TITLE: Configuration control on PLC applications at the SAFARI-1 RESEARCH REACTOR.

AUTHOR: Gordon Procter

AUTHOR AFFILIATIONS: Head: Facility Development
SAFARI-1 RESEARCH REACTOR

ABSTRACT: *There are 25 PLC systems in use at the SAFARI-1 Research Reactor, ranging from simple perimeter monitoring to complex safety functions. PLC based systems are required to function in their intended manner to ensure the safe and efficient operation of the plant. Stringent control mechanisms are imposed during the system development cycle, to ensure that systems meet the required level of safety.*
An extensive V & V program is applied to codes for safety critical systems. A system of version control is implemented to ensure that only approved code is in operation.
An audit trail of all changes to code is kept.

Introduction: PLC systems are used in a variety of applications at the SAFARI-1 Research Reactor. Applications range from simple perimeter monitoring to complex safety functions. Over the past few years, the numbers of PLCs have increased; there are now 25 PLC systems in routine use. With the increase in the number of systems and the enhancements in technology, the complexity and system reliability requirements have also increased.

The current applications of PLC systems are:-

	Description	**Category**	**Quantity**
	Auxiliary systems	General Purpose	3
	Building Monitoring	General Purpose	4
	Rabbit transfer (Irradiated samples)	Process control	2
	Secondary Cooling system control	Process control	1
	Ventilation Control systems (9 systems of which 4 have redundancy of control).	Safety Related	5
	Protection system (SIL 4)	Safety Critical	6
	Reactor hall Overhead crane	Safety related	1
	Experimental facilities	Safety related	3

The requirement that PLC based control systems function in their intended manner is essential to maintain the good safety record at the SAFARI-1 RESEARCH REACTOR. This requirement must be met for all operating conditions, for both normal and abnormal/fault conditions. Under abnormal conditions, the systems must prevent further usage of the system and ensure that the plant remains in a safe state.

In order to achieve these goals various control mechanisms have been implemented. The author has been responsible for the development of these mechanisms. The fault tolerance requirement is a characteristic that must be considered and built in at all stages of the development, it can not be added on at the end of the project.

The Design Cycle for safety related systems: Once a potential system has been identified the project cycle starts.

1. Identification of the user's needs/requirements. Discussions are held to ascertain the user's wish list. Potential technical obstacles are identified and alternatives listed. Input is obtained from all interested parties including operating and maintenance staff. The end result is a requirement specification.

2. The requirement specification serves as the input for the system design phase. During this phase various solutions are examined for meeting the user's requirements. Several design reviews, with high level technical input, are held to establish the best options for the system. During the design reviews, the following parameters are also taken into account:- fault tolerance, maintainability, reliability and safety issues. The output from this phase is the system technical specification.

3. The detail design of the system hardware follows the acceptance of the technical specification by the relevant authorities. Once again, a system of design reviews is used to ensure that an optimum hardware configuration results. During the design reviews the **What If** scenario is played out to ensure that fault tolerance and maintainability are designed into the system.

Once the hardware design configuration has been established, the structure for the coding is then considered. The hardware and coding structure then pass

through a further design review to ensure compatibility between hardware and software structures. Special emphasis is placed on fault tolerance and maintainability during this review.
The hardware configuration baseline is fixed and the procurement process is initiated. System level hardware documentation is generated.

4. The relevant coding standards are identified. The coding structure is verified to meet IEC 880 [1], and other relevant standards[2,3]. The code structure is defined down to Functional elements. The actual coding is done using only approved and traceable programming tools.
In parallel with this phase the detailed hardware design, down to actual wiring, is undertaken.

5. A competent person, who is independent of the programmer who wrote the code, validates each section of code that is written. This validation process is to ensure that the code meets the intended function.

6. A comprehensive Verification and Validation procedure is generated, this procedure defines what will be tested and how it will be tested. Where coding has to be changed due to errors, all code that interacts with the changed section of code has to be retested.

7. Where required, a complete system is built to enable the verification of the system performance to be undertaken independently from the plant. The actual functioning of the PLC with the installed code is tested in a simulation of the designated system and witnessed by the end users and other interested parties (e.g. Reactor safety Committee, Licensing authorities etc).
This test configuration also serves as a training facility for maintenance staff, who confirm that the system manuals are sufficiently detailed to enable routine maintenance of the system.

8. The system undergoes further verification and acceptance testing when it is finally installed in the plant. Only after all tests have been passed in the

presence of independent observers can the system be put into routine operation.

Documents generated during the design of the system include:-

- Requirement specification.
- Technical Specification.
- System manual, incorporating operating procedures.
- Hardware system manual. *
    - Includes drawings and circuit diagrams where applicable.
- Software system manual. *
    - Includes a list of programming tools and their versions.
- Code listings *
- Verification and Validation procedure.
- Design review notes.

Items marked * are incorporated in the automated version control system. Other items are only subject to manual configuration control.

The efforts that are put into ensuring that systems meet their intended function, during the design and testing phase, lose all significance if the version of code that is in use is not properly controlled.

It is essential to monitor the version of the code that is in use. To this end the author has designed a control strategy that meets all nuclear industry and regulatory requirements.

VERSION CONTROL

The requirement for a system of version control has been driven by two separate requirements.

i). Safety is our highest priority and the NNR (National Nuclear Regulator) must be satisfied that adequate controls are implemented.

IAEA (International Atomic Energy Agency) guidelines must be met or exceeded. [4]

ii). With the increase in systems and their complexity, more than one engineer or specialists can be involved in the development of each system. During the

lifetime of the system, upgrades may be implemented – to meet new requirements. This again means that the probability exists that more than one person will have worked on the system code.

Each new project is registered in the version control system. The various elements for the project that will be controlled are also registered. The initial draft version of the code is registered as the first version.

For a developer to perform any changes on the code, the code is booked out from the server. Once the changes have been completed, the code must be declared as a new version and booked back to the server. During the process of booking the code back to the server the developer is required comment each change in the code, including the justification for the change. Only the Head: Facility Development is permitted to declare a changed piece of code as a new version. The version control system keeps a complete history of all changes and archived copies of all previously registered versions.

The system manuals and essential drawings are processed in a similar fashion.

For safely related PLC systems the Verification and Validation procedures have to be updated to suit the changes made to the code. Only once the procedures and actual results of the V& V process have been completed can the revised code be declared as a new version.

The code can be directly downloaded onto the PLC from the development system.

There is a dual system in use, for the verification of the actual code in use.

- For PLC systems that are stand alone – a system termed PLC walker is used.
  In this system the latest version of code is booked out from the server onto a Laptop computer. A walk around to each PLC and a download of the code from each PLC is performed manually. The code booked out from the system and the code downloaded from each system are compared and any discrepancies displayed on the laptop.
  The resultant downloads with the results of the comparison for each system are then uploaded back to the main system.

- PLC systems that are connected to a data network, have their code downloaded and compared to the latest version in the version control system automatically. A scheduler in the version control system defines when the code for each system is to be downloaded and compared.

The version control system is configured to automatically provide notification of the results for each comparison via email to specified people. In the case at SAFARI-1 the email notification is sent to the Head: Safety & Training, Head: Facility Development and the QA manager.
If a discrepancy in the version is detected, the last approved version of the code is downloaded to the PLC to restore the status of only approved code being used.

The version control system incorporates an hierarchical system of security, thus access to the various functions in the system is well controlled. A complete log is kept of all accesses to the version control system, all booking in or out of code is logged. A log is kept of all comparisons performed with the associated results. The comparison results record a summary as well as a detailed display down to the actual line of code that has been changed.
A complete history including all versions of code for each PLC system is kept, by the version control system. An audit record is thus generated for all changes to each piece of code or documentation related to each of the systems.

The PC that runs the version control system has a mirrored 40Gb disc set for the data, in addition a weekly scheduled back up is made of the archived data.

The Version control system in use at SAFARI-1 is based on the VERSION WORKS system of control tools from GEPA software.

Conclusion: The system of version control outlined in this paper provides confidence that the code in use has been fully tested. This was a necessity before the application of PLC based systems, for safety critical applications could be implemented. The author is currently busy with the developmental work for the PLC based reactor protection system. This a complex system using dual redundancy failsafe PLC's, the Siemens Simatic S7 F/FH processors.

References

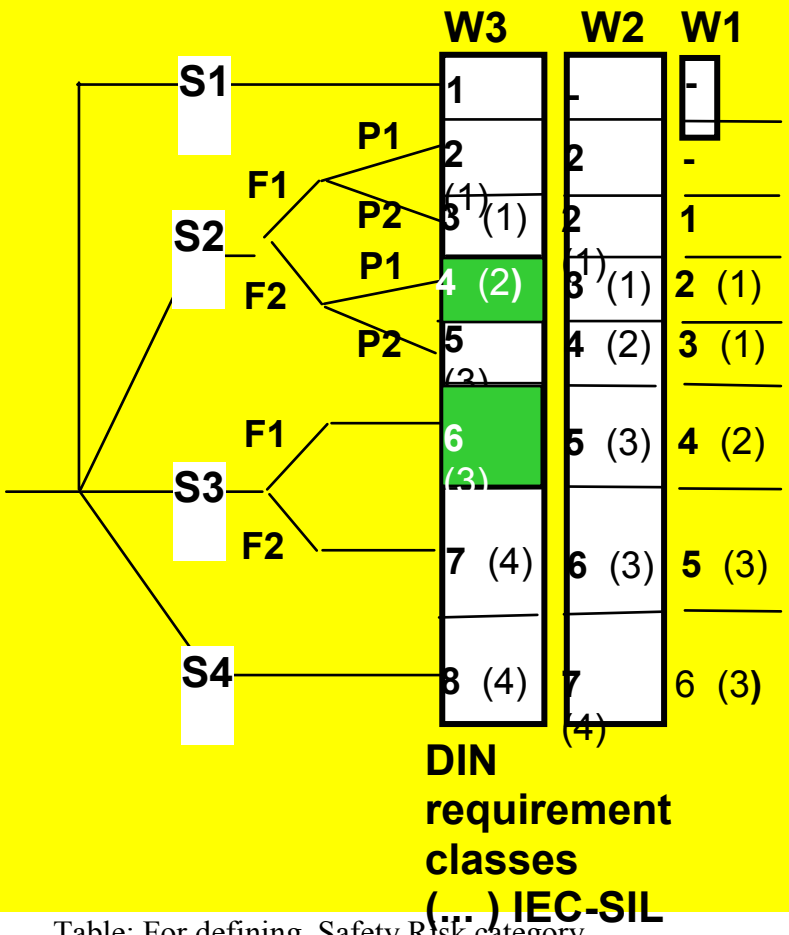
[1] IEC 880 – Software for computers in the safety of nuclear power stations.

[2] IEC 61513 – Nuclear power plants - - Instrumentation and control systems important to safety – General Guidelines.

[3] IEC 61508 - Functional safety of programmable electronic safety related systems.

[4] IAEA Safety Guides series 35.

Safety Risk (2)



Severity of injury/damage

S1: Slight personal injury;
minor environmental damage
S2: Serious irreversible injury to one or more persons or the death of a person;
temporary serious environmental damage
S3: Death of several people
long-term serious environmental damage
S4: Catastrophic effects, many deaths

Frequency and/or exposure time to hazard

F1: Seldom to quite often
F2: Frequent to continuous

Possibility of avoiding the

P1: Possible under specific conditions
P2: Scarcely possible

)* W1: Extremely low
W2: Low
W3: Relatively high

Table: For defining Safety Risk category.