the local maintenance copies contained a manual modification that had not been included on the master drawings.

Both these inconsistencies were resolved as follows:

- The schematic was updated to include a warning that some interconnections were not shown, and with references to the relevant drawings.
- A review was performed to determine why the change had been made and whether the manual change should form part of the design basis. The difference between the master drawing and a local maintenance copy was corrected by incorporating the maintenance version changes in the master drawing and issuing new copies of the master drawing.

The design basis document set was updated to reflect the revised versions of these drawings.

5.2 Analysis of design basis documents

The design basis documents have to be analysed to determine the operational, safety and maintenance requirements of the current system. This includes:

- the safety claims associated with the SIS logic
- the definition of the SIS interfaces
- the dependability requirements for the SIS
- the functional behaviour of the SIS
- the safety-related functionality of the SIS
- any real time performance requirements
- any known problems with the SIS
- any existing constraints (physical, environmental, etc.)

The analysis of the design basis documents are discussed in the sections below.

5.2.1 Establishing safety claims for the logic

The plant safety report for the transporter made a claim that the MHS safety interlocks preclude all identified plant hazards due to MHS operations. The safe operating states for the MHS components are summarised below:

Hoist operation

MHS component	State
Transporter	Stationary AND Locked
Transfer port	Docked with cell AND Open
Carousel	Stationary AND Aligned with transfer port

Carousel operation

MHS component	State
Transporter	Stationary AND Locked
Transfer port	Docked with cell AND Open
Hoist	Retracted
Carousel	Within rotation limits

Docking / Undocking operation

MHS component	State
Transporter	Stationary AND Locked
Carousel	Stationary
Hoist	Retracted

Transport operation

MHS component	State
Transfer port	Undocked AND Sealed
Carousel	Stationary AND Locked
Hoist	Retracted

5.2.2 Definition of the SIS interfaces

There should be documentation defining the interfaces between the SIS and the plant. This should not only include the connections, but also the behaviour of the interfaces.

In the case of the MHS there was a full input-output schedule, but it was important to capture the semantics of the input interfaces. For example, the interface signals were often implemented by relays with a pair of complementary inputs (i.e. one switch is closed and the other is open). The relays and switches can also have "make before break" or "break before make" behaviour. This determines whether the transient changeover state is "open-open" or "close-close" or other similar combinations. Relays can also have a default state of "normally open" or "normally closed", which determines the input state if interface power is lost or the relay fails. The following information was captured in the interface schedule:

Relay ref.	input signal	default state	Relay id.	Plant parameter (when closed)
R123	a	normally open	RMK24	Hoist retracted
R123	b	normally closed	RMK24	Hoist not retracted

Table 3: Extract for the MHS interface schedule

Restrictions on input interface restrict the range of behaviours in the logic and hence might be essential to maintain safety. Knowledge of input constraints can also affect the testing approach (i.e. the choice of input pair values).

The other aspect of the interface behaviour that is relevant to replacement is the changeover time of the relays. With discrete logic, processing of changes is almost immediate, but for a computer-based solution there is a finite scan time. If the scan time is greater than the changeover time, it is possible to observe "impossible" input combinations (e.g. both contacts being closed in the transient state on a relay where the

transient state should be one open and one closed). The current logic might rely on the "impossible" states being absent to avoid glitches, but this assumption might not be valid for the new implementation. So we also need to have a performance specification for the interface components, as shown in the example table below.

Relay id	Type	Close time (millisec)	Open time (millisec)
RMK24	Complementary pair "break before make"	35	40
RMK25	Latching relay	…	…

Table 4: Example relay interface characteristics

Also, to support reliability and safety assessments of the overall system, information on failure rates and failure modes should be provided. These can either be based on manufacturers data sheets or direct experience on the plant.

5.2.3 SIS dependability requirements

Ideally a SIS should never fail, and certainly not fail dangerously, so that the SIS satisfies the plant safety conditions at all times. In practice, equipment could be subject to unsafe failures, e.g. where an operation is permitted in the wrong plant conditions.
The required dependability properties need to be specified. These might include:

- probability of failure on demand (for demand-based systems)
- MTTF
- availability
- safe failure fraction (probability of a dangerous failure mode)

The nuclear materials plant had a quantitative safety case for the plant as whole, and this allowed a quantitative probability of unsafe failure to be set, which was derived from top level risk target for the plant as whole. For the MHS SIS, a decision had been made at the project viability stage to retain the external safety relays, and replicate the control *and* interlock logic within the SIS. Internal implementation of the interlock logic reduces the likelihood that a demand will be placed on the external safety relays. The dependability targets for the replacement SIS in the MHS were set at:

10^{-2} failure per demand (interlock movement logic)
10^{-4} failures per hour (spurious actuation)
1 hour MTTR (any failure)

As there are separate safety interlocks, the SIS is classified as a Class B control system under the IEC 61226 scheme [5]. In other circumstances (e.g. where the external relays were becoming obsolete), the replacement might have included the external relays so the target failure per demand might then have been set at 10^{-4} for the protection logic and the MHS SIS would have been classified as a Class A system.

Integrity requirements can also be expressed in terms of qualitative design safety rules. The rules underlying the design need to be captured. These may already be expressed in company design safety rules, by consulting design documentation, or by consulting the original designers (if available).

The utility had a defined set of safety rules that included the following requirements:

- Power failure should result in SIS outputs that maintain plant safety.
- Input-output failures should result in SIS outputs that maintain plant safety.
- No single failure should result in an unsafe control action.

These design safety rules have to be included in the requirements for the SIS that implemented the MHS logic replacement.

5.2.4 Functional behaviour

Logic drawings might be the primary source of information for the required behaviour of the logic. As described in the CEMSIS requirements guidance [2], it is important that the documentation set is consistent, correct and current, i.e. cover all the installed logic systems within the system boundary and is consistent with the actual logic implementation. However it is also important to analyse design documents that have appropriate level of detail. High-level drawings are likely to omit design detail and should be used to aid understanding rather than for the elicitation of detailed functional requirements. For the MHS, the official drawings were all correctly filed and complete.

An example of the legacy logic produced is shown in the figure below:

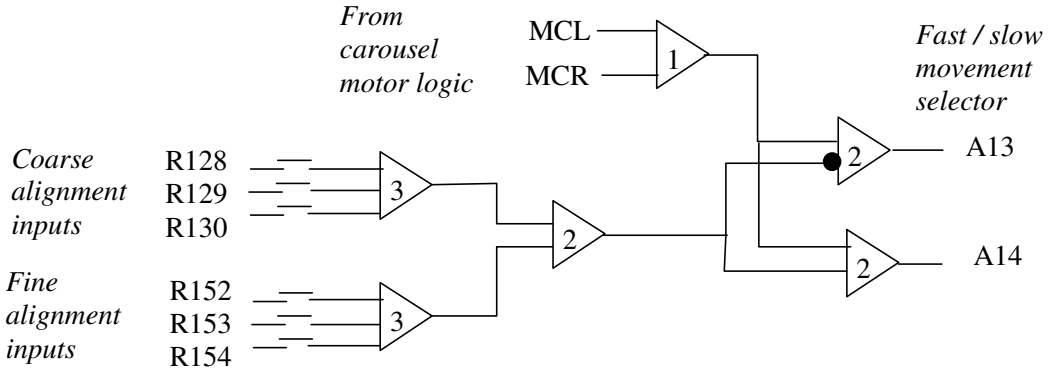


Figure 5: Example of existing logic diagram

The logic gate sums the input voltage and generates a unit output voltage if the sum exceeds the limit value (3, 2 or 1 in the example above). The logic example processes the triply redundant alignment signals that indicate that a chamber is aligned with the transfer port. The function of the logic is to ensure the carousel rotation is slowed before the chambers are fully aligned. This is to prevent overshoot, as there is a lot of inertia in the carousel.

The behaviour of the existing logic has to be known in order to replicate it (or re-engineer it) in the replacement system. To establish the design basis it was necessary to:

- identify the components used to implement the existing logic
- locate the supporting documentation for the components that specifies their behaviour
- verify their behaviour (e.g. are there any omissions or inaccuracies?)

This could have been problematic in the case of the MHS. The manufacturer of the logic components was no longer in business, and even if the company had been operational, there would have been no guarantee that it would maintain documentation for obsolete components.

Fortunately a full set of documentation on the commercial logic modules had been archived at the plant site, and it was possible to talk to I&C engineers who had experience with the logic. This illustrates the need to keep documentation on commercial components as part of the overall configuration management system for safety-related equipment (not just system design constructed using the components). The logic documentation was incorporated into the requirements documentation, together with a representation of the Sum gate in terms of more conventional AND/OR logic.

While logic diagrams are one means of expressing the functional behaviour, there may also be design requirements documents where the functionality is expressed in different terms (e.g. in natural language).

In the case of the MHS, a design document existed that included design requirement specifications such as:

1. When commanded via the operator pushbutton, rotate the carousel left (or right) and stop when the next chamber is aligned with the transfer port.
2. When a chamber is close to alignment with the transfer port, the carousel should rotate at its slow speed setting.
3. Operator indicator lights should indicate when:
   a) one of the chambers is aligned with the transfer port (and stationary).
   b) the transporter is docked via the transfer port to a processing unit.
   c) the transfer port is open (unsealed).

These requirements have no direct impact on safety, as there is a separate interlock logic hardware that prevents operation if the equipment is in the wrong state (e.g. hoist action is prevented if the port and chamber are not fully aligned). However reliable operation is important as failures place extra demands on the safety logic, e.g. a false indication might lead the operator to request an unsafe movement of the MHS.

5.2.5 Safety functionality of the SIS

The safety-related functions of the SIS should also be captured as part of the design basis document set. The original logic diagrams are one means of defining the required safety behaviour of the SIS, but there may also be design documents that express the requirements textually.

In the case of the MHS, a design document existed, which included the design requirement specification. An extract of this document is shown below:

1. Carousel movement is only allowed if all the following conditions apply:
   a) the transfer port is docked
   b) the transfer port is open
   c) the transporter brakes are on
   e) the hoist is fully retracted

2. Carousel rotation can be stopped at any time by pressing the emergency stop button.

These safety requirements could have been inferred from the logic design, but the intended functionality can be obscured by extra complexity to satisfy integrity and availability requirements. An explicit set of safety requirements also clarifies the purpose of the implemented logic and can be used to define acceptance tests.

5.2.6 Real-time performance

The existing design might have real-time performance characteristics that are necessary for correct operation, such as:

- response time
- maximum throughput rate

The real-time performance requirements should be determined if they are not fully documented in the existing documents (e.g. if they are implicit in the logic design).

In the MHS, the carousel has considerable inertia so the chamber alignment sensors are positioned to take account of the reaction time of the logic and stopping time of the carousel. The replacement logic should have a similar reaction time to ensure the chamber is correctly aligned when it stops.

The data gathering process failed to identify any documentation of the required response time, so an investigation was undertaken to derive that information. The reaction time of the existing logic implementation was computed from the response times quoted in the logic gate manufacturer's specification

sheet. With a 1 millisecond switching time per gate, the response of the logic circuitry was estimated to be 5 milliseconds.

Discussions with the plant designers suggested that the carousel stopping time was around 2 seconds, and that a reaction time error of 0.1 seconds was tolerable for maintaining alignment.

5.2.7 Operational and maintenance requirements

The operational and maintenance procedures were identified and the set of operating procedures are incorporated into the design basis documentation. The operating and maintenance procedures should be checked for completeness and correctness (e.g. by consultations with operations and maintenance staff).

A full set of MHS operations and maintenance procedures were identified. Typical examples of maintenance procedures are:

Maint. procedure ref	**Title**
PR/MT/MHS/08	Carousel movement interlock tests
PR/MT/MHS/09	Hoist safety interlock tests
PR/MT/MHS/09	Docking system tests

Table 5: Example MHS maintenance procedures

These documents may need to be updated when the MHS SIS is replaced. It may also be the case that a new technology may not be so easily testable, so additional requirements for test support features may be needed for the replacement system.

5.2.8 Outstanding issues with the current equipment

There may be documentation identifying performance and safety problems encountered in the existing system. This information can be reviewed and used to update requirements in the replacement to overcome the problems. The following documents were reviewed to identify outstanding problems:

- Operations reports.
- Maintenance reports.
- Engineering change requests.
- Safety review recommendations.

As a result of this analysis a set of problem reports were identified as a basis for assessing whether any of these issues could be addressed in the replacement system.

5.2.9 Physical constraints

Due to the limitations imposed by the mobile transporter, significant physical constraints were identified relating to:

- available space
- weight
- power supplies

5.3 New requirements for the replacement system

While the data gathering and validation of the existing requirements (and design basis) provides a solid basis for the existing system, it may not be sufficient for the replacement system. In most cases, the replacement system differs from the one it is replacing and there are new requirements that need to be taken into consideration. The possible reasons for changes in the requirements for a new SIS are described in [2]. Below we describe the new requirements identified for the MHS SIS.

5.3.1 New regulations

The company policy had changed since the original system was constructed. Programmable systems have to compliant to IEC 61508 SIL2 [6] for a Class B [5] safety function.

5.3.2 Assessment of outstanding issues with the existing system

Problems experienced with the existing system can be analysed to help identify any additional requirements for the replacement system. Documents identified in the data gathering process (see Section 5.2.8) were reviewed for outstanding issues. Experience was also captured by direct interviews with the operators and maintainers of the system.

An example of a minor safety problem with the MHS is that there was no display of the *direction* of movement of the carousel. If the wrong button is pressed when the carousel is at the limit of rotation, it will move towards the end-stop. As there is no indication of direction (or warning), the operator is not aware of the error and cannot rectify the situation by hitting the emergency stop and reversing direction. To address this problem, there was an engineering change request to:

a) have an operator interface that displays the direction of travel, or
b) prevent movement in the wrong direction if the operator hits the wrong button (and warn the operator)

This request had previously been rejected by the plant modification review panel as the power and space constraints made the addition of the new function infeasible. The request was reviewed again for the replacement system, and it was agreed to add a requirement for carousel direction displays on the replacement SIS, as it would reduce operational errors and delays.

Other operational problems might affect productivity rather than safety. An example of an operational problem reported on the existing MHS is that availability is lower than planned because the interface relays fail relatively frequently (but in a safe direction). This disables the MHS until it can be repaired. Such failures reduce the amount of material transported hence the maximum throughput of the plant. Availability might be improved if extra diagnostic logic made use of redundant interface signals to detect failure (e.g. by comparing complementary pair inputs) and report it to the maintenance engineer. This option was reviewed but rejected, because manual positioning can be invoked in these circumstances (under a defined procedure) so little time would be gained by faster repair.

5.3.3 Maintenance changes

The company wanted to change the maintenance policy, e.g. reduce staffing, shift working and extend the proof test intervals. Such constraints have to be documented within the new requirements as they will affect the assumptions underlying the reliability and availability calculations of the replacement SIS.

In the case of the MHS, there was a policy change to keep maintenance staff during the day only. Consequently, the average repair time would increase to around 7 hours, rather than the nominal 1 hour repair assumption with 24 hour staffing. This has to be taken into account when specifying the MTBF to ensure adequate system availability is maintained.

In addition, an analysis of the maintenance test procedure PR/MT/MHS/09 for the existing system showed that a series of tests had to be performed on the interlock logic, as shown below.

```
PR/MT/MHS/09
MHS Movement permissive interlock testing
Rev 4
21 March 2001
1. To configure the system for proof testing, follow procedure
PR/MT/MHS/01
2. Place a voltage probe on movement permissive terminal connector
TC/16/73
3. Energise all interlock input signals (TC/15/01 to TC/15/36)
4. Verify that the movement permissive signal (TC/16/73) is energised
5. De-energise TC/15/01 and verify that (TC/16/73) is de-energised
6. Energise TC/15/01 and verify (TC/16/73) is energised
7. Repeat for inputs TC/15/02 to TC/15/36
```

It can be seen that this procedure involves placing a probe on the final movement interlock output wire in the MHS logic cubicle, and then simulating interlock signal inputs to check logic operation. For a computer-based replacement of the MHS logic, this particular "probe" location would be inaccessible, as it would be implemented in the software. To address this difficulty, a requirement was added—an additional output was specified to display the computed movement interlock status. This enabled the current test procedures to be followed using the output display rather than a test probe connection (this change was subsequently incorporated into a new version the PR/MT/MHS/09 maintenance procedure).

5.3.4 Operational changes

There were changes in the operating modes of the plant that had to be supported within the replacement SIS: the company is implementing bar-code labelling of the materials containers throughout the plant. Previously, information about which drum is located in a given container was recorded manually on paper records. To automate this process, there was an additional requirement on the replacement system to read the bar code and record which chamber holds a specific drum. This should reduce operator errors where the wrong drum is delivered to a cell and avoid the risk of putting two containers in the same chamber.

5.3.5 Installation and commissioning constraints

The design basis data gathering process would have identified a number of physical constraints for the replacement SIS such as:

- space
- weight
- temperature
- power supplies

In addition, requirements could be imposed by the transition from the legacy system to the new system, e.g.:

- requirements for parallel operation of the legacy system and replacement system (together with greater environmental constraints)
- requirements on equipment delivery and installation times (e.g. to fit in with planned outages)

In the case of the MHS, parallel operation was impossible due to the physical constraints of the transporter. The replacement had to be scheduled for a planned outage. It was therefore important that the transition was implemented within the outage period of 40 days, and that the SIS replacement should be ready for installation at the next planned outage.

5.3.6 Safety justification requirements

Safety justification is described in more detail in a later section, but it is desirable for the utility to identify what aspects of the safety justification should be provided by the utility and which should be provided by the supplier. Documentation needed to support the safety justification should be part of the supply contract. In the case of the MHS, the utility was responsible for defining and validating the required safety behaviour, and the supplier had to indicate what design features and development processes would be used to ensure that the supplied system could implement the required functionality.

In addition, since correct definition and interpretation of the functional requirements is essential to safety, the tender requirements also included a continuing requirements validation activity. The control logic functions was to be implemented by the supplier and evaluated by utility safety and control engineers prior to full development. This allows the functionality of the SIS to be clarified at an early stage before dealing with other implementation issues issues (such as interfacing to the plant, assuring fail-safety, timeliness, etc.).

5.3.7 Integration of existing requirements with new requirements

The integration process combines the design basis information (the *requirements specification* for the existing requirements) with the additional requirements identified for the replacement system. This is part of the analysis phase of the new requirements part of the requirements engineering process. As described in [2], this consolidation process will:

1. Integrate existing requirements with new requirements.
2. Analyse the new and existing requirements for consistency and resolve any inconsistencies detected.
3. Remove requirements of the old system that are not relevant for the new system.
4. Remove redundant requirements.
5. Validate the requirements.
6. Review of the technical feasibility of the new requirements.

Additionally, the requirements should be structured in a coherent format.

In the case of the MHS SIS specification, the following functional changes were made to the requirements:

1. The obsolete logic relating to the self-tests of the Sum logic hardware were removed.
2. Addition of an interlock logic status display (to aid testing).
3. Operator interface change to show carousel movement direction (to reduce operator error).
4. A maximum response time figure of 100 milliseconds was specified.
5. Addition of a barcode tracking function to identify the drum that is located within a given chamber.

In addition, the control logic was re-specified in more conventional terms using AND/OR gates, updated to incorporate the changes and validated. An extract from the revised logic specification is shown below.

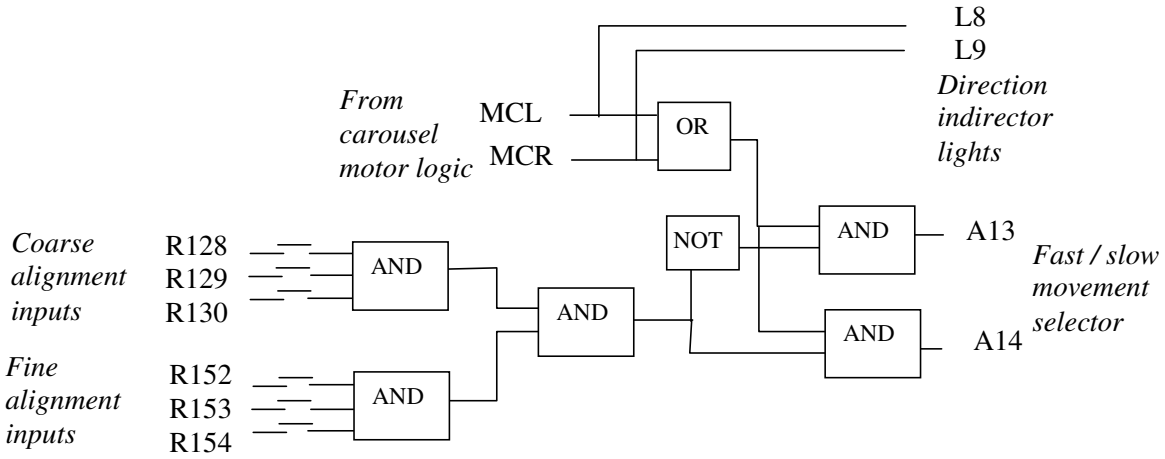


Figure 6: Example of re-specified logic (including extra direction indicator signals

A set of constraints were also specified:

1. Required environmental immunity levels (RFI, EMI, temperature, etc) .
2. A requirement for IEC 61508 SIL2 compliance [6] was included for the carousel logic.
3. Space, weight and power limits (which were quite limited as it is located on a mobile transporter).
4. Installation and commissioning time constraints.

The tender document was produced and included:

- plant context information
- plant interface details
- the SIS replacement requirements and constraints
- evidence requirements for the safety justification.

An example of the material included in the utility's equipment refurbishment requirements documents is given in Appendix B.

6. The tendered system

The successful bidder tendered the following system to implement the MHS SIS. The unshaded boxes represent the components of the replacement system.

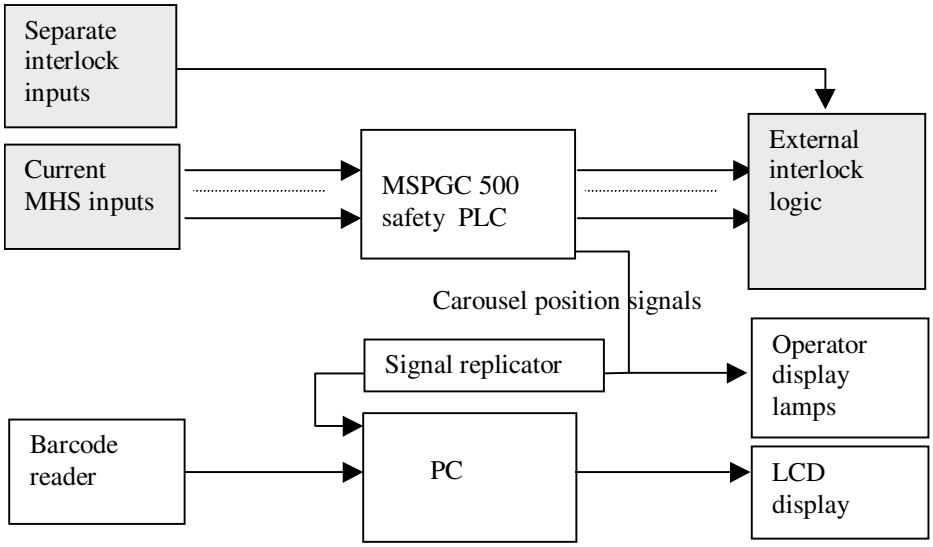


Figure 7: System design tendered by the supplier

A fail-safe PLC (dubbed the MicroSafe MSPGC 500 Safety PLC) replaces the existing discrete carousel Sum logic hardware, and some of the output signals (showing which chamber is aligned with the transfer port) are used as inputs to the bar-code reader. Bar-code data is not safety-related, so the function is implemented on a low integrity industrial rack-mounted PC. The signals from the MSPGC 500 to the PC are electrically isolated to prevent interference with the carousel control functions.

This design illustrates the recommendations in [3] where design of the system architecture limits the consequences of failures in COTS components (which in this example are the MSPGC 500 and the PC-based bar code reader). In this architecture:

- Failures of the MSPGC 500 are covered by external safety relays.

- PC failures (both hardware and software) are prevented from propagating to the MSPGC 500 by a one-way signal replicator.

The MSPGC 500 was chosen because considerable pre-qualification evidence existed to show that is suitable for the intended application (see [3] for more details). This helps to reduce uncertainties in the feasibility of implementing the intended application. In the pre-qualification, the MSPGC 500 was subjected to an assessment appropriate to a Class B safety system, and this pre-existing evidence can help to reduce licensing risk, and reduce the cost and effort needed to obtain evidence for the safety justification.

As the PC does not provide any safety functions it is not be included in the safety justification, but evidence is needed to show that the signal replicator provides adequate isolation and is fail-safe.

The revised operator panel (Figure 8) has a similar layout to the original panel to reduce the risk of operator errors due to unfamiliarity.

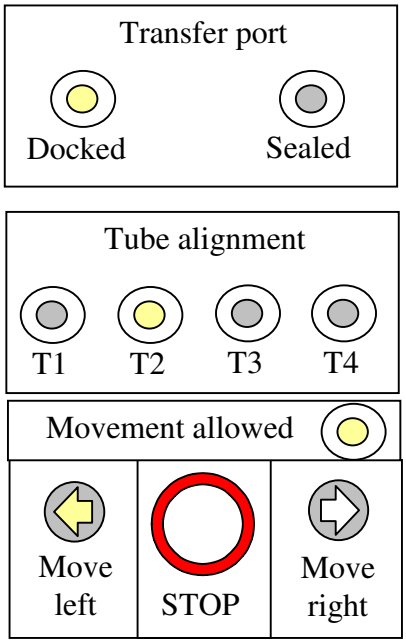


Figure 8: Revised control panel

In the revised panel the movement button is illuminated when the relevant motor drive is active. This design makes it easy to argue that the usability of the system is at least as good (and probably better) than the old system where there was no indication of movement direction.

The additional "Movement allowed" lamp presents the interlock status to the operator (so he does not think the equipment is faulty if there is no movement when the button is pressed). This light is also replicated on and the MSPGC 500 back panel and is used for testing the movement interlock logic. This replaces the potentially hazardous maintenance activity of putting a probe on the interlock wiring. So it is possible to argue that the protection against maintenance hazards should also be "at least as good as old".

The overall approach to developing the safety justification for the replacement MHS SIS is described in sections below.

7. Planning the Safety Justification

The plan for developing a safety justification has to:

- Define the structure and evolution of the safety justification.
- Decide on the regulator interface.

- ♣ Define who does what (regulator, supplier, utility).

7.1 Evolution of the safety justification

In many industries, the safety justification is developed in stages, starting with an identification of the claims that need to be made by end-user, e.g.

- The specified functional behaviour (if implemented) is sufficient to maintain plant safety given the assumed characteristics of the plant and the plant interface.
- The specified safety integrity and performance targets will (if achieved) result in a tolerable hazard rate.

During the tendering phase, the SIS supplier should be able to identify evidence (or means for obtaining evidence) to show that:

- The implementation of the SIS meets the functional, integrity and performance requirements.

This evidence should be supplied as part of the delivered SIS. This justification of SIS compliance might be conditional upon certain environmental, operational and maintenance constraints (like the types and frequency of testing that should be performed), or required operator actions. So it is necessary for the utility and the supplier to show that:

- The end-to-end functionality maintains plant safety.

It is also necessary to show that the system operates safely throughout its lifetime. It will be necessary to demonstrate that:

- The SIS hardware can be adequately maintained.
- The SIS can be safely updated (e.g. to address safety problems).
- Maintenance and operational procedures and training are sufficient to maintain safety.
- SIS failure incidents are investigated, the cause identified and suitable corrective action identified.
- Actual SIS performance is consistent with the assumptions in the safety justification (e.g. failure rates, safe failure fraction, etc.).

7.2 Regulator interface

The point at which the regulator is involved can vary between different replacment projects and different member states. Normally the regulator only has the right to refuse operation when the final safety case is presented. However, there are obvious potential benefits in inviting comments during the evolution of the project or its preparation. In particular, the regulator can indicate whether the structure of the safety case argument and its evidence (or planned evidence) is likely to be acceptable when the final version of the safety case is presented.

After discussions with the regulator it was agreed that the safety justification for the MHS would be made available for comment at several stages during its evolution, i.e.

- Preliminary justification, which identifies the top level claims (prior to the tendering process).
- Interim justification, which outlines the detailed claim structure and the supporting evidence that will be used to support the claims.
- Final justification where the full safety justification and the supporting are available.

Such a step-wise approach should prevent costly licensing delays that might arise if the regulator is unable to accept the justification. Early warning limits the effort expended on an unacceptable safety approach. In addition, gaining agreement on what should be demonstrated and what evidence is sufficient should limit the effort required to construct a justification.

7.3 Planning

The required evidence and safety justification production activities formed part of the overall project schedule. This plan identified the activities undertaken by regulator, utility and SIS supplier. This included stepwise deliveries to the safety regulator of the preliminary, intermediate and final safety justifications for the SIS replacement.

7.4 Structure of the safety justification

The CEMSIS approach to structuring the safety case is presented in [1] (see Appendix D for a comparison with other approaches). In the CEMSIS approach, the safety justification is composed of claims and evidence at a number of distinct levels:

0. top level
1. interface level
2. architecture level
3. design level
4. operational level

At each level there will be:

- a claim
- support for the claim, either as direct evidence or by sub-claims at lower levels, or a combination

In the initial safety case the required behaviour at the plant interfaces should be known, and possibly some aspects of the architecture (if, say, pre-qualified components are to be used). Later phases of development will provide justification of the architecture and design, including consideration of maintenance and operational aspects, and the post installation operational infrastructure. This justification has to remain valid and be maintained throughout the lifetime of the SIS and to be updated in the light of changes in the plant, technical changes to the SIS, and changes to the operational and maintenance requirements.

8. The MHS safety justification

Using the layered claims and evidence approach for the MHS, the initial set of claims are made about the safety functions. These claims are related to the safe operation of the MHS and enforce constraints that will maintain the safety of the MHS in the context of the plant (i.e. are linked to the safety claims identified in the design basis documentation). These claims are then expanded to claims and evidence at lower levels. An example claim expansion is given in Appendix C. The Level 0 claim is:

Claim ref.	**Claim**
<no_rot>.clm0	Carousel rotation may never occur while material is being transferred or when the transporter is in movement or docking modes

The <no_rot> claim states that no rotation of the carousel occurs under certain states of the MHS plant. This claim is expanded into three level 1 claims.

Claim ref.	**Claim**
<no_rot>val.clm1	The <no_rot> specification is valid
<no_rot>impl.clm1	The <no_rot> implementation correctly implements the specification (when working)
<no_rot>implfs.clm1	The <no_rot> implementation is failsafe (i.e. does not permit rotation when there is a failure)

Associated with each claim there is supporting evidence, and sub-claims at a lower levels. For example, the claim that the specification is valid, *<no_rot>val.clm1*, is supported by the following evidence:

Evidence ref.	**Document**
mach_spec.evd1	Specification of transporter control interlock logic
op_feedbck.evd1	Operational feedback reports from machine incidents
eng_exp.evd1	Competence and past experience of plant engineers
safety_rep.evd1	Plant safety analysis report
mdrn_rep.evd1	Upgrade specifications and motivation report
reg_req.evd1	Regulatory requirements

The evidence for such claims about specification validity can be provided by the utility at the start of the project.

The other claims *<no_rot>impl.clm1* and *<no_rot>implfs.clm1* are expanded into sub-claims about the system architecture, design operational levels and hence result in some combination of level 2, 3 and 4 claims. These claims can only be developed in conjunction with a specific SIS design, i.e. once a supplier has tendered a particular solution. The tender requirements for the SIS replacement should enumerate the functional, performance and dependability requirements, and request that the supplier provide:

- An overall system architecture (including OTS hardware and software components).
- A specification of the functionality offered by the tendered systems.
- A statement of the means used to justify the system satisfies the Level 1 claims (i.e. what sub-claims and evidence are planned).

For example the claim *<no_rot>impl.clm1* expands to the following set of sub-claims:

Claim ref.	**Claim**
inputch.clm2	Complete/Adequate set of control unit sensor input channels
motor_ctrl.clm2	Adequate carousel motor control and communication functional interface
corr_code.clm3	The application code satisfies the specification <no_rot>
segr_code.clm3	Protection of executable code against non-used code
time_code.clm3	Maximum execution + actuation time is less than 0.1 sec
spur_lock.clm3	Spurious locks are prevented

The supporting evidence for each sub-claim makes use of information that is system-specific. This evidence can include analysis, test and field experience evidence. Where the claim relates to an OTS product like the

MSPGC 500, use can be made of pre-qualification evidence. The use of pre-qualification evidence is discussed in the following section on the pre-qualification of the MSPGC 500 Safety PLC.

In some cases the claims will expand to include level 4 sub-claims. For example, the top-level claim *<no_rot>implfs.clm1* expands to a set of Level 2, 3 and 4 claims, and the level 4 claims include:

Claim ref.	**Claim**
serv_prcd.clm4	In-service procedures are adequate and robust (e.g. to operators' errors) for periodic testing, maintenance of transporter, and instrumentation equipment.
pertsts_prcd.clm4	Adequate periodic tests procedures

For a SIS containing many safety functions that are all implemented on the same basic platform, the use of separate claims for each individual safety function could lead to a large number of top-level claims, which use many of the same sub-claims (such as claims about platform dependability properties). An alternative justification strategy is to define a set of *composite* top-level claims and the evidence would apply to a set of safety functions rather than a specific safety function (see Appendix E) which follows a similar claim structure to that advocated for air traffic control computer systems [8]). The expansion of such composite claims into sub-claims about the dependability of the MSPGC500 platform would be very similar to the approach for claims about specific functions . However, evidence for safety functions (test evidence, analysis evidence) would then be related to the *complete set* of functions implemented by the SIS. For example, for a claim of correct functional behaviour, it would be necessary to show that the functional tests covered the complete set of safety functions.

8.1 Use of OTS products

Where OTS products are being used in the SIS, the safety justification can generate evidence or make use of *pre-qualification evidence* for the OTS products [3]. The purpose of the pre-qualification is to:

- share the cost and to avoid unnecessary wastage of effort
- reduce uncertainties in system development and justification
- reduce the delays of system development and justification

The approach to pre-qualification developed in this project is given in the CEMSIS guidance document on the use of OTS [3], where the pre-qualification of an OTS product comprises:

- *A functional assessment*, to assure that the functions, performances, interfaces, limitations and needs of the product are known to a level of detail that will allow an appropriate functional selection and a correct use in each target system.
- *A dependability assessment*, to provide evidence that the product behaves as specified, possibly according to dependability figures; that it complies with all relevant regulatory or standard safety requirements; and its possible failure modes.

The dependability assessment might include restrictions on product usage, e.g., exclusion of some functions or some parts, maximum load limits, allowable ranges of configuration parameter values, protection against postulated failures, etc.

In this guidance, the assessment strategy of an OTS product is determined by:

- the functional complexity of the product
- access to internal information about the product (including source code), i.e. none ("black-box"), some ("grey-box"), complete access to design documents and source code ("white-box")
- experience in actual operation

- the safety class of the SIS [5] (i.e. whether it is a Class A or B system)

Using this OTS classification scheme, the MSPGC 500 was characterised as:

- High functional complexity.
- Grey-box information (publicly available design documents, and independent TUV assessments).
- Extensive operating experience (around 2000 system years of operation).
- Class B system.

The CEMSIS OTS guidance can then be used to identify an appropriate assessment of strategy for the product. The relationship between the OTS and the assessment strategy is shown in the table below.

<table>
<tr><td colspan="2" rowspan="2">Availability of development information:</td><td colspan="2">White–box</td><td colspan="2">Grey-box</td><td colspan="2">Black-box</td></tr>
<tr><td colspan="6">Experience in operation</td></tr>
<tr><td>Safety class</td><td>Functional complexity</td><td>Yes</td><td>No</td><td>Yes</td><td>Yes</td><td>Yes</td><td>No</td></tr>
<tr><td rowspan="3">Class A</td><td>High</td><td colspan="2" rowspan="2">A1</td><td colspan="3" rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>Medium</td></tr>
<tr><td>Low</td><td colspan="2">A1 / A2</td><td>A2</td><td></td><td>A2</td><td></td></tr>
<tr><td rowspan="3">Class B</td><td>High</td><td colspan="4">B1</td><td></td><td rowspan="2"></td></tr>
<tr><td>Medium</td><td colspan="4" rowspan="2">B1 / B2</td><td>B2</td></tr>
<tr><td>Low</td><td colspan="2">B2</td></tr>
</table>

*Table 6: OTS assessment strategy table from the CEMSIS OTS guidance [3]**

*It should be noted that this table represents the consensus within the CEMSIS project. Regulators in Members States might have more stringent criteria for OTS assessment.

Using the table, it was determined that a B1 assessment strategy should be used. The B1 strategy is a grey-box approach for OTS products. It is based on a combination of analysis of available development information, and grey and black-box testing. Experience in operation, when available, is used as a complementary means of assessment. The assessment of the MSPC 500 described in the following section is consistent with this strategy.

8.2 Assessment of the MSPGC 500

8.2.1 Pre-qualification functional assessment

The MSPGC 500 is a programmable PLC (with the program stored in electrically erasable EEPROM). The manufacturer claims compliance to the IEC 61131-3 PLC language standard, hence the specification should meet the requirement for *precision* in the specification of the PLC functionality. An independent TUV assessment of the software has been performed to establish the *correctness* of the product implementation with respect to this specification.

The manufacturers claim that the associated 61131-3 compiler has extensive field use and that there is a system of reporting product faults (including compiler faults). All reported faults are recorded and their correction status is known. The compiled code of some reference application examples has been analysed to show that correct code was generated. The MSPGC 500 has built-in software to support the 'reading back" of compiled application code. This can be used to make independent checks that no errors have been introduced during compilation or uploading of application software to the MSPGC 500 via the programming port.

As part of the functional specification, Microsafe—the manufacturer of the MSPGC 500—claimed that the system design has predictable time response characteristics. A "round robin" scheduler design guarantees that all IEC 61131-3 applications can be executed within some specified time bound (or the system performs a safe shut-down). It is possible to compute the total execution time of the 61131-3 applications, as the execution time of the individual logic components (like ANDs and OR gates) is known. A tool is available that can compute total execution time of the application software executed in the round robin sequence.

The functional assessment also characterised the properties of the input-output system (types of input, maximum number, input and output accuracy, etc.).

8.2.2 Pre-qualification dependability assessment

The robustness to internal failures had been independently assessed. A TUV report is available which assesses the fail-safety features of the MSPGD 500 against IEC 61508 Part 2 requirements. On the basis of the dual processor cross-comparison architecture and the internal diagnostics, the fail safe fraction was assigned a 90% fail-safe classification.

A hardware reliability analysis report produced by Microsafe estimated that the MTBF should be better than 3×10^5 hours under the stated operating conditions. This is supported by an analysis of equipment failure reports from equipment users. Based on relatively conservative estimates of operating time, the MTBF was estimated to be 5×10^5 hours.

Microsafe has a field support infrastructure to handle problems reported by its customers. Failures in its PLC products are analysed to locate the cause, especially if the failure is dangerous. Diagnosed problems are recorded as fault reports and modifications are made to rectify the problem. A report containing an analysis of recorded MSPGC 500 software faults is available. This report shows that no PLC system software faults had been found in the last two years. Based on the estimated operating time of fielded PLC systems over this period, the MTBF of the operating system software is estimated to be better than 10^6 hours.

The design documentation of the MSPGC 500 shows that the operation of the round robin scheduler is linked to a separate hardware watchdog timer. This allows time overruns in the scheduler to be detected and this can be used to force the PLC outputs to a safe state (the de-energised state).

8.3 Assessment of suitability for the application

For the specific MHS SIS application, the OTS product was assessed for functional suitability and adequate dependability.

8.3.1 Functionality

The functions provided in the IEC 61131-3 compliant language were regarded adequate to implement the required functionality and the representation was sufficiently similar to the user specification to ensure that it would be easy to implement and review the application software.

The input-output requirement of 36 inputs and 13 outputs was well within the maximum capacity of the MSPGC 500.

A time estimate based on the number of logic gates and the specific MSPGC 500 logic processing times showed that the actual execution time should be well within the target response time of 100 milliseconds.

8.3.2 Dependability

The claimed dependability parameters for the MSPGC 500 (reliability of the processor and input-output systems, fail-safe fraction, etc.) were compared against the target levels assigned to the component at the

architectural design stage. As these were compliant, the component was judged to be suitable for the application.

The MHS environment specification was checked against MSPGC 500 environmental constraints and the device was shown to capable of operating in the environment (e.g. can withstand EMI and ambient temperatures), and that the equipment would not affect other equipment (e.g. EMC compliance, heat output, etc).

8.4 Relationship of the OTS pre-qualification to the MHS SIS safety justification

In summary, a SIS safety justification claim or sub-claim that involves an OTS product has to show that:

- The chosen OTS product matches the functional and dependability needs set for them by the system requirements specifications and the system design.
- Each OTS product is used according to the constraints identified or recommended by its pre-qualification.
- The functions and parts of OTS products which are not strictly necessary to the system cannot affect its operation (This is normally limited to Class A systems).

For example the sub-claim <*time_code.clm3*> for the MHS is supported using the following pre-qualification evidence about the MSPGC 500:

- The MSPGC 500 can guarantee execution of all application software within a predefined time bound (see *PLC_maxtim_clm0* in Section 3 of Appendix C).
- The MSPGC can process 10^4 logic gates/ second (see *PLC_timing_clm0* in Section 3 of Appendix C).

This evidence can be combined with further evidence relating to the specific application, i.e.

- The proposed application will have around 200 gates (including input-output), so the application response time should be around 20 milliseconds.
- This preliminary analysis can be confirmed using a detailed time estimation tool when the application is implemented, and by timing tests.

The pre-qualification evidence therefore simplifies the safety justification process by providing immediately available evidence. The application-specific evidence has to be generated during project development, e.g. the timing claim above could be supported by a timing analysis and timing tests at the factory acceptance test stage.

8.5 Evolution of the safety justification

The safety justification evolved during system development. As more design detail was produced, more detailed sub-claims were generated at the design level but this did not affect the existing higher level claims within the structure.

In principle, it is possible for the evidence to contradict a claim at some level, and this would need some modification of the system design or the justification. For example, if the implementation required more logic gates than expected, this could have an impact on the logic response time. At this stage it may be necessary to consider a major redesign, or consider whether the time requirement in the specification can be relaxed.

In the MHS, the scope for such problems was reduced thanks to the use of available pre-qualification evidence e.g. the timing evidence showed that the MSPGC 500 was capable of meeting the timing requirements even if the planned logic complexity was exceeded.

The Level 2 (architecture) and Level 3 (component design) claims together with the associated evidence were provided by the supplier. Where necessary, these were linked to Level 4 sub-claims about the operational environment (e.g. about the supporting maintenance and operational processes). In the interim

version of the justification, the sub-claims about operational support were made without supporting evidence. In order to complete the justification, the utility had to provide the evidence necessary to support the Level 4 sub-claims. For example, the utility had to provide evidence in support of <serv_prcd.clm4> to show that the test support procedures were appropriate (e.g. from past maintenance performance), and that they had been suitably adapted for use with the new SIS. For example the MHS proof test procedure has to be modified to use different diagnostic information.

```
PR/MT/MHS/09
MHS Movement permissive interlock testing
Rev 5
6 August 2004

1. To configure the system for proof testing, follow procedure
PR/MT/MHS/01
2. Energise all interlock input signals (TC/15/01 to TC/15/36)
3. Verify that the movement permissive indicator light (I/17) on the
control unit back panel is on
4. De-energise TC/15/01 and verify that (TC/16/73) is off
5. Energise TC/15/01 and verify that interlock indicator I/17 is on
6. Repeat for inputs TC/15/02 to TC/15/36
```

8.6 Evidence integrity

In addition to direct claims about the behaviour of the system outlined above, the submission to the regulator provided an analysis of the i*ntegrity* of the evidence used within the justification (using similar criteria to those used to assure requirements in requirements validation [2]). The submission sought to demonstrate that the safety justification evidence is:

- consistent (e.g. documents and cross references are internally consistent, test results consistent with the item, and version, tested)
- coherent (e.g. detailed requirements traceable to functional requirements, functional requirements traceable to user requirements, user requirements traceable to plant safety and operational needs)
- current, all evidence relates to the supplied version of the SIS
- complete, evidence exists to support all claims and sub-claims

These properties could, in principle, be assessed by the regulator (e.g. by audits of the available evidence). However if support for evidence integrity already exists, the regulator is able to focus on the main task of assessing whether the evidence provides adequate support for the safety claims.

9. Summary

This public domain example illustrates the use of the CEMSIS guidance within the modernisation lifecycle. The main features of the guidance illustrated in the example are:

- A systematic approach to requirements definition (which reduces the risk of late and costly "surprises", and of late changes).
- A structured approach to the construction of the safety justification. This reduces the risk of costly licensing delays as the key claims and evidence requirements can be agreed at an early stage and the evidence requirements can be included in the supplier contract.
- A systematic approach to the pre-qualification of OTS components. This reduces the risk that evidence is delayed or unsuitable.
- Architectural design strategies for reducing the safety criticality of OTS components.

10. References

[1] CEMSIS Deliverable D1.2, "A Dependability Justification Framework for NPP Digitall Instrumentation and Control Systems", CEMSIS doc. ref: wp1_avn010 v6.1. (restricted)

[2] CEMSIS Deliverable D2.3, "Requirements Engineering Best Practic e Guide for Refurbishment", CEMSIS doc. ref: wp2_ ade043 v1.0

[3] CEMSIS Deliverable D3.4, "Assessment and analysis guidelines for Off-The-Shelf Product-based Systems Important for Safety", CEMSIS doc. ref: wp3_edf037 v1.0.

[4] IEC 61131-3 "Programmable co ntrollers - Part 3: Programming languages", : International Electrotechnical Commission , IEC 61131-3 Ed. 2.0, 2003

[5] IEC 61226: "Nuclear Power Plants – Instrumentation and control systems important for safety – Classification", International Electrotechnical Commission, IEC 61226 Ed. 1.0, 1993

[6] IEC 61508, "Functional safety of electrical/electronic/programmable electronic safety-related systems". International Electrotechnical Commission, Parts 1-7 Ed. 1.0, 1993, 2000.

[7] IEC 61513, "Nuclear Power Plants – Instrumentation and control systems important to safety – General requirements for systems", International Electrotechnical Commission, IEC 61513 Ed. 1.0, 2001

[8] CAA CAP 670, 'SW01 - Regulatory Objectives for Software Safety Assurance", CAP 670 A ir Traffic Services Safety Requirements. CAA Safety Regulation Group, 1998.

Appendix A: Example Design Basis Documents

1. Description of the Materials Handling System

1.1 The materials handling machine

1.1.1 General

The materials handling machine is part of a processing system for radioactive material. Nuclear material, stored in cans, is transferred between materials processing units by the materials handling machine as shown in Figure 1.

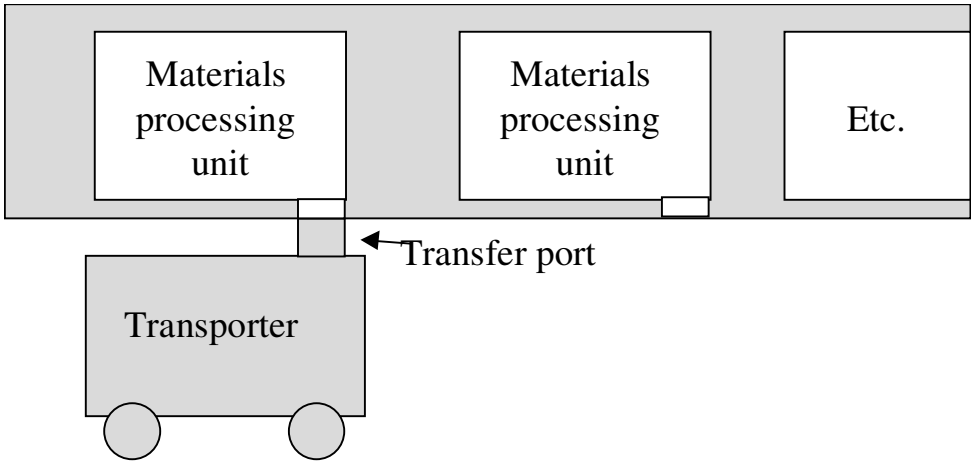


Fig 1. Materials handling machine, transfer port and processing unit.

The material in the materials handling machine is stored in individual vertical chambers in a shielded rotating assembly, named the "carousel". The carousel can be connected via a transfer port to a materials processing unit and, once connected, radioactive material is either drawn into the carousel or discharged into the connected unit using a hoist. See Figure 2.

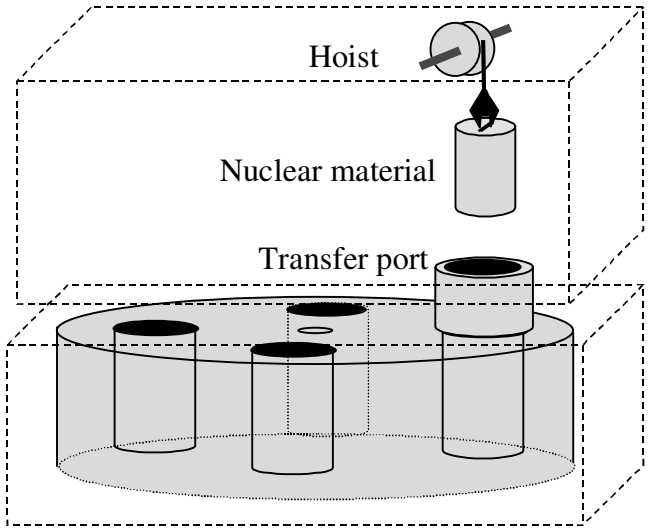


Figure 2. Carousel, transfer port and hoist for nuclear material

The carousel is a buffer store and is filled by rotating the carousel and transferring the material into successive chambers until all the chambers are filled. To connect with a different materials processing unit, the transfer port is disconnected from one unit, then the materials handling machine moves to a new unit and is reconnected via the transfer port, so the carousel can be emptied (and possibly refilled with material for the next location).

1.1.2 Use of the machine

The materials handling machine has three main operational modes: the docking mode, the handling mode, and the transporting mode.

In the docking mode the materials handling machine connects to a materials processing unit with the transfer port. The transfer port is subsequently unsealed.

In the handling mode, nuclear material can be transferred from or to the materials handling machine. First a chamber in the carousel is aligned with the transfer port and cans of nuclear material are transferred using the hoist. The carousel can then be rotated until the next chamber is aligned so that another container can be transferred.

The materials handling machine enters the docking mode. The transfer port is sealed and the materials handling machine is disconnected from the materials processing unit.

In the transporting mode the materials handling machine moves between transfer ports of different materials processing units.

1.1.3 Transitions between operational modes

Transition from the transporting mode to the docking mode is only possible when the transfer port of the materials handling machine is positioned under a materials processing unit and the brakes are applied.

Transition from the docking mode to the handling mode is only possible when the transfer port is docked and unsealed.

Transition from the handling mode to the docking mode is only possible when the hoist is in the upper position.

Transition from the docking mode to the transporting mode is only possible when the transfer port is sealed and not docked.

1.1.4 The Transfer Port

The transfer port is a cylindrical opening in the top of the materials handling machine that can be positioned at the entrance of a materials processing unit. The transfer port can dock to the unit, i.e. make a gas tight connection. The transfer port contains a seal on its top, which can be opened and closed using the control panel. The seal on the transfer port closes the materials handling machine.

Indicators on the control panel show when the transfer port is docked and whether it is sealed.

Transfer port docking and undocking and sealing and unsealing is only allowed in the docking mode. This is enforced by switching on the electrical supplies to the transfer port drive motors only in the handling mode.

1.1.5 The carousel

The carousel is a metal construction with four chambers that can each hold a can of nuclear material. It can rotate to place a chamber under the transfer port.

Carousel rotation is controlled by an operator using pushbuttons on the control panel. Indicator lights show when a chamber is aligned with the transfer port, and which chamber it concerns.

The output signals from the carousel control logic control two separate carousel drive motors. Two other outputs select fast and slow movement — slow movement is used when a chamber is close to alignment with the transfer port. It is also possible to "hand-wind" the carousel to correct alignment problems.

The carousel cannot rotate through 360° so there are end-stop sensors to detect when the carousel has reached the end of travel (left and right).

Carousel rotation is only allowed in the handling mode. This is enforced by switching on the electrical supplies to the carousel drive motors only in the handling mode.

1.1.6 Drive motors and brakes

The materials handling machine is equipped with two electric drive motors, one on the front axle, one on the back axle. There are two electrically operated brakes, one on each axle. The brakes can stop movement of the axle, even when the drive motor on that axle is activated at full power.

The drive motors are controlled by the operator using two pushbuttons on the control panel: forward and backward. Indicator lights show when the materials handling machine is positioned under a materials processing unit. When pushing either pushbutton, the brakes will be released. When releasing both pushbuttons, the brakes will automatically be applied after one second.

Two metres from the end of the rail track, the materials handling machine encounters an end position switch. Upon activation, the forward movement of the materials handling machine is disabled. The same applies to the backward movement two metres from the beginning of the rail track.

Drive motor operation is only allowed in the transporting mode. This is enforced by switching on the electrical supplies to the drive motors only in the transporting mode. When switching off the electrical supply, the brakes will be applied to the axles.

1.1.7 Interlocks and hand operation

The operations of the materials handling machine are all interlocked electrically or mechanically to prevent incorrect operation.

Provision is made for manual control of the carousel, the drive motors and the brakes in the event of failure. The use of these facilities overrides the safety interlocks and in view of this, great care must be exercised when manually operating, and the handles for all manual control devices must be retained under administrative control.

1.1.8 O ring seals and seal testing

All metal-to-metal joints in the materials handling machine are sealed against leakage of gas with double O rings. These are fitted in pairs of circular grooves in two types of arrangement. A pair of rings for sealing a circular shaft are normally both of the same size and are fitted in parallel grooves in parallel planes. The rings used for sealing two flat surfaces, such as pipe flanges, are of different diameters fitted concentrically in the same plane. The spaces between the rings in each pair (the interspaces) are all connected by individual pipelines to local test manifolds in various parts of the materials handling machine, so that the leak rates of the seals can be tested. For details of testing and the permissible leak rate for each seal, see Table 5.

A nitrogen supply for materials handling machine seal testing purposes is provided from a temporary nitrogen cylinder at the hall floor. The nitrogen supply pipe work is fitted with an isolating valve pressure gauge and vent valve. Connections are teed off from the main supply line at each platform level and a three way switching valve and Hansen quick release coupling fitted.

1.2 The materials handling machine control station

The control station containing the control panel for the materials handling machine is located on platform 4. There are no other control stations from which the materials handling machine can be controlled. The control station is air conditioned.

1.2.1 Control of the carousel

The control panel for the carousel is depicted in Figure 3.

Control system output signals are used to activate:

1. The leftward carousel drive motor.
2. The rightward carousel drive motor.
3. High speed drive mode.
4. Low speed drive mode.
5. Carousel alignment position indicators (T1 to T4).
6. Transfer port status indicators.

The inputs to the control unit comprise:

1. Transfer port status signals: docked/undocked and sealed/unsealed.
2. Hoist status signals via the transfer port.
3. Chamber alignment status: coarse and fine alignment for each tube.
4. Left and right end-stop sensors.
5. Hand wind mode.

6. Maintenance mode.
7. Left and right movement pushbutton.
8. Emergency stop pushbutton.

Operator indicator lights show when:
1. One of the chambers is aligned with the transfer port and the carousel is stationary.
2. The materials handling machine is connected via the transfer port to a processing unit (docked).
3. The transfer port is sealed.

The operator pushbutton can rotate the carousel left or right and movement will stop when the next chamber is aligned with the transfer port.

When a chamber is close to alignment with the transfer port, the carousel rotates at its slow speed setting.

1.2.2 Carousel Control Interfaces

The carousel movement is controlled through a control panel. See Section 1.2 for a description of panel

Inputs to the Carousel Control System are:

a) Plant status signals
- Chamber alignment indicators (3 coarse, 3 fine).
- Chamber identification signal (2 for each chamber)
- End-stop indicators of the carousel, two for each direction.
- Transfer port docking status signal(2 inputs)
- Hoist position signal (2 inputs – valid when the transfer port is docked).
- Transporter brake status signal.

b) Operator command signals
- Carousel movement command (1 pushbutton for left move, 1 for right)
- emergency stop button (2 inputs).

Outputs of the Control System are:

- Controls of the carousel.
- Controls of the transfer port.
- Controls of the axle motors and brakes.

The Control System of the Materials Handling Machine contains:

a) Control logic:
- To implement operator controls to move the carousel and align the next chamber with the transfer port.

b) Indicator logic showing:
- Alignment status of the carousel.
- Status of the transfer port.
- Status of the axle motors and brakes.

c) Interlock logic:
- To disable carousel movement.

- To disable transfer port movement.

2. Plant Safety Report

6.3 The transfer port

Drawing reference 6.14/2.

Report reference 6.15/4.

The transfer port is used to connect the materials handling machine with the materials processing unit. It consists of a steel cylinder and is moved by an electric actuator. The top of the transfer port has a seal, also moved by an electric actuator. The connection between the transfer port and the materials handling machine is sealed with double 'O' rings.

When connecting to the materials processing unit, the electric actuator moves the transfer port up, until this movement is blocked by the entrance of the materials processing unit. The actuators maintain an upward force. The 'O' ring on the top of the transfer port seals this connection.

There is a position switch to detect the upper position of the transfer port. Also there are three pins in the upper part of the transfer port, pushed down by the lower part of the materials processing unit. These mechanically block the movement of the seal if the transfer port is not properly docked to an entrance of the materials processing unit. Also, the control system will not open the seal unless the position switch indicates that the transfer port has reached the upper position.

Before unsealing, the transfer port clamps itself to the entrance of the materials processing unit. The clamps mechanically block the movement of the seal, unless they are all clamped to the entrance. On every clamp, a position switch indicates the clamp is active. The control system will not open the seal unless all clamps are active.

When the hoist is in use, the seal should not be closed, because this may damage the seal and/or the seal may not be properly closed. The control system will not close the seal, unless the position switch of the hoist indicates it is in the upper position.

6.3.1 Main interlocks of the transfer port

	Safeguard	Method
(a)	The transfer port cannot be unsealed if the materials handling machine is not docked (radiation hazard)	Position switch on the materials handling machine; mechanical blocking system
(b)	The Transfer Port cannot be sealed if hoist is being used (rupture of material container)	Three position switches on hoist

(c)	The Transfer Port cannot be undocked if it is unsealed (radiation hazard)	Three position switches on seal of transfer port; mechanical blocking system

For complete interlock schedule see report reference 6.15/3.

6.3.2 Radiation levels associated with the transfer port

(a)	Maximum radiation level at seal of transfer port	<10 mrem/h
(b)	Maximum radiation level at body of transfer port	<1 mrem/h

6.4 The carousel

Drawing reference 6.14/7.

Report reference 6.15/8.

The carousel can rotate through 330 degrees. rotation to the movement limits are detected by end-stop detectors. The drive motors are likely to burn out if the carousel hits the physical end stops. The carousel has four chambers to hold nuclear material. The position on the carousel is sensed by movement cams on the side of the carousel that operate position relays.
There are cam sensors for each chamber on the carousel which indicate whether it is in coarse alignment or fine alignment with the transfer port.

6.4.1 Main interlocks of the carousel

	Safeguard	Method
(a)	The carousel can only be rotated if the hoist is in the upper position. (Rupture of material container; General Damage)	Three position switches on hoist
(b)	The carousel cannot rotate past the end-stops. (General damage)	Position switches on carousel before end-stops

For complete interlock schedule see report reference 6.15/3.

6.4.2 Radiation levels associated with the carousel

(a)	Maximum radiation level at seals of the carousel	<10 mrem/h
(b)	Maximum radiation level at body of the carousel	<1 mrem/h

6.3 The hoist

Drawing reference 6.14/21.

Report reference 6.15/44.

The hoist is operated from the materials processing facility. When the MHS docks with the facility, electrical sensors are connected to the control logic to indicate the state of the hoist, i.e. whether the hoist is fully retracted.

6.3.1 Main interlocks of the hoist

	Safeguard	Method
(a)	The hoist cannot be used if the carousel is being rotated (general damage)	Motor drive current sensor; position switches on carousel
(b)	The hoist cannot be used if the Transfer Port is sealed or the Transfer Port is not docked (general damage, damage to radioactive materials container)	Three position switches on transfer port

For complete interlock schedule see report reference 6.15/3.

Appendix B: Materials Handling Machine Refurbishment Requirements

This appendix is an extract from the general refurbishment requirements for the replacement equipment of the materials handling system. Much of the document consists of standard clauses for the supply of I&C equipment. Some specific clauses relating to installation requirements are included, but most of the details relating to the materials handling system are covered by reference to supporting documents.

1. Introduction

The existing Control System of the Materials Handling Machine is reaching the end of its useful life. This document describes the requirements that the replacement equipment must meet.

This Functional Specification has been produced in accordance with the engineering and quality guidelines.

Throughout this project, a standard set of Abbreviations and Definitions are used. These are given in MHS/P2/002/3.

2. System Description

The replacement control system is to be functionally identical to the existing equipment and physically fit into the existing cubicle and be plug-for-plug compatible. The description of the existing equipment is given in MHS/P2/004/1. Specifications of the environmental conditions, maximum power consumption and power supplies, and weight limits are given MHS/P2/004/1 Appendix E.

To allow for maximum flexibility for testing and maintenance, all adjustments should be possible without the removing the control system from the cubicle. It should not be necessary to remove the control system for maintenance and/or calibration purposes.

Failsafe electrical interlocks must be provided so that if any module is removed a common alarm is generated.

The control system should be automatically tested. Automatic Test Equipment is to be provided. This equipment is to interface primarily with the front of the rack, and minimise the requirement to interface with the rear sockets. Any test equipment incorporated in the ATE must be removable to allow for routine certification to traceable standards.

The new control system and associated equipment are to comply with the System Design Safety Guidelines (Appendix B).

3. Extent of Supply

This extent of supply is as listed below:

- Control System for the Materials Handling Machine.
- Recommended spares, including the justification for these spares.
- Reliability Assessment and System Substantiation Documentation for the Control System for use in the production of the Safety Case (supporting a minimum of a 6 month test interval).
- Commissioning Documentation in accordance with power station procedures.
- Maintenance and Calibration instructions in accordance with power station procedures.
- Installation Documentation, to enable the customer to install the equipment.

The IPR of any Software developed for this project is to be vested with the customer.

4. Installation Requirements

The Interface Points for this equipment are:

- Mechanical: The existing cabinet, a 6U 19” rack.
- Electrical: Five Plessey Mk IV sockets at rear.

The contractor must carry out a complete survey of the existing interfaces to ensure that the supplied equipment is fully interchangeable.

The equipment must be capable of operating from a 48V 5A DC power supply.

The weight of the equipment should not exceed 20 kilograms

5. Dependability Requirements

The contractor shall demonstrate the system meets meet the following dependability requirements

- 10^{-2} failure per demand (interlock movement logic).
- 10^{4} hours (spurious actuation)
- 1 hour MTTR (any failure)

6. Design Safety Requirements

The equipment must comply with the company System Design Safety Guidelines (Appendix B) and the Plant Design Safety Guidelines – Annex VII (as revised in Appendix C).

Any software developed must meet IEC 61508 SIL2 requirements.

In the event of any conflict, the following order of precedence shall be followed:

1. This Functional Specification and the associated Technical Specification (to be produced).
2. System Design Safety Guidelines (Appendix B)
3. IEC 61508 SIL2
4. Plant Design Safety Guidelines, Annex VII – as revised in Appendix C.

The design shall be subject to the specific approval of the customer.

Any power supply regulation system and filtering devices shall be such that transients and electrical interference cannot actuate or prevent correct operation of the equipment.

The supplied control system must function and interface with the existing plant, in an identical manner to the existing system.

7. Functional requirements

The functional requirements are defined in the logic drawing and function specifications in document MHS/P2/004/2.

8. Performance requirements

The interlock logic must be capable of disabling movement outputs within 100 milliseconds of an interlock demand.

9. QA Requirements

A Quality System that meets the requirements of EN ISO 9001 is to be applied to this contract. Any software provided must be produced in accordance with the guidance set down in ISO 9000-3.

10. Maintenance, Inspection and Testing

10.1 Initial Testing and Commissioning

The initial (works) testing of the completed control system will be in accordance with the manufacturer's test documentation. This is to be approved by the customer before use. The works testing must include the use of any automated test equipment (ATE). The initial testing and commissioning will be carried out by the supplier.

10.2 Maintenance Principles

Maintenance shall be possible on every item of the equipment while the Materials Handling Machine is out of service. The time taken to check correct operation of the whole system shall be minimised by the provision of adequate installed test equipment and facilities.

Maintenance will consist of routine calibration, performance testing and system testing in order to identify any faulty or out of specification part. The control system shall not normally require adjustment at less than 6 month intervals.

10.3 In-Service Inspection and Testing Requirements

The equipment shall be designed so that inspection and testing is possible on every item of the control system, with the control system in operation. The time taken to check correct operation of the whole system will be minimised by the provision of installed test equipment and facilities. All test facilities (switches and indicators) and test connections to be accessible from the front of the control system.

Test equipment must be mounted on a test trolley suitable for access to the appropriate plant areas. All necessary interface equipment, e.g. cables, shall be supplied. Any necessary permanent test equipment shall comply with the same environmental requirements used for the associated equipment to be tested. All test equipment used shall be capable of being calibrated to NAAS traceable standards.

Test switches must be spring biased to the normal operation position and shall comply with ESI Standard 50-18 part 3 – Switching Devices

11. Documentation

All documentation supplied shall be in PDF format. Drawings shall be in AutoCAD 13 format. Certain documentation (specifically Test and Maintenance Documentation) should be produced in accordance with the customer's in-house procedures.

Documentation supplied by the Contractor will be required to support the customer to install, maintain and operate the equipment, and must be of a suitable quality to withstand Independent Nuclear Safety Assessment of the customer and also by the Nuclear Installations Inspectorate.

Required documentation to include:
- Reliability Assessment.
- Failure Mode and Effects Analysis.
- Routine Maintenance, Calibration and Test Procedures.
- Operating Instructions.
- System Substantiation.
- Software Substantiation.
- Design Detail.
- Drawings comprehensively describing the equipment.
- Works Test Documentation.

The following documents/records must be provided for any software provided:
- Configuration Management Plan.
- Design Specification.
- Test Specification.
- Source Code Listing(s).
- Data File Listing(s).

- Test Log and/or Test Output(s).
- User Documentation.
- Project Quality Plan.

Appendix B. System Design Safety Guidelines.

B.1. Functional Requirements

The Control System shall perform the following functions:

1. Control the materials handling machine.

B.2. System Availability

If testing, inspection or maintenance results in partial unavailability of the control system, the frequency and duration of such procedures shall be such as to provide an adequate balance between the system reliability and its availability.

B.3. Single Failure Requirements

No single failure within the control system should prevent it carrying out its functionality in the presence of any initiating event which places a demand on the control system during any normally permissible state of plant availability. Consequential failures resulting from the assumed single failure should be considered as an integral part of the single failure.

Judgement should be exercised to ensure that, in attempting to satisfy the guidance, unnecessary complexity and/or cost is not introduced, particularly from the viewpoint of some passive failures.

Any shortfall with regard to the system single failure guidance should be fully justified, taking account of reasonable practicability having regard to the frequency of the initiating event, the probability of the single failure, the severity of the consequences and the unavailability of plant for specified purposes and limited periods.

B.4. Interfaces

The proposed system will interface with the following systems:

1. The Materials Handling Machine.
2. The hoists in the Materials Processing Units.

The system should be designed such that it does not adversely affect the safety functions of the above systems. In addition it should not significantly affect the frequency of spurious operation of the above systems.

B.5. Equipment Fault Detection

The control system should operate, as far as is practicable, on failsafe principles.

B.6. Reliability Requirements

The Control System must have a failure rate of better than 10^{-4} failures/hour. This is to be supported by a test interval of no less than six months. The time taken to test the control system is to be no greater than 3 hours.

It should be recognised that these values are targets, less restrictive values could be accepted if it is shown not to be reasonably practicable to meet these targets.

The automated test equipment (ATE) should be designed to IEC 61508 SIL1. No claim should be made on the ATE that requires a more onerous requirement.

B.7. Testing

The control system must be designed so that it can be tested on load without negatively influencing the behaviour of the Materials Handling Machine. The reliability requirements should be met without the need for excessive testing. Testing of the control system must take no more than three hours. The required test interval must be 6 months or greater.

B.8. Equipment Location

The Control System is located in the Materials Handling Machine Control Room.

The equipment being supplied must be able to withstand the following environmental conditions:

- Temperature: 0 – 55^{o}C.
- Relative Humidity: 0 – 95%.
- Power supply: 110V, ± 10%, 50 Hz ± 5%, neutral solidly earthed.

- No maloperation of the equipment shall occur for supply interruptions less than, or equal to 200 milliseconds.
- RFI and EMI immunity to IEC 1000-4-3 1995.
- The equipment should withstand the seismic pressure (specified in Annex II).

B.9. Hazards

The Control System should not be vulnerable to, or should failsafe in the event of, any of the following hazards:

- Local flooding.
- Fire or explosion (*).
- Release of corrosive fluids (*).
- Disruptive failure of rotating machines (*).
- Dropped loads (*).
- Seismic event (10^{-4} Pa).
- Site flooding (*).

(*) These items are included on the basis that it is judged to be possible to provide protection against these hazards at negligible cost.

Note: The existing control system is located in a cubicle that provides the required protection against the above hazards. The new control system must not require any modification which may compromise the ability to withstand the above hazards.

Appendix C: Example safety claims for the MHS SIS

1. Introduction

In the CEMSIS safety justification approach, a layered approach is used in making safety claims. There is a level 0 claim which makes a claim about external plant behaviour, and this is supported by sub-claims and evidence relating at different levels. These levels relate to different elements of the SIS, namely:

1. interface level
2. architecture level
3. design level
4. operational level

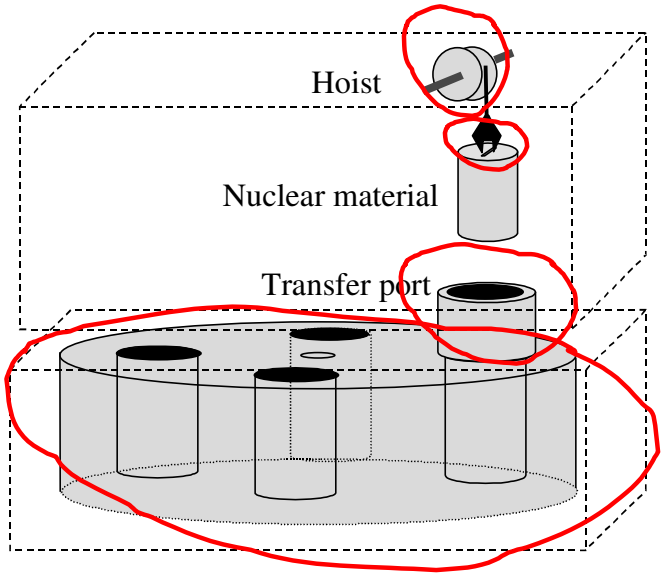
At each level there will be:

- a claim
- support for the claim, either as direct evidence or by sub-claims at lower levels, or a combination

Normally sub-claims at one level expand to sub-claims at the next level, but it is possible to expand to a sub-claim at any level below the current one.

To ensure clear and precise claims, the claims should be expressed in terms of entities that are "visible" at that level:

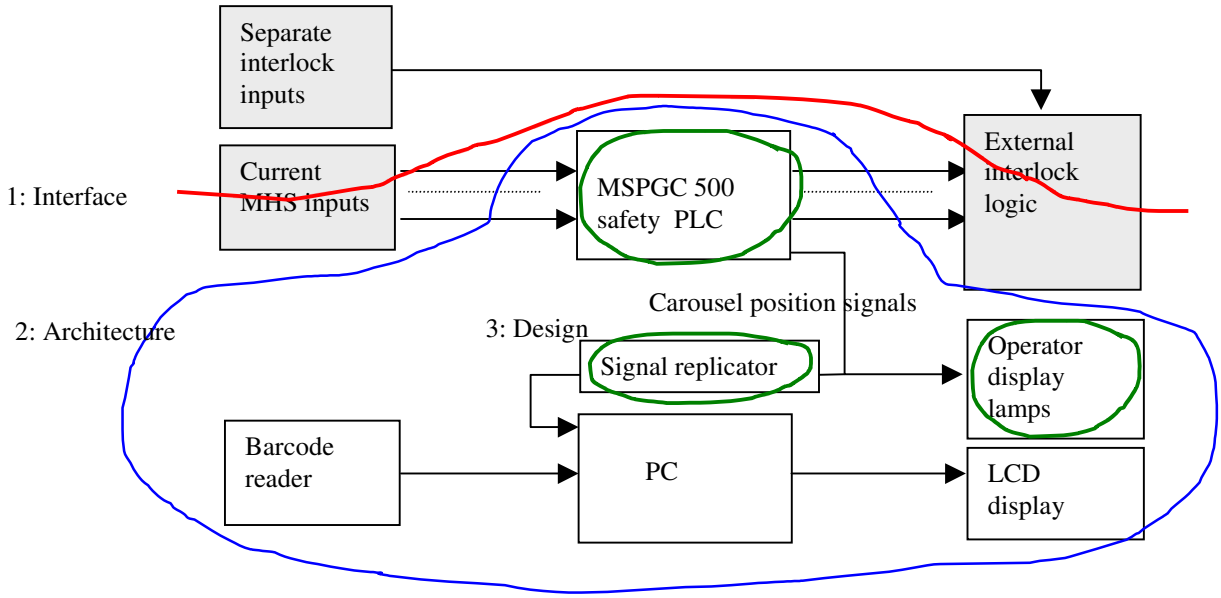
- Level 0 is related to the plant domain, and the observable entities are external to the SIS, and the claims are expressed in terms of the actual state of plant components like carousel position and speed, hoist position or transfer port location as illustrated in the figure below.



- Level 1 is related to the interface between the SIS and these real world entities. So claims are expressed in terms of sensor signals that monitor the state of the MHS components, and actuator outputs that change the state of plant components. Claims about the input-output behaviour at Level 1 should imply the required behaviour at Level 0, e.g. given adequate sensors on the plant, the sensor value (or set of sensor values) should unambiguously determine the plant state, given a claimed input-output relationship at the interface, the plant behaviour will be safe.
- Level 2 is related to the architecture of components within the SIS. So sub-claims are expressed in terms of the relationship between components. For example, in the MHS, the claims can be made in terms of

the externally observed behaviour of components or the composite behaviour of the components within the architecture.

- Level 3 should express claims in terms of the design of individual components, e.g. like the hardware and software within the MSPGC 500 (as illustrated in figure below).



- Level 4 should make claims about system operation and maintenance, and claims should be related to entities visible to the maintainer and the operator (like operator interfaces and diagnostic/maintenance facilities), or the general support infrastructure visible in that domain.

In Section 2 of this appendix we illustrate this layered claim structure approach by expanding a level 0 claim into sub-claims. The top level claim relates to safe rotation of the carousel, i.e. that it will not rotate if the MHS plant is not in a safe state (e.g. if the hoist is not retracted). This is expanded into claims at the interface, architecture, design and operational levels. The evidence used at each level is also given.

In Section 3 we show how to use the approach to construct claims for COTS components. These claims are independent of any application (and are hence developed as a separate claim structure). In this case the interface level (Level1) relates to the external interfaces of the MSPGC 500 PLC, and the subsequent levels related to the architecture, design and maintenance levels of the PLC. These claims could be assessed and accepted for the component, and the claims for the component could be used as supporting evidence for in other safety justification (e.g. for claims about claims fail safety or timeliness made about the MHS SIS).

2. Example safety claim expansion

This example claim structure is taken from the CEMSIS safety justification guidance. See [1] for further details on the approach.

2.1 Claim structure

The top level claim relates to safe rotation of the carousel, i.e. that it will not rotate if the MHS plant is not in a safe state (e.g. if the hoist is not retracted). This is expanded into claims at the interface, architecture, design and operational levels. The evidence used at each level is also given.

Top Level claim (0)			
Name	**Description**	**Evidence Components**	**Subclaim expansion**
no_rot.clm0:	Carousel rotation may never occur while material is being transferred or when the transporter is in movement or docking modes		<no_rot>-val.clm1 <no_rot>-impl.clm1 <no_rot>implfs.clm1

Environment-System subclaims (1)			
<no_rot>-val.clm1	1. The system specification <no_rot> is valid: where <no_rot> is: **IF** (transfer port not docked) **OR** (transfer port sealed) **OR** (handwind mode on) **OR** (hoist not fully raised) **AND** (drive mode on) **THEN** <DISABLE CAROUSEL LEFT- AND RIGHT-WARD DRIVE MOTOR MODES WITHIN 0.1 SEC>	mach_spec/evd1 op_feedbck.evd1 safety_rep.evd1 mdrn_rep.evd1 reg_req.evd1	
<no_rot>-impl.clm1	2. Implementation of the specification <no_rot> is correct		inputch.clm2 motor_ctrl.clm2 segcots.clm2 corr_code.clm3 time_code.clm3 spur_lock.clm3
<no_rot>implfs.clm1	3. Implementation of the specification <no_rot> is fail-safe No single failure inhibits prevention of rotation No double failure is unsafe.		

Architecture level subclaims (2)			
inputch.clm2	1. Complete/Adequate set of control unit sensor input channels: transfer port status signals (docked/undocked, sealed/unsealed, hoist positions, drive mode) are correctly captured by corresponding sensing channels.	sens_spec.evd2	
fsinputch.clm2	2. Sensor input channels are fail-safe	sens_spec.evd2	validIO_chk.clm3 autotsts_cov.clm3 oper_fma.clm4
motor_ctrl.clm2	3. Adequate carousel motor control and communication functional interface	motorctrl_spec.evd2	
fsmotor_ctrl.clm2	4. Failsafe motor drive locking mechanism and control	motorctrl_spec.evd2	fs_code.clm3 autotsts_cov.clm3 oper_fma.clm4
fscots.clm2	5. Adequate and failsafe COTS software platform	COTS_fs_evd3;	oper_fma.clm4
segrcots.clm2	6. No interference from non-used COTS functions		segr_code.clm3

Design level subclaims (3)			
corr_code.clm3	1. The application logic satisfies the specification <no_rot>	code-ana.evd3 code_utst.evd3 code_itst.evd3 prog_exp.evd3 COTS_logic.evd3	
segr_code.clm3	2. Protection of executable code against non-used code	code-ana.evd3 code_utst.evd3 code_itst.evd3 COTS_seg.evd3;	
time_code.clm3	3; Maximum execution + actuation time is less than 0.5 sec	code_itst.evd3 COTS_maxtim_evd3 COTS_timing_evd3 code-ana.evd3	
validIO_chk.clm3	4. Adequate validity checks of input and output variables	code_utst.evd3	oper_fma.clm4
autotsts_cov.clm3	5. Complementary coverage of code by auto-tests and periodic tests	code_utst.evd3	oper_fma.clm4 pertsts_prcd.clm4
afs_code.clm3	6. Fail-safety of application code wrt: - Invalid Input/output - Errors trapped by autotests - Other defects	code_itst.evd3 code_utst.evd3 code_itst.evd3	oper_fma.clm4 serv_prcd.clm4
spur_lock.clm3	7. Spurious locks are prevented	code_itst.evd3	serv_prcd.clm4

Operational level subclaims (4)			
oper_fma.clm4	1. Adequate anticipation of failure modes of transporter, transfer port, com, sensors, actuators, power supplies.	io_rex.evd4 hw_rex.evd4 protype_rep.evd4 opr_rex.evd4	
pertsts_prcd.clm4	2. Adequate periodic tests procedures	io_rex.evd4 hw_rex.evd4	
serv_prcd.clm4	3. In-service procedures are adequate and robust (e.g. to operators' errors) for periodic testing, maintenance of transporter, and instrumentation equipment.	hw_rex.evd4 io_rex.evd4 protype_rep.evd4 opr_rex.evd4	

2.2 Evidence supporting the sub-claims

Identifier	Description and references
mach_spec.evd1 op_feedbck.evd1 eng_exp.evd1 safety_rep.evd1 mdrn_rep.evd1 reg_req.evd1	1. Specification of transporter control interlock logic 2. Operational feedback reports from machine incidents 3. Competence and past experience of plant engineers 4. Plant safety analysis report 5. Upgrade specifications and motivation report 6. Regulatory requirements
sens_spec.evd2 motorctrl_spec.evd2	1. Specifications of transporter sensors 2. Specifications of transporter communication /control interface
code-ana.evd3 code_utst.evd3 code_itst.evd3 autotst_spc.evd3 prog_exp.evd3 COTS_logic_evd3 COTS_maxtim_evd3 COTS_timing_evd3 COTS_seg.evd3	1. Back-translation of compiled application code. 2. Reports of code unit tests 3. Integrated on-site test reports 4. MSPGC 500 autotest specifications 5. Competence and past experience of programmers and of suppliers of instrumentation. 6. See Appendix D claim "PLC_logic_correct_clm0" 7. See Appendix D claim "PLC_predictable_timing_clm0" 8. See Appendix D claim "PLC_performance_clm0" 9. See Appendix D claim "PLC_functional_seg_clm0"
io_rex.evd4 hw_rex.evd4 opr_rex.evd4 protype_rep.evd4	1. Operational data on sensor, relay and motor actuator failure modes 2. Operational data on transporter, transfer port, computer failure modes 3. Conclusions from probation period reports, operator reports, other similar fuel handling systems 4. Report on prototype experiment

3. Example COTS pre-qualification claims

These claims are independent of any application (and are hence developed as a separate claim structure). These claims could be assessed and accepted for the component, and the claims for the component could be used as supporting evidence for in other safety justification (e.g. for claims about claims fail safety or timeliness made about the MHS SIS).

Name	Description	Evidence components	Subclaim expansion
PLC_logic_correct_clm0	Logic functions compliant to IEC 61131-3 syntax and semantics		PLC_compiler_OK_clm2 PLC_logic_OK_clm3
PLC_failsafe_clm0	PLC sets outputs in safe direction for the following sets of failures: inputs, outputs, processor hardware	TÜV MSPGC 500 certification report, rev. 2.0, §3.4.	
PLC_predictable_timing_clm0	Deterministic maximum timing bound for execution of software applications		HW_int_bounded_clam2 OS_cycle_bound_clm3 SW_times_bound_clm3
PLC_perfornance_clm0	The PLC can process 10^4 logic gates per second	MSPGC 500 Dependability and performance analysis, Section 4.3	
HW_int_bounded_clam2	Hardware interrupt time delay bounded	MSPGC 500 Design doc, Chapter 4	
PLC_compiler_OK_clm2	Compiler correctly translates 61131-3 code	Report on Analysis of MSPGC 500 user problem reports. Section 5 Microsafe tool qualification report MS/PGC/20/4	
PLC_logic_OK_clm3	PLC correctly execute 61131-3 code	TÜV MSPGC 500 certification report, rev. 2.0, §5.1	
OS_cycle_bound_clm3	OS performed round robin scheduling	MSPGC 500 Design doc, Chapter 5	
SW_time_bound_clm3	Application logic execution times are bounded	MSPGC 500 Design doc, Chapter 7	

Appendix D: Relationship to other justification approaches

One common basis for justification is the work of Toulmin on the structure of arguments [Toulmin1958]. This method has been claimed as the basis for the goal structuring notation (GSN [McDermid1994, Kelly1997]) and the Adelard safety case methodology ASCE which uses a claims-argument-evidence (CAE) approach [Bishop1998]. Toulmin's argument structure addresses all types of reasoning whether scientific, legal, aesthetic, colloquial or management. So it is applied more generally than the structures designed specifically for safety justifications. These structuring methods were originally concerned with the safety behaviour of engineered computer-based systems, but they have now been broadened to more general dependability claims for all classes of operated systems whether computer based or not.

According to Toulmin, the general shape of arguments consists of:

- grounds
- claims
- warrants and backing

Claims, as the name suggest, are assertions put forward for general acceptance. The justification for the claim is based on some **grounds**, the "*Specific* facts about a *precise* situation that clarify and make good the claim". We might call the grounds "evidence". Next the basis of the reasoning from the grounds (the facts) to the claim is articulated. He coins the term **warrant**[1] for this. These are "statements indicating the *general ways of arguing* being applied in a particular case and *implicitly relied on*, and whose *trustworthiness* is well established". Next we may question the basis for the warrant and here Toulmin introduces the notion of **backing** for the warrant. Backing might be the validation for the scientific and engineering laws used.

These are summarised in the table below:

Ground	*Specific* facts about a *precise* situation that clarify and make good the claim
Claim	Assertions put forward for general acceptance
Warrant	Statements indicating the *general ways of arguing* being applied in a particular case and *implicitly relied on* and whose *trustworthiness* is well established
Backing	Next we may question the basis for the warrant and here Toulmin introduces the notion of backing for the warrant. Backing might be the validation for the scientific and engineering laws used

Next we need to consider that the implication from grounds to claims may not be deterministic: it may be possible or probable that the claim follows from the grounds so there may be modifying *modalities*.

Lastly there is the issue of rebuttal. Toulmin discusses this as "the *extraordinary or exceptional circumstances* that might *undermine the force* of the supporting arguments." We could see the negation of the rebuttal as a form of precondition.

The relationship between Toulmin's scheme[2] and more recent approaches is summarised below.

[1] So the claim could be unwarranted from the evidence.

[2] He notes the skill of the expert is in establishing the Warrant and Backing. This process of selection from the vast array of potentially relevant information and the consequential shaping and scoping of the problem is what expertise is all about and why it takes so long to become an expert in the professions. This has echoes with our own work where we find that is the basis of the argument that is often not clear. Similarly he was concerned with establishing an approach to criticism, just as we are concerned with the assessment problem. Note the importance of making the basis of the reasoning a clear "first class" object.

Toulmin	**GSN**	**ASCE-CAE**	**CEMSIS**
ground	evidence	evidence	evidence
claim	claim	claim	claim
warrant	argument	argument	conjunction of sub-claims and evidence
backing(for warrant)	backing (for evidence)	separate argument	evidence integrity
modalities	context	part of claim	implicit model

All these approaches have associated notations. In the case of Toulmin and ASCE CAE, the arguments can be quite closely reasoned and contain a considerable amount of text. The CEMSIS claim structure can be represented in tabular format, and the structuring rules are more strict—a claim is a simple conjunction of sub-claims and supporting evidence. No additional argument notation is used as the sub-claims should be self evident. In the ASCE CAE notation the strength of arrows can be used to convey modalities but this is not well developed in use. Frequently uncertainty is taken into account by making the claim probabilistic or modal. The GSN notation can define a "context" which defines what "domain" is relevant to the argument.

More generally, claim-based approaches are being introduced into safety standards and guidance. This is normally termed a "goal-based approach". However the nature of the goals differs with different standards. The CAA SW01 regulation [CAA2001] identifies a standard set of top-level goals for a software based systems which are generic, (e.g. specification is valid, specification is correctly implemented, etc.). The MOD gives guidance on the safety justification documentation [JSP454], which is linked to current standards requirements ([Defstan00-55, Defstan00-56], Defstan00-58]). This justification focuses on hazards and their control, i.e. identification of hazards, risk assessment and hazard mitigation, together with compliance to regulations and long term support. These could be viewed as elements of an argument to show that the system will be adequately safe. The MOD also provides guidance on software safety-cases in [Defstan00-55], which again recommends safety case structured on claims and evidence, but focused on demonstrating particular specific safety properties. In the guidance produced by the HSE [HSE2001], the justification is directed towards the demonstration of safety properties such as:

- functional correctness
- timeliness
- accuracy
- reliability
- availability
- robustness
- fail safety
- security
- maintainability
- modifiability
- usability

The properties are only safety relevant in a given application context. For example "timeliness" might not be safety relevant for an advisory system, but "accuracy" could be. By focusing on desired behaviour, the argument and evidence are primarily related to the product rather than the process. Typically the evidence for the product comes from:

- analysis (of the system, hardware or software) e.g. static analysis or review
- testing (of components or the overall system, to check some property)
- field experience (e.g. analysis field problem reports to identify residual faults or to estimate reliability)

For example, accuracy might be justified by an analysis of the accuracy of the inputs, outputs and the computational algorithm, or by black-box tests using known results. Process aspects (such as standards

compliance) can help to provide such evidence (e.g. the results of functional tests) and give confidence that the test results are valid

References

[Bishop 1998] P.G. Bishop and R.E. Bloomfield, "A Methodology for Safety Case Development", Safety-Critical Systems Symposium (SSS ' 98), Birmingham, UK, Feb 1998

[CAA 1998] CAA CAP 670, "SW01 - Regulatory Objectives for Software Safety Assurance", CAP 670 Air Traffic Services Safety Requirements. CAA Safety Regulation Group, 1998.

[Def Stan 00-55] "The Procurement of Safety Related Software in Defence Equipment" - Parts 1 & 2, UK Ministry of Defence, Defence Standard 00-55/Issue2, August 1997.

[Def Stan 00-56] "Safety Management Requirements for Defence Systems", UK Ministry of Defence, Defence Standard 00-56/Issue 2, December 1996.

[Def Stan 00-58], "Hazop studies on Systems Containing Programmable Electronics". Part 1: Requirements. Part 2: General Application Guidance. UK MoD, Interim Defence Standard 00-58, 1996

[JSP454] JSP 454, "Procedures for Land Systems Equipment Safety Assurance", Issue 2, January 2000

[HSE2001] P.G. Bishop, R.E. Bloomfield and P.K.D. Froome, "Justifying the use of software of uncertain pedigree (SOUP) in safety-related applications", Health and Safety Executive Contract Research Report, CRR 336/2001, ISBN 0 7176 2010 7, HSE, May 2001

[McDermid 1996] J.A. McDermid, "Support for safety cases and safety argument using SAM", Reliability Engineering and Safety Systems, Vol. 43, No. 2, 111-127, 1994.

[Kelly 1997] T.P. Kelly and J.A. McDermid, "Safety Case Construction and Reuse Using Patterns", SafeComp97, Springer Verlag, 1997

[Toulmin 1958] S. Toulmin "The uses of argument", Cambridge University Press, 1958

Appendix E: Composite safety claims

Less strict, but structured approaches like the claim argument and evidence (CAE) method (see Appendix D) could also be used to make the justification, but the arguments can still be structured to follow the layered approach advocated in the CEMSIS safety justification guidance [1]. For example there could be a set of generic claims such as:

1. The SIS requirements are valid.
2. The specified SIS architecture can implement the SIS requirements.
3. The SIS components meet the architectural requirements.
4. The SIS implementation will remain safe throughout the planned lifetime.

Such a structure is also convenient as it partitions the effort needed to substantiate the claims: the first is the responsibility of the utility, the second and third claims are the responsibility of the SIS supplier, and the final claim is a combined responsibility.

Example claims on the overall SIS functionality are shown in the tables below: Note that evidence in italics is not available initially, but can be used to provide evidence at a later date.

We also include a example checklist on "adequate safety justification" that can either:

- be used by the regulator to assess the safety justification
- be used by the utility to make a separate argument that the safety justification is adequate. This is similar in principle to the "backing" used in the justification approaches described in Appendix D.

1. The SIS requirements are valid

Ref	Claim	Argument	Evidence
SIS_func_spec_ok	Specified functions are sufficient to prevent the known plant hazards	The specified MHS safety functions can be shown to cover all plant hazards and the functionality is sufficient to prevent the hazard	Plant safety report Plant safety claims Traceability analysis of MHS safety functions with the plant safety claims Modelling of specified logic and plant behaviour *Installation and commissioning tests* *Probationary operation reports*
SIS_time_resp_ok	The specified time response is correct.	The maximum time lag specified between an input change and an output change is sufficient to prevent erroneous MHS state.	Data on existing interfaces Measurements made on existing MHS *Installation and commissioning tests* *Probationary operation reports*
SIS_dep_spec_ok	Specified dependability requirements for the MHS result in an acceptable plant hazard rate	Analysis of the impact of departures from specified MHS behaviour on plant safety show that the specified hazard rates are consistent with the tolerable accident rate target for the plant	MHS functional hazard analysis Plant fault tree analysis incorporating the SIS interface hazards/failure modes. Predicted accident rate from the fault tree analysis *Probationary operation reports*

2. The specified SIS architecture implements the SIS requirements

Ref	Claim	Argument	Evidence
SIS_spec_ok	The user safety requirements have been captured in the system supplier's specification	All identified safety requirements in the user spec are traceable to requirements in the system specification. The safety function requirements will be simulated and agreed with the client	Traceability analysis *Logic simulation of core safety logic* *System acceptance tests*
SIS_arch_ok	System architecture is capable of meeting dependability requirements (fail-safety, MTBF. availability)	The primary components are COTS whose dependability properties have been pre-qualified. The SIS architecture and environment satisfies the COTS constraints identified in the pre-qualification. A dependability analysis has been performed for the system architecture to derive the system dependability properties.	COTS Fail-safety analysis COTS Reliability analysis COTS Diagnostic performance analysis Analysis of compliance with COTS constraints System dependability analysis Common cause failure analysis *System acceptance tests (simulated failures)*

	System architecture capable of meeting performance requirements (data rates, response time, etc.)	The primary components are COTS whose performance properties have been pre-qualified. Given constraints in the pre-qualification, the worst case throughputs and time delays in components are predictable. The SIS architecture and environment satisfies the COTS constraints identified in the pre-qualification. A system performance analysis has been performed showing that the system performance requirements are met it the assigned time budgets are met for each component	COTS architecture - predictable timing analysis. Time budgets for functions allocated to each component Compliance of budgets with timing constraints Overall system timing analysis *System acceptance (performance tests)*
	Architecture consistent with design safety criteria	Analyses will show architecture is compliant with design safety criteria	*Design safety criteria compliance analyses*
	Functionality assigned to architectural components consistent with required behaviour of overall system	Fail-safety and redundancy features of the COTS do not affect logical operation. Required user functionality is traceable to specific component functionality. Component functionality is traceable to system requirements (function, performance or dependability)	Redundant vote architecture analysis Traceability analysis

3. The SIS components meet their specifications

Ref	Claim	Argument	Evidence
SIS_design_ok	Specified component functionality is correctly implemented	The COTS logic platform is pre-qualified. This shows the behaviour of the logic network and logic elements are consistent with the documented behaviour. Back translation of the compiled logic will show that is consistent with the original logic specification Component testing confirms functional behaviour of applications complies with their specification	COTS functionality pre-qualification *Back translation and comparison* *V&V test results*
	There is no untended functionality	Non required COTS functionality is identified and measures have been implemented to prevent unintended activation or interference with intended functions	*COTS function analysis and countermeasures*
	Specified component performance targets are met	Analysis of the implemented applications shows that the timing budget has been met Systems performance test will show the targets are met	*COTS logic timing benchmarks* *COTS load factor estimation tool* *System tests (performance)*
	Specified component dependability targets are met	Component dependability has been pre-qualified and operational environment meets COTS constraints	FMEDA analysis COTS constraint compliance analysis
	SIS operational interface is adequate	The interface replicates the current operator interface apart from the additional movement indicators specified. So the interface should be at least as good as the existing interface. The bar code reader presents its information on a video display	Planned operator interface layout
	SIS maintenance facilities minimise the risk of error	Diagnostic features help to identify failed components and to aid replacement	COTS diagnostics documentation

4. The SIS implementation will remain safe throughout the planned lifetime

Ref	Claim	Argument	Evidence
SIS_support_ok	SIS_support infrastructure adequate (for operation, maintenance and modification)	There is comprehensive documentation on the design and maintenance of the COTS PC based software tools exist to store and modify the existing logic Access controls exist to prevent unauthorised modification. Software and hardware support will be maintained during the planned lifetime of the system.	COTS support documentation COTS software tool documentation COTS support policy
site_support_ok	The site infrastructure is adequate to maintain safe operation	Adequate procedures exist for maintenance Staff have the appropriate competencies and training	Site procedures Procedure modification reviews Staff competency procedures
site_mods_ok	The site infrastructure is adequate to permit safe modification of the SIS functionality	An adequate infrastructure exists for authorising and implementing SIS design changes An adequate infrastructure exists for updating the safety justification	Site procedures Procedure reviews Staff competency procedures
site_monitor_ok	SIS the performance of the SIS is monitored	SIS failure incidents are investigated: - to identify the cause and suitable corrective action. - check SIS performance is consistent with the assumptions in the safety justification (e.g. failure rates, safe failure fraction, etc.)	Incident reporting and analysis procedures

5. Adequate safety justification

As noted earlier in this appendix, the following list could be expanded into a claim structure like the previous sections, or it could be used as the basis for a checklist for use by the regulator. Note that this should be viewed as an example and requires further development.

- Adequate safety justification
  - system defined
  - application defined
  - environment defined, characterised
    - maintenance and modification
    - security
    - operation (part of application at a higher system level)
  - adequately safe defined
    - interface to wider system, boundary conditions
    - safety properties
    - risk
    - health and safety
  - convincing argument
    - reviewable by different stakeholders
    - correct arguments
  - valid argument strategy
    - claim structure adequate
    - warrant
      - supported in scientific literature
      - complies with relevant standards
    - backing
      - complies with relevant standards
      - supported in scientific literature
      - applied in relevant way
  - convincing evidence
    - adequate rigour
    - traceable
    - relevance
  - trusted evidence
    - consistent
    - complete
    - up to date
    - trusted organisation producing the evidence