CEMSIS

Cost Effective Modernisation of Systems Important to Safety

Work Package 0
Final Public Synthesis Report
(first issue)

Edited by D J Pavey, British Energy

COST-EFFECTIVE MODERNISATION OF SYSTEMS IMPORTANT TO SAFETY

CO-ORDINATOR

Mr. P. A . TOOLEY
British Energy
Barnett Way
Barnwood
Gloucester
GL4 3RS
UK
Tel.: + 44 1452 653503
Fax: + 44 1452 654897

LIST OF PARTNERS

1. British Energy, Gloucester, United Kingdom
2. Adelard, London, United Kingdom
3. AV Nuclear, Brussels, Belgium
4. British Nuclear Fuels, Risley, United Kingdom
5. Electricité de France, Chatou, France
6. Framatome ANP, Erlangen, Germany
7. CarlBro, Malmo, Sweden
8. TU Lund, Lund, Sweden

CONTRACT N°: FIKS-CT-2000-00109

EC Contribution:	≤ EUR 775000
Total Project Value:	EUR 2274597
Starting Date:	January 2001
Duration:	36 months

CONTENTS

Acknowledgements: The main active members of the CEMSIS consortium who contributed to this report are listed here. The section references in parentheses indicate the principal authorship of key sections of this report: P Bishop (C.5), R Bloomfield, H-W Bock, P-J Courtois (B.1,C.1), P Caspall-Askew (B.2), J-B Chabannes (B.3,C.3), S Guerra (C.2), T Hall, D Howie, B Liwang, A Miller, T Nguyen (B.3,C.3), A Klein, D Pavey (C.6), N Richer, P Tooley, J Tuszynski (B.4), L Winsborrow (C.4).

LIST OF ABBREVIATIONS AND SYMBOLS

BE-SECBS	Benchmark Exercise on Safety Evaluation of Computer Based Systems
CEMSIS	Cost Effective Modernisation of Systems Important to Safety
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
EC	European Commission
EU	European Union
FSR	Fundamental Safety Rule (France)
GL	Graphical Language
GUI	Graphical User Interface
HAZAN	HAZard ANalysis
HAZOP	HAZard and OPerability Study
I&C	Instrumentation and Control
NPP	Nuclear Power Plant
NRWG	Nuclear Regulator Working Group
OTSP	Off The Shelf Product
PDS	Pre-Developed Software
PES	Programmable Electronic System
PWR	Pressurised Water Reactor
SIL	Safety Integrity Level
SIS	System Important to Safety
WP	Work Package (of the CEMSIS project)

ASCE (Adelard Safety Case Editor) is a product of Adelard LLP.

DOORS® is a product of Telelogic AB.

LabVIEW® is a product of National Instruments Corporation.

MFM (Multilevel Flow Model) is a methodology developed at the Technical University, Copenhagen and the University of Lund. The MFM Model Builder is a product of GoalArt®.

Microsoft® Excel is a product of Microsoft Corporation.

Teleperm^{TM} XS is a product of Framatome ANP.

EXECUTIVE SUMMARY

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). 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 specific technical objectives of CEMSIS were to:

- Develop a safety justification framework for the refurbishment of SIS that is acceptable to different stakeholders (licensing bodies, utilities, suppliers) 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

The results of the CEMSIS project are recorded in a set of deliverables, of which the main ones are listed below and in Table I.

D1.2 Safety Justification Framework
D2.3 Requirements Best Practice Guide
D3.4 Guidelines for Off-The-Shelf Product-based SIS
D5.5 Final Report on Case Studies
D5.6 Public Domain Case Study

The deliverables provide guidance that has been the result of long consideration, debate and refinement by experts and practitioners representing the main stakeholders:

- Nuclear Power Plant operators
- Safety Regulators, and
- I&C Suppliers

Increased harmonisation of regulatory practice across Europe faces many obstacles and understandable concern, but has significant potential benefits. CEMSIS has stimulated European co-operation, and highlighted many areas of common interest for EU member states.

Substantial guidance reports have been produced that offer detailed advice to those involved in I&C refurbishment projects, and as a basis for continuing improvement of modernisation practice. We consider that the project has met its goals and the results will be of practical benefit to the nuclear industry, whilst also laying a foundation for further European collaboration for mutual benefit.

The project public deliverables are available on the project web-site: www.cemsis.org.

A OBJECTIVES AND SCOPE

CEMSIS was a 36-month cost-shared contract that started on 1 January 2001. This report describes the objectives and strategy of CEMSIS, and summarises the main results. A project public web-site with further information can be visited at www.cemsis.org.

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). The CEMSIS project sought 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.

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 Member States.

A typical NPP I&C modernisation process is complex, involving many stages and stakeholders. Figure 1 provides a simplified overview of the process to help illustrate the context of the CEMSIS project.

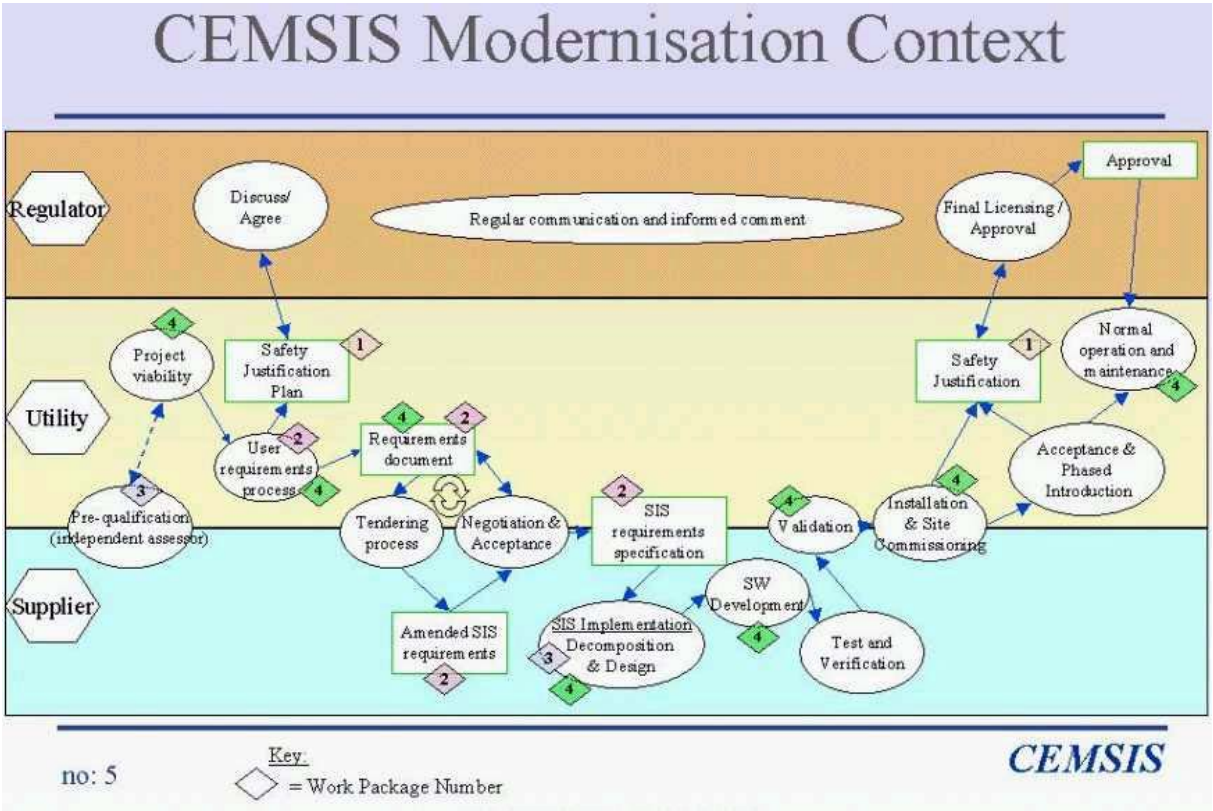


Figure 1: CEMSIS Modernisation Context Diagram

The specific technical objectives of CEMSIS were to:

- Develop a safety justification framework for the refurbishment of SIS that is acceptable to different stakeholders (licensing bodies, utilities, suppliers) 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

B WORK PROGRAMME AND WORK PERFORMED

The main innovative aspects of CEMSIS are in addressing the following key issues in the refurbishment of nuclear I&C systems:

- The harmonisation of safety justification approaches across Member States
- The definition of safety requirements for the replacement SIS
- The use of pre-developed software products in SIS, potentially even for Class A systems

CEMSIS took input from regulators on licensing issues and drew on existing experience of nuclear regulators within the EU on acceptable approaches. This experience was fed into our justification framework. CEMSIS also drew on the experience of a wide range of "stakeholders" in the industry: operators, I&C suppliers, system integrators and software specialists to identify acceptable and economic approaches to refurbishment.

Existing published standards and guidance were taken into account (e.g. Ref. [1] to [5]). Some consortium members are involved in the standards process, and expect to feed back the CEMSIS results into their development and revision.

The project has kept close contacts with the Task Force on Licensing Safety Critical Software of the Nuclear Regulator Working Group (NRWG) of the DG for Energy and Transport, Directorate H Nuclear Safety and safeguards. The safety justification framework has been influential in the guidance being currently developed by the task force (see Ref. [3] for the reports already issued by this task force).

The issues addressed in the main deliverables are outlined in more detail in the following sections. WP1 developed an innovative safety justification framework for the project. The core technical work packages on refurbishment requirements (WP2) and pre-developed software (WP3) were developed in parallel. A study of languages and tools (WP4), including graphical languages and modelling issues was made. The interim results were subjected to industrial evaluation in WP5 before being consolidated into final reports and a safety case support tool (ASCE) was extended to support the CEMSIS framework. Throughout the project there has been a dissemination and liaison task (WP6) that provided liaison to the wider community and ran workshops to focus and disseminate the public aspects of the results. The major information flows between the work package tasks is shown in Figure 2:

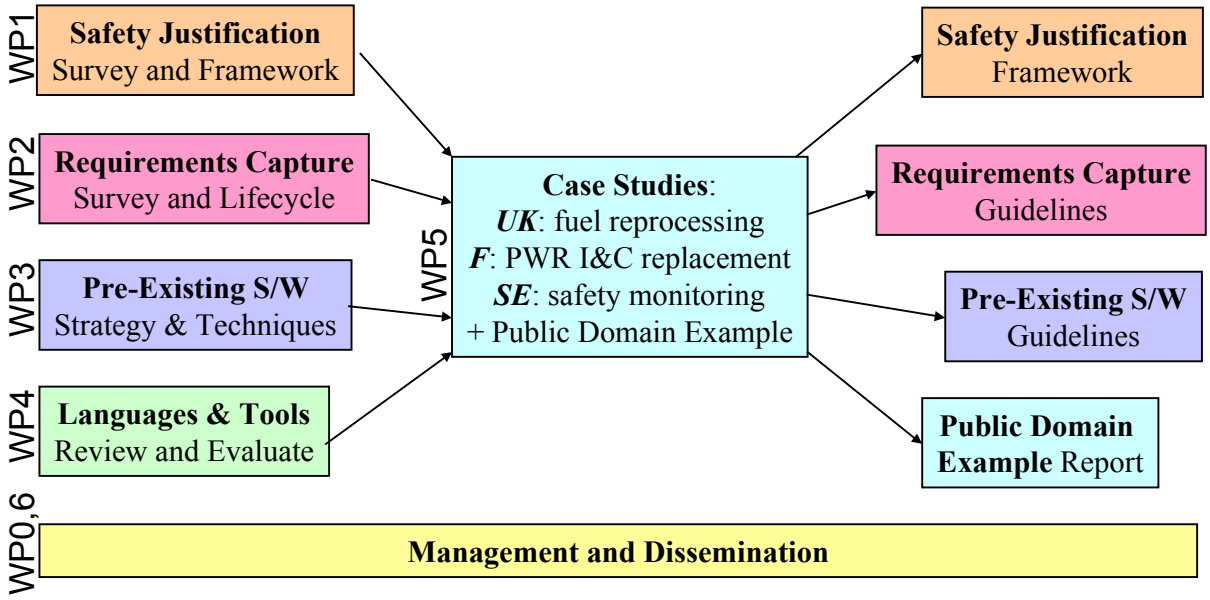


Figure 2: Information Flow between Work Package Tasks

B.1 Safety Justification Framework

The process of approving software-based equipment for executing safety critical functions is not yet easily mastered by regulators, licensees and suppliers. A review of licensing approaches (CEMSIS deliverable WP1-D1.1) clearly showed that except for procedures which formalise negotiations between licensee and licensor, no systematic method is clearly defined or in efficient use yet in CEMSIS member countries for demonstrating the safety of a software based system. If a systematic and well-planned approach is not followed, licensing costs in resources and delays may affect the benefits expected from upgrades or modernisation.

The first task of this workpackage was to itemise the differences in the overall systems engineering and reactor licensing approaches for software based systems in the different Member States. The goal was not to seek to harmonise these approaches but to document them in a way that would enable a clear specification of what should be a common foundation for the safety justification of SIS.

The second and main task was to propose an approach and a framework that would be useful and efficient to demonstrate safety, and that could accommodate without restriction the different national practices. The focus was on studying and proposing a method to produce and assemble the basic elements of a safety justification, typically:

- the system dependability properties to be justified
- the overall structure, and levels of the safety case
- the types of argument and plausible evidence that should be deployed at different levels to justify that the system design, implementation, control and maintenance satisfies the required dependability properties.

Another essential aim of the work was to achieve a cost-effective demonstration of the dependability of the equipment being replaced or upgraded and of its software, that is:

- To propose accurate models and representations of the environment and the system, with interpretations at the plant interface, design and operation level, that would make justification and consensus less ambiguous and easier to achieve;

- To structure arguments and disparate sources of evidence in ways that allow for modularity and integration of sub-safety cases.

The main tasks of the WP1 programme to achieve these goals were:

WP1.1 Topical review of approaches to licensing computer systems;

WP1.2 Formulation of the safety justification framework

B.2 Requirements Capture for Refurbishment

B.2.1 Review tools and techniques for requirements capture and analysis.

The review included a review of existing requirements engineering technologies to determine those that are best suited to refurbishment projects. An information collection exercise was undertaken, including sources such as:

- Nuclear industry regarding relevant related projects,
- Literature review: forthcoming conferences, publications of relevant journals,
- University departments; centre for software reliability,
- Suppliers for opinions and product details, Internet search,
- Previous experience of the participants' companies. (questionnaire),
- Previous research experience including the REAIMS project

The main body of the report consists of a description of the approach taken to carry out the review, how the questionnaire feeds into the review, how the review feeds into the framework document, a table which lists all the techniques which have been reviewed/classified for their applicability to CEMSIS according to process, a conclusion and finally two appendices with the results of the review. 84 techniques were identified and assessed for their applicability, which spanned the CEMSIS themes.

The review document can be used by any organisation that is involved with refurbishment. It allows the reader to select a technique. In essence the review document is a directory of methods/techniques for system design. It is designed to act as a reference for the Best Practice Guide, although it can be used on its own.

B.2.2 Establish the background and rationale and lay the principles, activities and goals for the Best Practice Guide.

This document describes the CEMSIS approach to Requirements Capture for Refurbishment. It is a pre-cursor to the final deliverable: the Requirements Engineering For Refurbishment Best Practice Guide (D2.3). It establishes the background and rationale for the Best Practice Guide and although the principles, activities and goals for the Best Practice Guide are laid in this document, they will be further operationalised in the deliverable D2.3, taking into account the experience of the project partners with the case studies.

It aims to provide practical assistance for establishing the safety requirements for SIS refurbishment. It presents a simple requirement engineering lifecycle for a refurbishment project and it provides practical general guidance covering the lifecycle phases of the requirements engineering process, as described in. It also contains general principles and goals that should be considered during the requirement's lifecycle and links those goals to specific phases of the requirements engineering process.

To study current Requirements Engineering practices, development needs, and preferred ways of technology transfer; a questionnaire was compiled and sent to the CEMSIS partners. The questions addressed basic issues of Requirements Engineering knowledge to assess at what level of maturity the partners organisations and a few NPP personnel where at. Since

only seven organisations were interviewed and not all of the questions were answered, the results were not suitable for statistical analysis. Even if the sample size of the survey didn't allow us to utilise the numerical data to its full potential, it helped to assess the current state-of-the-practice in the nuclear industry in a more objective way than merely qualitative studies.

As CEMSIS is about technology transfer a classical Requirements Engineering process was described including, its phases and aims of main activities. This would allow the user of D2.2 to learn and get familiar with Requirements Engineering in order to create a level playing field at which refurbishment commences. Although specific projects have variations in the implementation of the process phases, the general activities and their principles are constant. When using the requirement's process for a specific application, the generic features will have to be combined with the particulars of the application.

Meetings were held between BNFL and Adelard in order to adjust the classical requirements engineering process in order for it to be tailored to modernisation projects.

Given the fact that a modernisation project starts from an existing system that is replaced by a possibly slight different system, we discussed the fact that the classical requirements process has to take place twice. Therefore, each of the phases of the classical requirements engineering process takes place twice. Although the specific way the same "classical" phase occurs is different (e.g. identification of the existing requirements is different from identification of new requirements), the main principles are the same. The document describes the specificity of each occurrence of the classical process phases in a modernisation context. However, the specifics have to be combined with the general principles to have a full understanding of what each phase involves.

B.3 Justification of COTS-based systems

The first requirement of this work package was to define what is COTS (Commercial Off The Shelf). Several animated discussions did not lead to a common position on the term so it has been decided to use the term "Off The Shelf product", which will cover equipment families, dedicated devices and software components. An OTS product is defined as "product that already exists, is available as commercial or proprietary product and is being considered for use in a computer-based system".

The first task enabled the proposal of an optimised strategy for the safety justification of OTSP-based SIS. The retained strategy is to decompose the safety justification in two phases:

- The pre-qualification of the OTS product embedded in the system;
- The effective safety justification of the SIS.

The first task enabled the definition of:

- a taxonomy for the functional assessment of OTS products ;
- a taxonomy for the dependability assessment of OTS products.

The next step of this work package was to define the properties essential to safety at a SIS level (i.e. characterisation, functional adequacy, correctness, robustness, maintenance) and to deduce the OTS product properties that can be assessed independently from any modernisation project during pre-qualification.

The framework for safety justification proposed by WP1 is based on a claim-argumentation-evidence approach, where each claim made regarding the dependability of the SIS is supported by a structured argumentation. Taking into account this safety justification framework, WP3 studied the four types of demonstration that can be adopted to provide evidence, i.e. systematic proofs, demonstrations by sampling, demonstrations by inspection and demonstrations by development process. The global approach for the dependability

assessment led to building 5 tables (in accordance with the taxonomy for dependability assessment) that provide practical methods to demonstrate the OTS products properties.

This framework then focused on the functional assessment of OTS products and their matching with user requirements. Four tasks have been developed:

- Task 1: Functional modelling, for each main category of OTS product (product and project-independent);
- Task 2: Functional description of candidate OTS products (product-dependent and project independent);
- Task 3: Specification of user requirements for each category of OTS product (product-independent and project-dependent);
- Task 4: Matching of OTS products with corresponding user requirements specifications (product and project-dependent).

To be complete, this work package addressed the effective safety justification of OTSP-based SIS. This activity mainly focused on:

- The effective criticality of OTS products in SIS;
- The sources of Common Cause Failures and the possible defences to be adopted.

The last task of this work package was to synthesise from this amount of work a single deliverable document (D3.4).

B.4 Justification of Graphical Languages

Development of general justification approaches for graphical specification languages, the initial objective of this work, encountered difficulties:

- The subject of graphical languages (GL) turned out to be difficult to integrate with the main issue of the project – modernisation of SIS. The subject was difficult to define and easily misunderstood.
- The scope of this work package was changed from GL to GL-based tools and models or representations of specifications or programs for SIS modernisation.
- The distinction between WP4 and other work packages became difficult to maintain.

It was decided that the partially complete WP4 work would remain as an internal report (section B.4.1) and some of issues would be addressed in other packages. Models are an important aspect in the WP1 framework. Requirements specification tool issues were addressed in WP2 (section B.2.1). The unused resources of WP4 were used in the case study concerning I&C modernisation of a reactor shutdown system (section C.4.4), through practical application of a GL tool based on the Multilevel Flow Models.

The GL of MFM is representative of general properties of the graphical languages applicable for development of I&C systems.

B.4.1 Review and evaluation of sought-after properties of tools based on graphical languages of models and representations

The main focus of this internal investigation was on the sought-after properties of tools based on graphical languages for models and representations applicable in SIS I&C development. The tool properties were identified in the context of the needs of stakeholders in the I&C modernisation (Figure 3) process:

- to identify and specify the main results to be achieved and in that way to understand and co-ordinate their activities
- to achieve and document those results
- to prove that the stage requirements are complete and relevant

- to prove that the results fulfil requirements

A main theme of the report is that graphical language tools can support safe and cost-effective modernisation in the following way:

- modelling of stage activities demonstrating clearly stakeholders' roles and objectives
- modelling of the product, enhancing product analysis and demonstration of functionality by simulation, test generation, software code generation, etc
- execution of the model to support stakeholders' activities, mainly by answering inquiries, and providing documented evidence to claims

The above approach is developed by identifying kinds of models required (architecture, functional, state and dimensioning models), a method for evaluation of properties and giving an overview of the tool properties generally required. The properties are then identified and analysed with examples of applicable tools. That approach is used to identify generic tool properties, and properties required for two principal stages of the modernisation process: requirements engineering and software development. Finally an overview of the applicable standards is given, including the recent version of standard IEC60880.

B.5 Application and Evaluation

Case studies were undertaken to evaluate the results of the initial guidance documents on realistic examples taken from actual projects. To focus the effort, different aspects of the concepts outlined above were applied to three industrial case studies (led by BNFL, Carl Bro, and EDF):

- Replacement of PDP11-based control software on nuclear fuel reprocessing plant
- Justification of typical safety claims for I&C based on a specific COTS platform in the context of the French Fundamental Safety Rule, and of UK licensing experience
- Replacement of a safety monitoring system in a Swedish Nuclear plant

In order to facilitate dissemination of the CEMSIS method, a fourth (generic) example was developed to demonstrate the method end-to-end. This generic example (see section C.5) incorporates features from several real applications in the nuclear industry. Because the example is not identifiable with any specific installation, it can be placed in the public domain.

The public-domain example was used as a vehicle for performing activities following the CEMSIS guidance. The activities covered the early phases of development, and specified the later development phases in sufficient detail to enable the production of a safety justification. The findings from the activities performed for the public domain example are described in Ref. [9].

B.5.1 Case Study 1

The first study, led by BNFL, took as its example a skip handler interlock protection system. The plan for the study included the following activities:

- Safety justification in accordance with the CEMSIS WP1 guidelines;
- Requirements engineering and detailed specification via the methods defined in WP2, WP3 and WP4;
- Implementation incorporating COTS items via guidance developed in WP3.

The first task was the collection of legacy documents, of which a reasonably complete set was available. The safety justification activity ran concurrently with the other tasks and provided an opportunity of comparing the guidance given by CEMSIS WP1 with the company processes and regulatory regime of the organisation performing the case study.

The WP2 recommendations were followed in a requirements engineering process. A desktop exercise (existing requirements discovery) was performed and formal meetings were then held with the client and the vendor in order to elicit any new requirements. A few requirements were removed because they related to the old technology and because of changes in operator instructions and maintenance. A series of detailed hazard analysis exercises was then performed followed by detailed specification of user requirements. Unfortunately the intended IEC 61508-certified COTS product was not available within the timescale and therefore it was not possible to exercise the recommendations of WP3.

B.5.2 Case study 2

The second study, led by EDF, concentrated on consideration of the CEMSIS safety justification guidance as it relates to a COTS platform.

Certain selected claims were expanded and evidentially supported. Framatome ANP played the role of COTS platform supplier, and was very helpful with information about platform design and development. The strategy of the case study was:

- Presentation of the operating principles of the PES-based platform;
- Identification of safety properties to be satisfied by such a platform;
- Application of the WP1 safety justification framework to one significant safety property chosen from those identified.

There were two parts to this case study. In one part Framatome ANP and the French end-user worked together to construct a justification strategy to demonstrate compliance with the determinism principle. In the other part F-ANP worked with the UK end-user to construct a justification strategy for the claim that there is a required set of time margins within which the safety functions will be performed. This was presented as:

- a pre-qualification case for predictability of platform response time, with
- an argument for a typical application, invoking the above argument, to justify the claim.

B.5.3 Case study 3

The third case study, led by CarlBro, took as its starting point a reactor protection system that has recently undergone refurbishment. The tasks undertaken were:

- Production of safety justification to identify the most important features of the requirements.
- Collection of data regarding legacy information, product viability, project management, user requirements and necessary information for supplier.
- Information transfer between teams playing the roles of customer and supplier, in a sufficiently detailed form that is understandable for the end-user, customer and supplier.
- Identification of documents and tasks required as evidence in support of the justification framework.
- Review of the documents for completeness and quality, performed by the case study team and by comparison with the actual refurbishment project.

The interaction between the "customer" and "supplier" took the form of discussion and review of each other's documents. The activity led ultimately to a proposal for an alternative model of customer/supplier interaction, based on a partnership approach rather than on presentation of a fixed user specification followed by identification of the supplier whose COTS product most closely fits the specification.

B.6 Dissemination and Liaison

A number of initiatives to disseminate the CEMSIS experience and results have continued throughout and beyond the project itself.

- Contact was maintained with a related project, BE-SECBS, which combined with CEMSIS to present the public workshop. Framatome ANP, a partner in both projects, gave regular updates to CEMSIS on the progress of BE-SECBS.
- Both CEMSIS and BE-SECBS members participate in the European Regulators Working Group, which continues to meet. It is anticipated this will continue to provide a valuable forum for feedback and dissemination of CEMSIS proposals.
- An intermediate workshop, with invited participation, was successfully hosted in October 2002 by EDF in Paris to foster the liaison with key stakeholders in the licensing process. Feedback from this event was taken into account in the case studies and the ongoing development of CEMSIS ideas.
- The final workshop, which was open to all interested participants, was held in conjunction with the FISA conference in November 2003. Further details of this workshop are given below in section C.6.
- Project members are involved in the ongoing development of international standards in the field of I&C systems important to safety. This includes the development and revision of the influential generic standard IEC 61508, and the nuclear sector standards IEC 60880 and IEC 62138.
- The project website has a public part at www.cemsis.org.

C RESULTS

The results of the CEMSIS project are recorded in a set of deliverables, of which the main ones are summarised in Table I.

Table I : CEMSIS main deliverables

no.	title	reference	public
D1.2	A Dependability Justification Framework for NPP Digital Instrumentation and Control Systems	wp1_avn010	
D2.3	Requirements Engineering Best Practice Guide for Refurbishment	wp2_ade043	P
D3.4	Assessment and analysis guidelines for Off-The-Shelf Product-based Systems Important for Safety	wp3_edf037	P
D5.5	Final Report on Case Studies	wp5_beg038	P
D5.6	Public Domain Case Study: Example application of the CEMSIS guidance	wp5_ade039	P
D6.1	Paper for presentation to the FISA conference in November 2003	wp6_beg035	P
D6.2	Report of post-FISA workshop number 4 "Safe and Cost Effective Modernisation of Programmable Systems"	wp6_beg039	P

The following sections provide a summary of these deliverables.

It should be borne in mind that, as for any research, some of the proposals are 'groundbreaking' and not necessarily supported by every project member, but they are agreed to be a good basis for further development and research.

C.1 Safety/Dependability Justification Framework

The questions addressed by work package WP1 concern the evidence and the arguments needed to justify the safety of a computer-based system: How should evidence be presented to certification or regulatory authorities? What best practices should be applied? How should we decide whether there is enough evidence to justify the release of the system? To help to solve these problems, a method is proposed for the justification of the dependability of a system. The method specifically aims at dealing with the difficulties raised by the validation of software, taking into account the challenges and the constraints of up-grades and modernisation of NPP instrumentation important to safety (SIS).

To this end, a pragmatic framework is proposed to make a cost-effective justification of dependability. The framework provides a *hierarchical structure for constructing arguments* relying on a variety of disparate sources of evidence; this structure provides modularity and allows the integration of arguments from previous subsystem safety cases. The approach emphasises the necessity - for the demonstration of dependability - of adequate models and representations of the system at the plant, architecture, design, and operation levels.

Structured layers of evidence and relational models are the two tropisms, which showed the way to design the framework and to recommend *a set of practices* - or a *discipline* - that a licensee and a regulator can adopt to produce a convincing justification of the dependability of a given system.

This approach may depart from certain current licensing practices, which are based on rule-, design principle- or standard- compliance. Because they often fail to demonstrate convincingly by themselves that a system has the specific dependability properties required by a given application, such practices often entail licensing delays and costs. In this respect, a dependability properties-oriented approach may be more efficient and flexible: it may remain applicable in situations where standards are not. A standard, for instance, may not accept certain practices or alternative sorts of evidence that may be perfectly adequate or even necessary to implement and justify specific dependability properties.

The presentation of the framework is organised into four parts: prescriptive, descriptive, structural and analytical part.

The **prescriptive part** gives recommendations on how to start the justification with initial dependability claims, and on how to organise claims, evidence and arguments. The claim-evidence-argument multi-layer structure rests on news concept of *claim expansion and delegation* into sub-claims. These concepts allow initial top-level dependability claims to be justified by different types of evidence at the plant interface, the architecture, the design and the control of operation layer.

The framework can accommodate deterministic logic as well as probabilistic claims when uncertainty is present. Whatever degree of rationalisation the framework achieves – a consensus among stakeholders remains however necessary. An objective of the framework is to identify the nature and the scope of this required consensus, and to reduce it to what is strictly required by an axiomatic approach. The relations between the framework and three basic principles, or "theories", of safety are also investigated: prevention, precaution and enlightened catastrophism.

The **descriptive part** studies an as yet unexplored aspect – albeit essential - of dependability cases: the essential roles played by models. Models are critical in the demonstration of dependability, in two different ways. First, dependability like other attributes of a system can only be apprehended by means of observations and models, the latter being necessary to give meaning and purpose to the former. And even more importantly, models are indispensable for the construction of arguments and the delivery of proof obligations.

At the moment we are completing the investigation of the types of models needed. Models must be chosen for their usefulness and effectiveness in interpreting, explaining, predicting and proving, balanced against the cost of designing and using them. The generic approach followed for this investigation is based on structures, states (or classes of), relations between state variables, time and event classes. This study of models has other benefits. Some new aspects of the nature of claims on diversity, hazard mitigation and controllability, and on requirement properties are revealed. Models also provide a precise definition of *the types of evidence and documentation* needed.

The **structural part** identifies the inter-relations between models at the different levels of evidence (plant interface, architecture, design, operation). Conditions for re-using arguments and for the composability of safety cases result from these model inter-relations. Different instantiations of the framework have been considered, in particular for systems of different safety criticality, and for systems using pre-existing platforms or COTS software.

Dependability interrelations between subsystems are then of the "*guaranteed service – rely condition*" type.

Finally, recommendations are given for building a safety case. Those are discussed in the **analytical part**. Basic rules for the expansion of claims and the *construction of dependability arguments* are given. A method is also proposed to systematically elicit claims and the evidence they require.

To **conclude,** the main innovative features of the approach are (i) the use of layered models for the representation of the system and the organisation of the evidence, and (ii) the mechanisms of inductive claim expansion and delegation of evidence onto lower layers for the construction of arguments. The major benefits are:

- Better structuring of arguments to back up and to limit subjective expert judgement;
- More natural and easy transformation of non-functional requirements into functional claims;
- Possibilities of assessing the weight of particular components of evidence,
- Modular re-use of arguments of sub-safety cases.

Thus, this dependability justification approach gives precedence to - and focuses on - the dependability properties of the system. By the same token, it is more cost effective in terms of efforts and resources spent on the justification: two advantages which meet the respective priorities of the regulator and the licensee, and should therefore make their negotiations easier and more efficient.

Not all aspects of the framework have been thoroughly explored yet. Some aspects of the inter-relations between the layers of evidence would in particular need further investigations and experiments. Because claims and arguments should dictate which evidence is required, and not the opposite, these further experiments should be carried out by research projects intimately associated with real industrial system design and safety cases developments. This would allow a realistic assessment of the framework with the freedom to determine the evidence to be produced, preferably to being assessed against available pre-existing evidence.

C.2 Requirements Best Practice Guide for Refurbishment

This section describes the Best Practice Guide on the development of safety requirements of SIS refurbishment. The guide aims to provide practical assistance for establishing the safety requirements for SIS refurbishment. It presents a simple requirements engineering lifecycle for a refurbishment project and it provides practical general guidance covering the lifecycle phases of the requirements engineering process. It also contains general principles and goals that should be considered during the requirements lifecycle and links those goals to specific phases of the requirements engineering process.

C.2.1 Introduction

Capture of requirements is a crucial but difficult part of SIS refurbishment. The requirements to be captured are safety, application and system requirements including those arising from interfaces. This includes both the recovery of requirements from available documentation and methods for identifying new and requirements not documented but part of tacit knowledge.

The additional requirements to be identified are those not already captured by analysis of the existing documentation. These will be identified by a stakeholder viewpoint analysis to ensure that the requirements of all stakeholders (supplier, designer, client, regulator, operations, maintenance etc.) are recognised and fulfilled. In addition, change of environment

in which the control system resides can also be a source of new requirements, for example new regulatory requirements, new interfaces to plant and operators and new technologies.

The Best Practice Guide has three main components:

- A requirements engineering process (C.2.2).
- A set of stakeholder or viewpoints (C.2.3).
- A claim-based view (C.2.4).

The requirements engineering process describes the activities and aims of the phases of the requirements process for modernisation. The process is based on the "classical" requirements engineering process, but the process is modified and expanded in order to take into consideration the features of a modernisation project of a SIS.

The claim-based viewpoint of Requirements Capture for Refurbishment describes the properties we would like to see of the requirements and their specification and provides a clear link to safety justification framework.

The set of stakeholders or viewpoints guide the activities of the requirements process, to increase the likelihood of achieving a complete requirements specification, where requirements are not left unspecified because some of the stakeholders were not consulted for the requirements identification.

The requirements engineering process is linked with the claims that will be made about the specification developed and the goals to be achieved at each phase of the process. The claims are linked to different phases of the process. In this way, the developers know what has to be achieved and demonstrated in each of the phases of the process. This is described in C.2.4 and provides a link to the WP1 Safety Justification Framework. C.2.5 provides some comments on the cost-effective aspects. Finally we conclude in C.2.6.

C.2.2 Requirements engineering process for modernisation

The requirements engineering process for modernisation is based on a generic requirements engineering process, modified to take into account the specific case of modernisation, as described below.

In the case of refurbishment projects, the system being developed has to be integrated into an existing and working environment. Even in the case when the refurbished system is to keep exactly the same functionality of the existing system (and hence will have the same requirements), the requirements of the existing system have to be gathered and a complete requirements specification is essential for the successful completion of the project. This requirements specification is typically a collection of pre-existing documents that might be extended (in the case where the existing documentation is not appropriate) to fully specify the existing system. A full understanding of the existing functionality is essential to ensure that the system will satisfy the user's needs and do exactly what is intended.

In addition, if some of the functionality or features of the new system are different, the new requirements have to be gathered and integrated with those of the existing system.

Therefore, the standard requirements process takes place twice:

Initially, the requirements process takes place to gather the requirements and their documentation before modernisation and to establish the design basis, i.e. the existing requirements of the working system that is being modernised.

Finally, if new requirements exist, they also need to be elicited and combined with the existing requirements. The integration of the new requirements with the existing

requirements, with any potential inconsistencies solved, will be the base for the refurbishment project.

We note that the fact that the process is described as having two iterations does not mean that one should discard everything that has been previously done, but rather that the requirements specification is incrementally developed in two steps. The point is that it is important to consider whether the existing documents are complete and include all the information needed for the refurbishment.

The refurbishment process should start by looking at the existing documentation. While looking (and analysing) that documentation, it is important to assess whether the information is enough and appropriately documented, or there is a need to gather more information that was not adequately documented (e.g. maintenance procedures that were followed but are not part of the requirements documentation). However, if the existing documentation is appropriate, the existing documents could (and should) be used. One cannot assume that the existing documents are enough, though. They need to be assessed and analysed (and completed when necessary) before moving on to the next stage of the process.

The first iteration of the process, i.e. the lifecycle for the existing requirements, has as objective the development of a requirements specification. This requirements specification describes the existing system that is being replaced and it will be one of the inputs for the second iteration. As we have said before, this requirements specification is a collection of documents. It might include several pre-existing documents, which might be completed with further information if needed.

New and old requirements will then be combined in the second iteration of the process. In this second iteration the requirements specification is extended and modified to include the new requirements, and inconsistencies or redundancies corrected. This will form the requirements specification for the modernisation process. These two steps of the lifecycle support an incremental development of the requirements specification for the refurbishment (Figure 3).

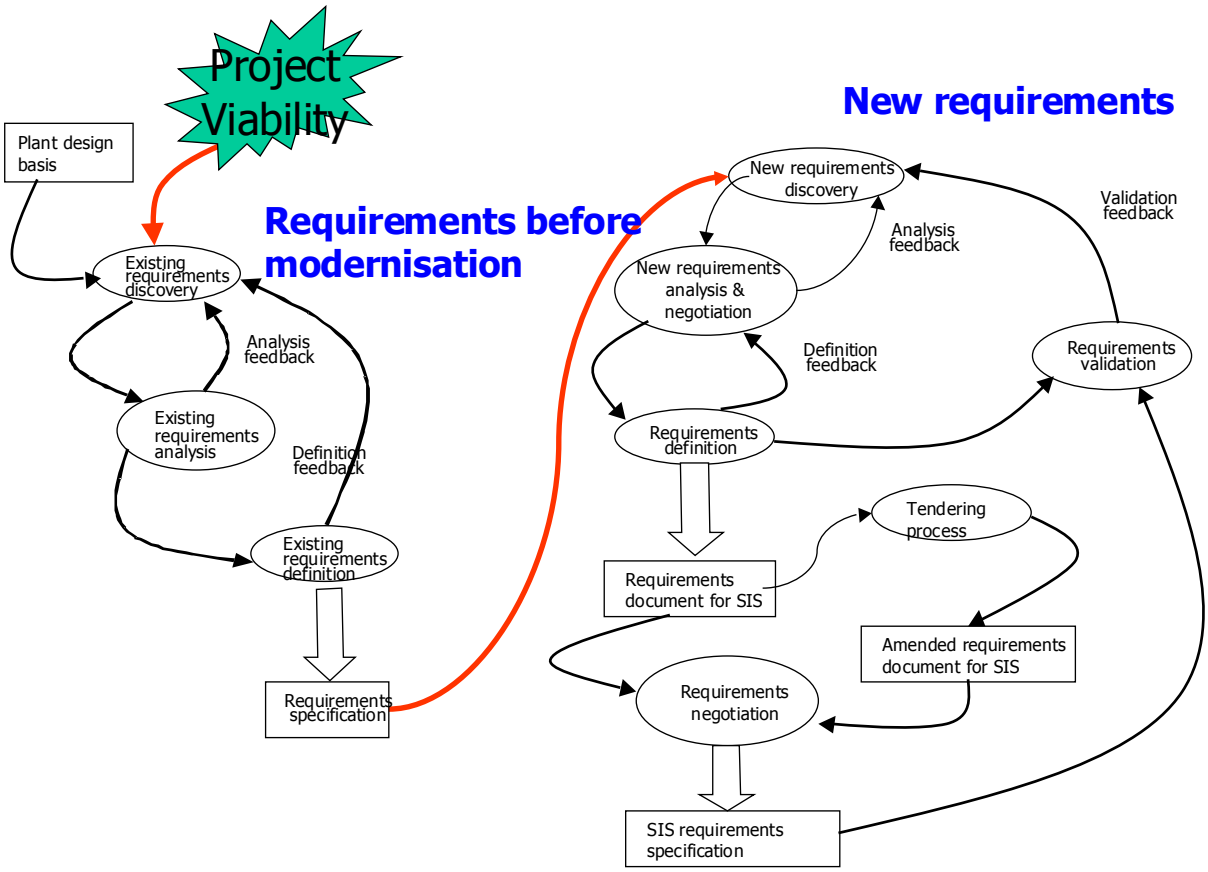


Figure 3: Requirements process for modernisation

However, before the requirements process actually starts, a project viability study has to take place in order to decide whether the modernisation process will actually happen. The

results and documents produced for the viability study are inputs to the other phases of the requirements process.

Once the requirements process is sufficiently complete, the design phase starts. The design phase transforms the requirements specifications into design that will be the base of the system. Design determines the components and devices needed for the product to be built.

We note that in most projects, the requirements process is not exclusive of the front-end of the lifecycle. The different phases of the development process increase the awareness of the stipulations made in the requirements specification, and more requirements are added, deleted or modified. However, the late modifications of the requirements specification are costly and they should be minimised. In the case of Cemsis this is even more the case, as there are several safety implications of late requirements changes. Once a requirements specification is approved, it can be subject to changes, but through a strict quality assurance plan that ensures that all required verification and validation and independent assessment activities are done again to avoid non-regression.

Note that the process shown here is general. Each of these phases can be divided in more specific phases, depending on the practices of the organisations undertaking the refurbishment. The specific details included in each of the specifications, and in particular in the user requirements specification, vary among partners of the project. However, the activities described here always take place, and this process can be further developed and extended to fit the needs of specific users.

In the Best Practice Guide, each phase of the lifecycle is described according to a common template, which includes aims of the phase, main activities involved and goals to be achieved (according to the goals set as described in C.2.4).

C.2.3 Stakeholders and viewpoints

A stakeholder is anyone who will be affected by the product. It includes people that use the product, that build the product, and whose knowledge is needed to build the product. Examples of stakeholders include users, sponsor, testers, business analysts, technology experts, system designers, legal experts, marketing experts and domain experts.

It is important to identify all the stakeholders for a given project. If we fail to identify some of them, we might miss some of the requirements. In this case, several modifications will be necessary later in the development process to accommodate the requirements of the stakeholders not included originally.

For each stakeholder it is necessary to identify:

Stakeholder identification (e.g. role/job title, person name, organisation name).

Knowledge needed by the project.

Degree of influence for that stakeholder/knowledge combination.

Different stakeholders have different perspectives or views of the system they are trying to describe. These perspectives are partial or incomplete descriptions that arise from the different roles or responsibilities of the stakeholder. The agent or stakeholder combined with the view of the agent is called viewpoint [7].

Organising requirements in different viewpoints helps to structure the elicitation. It also helps the prioritisation and management of requirements [8].

Different stakeholders might have common goals and be involved in similar parts of the system. However, in the case of the different goals it is natural that some of their requirements are contradictory.

C.2.4 Claim-based view

The development of the requirements engineering lifecycle for a refurbishment project should be based on the objectives and goals that are trying to be achieved. Stating clear goals for the results of the requirements lifecycle gives the freedom to develop the process in different ways and accommodating different techniques, but keeping in mind what is ultimately trying to be achieved.

If a goal-based view is adopted, it is necessary to provide a justification that the goals are achieved. Goals become claims and the Claim-Argument-Evidence framework can be developed to show how they are progressively satisfied: explicit *claims* are stated, convincing *arguments* to justify the claims are met are presented, and adequate *evidence* to support the arguments is described. So we have

- goals used to design the requirements process
- claims to be made about the requirements to support the safety justification

This Claim-Argument-Evidence approach provides a clear link with the WP1 justification framework. The Cemsis safety justification framework is based on the notion of "claim" and provides a structure to justify these claims. Claims correspond to system dependability properties and are inferred from (sub)claims at different levels: subclaims on the system requirements properties, on the architecture, on the design and on the operation. Subclaims at the system requirement level are those to be considered here by the requirement process.

The Claim-Argument-Evidence framework provides simultaneously guidance for the requirements process and a justification for its completeness. In this structure, the top-level claim is divided into two overall objectives (sub-claims):

Requirements validity. To ensure that arguments and evidence are available which show that the requirements correctly state what is necessary and sufficient to achieve adequate safety and the desired functionality, in the system context.

Requirements integrity. To ensure that the arguments and evidence are available to show that the requirements are derived from relevant sources and traceable to both its sources and to design and implementation. Requirements integrity can be divided into *configuration consistency* and *requirements traceability:*

Configuration consistency. To ensure that the arguments and evidence are at all times derived from: a known set of supporting documentation and a known set of software products and descriptions that have been used in the production of that version. Examples of items under configuration consistency include: plant description, drawings, safety requirements, design rationale for safety system, user manuals and operating instructions and results of hazard analysis.

Requirements traceability. To ensure that arguments and evidence are available which show that all requirements (and in particular safety requirements) can be traced to their source (in particular the plant safety analysis), to the design, are satisfied in the implementation of the software, and that other functions implemented in the software do not adversely affect safety.

As discussed in C.2.2, for refurbishment projects, we divide the requirements process and specification in two parts: the existing requirements and the new requirements. Similarly, the goal for the validity of the requirements is divided in two parts: validity of existing requirements (including in the *existing requirements specification*) and validity of new requirements.

C.2.5 Cost minimisation

The framework should help to control the costs of the overall refurbishment in variety of ways:

- By identifying requirements errors early in the lifecycle. Requirements errors found later in the lifecycle are considerably more costly to fix.
- By allowing changes to the existing system to be minimised, but integrating new requirements if desired.
- By using an incremental requirements process, where existing documents are reused, updated and extended as necessary.
- By correctly and completely documenting requirements, the next refurbishment would be based on completely specifications that would not have to be redone.

C.2.6 Conclusions

This document summarises the Cemsis approach to Requirements Capture for Refurbishment.

The Cemsis approach aims to provide practical assistance for establishing the safety requirements for SIS refurbishment and it provides guidance on eliciting, analysing and documenting the safety requirements for a refurbishment project. It presents a simple requirements engineering lifecycle for a refurbishment project and it provides practical general guidance covering the lifecycle phases of the requirements engineering process. It also contains general principles and goals that should be considered during the requirements lifecycle and links those goals to specific phases of the requirements engineering process.

C.3 Guidelines for Off-The-Shelf Product-based Systems

There are many definitions and different understandings for the term “COTS” (Commercial Off The Shelf). In order to avoid unnecessary controversy, for the purpose of CEMSIS and notably of WP3, it has been proposed to use instead the term “Off The Shelf Product” (OTSP). “Off The Shelf Product” could be defined as “a product that already exists, is available as commercial or proprietary product and is being considered for use in a computer-based system”.

The notion of OTS product covers a very wide range. E.g., an OTS product may be an equipment family, a dedicated device such as a sensor or a software component.

C.3.1 Properties essential to safety

WP3 proposes to base the safety justification on the demonstration that properties essential to safety are satisfied at the SIS level. The top-level safety property that needs to be justified for the SIS is the **adequacy of the SIS over its lifetime to satisfy the real safety needs**. This main property may be decomposed into the following first level properties:

- the ***characterisation*** of the SIS (including its description), so as to know with precision the system we are dealing with;
- the ***functional adequacy*** of the SIS to the real safety needs, so as to guarantee that the SIS fits in its complex environment where it interacts;
- the ***correctness*** of the SIS with respect to its description, so as to ensure that the SIS is and behaves as specified in its description;
- the ***robustness*** of the SIS with respect to postulated internal and external non-nominal conditions, so as to guarantee a predictable behaviour of the SIS even in non-nominal conditions and that safety is not jeopardised;
- the ***maintenance*** of the adequacy to safety during the lifetime of the SIS.

C.3.2 Demonstration that safety properties are satisfied

The framework for safety justification proposed by WP1 is based on a claim-argumentation-evidence approach, where each claim made regarding the dependability of the SIS is supported by a structured argumentation. In the same way, properties may be decomposed in sub-properties, claims, argumentation and evidence. The demonstrations adopted to provide evidence can be categorised into four different types:

- Systematic proof; it is based on rigorous principles and formal reasoning that provide an objective evidence that a claim is satisfied in all considered situations; it may be built in *a priori* (e.g., by the application of design rules precluding the item from violating the claim), or it may be achieved *a posteriori* (e.g., by a formal analysis of the item at the end of the development process);
- Demonstration by sampling; it provides a systematic evidence, but only on a finite and limited set of discrete samples; it includes tests, measurements, simulations, and experience in operation; the satisfaction of the claim on the full range of situations may be extrapolated if the set of samples is accepted as representative of the full range of situations;
- Demonstration by inspection by human experts; it is based on the capability of human experts to correctly assess the satisfaction of a given claim; different types of inspection may be considered, e.g., informal re-reading, guided re-reading, critical design review and walkthrough; it may provide some level of confidence on aspects which are difficult to formalise and/or to prove formally, it is often highly subjective and difficult to repeat many times;
- Demonstration by development process; it does not deal directly with the item on which the claim is made, but with development processes and lifecycles, quality assurance and with methods, rules and tools; such types of evidence give confidence that the item and its future upgrades are produced in a coherent and controlled manner; as such, it gives confidence that the other results and measurements, performed as part of the justification, are valid; this type of demonstration is usually readily available and may constitute the first step of an assessment.

C.3.3 Optimised Safety justification strategy for OTSP-based SIS

The proposed safety justification strategy for OTSP-based SIS may be divided into two main phases:

- **The pre-qualification of the OTS product embedded in the system;**
- **The effective safety justification of the SIS.**

The purpose of the pre-qualification is to factorise, whenever possible, the justification effort regarding this product, so as to share the cost and to avoid unnecessary wastage of effort, to reduce uncertainties in system development and justification and to reduce the delays of system development and justification. It is proposed to organise the pre-qualification of an OTS product in two main activities:

- A **functional assessment**; the objective of the functional assessment of an OTS product is 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**; this is to provide evidence that the product behaves as specified, possibly according to dependability figures, to provide evidence that it complies with all relevant regulatory or standard safety requirements and to identify its possible failure modes.

The safety justification of the complete SIS still needs to be performed, even when all the OTS products it contains have been pre-qualified. This includes evidence that:

- The chosen OTS products match 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 conditions considered or recommended by its pre-qualification;
- In class A systems, the functions and parts of OTS products that are not strictly necessary to the system cannot affect its operation.

C.3.4 The functional assessments in renovation projects

For the cost effectiveness of the functional assessments, it is useful to make a distinction between project-independent and project-specific activities. Furthermore, the functional assessment for a given category of OTS products may be prepared independently of any specific OTS product, and then concretely adapted and applied to targeted OTS products. This reflection leads to the definition of four tasks, which are summarised in Figure 4.

In the first task, a generic functional model for each main category of OTS products is defined. Its goal is to answer as exhaustively and accurately as possible the following question: "What are the functions and services that are generally expected from this category of product?"

The objective of the second task is to provide a suitable description of the features of the OTS product that are considered for future projects. This description, for a given OTS product or category of OTS products, is organised according to the corresponding functional model established in the first task.

The third task formalises the user requirements of a specific project regarding each category of OTS products. These requirements are also organised according to the corresponding functional model.

Finally, the last task compares the results of the two preceding tasks, so as to decide, for a given project, which OTS product better fits the specified user requirements for a given category, possibly with specific conditions.

	PRODUCT INDEPENDENT	***PRODUCT DEPENDENT***
PROJECT INDEPENDENT	Task 1: Functional modelling, for each main category of OTS products	Task 2: Functional description of candidate OTS product
PROJECT SPECIFIC	Task 3: Specification of user requirements for each category of OTS products	Task 4: Matching of OTS products with corresponding user requirements specifications

Figure 4: The four tasks of functional assessment.

C.3.5 Dependability assessment of OTS products

A cost effective dependability assessment of an OTS product must usually take into account the key characteristics of the product and of the SIS in which it will be embedded. It is proposed to consider mainly:

- The safety class of the SIS in which the product will be embedded;
- The functional complexity of the OTS product;
- The availability of information regarding the development of the OTS product;

- The availability of information regarding experience in operation.

Not all combinations of characteristics are likely to be acceptable for safety application. Figure 5 indicates the combinations considered by CEMSIS. Dark cells indicate combinations that were not considered. These combinations are not necessarily forbidden, but if they occur, they will require a case by case approach. White cells are grouped and labelled according to possible assessment strategies.

<table>
<tr><td colspan="2">Availability of the 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="2"></td><td colspan="6">Experience in operation</td></tr>
<tr><td>Safety class</td><td>Functional complexity</td><td>No</td><td>Yes</td><td>No</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="4" rowspan="2"></td></tr>
<tr><td>Medium</td></tr>
<tr><td>Low</td><td colspan="2">A1 / A2</td><td></td><td colspan="2">A2</td><td rowspan="3"></td></tr>
<tr><td rowspan="3">Class B</td><td>High</td><td colspan="4">B1</td><td></td></tr>
<tr><td>Medium</td><td colspan="4" rowspan="2">B1 / B2</td><td>B2</td></tr>
<tr><td>Low</td><td>B2</td></tr>
</table>

Figure 5: Strategies for dependability assessments.

Caveat : Figure 5 presents the possibility to use black boxes for SIS of safety class A. In order to avoid unnecessary controversy, it may be necessary to emphasise that, for safety class A SIS, at least some information regarding internal design, implementation and development needs to be available and accessible on the embedded OTS products. Black boxes are meant in this document as source code black boxes.

C.3.6 Properties of OTS products

The CEMSIS strategy for a cost-effective safety justification is based on the pre-qualification of OTS products independently of projects. The properties of an OTS product that need to be claimed and justified during pre-qualification are those that can contribute to the safety justification of future SIS, and that can be justified independently of any specific renovation project.

The SIS properties that are essential to safety, and the justification of which may be facilitated by a pre-qualification of the OTS products are:

- The **characterisation** of the SIS;
- The **correctness** of the SIS with respect to its description;
- The **robustness** of the SIS with respect to postulated internal and external erroneous conditions.

The OTS product properties supporting the **characterisation** of the SIS are:

- The identification of the OTS product, so as to allow the complete identification of the SIS;

- The description of the OTS product, so as to facilitate the description of the SIS;
- The integrity of the OTS product, which is an integral part of the integrity of the SIS.

In addition, the identification and the description of an OTS product are necessary for the justification of its correctness.

The **correctness** of an OTS product, with respect to the services it provides for the SIS, is necessary to justify the correctness of the SIS. However, the argumentation of correctness of the OTS product will strongly depend on the information that is available regarding its internal design, its implementation, its development and its experience in operation.

In some cases, the **robustness** of the SIS is totally or nearly totally dependent on the robustness of the OTS product. In such cases, the sub-properties expected for the robustness of the SIS are also expected of the OTS product. In other cases, the robustness of the SIS is obtained by means that are external to the OTS product. In such cases, the robustness of the OTS product is not a necessity and may be replaced by the completeness of the characterisation of the failure modes of the OTS product, so that appropriate actions may be taken in the rest of the SIS. Appropriate actions aim to prevent a failure propagation that would lead to an overall SIS failure and shall guarantee that the OTSP failures will not lead to unsafe and not-specified SIS behaviours. In most cases, the robustness of the SIS will be based on the joint capabilities of the OTS product (e.g., detection of the failures of the OTS product) and of the rest of the SIS (e.g., signalling and containment).

C.3.7 Notion of OTS product criticality

Independently or not of the pre-qualification phase of the OTS products, the safety justification of SIS needs to provide proof elements on the dependability of the SIS. The dependability argumentation of SIS may rely on the dependability of its OTS products. However it is likely that SIS embed OTS products on which no conclusion on their level of dependability has been reached based only on what is known in advance of these OTS products. In such cases, and considering that it is the dependability of the SIS that needs to be justified, it may be worthwhile to consider the effective criticality of the OTS products within the SIS.

Moreover, it is likely that the low amount of information available on some types of OTS products may rationally lead the designers to adopt specific methods of integration so as to prevent the failures of these products. The safety justification may lean on these specific methods to justify the safe use of the OTS products.

Criticality may be defined as “the potentiality that the occurrence of an OTS product failure may have an adverse effect on safety”. In the three following sections, three levels of criticality are proposed.

- **Criticality C2**: An error in the OTS product may lead to an unsafe situation.

OTS products of criticality C2 are as critical as the SIS in which they are embedded. This is the highest level of criticality. It is by default the criticality level that is assumed for the OTS products when no claim on criticality is made for their justification.

- **Criticality C1**: An error in the OTS product can lead to an unsafe situation only if another error occurs in some other part of the SIS.

The notion of criticality C1 partly results from the principle of single failure criterion. Instead of requiring that the system must be capable of performing its task in the presence of any single failure, the idea is to take advantage of the design or architecture measures that may have been applied so as to ease the justification of OTS products for a given SIS. Here,

the overall objective is not the continuation of the system task but the guarantee to remain in safe situations.

The demonstration that OTS products have a C1 criticality level rely, in most cases, on the architecture or the design of SIS. It requires that clear measures have been specifically applied in the SIS either to prevent the failures of the OTS product at stake or to maintain a safe state in spite of the failures of the OTS product. Redundancy, diversity and wrapping are the three main usable principles to achieve these goals.

- **Criticality C0**: An error in the OTS product cannot lead to an unsafe situation.

This is the lowest level of criticality. With the implementation of new technologies and notably the use of pre-existing I&C platforms to design SIS, it is likely that some parts of the SIS do not participate in the safety functions. Moreover, some of these parts might actually have no adverse effect on any safety functions. However, the innocuousness of the non-critical parts on the critical ones needs to be justified. Three cases of OTS product of C0 criticality can be considered within a SIS:

- The product is completely separated from all the safety functions: justification mainly based on the architecture of the SIS;
- The product cannot influence any safety function: justification based on the properties of the management of resources shared between the OTS products and the rest of the SIS;
- The product cannot have adverse influence on any safety function: justification based on the defences implemented in the rest of the SIS so as to guarantee that the failures of the OTS products cannot jeopardise the correct operation of the safety functions.

The justification of the low criticality (C1 or C0) of an OTS product leads to assessment of the ways in which the product may jeopardise the correct operating of the safety functions. The OTS product may interact with the SIS and some other systems. Thus, the strategy may be decomposed in two sets of sub-claims:

- The claims on the interaction mechanisms between the component and the rest of the SIS;
- The claims on the interaction mechanisms between the component and the other systems of the plant.

Each interaction mechanism needs to be characterised so as to clearly identify the potential means of error propagation between the systems or the sub-systems. The second step of the criticality justification deals with the demonstration that correct provisions are applied according to the potential threats of error propagation.

C.4 Final Report on Case Studies

C.4.1 Introduction

The CEMSIS project has developed a methodology for refurbishment projects that consists of the following main components:

- A goal-based safety justification framework (section C.1.)
- A process for requirements engineering for refurbishment projects (section C.2.)
- A strategy for integration of COTS components into the architecture (section C.3.)

The goal of CEMSIS WP5 was to exercise the methodology by applying it to three case studies based on real refurbishment projects. It should be noted that at the time of performing the case studies the CEMSIS guidance was available only in draft form. Furthermore the limited time and resource available in a project of this nature inevitably restricted the areas of the guidance that were covered by the case studies.

C.4.2 Case Study 1 (WP5.2): A skip handler protection system

Case Study 1 took as its example a skip handler interlock protection system. Two skip handler machines transport and stack fuel containers within a spent fuel storage pond, the containers being stacked up to three deep. These machine activities are directed by a control system. A potentially dangerous failure could occur in the event of the machine's hoist exceeding the transport height - such an event might raise a fuel container above water level and expose operators to radiation. To guard against such an event, an independent protection system removes power from the hoisting circuitry in the event of an "over-raise". In reality the situation is more complex because two legitimate operations require the hoist to operate above its usual transport height. These operations are: transit of the skip handler machine into its maintenance bay when maintenance and repair of the machine are required, and transit of the skip handler machine across the area above a triple stack of fuel containers (the triple stack clearance is not as high as the clearance required for travel into the maintenance bay). In order to enable these operations to take place, two overrides are provided; both overrides are disabled by hardwired interlocks if the skip handling machine is carrying a fuel container.

Resource limitations precluded production within this case study of a full safety justification, and the justification guidance was exercised only on two top-level claims. Because this case study was based on a recently refurbished system, high-quality information was available relating to the requirements, specification, design and implementation of the existing system. The available information was more complete and correct than is often the case. In this respect Case Study 1 was perhaps not an entirely realistic test of the CEMSIS requirements capture and specification guidance.

Also the case study plan included use of a particular controller product specially developed for safety-related applications; this was a new product that was expected to be available within the case study time-scale. Unfortunately at the time of performing the case study the launch of the controller was delayed and it was still not available. Consequently the case study was not able to apply the COTS guidance as planned.

C.4.3 Case Study 2 (WP5.3): A platform for implementation of safety I&C systems

Case study 2 concentrated on consideration of the CEMSIS safety justification guidance as it relates to a COTS platform; the other aspects of CEMSIS were not addressed.

This case study applied the safety justification guidance of WP1 to pre-qualification (as proposed in WP3) of an off-the-shelf PES-based component. The chosen component, Teleperm XS, is designed and manufactured by Framatome ANP for use in safety applications and therefore is a suitable candidate platform for the implementation of safety-critical systems in the nuclear field.

The strategy of the case study was:

- Presentation of the operating principles of the PES-based platform;
- Identification of safety properties to be satisfied by such a platform;
- Application of the WP1 safety justification framework to one significant safety property chosen from those identified.

It was recognised that the requirements of national regulators may differ on some points. Therefore the case study strategy was applied separately by two end-user organisations that are answerable to different national regulators.

Certain selected claims were expanded and evidentially supported. The rôle of COTS platform supplier was played by Framatome ANP, who were very helpful with information

about platform design and development; such a level of helpfulness may not be typical of platform suppliers in general.

C.4.4 Case Study 3 (WP5.4): A reactor shutdown system

This case study took as its starting point a reactor protection system that has recently undergone refurbishment. The case study concentrated particularly on the Reactor Shutdown System, which is actuated by a signal from the protection system. The Reactor Shutdown System contains four redundant trains and actuates shutdown on a 2oo4 vote, by controlling and supervising the hydraulic valves and other components in order to drive the control rods into the core. It also performs two auxiliary functions: to drive in selected groups of control rods in the event of a partial shutdown, and to ensure minimum water and gas levels for the shutdown function and provide continuous flush flow for the control rod drives. The refurbishment project had already assembled legacy information detailing the environment and functions of the old shutdown system.

The study concentrated mainly on interactions between supplier and customer during the tendering and requirements gathering processes, a major theme of the WP2 guidance. The WP3 and WP4 guidance was covered by means of examples, and similarly it was only possible to demonstrate a small selection of tools.

A safety justification following the WP1 guidance was developed only at the requirements and architecture levels; sub-claims relating to detailed design and implementation were not identified or developed. The COTS aspects were investigated with Framatome ANP (a CEMSIS partner) acting as COTS supplier and Teleperm XS as the platform.

C.4.5 Summary and Conclusions

WP1 (justification): All of the case studies used the WP1 guidance to build justifications to differing levels of detail. Topics that were singled out for comment included the following.

- The concepts of claim and evidence were agreed to be essential for a sound and practical approach to safety justification. The case studies constructed claim hierarchies; in general the justifications were not supported by detailed evidence because of lack of time and resource, but a full application of the CEMSIS WP1 guidance would certainly require detailed evidence gathering.
- The concept of justification levels was recognised as a useful structuring and focusing device, although some users queried the restrictions that the guidance placed on the use of this concept.
- The detailed structure of the levels, and the way in which sub-justifications (for example, of a smart sensor) should fit into a main justification, presented difficulties for some users.
- Some users believed that the framework would benefit from a more flexible mechanism for recording arguments and their justification.
- Some practical difficulties were experienced in fitting in essential process requirements.
- The availability of a more comprehensive "user guide" would assist in adoption of the framework.

WP2 (requirements engineering): WP5.2 and WP5.4 both examined the WP2 recommendations on requirements elicitation, analysis, specification and negotiation. The CEMSIS approach was considered to work well. Some findings were as follows.

- The updating of a set of system records to render them correct, consistent and accessible is inevitably an expensive activity; its cost-effectiveness depends on factors such as the

expected lifetime of the system and whether further modernisation will take place in the future.

- Tool usage has the potential to assist with the requirements-gathering activity if the tools are carefully chosen and the organisation has prior experience of them.
- Tool usage should be mandated because tools would improve insight into the development processes and would facilitate demonstration and validation of the required functionality.
- However, some tools, e.g. DOORS might necessitate extensive reconfiguration of the documents.
- Such activities would probably only be worthwhile if the anticipated lifetime of the system was such that it would undergo more than one refurbishment before being scrapped.
- A specification format previously agreed with the vendor at the start of the requirements phase has the potential to save time and prevent misinterpretation. Diagrammatic presentation and animation are also helpful in facilitating understanding.

WP3 (COTS/PDS qualification): It was not possible to trial the recommendations of this work package to the extent that had been originally planned, but WP5.3 and WP5.4 performed some investigation of the topic; their findings supported the general CEMSIS approach and made some recommendations.

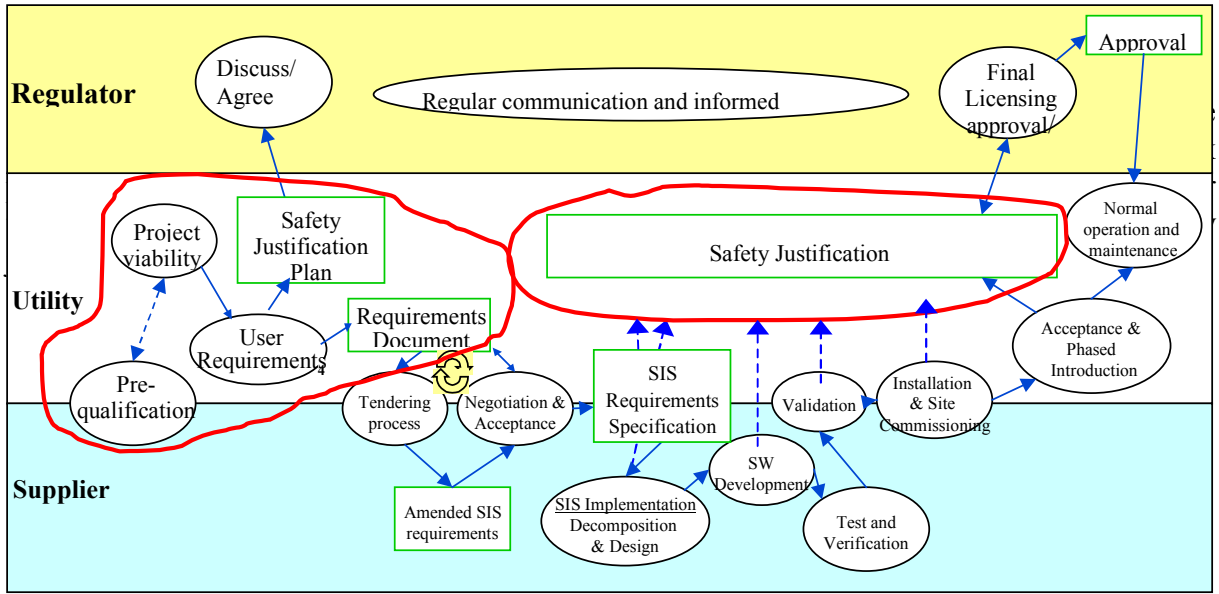
- Where the design of the proposed COTS item is not strictly in conformance with regulatory statements, a flexible justification approach considering the features of the COTS item may still result in a suitable argument.
- The pre-qualification approach to COTS items enables early identification of potential areas of justification difficulty.
- A change of procurement approach to target the identification and involvement of an appropriate partner supplier from the very start (rather than exact specification of COTS items) seems to offer real advantages in the procurement and commissioning of safety systems.

WP4 (graphical languages): This work package was touched on by case study WP5.4, which concluded that use of a graphical tool has some advantages for early validation of safety claims.

In conclusion, the CEMSIS guidance challenged the existing organisational approaches to refurbishment in a positive way and held out the possibility of a more methodical and cost-effective approach to projects of this nature.

As discussed earlier, the case studies were limited trials of some aspects of the CEMSIS guidance, based partly on role-playing situations. Further case-study work, perhaps exercising the full CEMSIS guidance directly on large projects, would be of interest.

C.5 Public Domain Case Study



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

- the utility
- the supplier
- the regulator

The example SIS replacement used to illustrate the CEMSIS guidance is the replacement of a control system for a nuclear materials handling system (MHS). Such systems are common in both nuclear power production and nuclear fuel reprocessing, so it provides a realistic (if simplified) example. Nuclear material, stored in cans, is transferred between processing units by a nuclear materials transporter as shown in Figure 7.

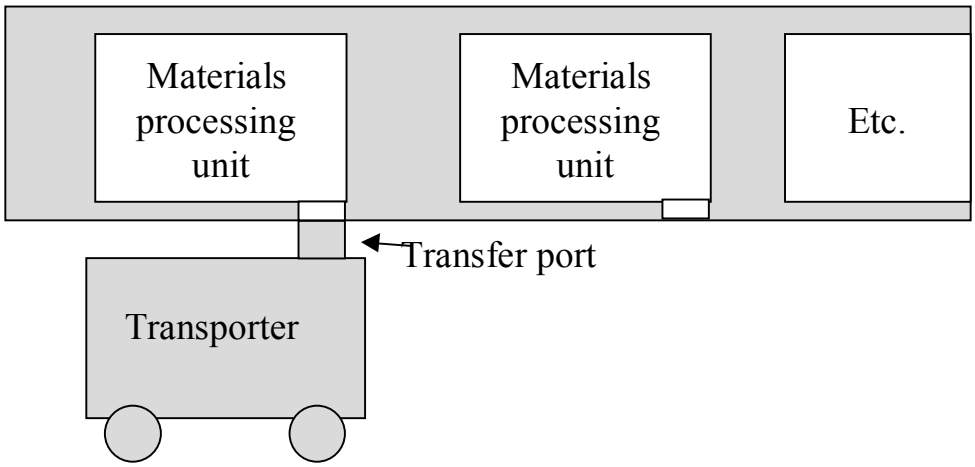


Figure 7: Materials Handling System

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 8).

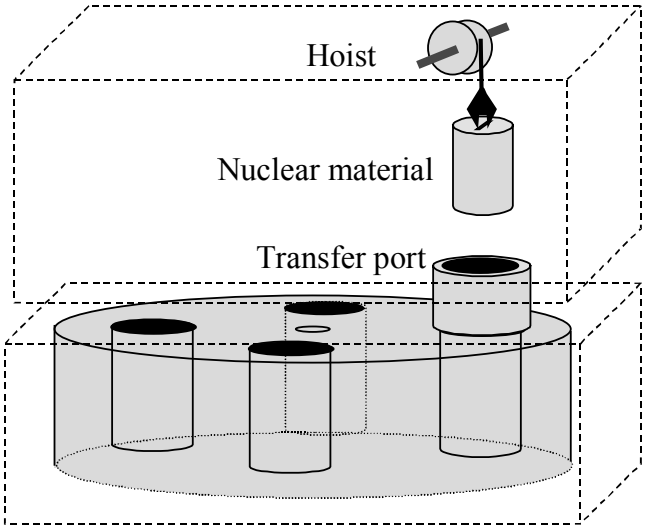


Figure 8: MHS grab and hoist

The carousel is a buffer store and is filled by rotating the carousel and transferring the material into successive chambers until the 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).

The existing SIS was implemented using relays and discrete electronic components, while the replacement SIS is a computer based on a commercial off the shelf (COTS) computer-based system. The various stages of the MHS replacement covered by the CEMSIS guidance are illustrated in the sections below.

C.5.2 Project viability

A key phase in the whole process is the viability of a SIS replacement, which can have a major impact on the cost of operation. This phase is described in more detail in D2.3 (see section C.2). The project viability study assesses:

- Whether a replacement is needed (e.g. due obsolescence, unsatisfactory performance, operational changes or changes in regulations)
- The costs involved in replacing the SIS (both in implementation and subsequent operation)
- The safety implications of a change
- The project risks (e.g. delays in implementation and licensing)
- Whether (and when) the system is replaced
- What implementation constraints are imposed (e.g. cost, system boundaries, choice of technology)

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 has to decide whether the replacement should proceed. 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. For the MHS example, a project viability report examined the issues itemised above and concluded that it would be cost effective to replace the current SIS. To minimise project risk a constraints were imposed

C.5.3 Requirements for the replacement system

Once the replacement decision has been made, it is necessary to prepare the requirements for tender. The requirements documentation has to include any constraints imposed in the project viability stage, such as preferred technologies/suppliers, budget and schedule constraint, but the bulk of the requirements are established in the user requirements phase. The CEMSIS guidance document, D2.3, defines a two-stage requirements capture process. Its application to the MHS SIS is described below.

C.5.3.1 Establishing the design basis (existing requirements)

The design basis established for the MHS gives illustrations of relevant documents that can be assembled. This includes general information about the materials processing plant, e.g.:

- Plant descriptions and schematics
- Plant operating and maintenance modes

and information about the MHS control systems, e.g.:

- Safety claims made on the MHS SIS
- MHS Interface drawings
- MHS Operating procedures
- MHS Maintenance procedures

- MHS Functional requirements
- MHS dependability requirements (such as the probability of failure on demand, spurious actuation rate and availability)
- Physical constraints (e.g. space, weight, power limits)
- Environment constraints (e.g. temperature, humidity, EMI, etc)

The process of validating the design basis data is also illustrated for the MHS, e.g. by checking the consistency between documents and drawings, and by comparing the logic drawings with the actual implementation.

C.5.3.2 Identification of new requirements

While the data gathering and validation of the design basis provides a solid basis for the existing system, it may not be sufficient for the replacement system. New requirements for the SIS replacement might be needed to address:

- satisfy new regulations
- rectify safety and operational problems encountered with the current SIS
- support changes in maintenance practices
- support changes in operational practice
- interoperate with other systems

These needs might be addressed by including requirements for:

- new functionality
- revised dependability targets (availability, reliability)
- support infrastructure (e.g. documentation and tools)
- security requirements

These changes have to be combined with the design basis documents to produce a consistent and correct specification for the replacement system.

In addition it is necessary to identify any constraints on the implementation of the replacement, such as:

- requirements to identify and provide the evidence to support the safety justification of the delivered system
- restrictions on permitted technology (e.g. whether discrete logic or a computer system can be used)
- compliance to specific design and implementation practices (e.g. company design safety rules, IEC 61508 or IEC 60880)
- transition requirements, e.g. the need to run the new and legacy systems in parallel for a limited period of time
- installation and commissioning constraints (e.g. delivery dates, limits on installation and commissioning time)

Following this process for the MHS, a number of changes are identified including:

- Removal of self-test logic (only relevant to the old logic technology).
- Addition of operator warning indicators (rotation direction indicators and end-stop warnings).
- Additional of diagnostics (to implement overrides that previously needed physical rewiring).
- Inclusion of a barcode reader to identify the drums in the carousel (a new plant-wide administrative requirement).

In addition the following constraints were imposed.

- Compliance of the development process and hardware to IEC 61508 SIL2 for the computer-based replacement control function (but excluding the barcode reader).
- Compliance to company design safety rules

C.5.3.3 Safety Justification

The modernisation process includes the preparation of an initial safety justification plan. This will be supplemented with more detailed plan after the tender phase that include safety justification work of the chosen supplier.

The plan for developing a safety justification has to:

- Define the structure and evolution of the safety justification
- Decide on regulator interface
- Define who does what (regulator, supplier, utility)

The plan for safety case construction will vary with the type of project and the level of involvement of the regulator. In the MHS example, an evolutionary approach is followed where the justification is developed in stages, and the evidence requirements for the justification are identified at an early stage. The justification plan includes scheduled interactions with the regulator during the project.

The MHS safety justification follows the approach developed in D1.1, with a set of claims supported either by direct evidence or by sub-claims. In the MHS example, an evolutionary safety justification approach is used where a series of top level claims are made and expanded into sub-claims and evidence as the implementation progresses:

- The SIS requirements are valid
- The SIS implementation satisfies the requirements
- The SIS can be operated and maintained safely throughout the planned lifetime

Evidence for the first claim comes from the utility, and involves evidence about unsafe states of the plant and the adequacy of the specified SIS functionality to maintain safety. These claims can be made prior to tendering and would be open to review by the regulator.

The justification for the second claim requires evidence about the SIS implementation from the SIS supplier (dubbed MicroSafe Corp in this example). The claims and sub-claims about correct implementation are assisted by *COTS pre-qualification* evidence (see the recommendations in D3.3). In the MHS example, the pre-qualification of a fail-safe PLC (dubbed the MSPGC 500 Safety PLC) makes a specific set of claims about its functionality and dependability properties, and these claims are assumed to be already accepted by some authoritative body. This pre-qualification evidence is used in constructing the safety justification for the MHS SIS as a whole. For example, a claim of compliance to an MHS response time of 100msec is supported by evidence that the MSPGC 500 PLC has a predictable maximum response time for a given configuration of application software. Similarly a claim that “the functional behaviour of the MHS SIS is correct” is supported by pre-qualification evidence that the MSPGC 500 logic functions and the logic network compiler are correct. The safety justification of a SIS can also be facilitated by designing an architecture that reduces the safety criticality of COTS components (as recommended in D3.4). The architecture chosen for the MHS SIS illustrates this strategy, as shown in Figure 9. Note that the shaded boxes represent pre-existing equipment. The unshaded boxes represent the replacement system.

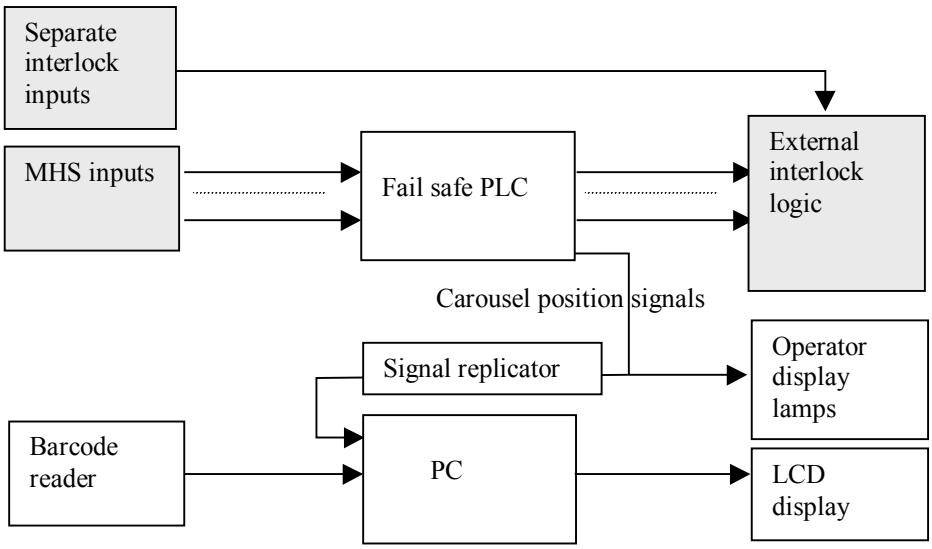


Figure 9: Architecture for the MHS SIS

The safety criticality of the MHS carousel control logic was reduced at the project viability stage by the use of independent relay-based safety interlocks on carousel movement. In addition, the MHS SIS functionality was implemented using two separate systems: MSPGC 500 for carousel control, and a standard PC for the barcode reading system. Barcode data is not safety-related, so the function can be implemented on a low integrity PC. As the PC takes data from the MSPGC 500, the signals are electrically isolated to prevent interference with the carousel control.

The justification of the final claim "the SIS can be operated and maintained safely throughout the planned lifetime", required evidence from both the supplier and the utility. The supplier had to show that the MSPGC 500 has adequate design features to support operation and diagnosis and repair, and that there is an adequate supplier support infrastructure over its lifetime (including facilities for safe modification of the MHS SIS functionality). Evidence for these claims were requested at the tender stage, as this was an important factor in the choice of an appropriate SIS. From the utility side, evidence was required to show that the site infrastructure (e.g. staff levels, training and procedures) is sufficient for safe operation and maintenance. Much of the evidence to support this part are only likely to became available towards the end of the project when there is more information on the MHS SIS implementation. However the claims and the type of evidence were identified at the beginning of the project to ensure that the infrastructure could be justified as capable of maintaining safety.

In addition to these claims about the behaviour of the system, there is a separate justification for the *integrity* of the safety justification evidence itself, i.e.

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

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

C.5.4 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 risk of late and costly "surprises", and late changes).
- A structured approach to the construction of the safety justification (which reduces the risk of costly licensing delays by agreeing the key claims and evidence requirements at an early stage and including the evidence requirements in the supplier contract).
- A systematic approach to the pre-qualification of COTS components (reduces the risk that evidence is delayed or unsuitable).
- Architectural design strategies for reducing the safety criticality of COTS components.

C.6 Public Workshop

C.6.1 Post-FISA-2003 Workshop

A workshop entitled "Safe and Cost Effective Modernisation of Programmable Systems" and subtitled "Increasing safety and reducing project risk of using computer based systems" was held in association with FISA-2003 in Luxembourg on November 13th 2003.

The objectives of this workshop were:

- To present an overview of the results, and deliverables, of two framework V projects in this context:
  - Cost Effective Modernisation of Systems Important to Safety (CEMSIS)
  - Benchmark Exercise on Safety Evaluation of Computer Based Systems (BE-SECBS)
- To review the safety justification practices for programmable systems in other industrial sectors
- To stimulate debate on future safety justification practices in the European Union
- To consider the options for further progress in this field including the EC Framework VI programme

The workshop was attended by about forty participants and was in four sessions starting with 'CEMSIS summary and achievements' and 'BE-SECBS overview and achievements'. 'Practices in other sectors' was presented by invited speakers from outside the Nuclear industry, and finally 'Current and emerging issues' gave an opportunity for any participant to present their views on the subject, and identify issues that need further work. The presentations are described briefly below, and the slides accompanying the original presentations are available at www.cemsis.org.

The first session covered "CEMSIS Summary and Achievements" with the following presentations:

- "CEMSIS Best Practice, illustrated by an industrial-based example" (Robin Bloomfield, Adelard) gave a project overview and described the public domain example (see section C.5 of this report)
- "Safety Justification Framework – key issues" (Pierre-Jacques Courtois, AVN) covered the subject of section C.1 of this report
- "Pre-Developed Software – key issues" (Thuy Nguyen, EDF and EPRI) covered the subject of section C.3 of this report

The second session addressed "BE-SECBS Overview and achievements" as follows:

- "Overview of the project (objectives and achievements)" (Vytis Kopustinskas, JRC)
- The IRSN assessment approach and its application (Pascal Regnier, IRSN)

- The ISTec assessment approach and its application (Josef Märtz, ISTec)
- The VTT-STUK assessment approach and its application (Urho Pulkinnen, VTT-STUK)

The BE-SECBS consortium consisted of an industrial partner (FANP), providing the reference study case, three assessor teams (IRSN, ISTec and VTT/STUK) and the project co-ordinator JRC-IE, which apart from general co-ordination performed the comparison study.

The project's primary target is a comparative evaluation of existing safety critical computer based systems assessment methodologies in use in the nuclear field among regulators and technical support organisations in EU Member States. Framatome ANP provided a reference case study of a hypothetical reactor protection system, including the requirements and functional specification of a limited number of safety functions that were selected by the project partners. Each assessor applied its specific assessment methodology to the reference case study. The comparison study was performed in order to highlight the current practices and methods used in the field by major research and regulatory support organisations.

The third session covered some related "Practices in other sectors" with two presentations from invited speakers in the transport industries:

- Software Aspects of Certification in the Aerospace Sector (Gérard Ladier, Airbus). A number of questions about application of the sector standard DO-178 were addressed including cost of application, use of COTS, and replacement of test by proof. For the future there are signs that a more 'product based', rather than 'development process based' assessment may become possible.
- Experience with goal based regulation in air traffic services (Andrew Eaton, CAA). Andrew Eaton represents the UK Civil Aviation Authority. He outlined some experiences from introducing goal-based safety regulation for Air Traffic Services. The move from prescriptive standards-based regulation to a goal based approach was driven by the Robens and Pipa Alpha reports in order to be more complete, consistent and responsive to new technology.

The fourth and final session gave the opportunity for Position Statements from workshop participants on "Current and emerging issues"

- Gustav Dahll (Halden Reactor Project, Norway) outlined some current Halden research areas in software dependability
- Rob Stockham (Moore Ind., UK) explained that manufacturers who hold 'Accredited Certification' for their Functional Safety Management can offer much more comprehensive and 'open' safety related information about their products.
- Arian Slagt (Yokogawa SCE) gave an overview of the Yokogawa activities related to the nuclear industry. He stressed the importance of clear and un-ambiguous procedures that are accepted by all parties in all European countries
- Björn Wahlström (VTT) described the I&C activities of IAEA, concentrated in the Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI).
- Ivan Ivanov (TU Sofia) described the Bulgarian interest in this field as the need to transfer good new knowledge and advanced EU experience for practical uses in order to support sustainable and safe long term operation of the NPP
- Freddy Seidel (BfS) gave an overview on recent research projects, which the German Federal Office for Radiation Protection has initiated in the field of safety I&C qualification and justification.
- Paul Tooley (BE) outlined the ongoing UK research programme controlled by the C&I Nuclear Industry Forum. Current topics include safety demonstration of SMART

instruments, use of PC technology for low SIL applications, and the application of formal methods to hardware based safety equipment design.

- Thuy Nguyen (EDF and EPRI) spoke on the Development of Guidance by, for example, IEC and EPRI. A claim-based, rather than rule-based, approach to safety justification may be particularly useful where unanticipated or new issues are involved, such as in the EPRI RID3 project.
- Pierre-Jacques Courtois (AVN) outlined the work of the NRWG Task Force on Critical Software Licensing. The Task Force was set up in 1994 and a major milestone was the publication in May 2000 of the consensus report: "Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors" (ref.[3])

The workshop concluded with remarks from Pierre-Jacques Courtois. We have reviewed two framework V projects that complement each other well, revealing commonalities in assessment approaches in Europe, and building on advances in provision of evidence and construction of safety cases. We have learned a great deal from each other, and many thanks are due to the EC.

Safety justification remains a complex problem, and the workshop discussions noted issues that require further efforts including: how to 'scale-up' the results, how to identify 'sufficient' V&V, how much the regulator should guide the licensee, the role of 'type testing' and a 'plug and play' approach, and the use of goal based rather than prescriptive safety justification. We need to keep working away at these concerns.

Finally Panagiotis Manolatos, CEC, outlined the Euratom 6th Framework Programme, which is being considered as a vehicle for continuing to develop international collaboration in this field.

CONCLUSION

Refurbishment of Nuclear Power Plant Instrumentation and Control is being actively pursued in many EU member states, and the CEMSIS consortium has addressed several important and difficult issues in this field. The deliverables provide guidance that has been the result of long consideration, debate and refinement by experts and practitioners representing the main stakeholders:

- Nuclear Power Plant operators
- Safety Regulators, and
- I&C Suppliers

Substantial guidance reports have been produced that offer detailed advice to those involved in I&C refurbishment projects, and as a basis for continuing improvement of modernisation practice. We consider that the project has met its goals and the results will be of practical benefit to the nuclear industry. The results are in the form of guidance documents illustrated by realistic examples that can be easily related to practical refurbishment situations.

The main features of the guidance developed by the project are:

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

The key audiences for the CEMSIS results are:

- I&C engineers with responsibility for developing and implementing refurbishment projects
- Managers of these projects wishing to understand the issues and solutions
- Product development managers within the supply industry wishing to understand how to orient their product to the nuclear market through a better understanding of utility and regulator requirements
- Development engineers within the supply industry wishing to understand the technical approach in the utilities
- Small and medium size enterprises (SMEs) and other service companies wishing to participate in the refurbishment market
- Regulators, safety software assessors and policy makers wishing to develop an approach to licensing computer based systems important to safety, including systems which make use of off-the-shelf components
- Standards bodies and committees charged with providing authoritative and effective requirements and guidance for the implementation of Systems Important to Safety

The project public deliverables are available on the project web-site: www.cemsis.org.

Increased harmonisation of regulatory practice across Europe faces many obstacles and understandable concern, but has significant potential benefits. CEMSIS has stimulated European co-operation, and highlighted many areas of common interest for EU member states. The EC plays an important role in maintaining progress in this direction by support of research and collaboration. In particular the following opportunities to encourage further progress are commended:

- Continued support of the ongoing activities of the European Nuclear Regulators Working Group Task Force on Critical Software Licensing
- Inclusion in the Framework VI programme of an activity on Safety, Efficiency and Reliability of Modernisation of nuclear power plant Instrumentation & Control, in order to define common best practices for safe, reliable, efficient and cost-effective modernised I&C, with supporting methods, tools and guidelines

REFERENCES

[1] "Four Party Regulatory Consensus Report on The Safety Case for Computer-Based Systems in Nuclear Power Plants" AECB Canada, DSIN/IPSN France, NII UK, USNRC USA

[2] Fundamental Safety Rule II.4.1.A on Software for Safety Systems, DSIN/IPSN, France

[3] Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors. European Commission Report EUR 19265 EN, May 2000. ISBN 92_828_8178_4, 2000-IV, 81pp.

[4] "Justifying the use of Software of Uncertain Pedigree (SOUP) in Safety-Related Applications" CRR336 HSE Books 2001 ISBN 0 7176 2010 7

[5] "The use of Computers in Safety-Critical Applications", Final report of the study group on the safety of operational computer systems, HSE Books 1998 ISBN 0 7176 1620 7

[6] Semantic Structures and Logic Properties of Computer-Based System Dependability Cases." P.J. Courtois, Nuclear Engineering and Design 203 (2001) 87-106

[7] Finkelstein and I. Sommerville. The Viewpoints FAQ. Software Engineering Journal, 11, 1, 1996.

[8] Ian Sommerville and Pete Sawyer. Requirements Engineering: a good practice guide. Wiley, 1997.

[9] P.G.Bishop and M.J.P. van der Meulen, *CEMSIS public domain case study,* CEMSIS report no. wp5-ade039 (2004), available on www.cemsis.org

[10] D. Pavey, R. Bloomfield, P-J. Courtois, P. Caspall-Askew, T. Nguyen, H-W. Bock, J. Tuszynski, B. Ekdahl, "Cost Effective Modernisation of Systems Important to Safety", FISA-2003, EU research in reactor safety, 10-13. Nov. 2003, Luxembourg