Environment Project FIS5-1999-00355

CEMSIS:
Cost Effective Modernisation of Systems Important to Safety

D5.5 Final Report on Case Studies

V3.0

Editor

L.A.Winsborrow, British Energy Generation Ltd

Revisions

v0.1	Partial draft for informal BE comment	20/11/03
v0.2	Full draft for BE comment	8/12/03
v0.3	Draft for consortium comment	10/12/03
v1.0	First formal issue for consideration by consortium partners. First round of consortium comments addressed.	15/12/03
v1.1	Second round of consortium comments (from December 2003 Brussels meeting) addressed and issued for BE comment.	07/01/04
v2.0	Second formal issue for consideration by consortium partners. BE comments addressed.	07/01/04
v2.1	Third round of consortium comments addressed.	27/01/04
V3.0	Final version	19/02/04

Circulation

Unrestricted

Contents

1. Introduction 4
2. Abbreviations 4
3. Summary of Case Studies 5
3.1 Case Study 1 (WP5.2): A skip handler protection system 5
3.1.1 Coverage and limitations of WP5.2 case study 5
3.1.2 Activities performed for WP5.2 case study 5
3.1.3 Findings of WP5.2 case study 7
3.2 Case Study 2 (WP5.3): A platform for implementation of safety I&C systems 8
3.2.1 Coverage and limitations of WP5.3 case study 8
3.2.2 Activities performed for WP5.3 case study 9
3.2.3 Findings of WP5.3 case study 10
3.3 Case Study 3 (WP5.4): A reactor shutdown system 11
3.3.1 Coverage and limitations of WP5.4 case study 11
3.3.2 Activities performed for WP5.4 case study 12
3.3.3 Findings of WP5.4 case study 13
4. Summary and Conclusions 14
5. References 15

1. Introduction

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

- A pragmatic (goal-based) cost-effective safety justification framework that
  - elicits and organises disparate claims and evidence;
  - permits modularity and the reuse of elements of existing safety cases;
  - deals with system models at different levels (plant, architecture, design, operation).
- A process for performing the requirements engineering for plant refurbishment projects that
  - Is oriented towards modernisation of existing plant;
  - Takes a claim-based view with links to the safety justification framework;
  - Provides for a complete set of stakeholder viewpoints.
- A strategy for the integration of commercial off-the-shelf components into the architecture, structured as
  - Two assessment phases, pre-qualification (providing in advance the evidence for justification of a COTS item in a range of applications) and application qualification (providing the evidence specific to a given application);
  - Two types of assessment, functional and dependability, together providing the evidence that the product has the necessary features to perform the required safety functions and that it is sufficiently reliable to perform functions of the required safety class.

(Further details may be found in Ref.1).

The goal of CEMSIS Task 5 was to exercise the methodology by applying it to three case studies based on real refurbishment projects. This report constitutes the final deliverable D5.5 of Task 5 of CEMSIS. Firstly, the report describes each case study and summarises its findings; finally it considers the implications of the case study findings for the CEMSIS methodology. 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.

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 (Ref.2) 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.2.

2. Abbreviations

COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
FSR	Fundamental Safety Rule (France)
GUI	Graphical User Interface
HAZAN	HAZard ANalysis
HAZOP	HAZard and OPerability Study
I&C	Instrumentation and Control

PDS	Pre-Developed Software
PES	Programmable Electronic System
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.

Microsoft® Excel is a product of Microsoft Corporation.

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®.

Teleperm™ XS is a product of Framatome ANP.

3. Summary of Case Studies

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

3.1.1 Coverage and limitations of WP5.2 case study

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.

3.1.2 Activities performed for WP5.2 case study

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.

A HAZOP process had identified several hazards arising from the functional demands upon the plant, and the original (legacy) system had incorporated both automatic protection systems and measures alerting the operator in order to address these hazards and prevent a failure. The load over-raise hazards are protected

against by interlocks, by an overload registered at the hoist's retractable mast, and by gamma radiation monitors and alarms at various points on the skip handling machine.

The original (legacy) skip handler protection system had been replaced in the recent past by a new system that employed traditional (hardware-only) technology. Traditional technology was employed to ensure a smooth safety justification process and to reduce the probability of a systematic failure.

The CEMSIS case study was to focus on the skip handler over-raise protection function of the protection system (a system important to safety). The study would propose a PES-based solution employing a COTS item.

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 actual plant refurbishment had recently been performed, and in addition a safety case for continued plant operation had recently been produced, so the documents were in good order). This was the best situation that could be expected; a more common starting position might be the unavailability of information or personnel. In addition, a PES had been identified that would form the basis of the CEMSIS notional refurbishment, and information was gathered about the architecture and certification of the proposed PES.

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 case study focussed on two top-level claims:

- The skip handling machine shall not over-raise a fuel container above the transport height under normal operating conditions;
- The identified requirements are adequate for implementation of the refurbishment.

A claim/sub-claim structure was drawn up, using the ASCE safety case engineering tool and attempting to follow the tenets of CEMSIS WP1.

The WP2 recommendations were followed in a requirements engineering process; the following description indicates in parentheses the mappings to the CEMSIS recommendations. As indicated above, the plant documentation had recently been revisited, so there were no problems of poorly maintained documentation or missing requirements. A desktop exercise (existing requirements discovery) was performed to identify safety functions, their importance, and the associated systems, structures and components that supported them. It was concluded that a complete set of legacy system requirements was available. Formal meetings were then held with the client and the vendor in order to elicit any new requirements for a PES-based replacement system (new requirements discovery). Using the checklist proposed in the WP2 guidance for possible sources of new requirements, new requirements were identified, arising from

- IEC 61508 SIL 1 (Ref.3);
- New technology;
- Operational needs (GUI);
- Necessity to run the new system in parallel with the legacy system for a while;
- Availability;
- Reliability;
- Human factors (company guidelines);
- User requirements checklists;
- Operation and maintenance.

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 and fault trees generated.

Detailed specification of user requirements (new requirements analysis and negotiation) was then performed. The requirements specification was extended and modified to include both old and new requirements. A meeting was then held with the vendor at which a common requirements notation of text and diagrams was agreed. In addition it was agreed that the protection system logic would be modelled in LabVIEW, providing a plant simulator against which the new system could be tested as well as an executable model of the legacy protection system. A requirements specification was produced (requirements definition) and examined for completeness against a checklist. Further meetings were held between the plant and system engineers and the vendor to analyse and agree on the final content of the requirements specification (requirements negotiation).

It had been intended that the fourth case study task would be the integration of a pre-determined COTS product (that was to be certified under IEC 61508 within the case study schedule) into a protection system architecture generated from the detailed specification produced using the CEMSIS guidelines. Unfortunately the IEC 61508-certified COTS product was not available within the timescale and therefore it was not possible to exercise the recommendations of WP3.

3.1.3 Findings of WP5.2 case study

WP1 (justification): Some practical difficulties were experienced in the design of a claim structure to fit the CEMSIS WP1 framework. It was not clear where process requirements such as verification activities, functional safety management, roles and competency, audits, functional safety assessment and configuration management should be placed. Decommissioning is sometimes an important lifecycle phase and it was not clear where this would fit either.

The use of the conjunction node in the ASCE tool was invaluable in permitting some organisation and refinement of claims. However, the ability to use an argument node containing text would have made the safety case more informative and less ambiguous.

Application of the framework seems to require safety case engineering skills that a plant engineer would typically not possess. The CEMSIS safety justification guidance could be more user-friendly - the theory behind the framework could be hived off into a separate document. Some of the rules could be less rigid, or perhaps their application could be dependent on the target integrity of the justified system.

The reuse of existing evidence from HAZOP and HAZAN, with text wrappers containing limited reassessments and clearly indicating arguments relating to identifiable claims, was considered to be a focussed and cost-effective technique.

WP2 (requirements engineering): This case study performed a comprehensive trial of the CEMSIS Work Package 2 recommendations, split into several phases.

A highly desirable principle is that a set of adequate system records should be officially kept in a known, retrievable location to help with future maintenance. Such information would include operation, maintenance, project delivery and safety as well as technical design and would need to be approved by a number of people outside the immediate project.

Once documents have been reviewed, further updating may be required to eliminate gaps, contradictions or mismatches. A decision to invest effort in the performance of such an updating exercise, as well as its timing, would depend upon plant lifetime, technology change, and requirements for safety case support. The expense of such an activity may even affect the commercial viability of plant operation or refurbishment.

The following techniques (in which the company has expertise) were used to support requirements elicitation:

HAZOP
HAZAN
Design Basis Accident Analysis
Probabilistic Safety Analysis
Fault Tree Analysis

Fault Hazard Analysis
Brainstorming
Checklists
Data Mining
Interview
Formal Review

These techniques worked well together. Their suitability for the task in hand, and the organisation's familiarity with them were considered to be the primary reasons for employing them.

In order to obtain input from the operators, a focus group was held, facilitated by the engineer. In order for this to be totally successful the engineer would need to be independent of the project.

The DOORS tool, which had been recommended for use in other parts of CEMSIS, was initially used by the case study to provide requirements management and traceability, but was subsequently discarded for the following reasons.

Inputting of legacy documents was time-consuming. Such documents needed extensive reconfiguration for use in DOORS, and if this was not done then the traceability feature of DOORS could not be used. Ideally the documents should be written in DOORS from the outset in order to receive maximum benefit from the tool capabilities.

DOORS cannot give traceability within a logic diagram but can only point to the diagram as a whole. Therefore documents making extensive use of logic diagrams are not well handled by DOORS.

In general it is desirable for an organisation to use consistently in all refurbishments an agreed set of complementary techniques. The setting up of a requirements database would be useful and cost-effective if most requirements were defined textually and at least one more refurbishment was considered likely in the future.

It was found that time could be saved and scope for misinterpretation cut down if a specification format was agreed with the vendor at the start of this phase. Unique identification of requirements for traceability was found to be essential, as was formal review with stakeholders to agree the final document.

Diagrammatic presentation and requirements animation were helpful to the vendor in understanding the fault sequences. Requirements checklists and a requirements specification checklist ensured full consideration of all aspects of the system. Configuration management from the start was essential to establish and maintain the lifetime quality records.

General findings: As indicated above, the application of the CEMSIS justification framework was the most contentious area within this case study. It was perceived as a considerable change from the organisation's current safety justification methodology (which is heavily geared to current understandings with the national regulator).

The requirements capture aspects of CEMSIS mapped well onto the organisation's existing techniques and this part of the case study went smoothly.

As noted previously, the case study could not be completed as intended because of lack of availability of the identified PES off-the-shelf component.

Also the intended cost comparison of the case study with the actual plant refurbishment could not be performed because the full plant refurbishment was put "on hold" and the real costs are therefore not known as yet.

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

3.2.1 Coverage and limitations of WP5.3 case study

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.

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.

3.2.2 Activities performed for WP5.3 case study

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.

Under the confidentiality arrangements of CEMSIS the manufacturer made available a considerable amount of information regarding the architecture of the platform. Hence the assessors had access to more information than would normally be available to end-users. The underlying principle of operation is as follows. On CPU start-up, an initialisation routine is executed and comprehensive self-tests are performed. If the results of the self-tests are satisfactory, the CPU is switched to its normal status and commences cyclic operation. The engineered cycle time is controlled by the internal system clock, which provides an interrupt every millisecond giving a basis for software timings. Each processing cycle consists of eight phases controlled by the runtime environment, to which are assigned the following processing activities (covering all activities for cyclic input, processing and output of the application-specific data in a single loop).

- Read input messages;
- Check input messages;
- Process the application input function;
- Process the individual application computation functions;
- Process the application output function;
- Prepare output messages;
- Write output messages;
- Self-test and service tasks.

The response time of an integrated I&C system based on this platform depends on the engineered cycle time of the individual processors (t_c > 10ms), any engineered time delays in the application algorithm, and the number of subsequent processing lines. The shortest possible response time is the processor board cycle time multiplied by a factor depending on the system architecture. Deterministic best- and worst-case limits for system response time exist. This behaviour is mainly determined by the absence of co-ordination of the sub-systems, which ensures robustness against common cause failure.

3.2.2.1 French Fundamental Safety Rule

The Fundamental Safety Rule (issued by the Institut de Radioprotection et de Sûreté Nucléaire in 1999) presents the French technical regulatory practice for safety systems software in nuclear installations. The Rule states that software in Class E1 systems must satisfy the determinism principle. The FSR states that an acceptable practice would be to make no use of interrupts, keep the number of iterations in a calculation constant, and employ only static memory allocation.

The off-the-shelf platform considered by the case study makes restricted use of interrupts and therefore its architecture is not in conformity with the determinism principle's statement of acceptable practice. However, the Fundamental Safety Rule also states that there is no obligation to comply if it can be demonstrated that the safety objectives of the rule are achieved by other means, proposed within the framework of regulatory procedures. Therefore Framatome ANP and the French end-user worked together to construct an alternative justification strategy to demonstrate compliance with the determinism principle.

A top-level claim was adopted as the goal of a justification:

The interrupt mechanisms implemented in the platform for processing safety functions in a CPU are compatible with the determinism principle.

The top-level claim was decomposed into a series of six sub-claims using the CEMSIS WP1 approach:

1. All sources of possible interrupts in the CPU are identified and documented.
2. The effects of the interrupts on the software are known.
3. The priority of the interrupts is known.
4. The effects of nested interrupts are analysed for all relevant cases.
5. The initialisation of the interrupts is known.
6. Correct interrupt processing cannot be jeopardised by the operation of the self-test tasks.

All of the above sub-claims were supported by detailed design information.

3.2.2.2 Timeliness claim

The second part of case study WP5.3 was performed jointly by the platform manufacturer and the U.K. end-user. The end-user studied the available information about the UK regulatory approach to safety software and identified nine main regulatory requirements. From the list, one requirement was chosen that was considered to present a suitable exercise for the WP1 guidance but that also fitted well with the first part of WP5.3:

The specified set of time margins (within which the safety functions are to be performed) is achievable by the proposed software/hardware architecture.

The justification strategy was divided into two parts:

a pre-qualification case for predictability of platform response time;

an argument for a typical application, invoking the above argument, to justify the claim that there is a required set of time margins within which the safety functions will be performed.

Using the detailed design information provided by the manufacturer, the end-user drew up expansions of the two claims following the WP1 guidance and using the ASCE safety case tool. The sub-claims were evidentially supported (for the pre-qualification case by references to the manufacturer's documentation and for the hypothetical application by statements of what evidence would be required).

3.2.3 Findings of WP5.3 case study

CEMSIS WP3 proposes two changes to existing practice regarding safety justification of systems important to safety based on off-the-shelf products:

1. The justification should demonstrate that the System Important to Safety (SIS) satisfies properties essential to safety. Assessment against a set of rules may require unnecessary effort and may not demonstrate that the proposed system has the required safety properties. WP3 proposes that the properties essential for safety should be identified and satisfaction of these properties should be confirmed by a structured argumentation.
2. A pre-qualification of an off-the-shelf product should be performed that assesses, independently and prior to any modernisation project, that the product has intrinsic qualities rendering it suitable for use in a SIS.

The examination of Teleperm XS for conformity with the French Fundamental Safety Rule revealed that there was a discrepancy between the design of the platform and the FSR's "acceptable practice" statement. Nevertheless it was argued that the use of interrupts in Teleperm XS does not clash with the determinism principle. The argument employed a flexible justification approach and took into account the features of the off-the-shelf product. This finding is in accord with the WP3 approach.

Although a full pre-qualification could not be performed within the resource limitations of CEMSIS, the French justification exercise confirmed that pre-qualification factorises the justification in a practical manner. The case study revealed information about the internal functioning of the platform that would be needed when selecting candidate platforms for use in future renovation projects. It also enabled early identification and addressing of potential justification difficulties for a system based on the platform.

The UK "timeliness" exercise confirmed that it is practical and effective to take a typical claim based on UK practice and to construct a safety argument using the WP1 claims-argument-evidence structure.

The UK study also confirmed that it is practical and effective to construct a "pre-qualification argument, as proposed in WP3, for a part of the overall argument that is common to all systems based on a pre-existing platform. It would then be possible to re-use this argument cost-effectively for all safety systems based on the given platform.

The UK study had some specific findings regarding the WP1 framework.

- It would be helpful to have a recognised way of 'aggregating' claims within a level to improve readability.
- Breaking the overall safety case into 'sub-arguments' for claims on subsystems is a useful structuring facility even where the subsystem is not pre-existing or off-the-shelf.
- The WP1 naming convention works well once the argument is constrained to the four levels.
- Safety case maintainability needs consideration. If information is copied from source documents then maintaining consistency following revisions would be difficult; on the other hand relying on references to source documents could result in loss of supporting evidence when documents are updated.
- It would be helpful to record the rationale for necessity and sufficiency of sub-claims and evidence. The ASCE 'argument' box seems ideal, but this would not be consistent with the usage of 'argument' in the WP1 framework. (The ASCE tool permits the display in the 'argument box' of any combination of sub-claims or supporting discussion, typically to explain how sub-claims and evidence combine to justify a claim. The WP1 framework defines an argument more rigorously, as the set of nested sub-claims and evidence components that support a claim together with the complete sequence of inferences relating these evidence components and nested sub-claims to the claim.)
- The ASCE tool supports the WP1 framework well.

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

3.3.1 Coverage and limitations of WP5.4 case study

This case 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.

3.3.2 Activities performed for WP5.4 case study

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 chief objective of the case study was application of the CEMSIS method to requirements capture, examination of implementation options, and safety justification; a secondary objective was comparison of the CEMSIS approach with that actually taken by the refurbishment team. Assistance was available, from the personnel who had performed the actual refurbishment project and from a "potential COTS supplier" (the latter rôle being played by Framatome ANP).

Because of limitations of time and resources, the case study could not address the whole implementation process. It focussed on the first part of the lifecycle, i.e. tendering and selection of supplier and requirements gathering and transfer of information from the customer to the supplier. CEMSIS recognises that major progress in improving safety aspects of I&C systems can only be achieved cost-effectively through deployment of suitable models and tools. A number of tools were identified as suitable candidates but the high costs of obtaining tool licences and the costs of training necessitated restriction of the case study to three tools only. These were ASCE for safety justification (WP1), DOORS for requirements management (WP2) and MFM as an example of a graphical language (WP4) for requirements modelling and validation. A simplified form of configuration management was provided for the case study by overview diagrams and Excel tables showing document dependencies.

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 rôles 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 safety justification has as its top-level claim:

- The minimum number of control rods will be injected on auto-demand (reactor protection system) or operator-demand in a time that is less than or equal to the maximum time.

This claim is then subdivided into two "level 1 claims" relating to the requirement:

- User requirements complete and valid
- Implementation of safety system requirements is correct.

The first claim is mainly the responsibility of the customer and the second is mainly the responsibility of the supplier.

At level 2 (system architecture) the following claims occur:

- User's requirements statement, and the supplier's obligations, are clearly defined and accepted (this is necessary to support both level 1 claims);
- Implementation of requirement is fail-safe (supporting level 1 claim of correct implementation);

- A set of claims that certain architectural features support the implementation of the required safety functions.

At all levels, evidential items are identified that are required in support of the claims. In particular, evidence is required that the requirements on qualification of pre-developed and COTS systems are defined and accepted, and that the pre-developed software libraries are appropriate for inclusion in safety systems.

In order to demonstrate traceability of the requirements to the legacy documents and tendering documentation, an example of a document database was set up using the DOORS requirements management tool. To these were added two documents written as input for the case study "supplier", a design concept specification and a requirements specification. Example specifications were then transferred to DOORS to demonstrate that traceability is feasible.

In support of the claims regarding completeness and correctness of the user requirements, requirements validation was performed by modelling with the Multilevel Flow Modelling (MFM) tool. This tool enables modelling of the physical system and I&C functions to demonstrate the required functionality, information flow and failure modes.

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.

3.3.3 Findings of WP5.4 case study

WP1 (justification): The safety demonstration produced by the modernisation project may perhaps be seen as a first step towards the CEMSIS approach. Justification was usually through presentation and examination of the arguments rather than through detailed inspection of the product evidence. The regulatory enquiries were mainly directed towards development process rather than towards top-level functional claims; they could easily be reformulated into claim expansions.

The actual refurbishment safety justification had concentrated on processes and safety activity. The CEMSIS approach was more goal-based and allowed the assignment of concrete tasks to the project partners to provide evidence in support of the claim. As such, the CEMSIS approach appears to provide a useful contract document defining responsibilities. Some specific problems were experienced relating to assignment of evidence to the four CEMSIS framework levels, failure to distinguish clearly between sub-claims and evidence, and general structuring of the large claim/argument/evidence networks that are generated in justification of a real system.

The ASCE tool was found to be easy to work with, but some aspects could perhaps be improved, such as the inclusion of features allowing substructures reflecting the process structure of the plant, and more syntax control of expansion levels.

WP2 (requirements engineering): The actual refurbishment had performed a complex analysis of the legacy documents, requiring complete documentation restructuring. In practice a complete specification of the new system at the pre-contract stage was not attempted. One of the main reasons for modernisation was that the plant did not comply with the new regulations relating to seismic safety, redundant and diverse functionality, and equipment separation. Therefore the contract requirements were not refined in any detail, but were supported by regulatory and plant criteria. Specification was largely left to the suppliers, but the user together with the supplier had to show that the COTS platform (which was still under development) fulfilled the regulatory requirements.

Requirements validation was performed mainly by special functional analysis meetings. Initially it had been envisaged that SIS requirements validation would be performed on a training simulator; this option was not pursued because validation activities on the simulator mainly provided feedback in the areas of human-machine interaction and control-room philosophy rather than detailed SIS requirements. The refurbishment did not use any special tools for requirements elicitation (perhaps because tool usage was not mandatory). Tools would improve insight and would facilitate demonstration and validation of the required functionality. The case study found that the number of legacy documents was huge and substantial effort was required to structure it and to data-mine for necessary information. The actual refurbishment project had produced a

catalogue permitting efficient searching of refurbishment documentation, but CEMSIS would recommend a configuration management system permitting tracing of the specification back to legacy items.

WP3 (COTS/PDS qualification): The refurbishment project included both pre-contract requirements on component and platforms qualification and subsequently produced a plan for qualifying the previously-procured platform for nuclear safety applications. CEMSIS does not give particular guidance on contractual requirements specification for COTS but it does give hints on what could have been improved in the refurbishment.

WP4 (graphical languages): The case study concluded that the MFM tool would provide a common basis within a project for development of the I&C architecture and for early validation of some safety claims.

Partnership concept: The case study concluded that provision of the complete requirements specification is a very complex problem requiring elicitation of knowledge from several parties, and such knowledge is often not available at the time of procurement. A major dilemma is posed by the necessity of producing detailed and validated specification before the I&C platform has been selected. Specifications are changed after commencement of the contract, leading to conflicts, costs and delays. This was apparent both from the real refurbishment and from the case study rôle-playing activities. This case study has proposed a different model, shifting the focus of procurement away from exact definition of the items to be delivered towards selection of an appropriate partner, able to co-operate in a common project organisation with resources to deliver a modernised I&C system. Complete and exact specifications cannot be achieved without deep knowledge of I&C platforms and tools. This is particularly the case where the supplier offers a platform having a set of tools that generate the final executable code automatically from the specification and support specialised validation activities targeted at the automatic development process.

4. 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 rôle-playing situations. Further case-study work, perhaps exercising the full CEMSIS guidance directly on large projects, would be of interest.

5. References

1. *CEMSIS final report* edited by D.J.Pavey. CEMSIS report no. wp0_beg041.
2. *CEMSIS public domain case study* by P.G.Bishop and M.J.P. van der Meulen. CEMSIS report no. wp5-ade039.
3. IEC61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems* Parts 1 to 7. CENELEC 2001 (also published by national standards bodies).