

---

## FRENCH EXPERIENCE ON RENEWING I&C SYSTEMS IN NPP'S

### Feedback from assessing nuclear instrumentation system (RPN) refurbishment at French CP0-series plants

O. Elsensohn, F. Fradet, J.C. Péron, B. Soubiès

*Institut de Radioprotection et de Sûreté Nucléaire  
B.P. 17 – 92262 Fontenay-aux-Roses Cedex France*

---

**Abstract:** In 1996, the utility operating France's nuclear power plants launched feasibility studies for the refurbishment of the nuclear instrumentation system (RPN classed category A) installed in its CP0-series (900 MWe) units. The system was ultimately upgraded with digital I&C system, using a SPINLINE 3 platform.

This article describes feedback from an evaluation conducted on the refurbishment by the Institute of Radiological Protection and Nuclear Safety (IRSN), technical support arm of the Directorate General for Nuclear Safety and Radiological Protection (DGSNR). The study begins with a historical overview of the refurbishing operation, then discusses the IRSN assessment method and the lessons learned from this first major revamp of an I&C system in the French nuclear reactor series.

Based on its previous experience in evaluating I&C systems for P4/P'4 (1300 MWe) and N4 (1450 MWe) plants and to account for the first-ever aspect of such an upgrade, IRSN partitioned its assessment into four phases. This approach enabled taking into account the impact of RPN refurbishment at every level – system, hardware and qualification, software, operation, onsite requalification, health physics, fire protection and human factors.

All six units in the CP0 series have now been equipped with the new digital RPN.

## 1. INTRODUCTION

This article presents feedback from an assessment by the Institute of Radiological Protection and Nuclear Safety (IRSN) – technical support to the French safety authority (Directorate General for Nuclear Safety and Radiological Protection) – of a nuclear instrumentation system upgrade (classed category A) from analog to digital technology at Fessenheim and Bugey (the first french units of the 900 MWe series plants). The article begins with a historical overview of the refurbishing operation, followed by a discussion of the method adopted to assess it, with emphasis on lessons of interest for future upgrades.

The purpose of the RPN is to permanently monitor reactor instantaneous power, power level changes, and axial and radial power distributions in various plant states such as operation at power or refueling shutdown. Where necessary, it also provides requests for protection action to the reactor protection system (RPR) and for alarm indications in the control room.

The RPN covers three measurement ranges (source, intermediate and power). The system comprises the neutron flux detectors, protection/control signal conditioning and processing equipment and interface relays.

The refurbishment undertaken by the NPP operator in CP0-series units had two objectives:

- enhance system availability and reliability by significantly reducing spurious actions related to maintenance,
- solve the problem of obsolete hardware (cabinets and power range detectors) and facilitate incorporation of subsequent programmed system developments.

This operation, for which Framatome acted as prime contractor, called for an upgrade from analog I&C system to a digital technology derived from that used in the N4 plant series, while preserving the existing interfaces with other systems, in particular RPR analog circuitry. In concrete terms, this meant replacing RPN analog processing cabinets with digital models and substituting CBL15-type detectors with collimating capability for the older-design power range detectors, to afford a more accurate image of neutron flux.

The functional breakdown of a digital RPN calls for three separate PLC-like units corresponding to the three – source, intermediate and power range – protection channels. Each of these units is developed on the SPINLINE 3 platform supplied by Schneider Electric and consists of I/O boards for functional data and a CPU board equipped with a Motorola 68040 microprocessor that incorporates generic system software. Protection software for each RPN unit includes both customer-specific "application" software developed by Framatome and the already mentioned system software.

This refurbishment is the first major revamp of an I&C system to be carried out in the French nuclear reactor series. It was initiated by the NPP operator following the conclusions of its study on I&C systems hardware aging and obsolescence in 900 MWe plants.

## **2. BRIEF HISTORY OF THE UPGRADE**

The Operator launched feasibility studies on the RPN refurbishment in 1996 and, in June 1998, presented the project to the French nuclear safety authority and its technical support organization (IRSN). The first operational version of the digital RPN was installed at Fessenheim unit 1 (FS1) in January 2000.

Since then, the new system has been installed, as part of second ten-year inspection activities, to all six units of the CP0 series, after allowance for feedback from its integration into the first unit. Subsequent developments gave rise to a new version of the programmed system, enabling better interfacing with existing systems, particularly under special operating conditions. These changes likewise elicited technical advice from the IRSN.

## **3. METHODOLOGY AND FEEDBACK FROM RPN SAFETY ASSESSMENT**

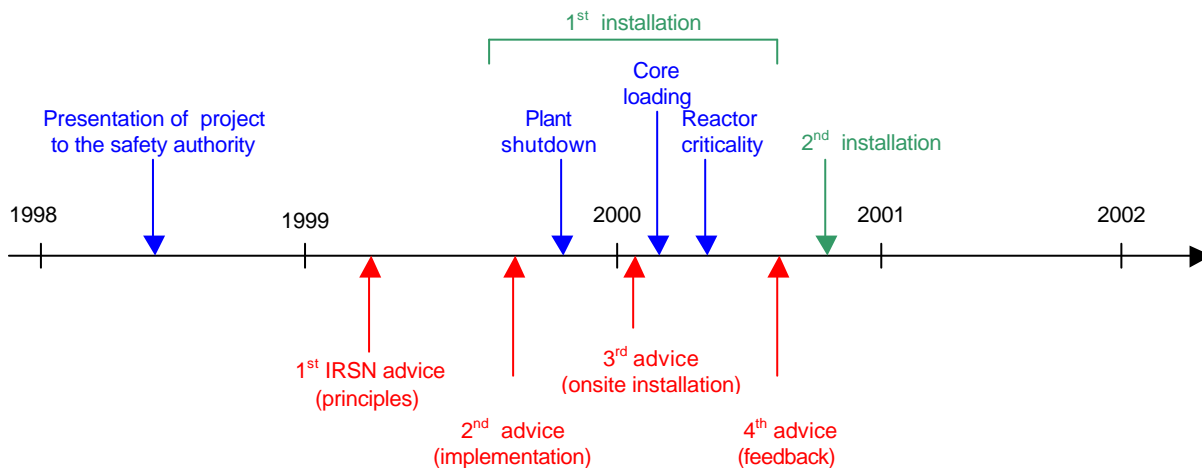
The purpose of the assessment was to verify the compliance and the completeness of the safety demonstration made for refurbishing the RPN. This essentially meant checking that safety requirements had been met at all levels in the operation, from system specification through design and implementation to onsite requalification. The development process was assessed to ensure the consistency of relationships and requirements between its various stages. Documentation associated with each stage was assessed according to the basic safety rules ([1] to [4]) and standards ([5] to [10]) applied in France.

Based on its previous experience in evaluating I&C systems for P4/P'4 (1300 MWe) and N4 (1450 MWe) plants and to account for the first-ever aspect of such an upgrade and its implications for the safety of CP0-series plant units, IRSN performed its assessment in four phases, three of which were spread out

over a year, and the fourth timed to end six months before installation of the new system in the second CP0 unit. These four stages consisted of analyzing:

- principles of the modification (justification and rules for design and development),
- quality of its proposed implementation,
- quality of the installation after integration of changes in onsite requalification tests,
- operating behavior.

The first update took place at Fessenheim 1 during the unit's second ten-year inspection. The following diagram shows assessment milestones and their relation to installation constraints:



IRSN's objective was to provide its technical advice of upgrade principles and their proposed implementation before Fessenheim was shut down, so that the safety authority could authorize the Operator to install the new system during the outage. Analysis of operating feedback was then intended to determine the acceptability of generalizing the upgrade to all other units in the CP0 series.

At the joint request of the safety authority and IRSN, the Operator provided documentation on specific aspects of the refurbishing operation, including:

- systems (system software specification manual, system architecture, etc.) and functional design (functional protection diagram, functional control diagram, etc.),
- "system" and "application" software (software quality plan, specifications, design, source and binary codes, etc.),
- validation: analysis and results of integration and validation tests; interconnected tests, etc.,
- requalification integrating health physics requisites (site operation file),
- neutronics (rules for core physics tests on restart, etc.)

The IRSN assessment thus covered all of the following: system, hardware, software, functional design, operation, health physics, fire protection and human factors. The broad outline of analyses for each of these aspects is outlined below:

- for the system,
  - architecture (redundancy, independence, emergency power supply), capacity of system to detect and report its failures, degraded mode management (failsafe features, inhibits),

- reliability (study of the validity of system and failure rate models – adequacy of selected periodic test frequency to reach the reliability target),
- interconnected tests (relevance and coverage of functional tests with respect to specifications)
- parameter setting management (analysis of process and organization used to modify parameters and ensure traceability of the modifications),

○ for hardware,

- periodic tests (verification of test principles, test method and test exhaustiveness as well as overlapping between tests),
- qualification (ability of hardware to perform its functions in the service environment, to withstand EMI, earthquakes, etc.),

○ for software [11], [12], [13],

- observance of and compliance with IEC standard 60880 (development of 1E class programmed systems),
- analysis of source codes and software architecture,
- validation test and integration test coverage,
- independent testing of executable code using a simulation tool.

IRSN views safety must be evaluate for the system software of each RPN unit rather than for system or application software taken separately. This means that the software of a unit as a whole is responsible for safety functions assigned to the hardware on which it runs. System software for the SPINLINE 3 platform was thus assessed in accordance with its utilization in RPN units.

This included evaluating performance of protection functions, verifying that the programmed units responded as expected to failures and confirming that manufacturer tests afforded suitably exhaustive coverage.

○ for neutronics and system operation

- periodic tests,
- restartup core physics tests (power reconstruction process, calibration of neutron detectors, protection threshold adjustments),

○ for requalification and health physics

- test program and prerequisites for associated operations
- dosimetry of operations associated with the revamp (analysis of optimization initiatives and operating feedback relating to collective and individual doses and operation times),

○ for human factors,

- control room alarm management,
- human-machine interface (adaptation to personnel activities involving the RPN cabinets),
- training and operator mastery of digital system maintenance.

IRSN based its choice of means for the assessment on a critical study of documentation supplied by the Operator. Software assessment relied principally on automated tools. Note that study of human factors entailed interviewing personnel onsite and during system operator training sessions. Assessment of such a revamp requires considerable human resources to cover the various technical fields involved.

At the request of the safety authority, analysis of the different topics listed above led IRSN, to give its opinion on the acceptability of the upgrade in safety terms and on the non-regression, of an appropriate level of design, development capability and installed system quality.

#### **4. LESSONS DRAWN BY IRSN AND OUTLOOK FOR THE FUTURE**

The assessment approach adopted by IRSN thus enabled analysis of the multifarious impact of a RPN digital upgrade in a period of time that was short for such a heavy workload. This experience revealed that the following points should be given special emphasis in future revamp assessments:

- interfaces (even where identical) between the refurbished system and its environment, and specifically their dynamic aspects (time required for signal state changes). This is because signal processing times differ from analog to digital systems and require specific adaptations.
- increase in the number of parameters required by the upgrade to digital I&C system, and the more thorough documentation needed to suitably credit requirements applicable to each parameter category,
- maintenance problems inherent in use of generic software, specifically where this software must evolve to meet requirements of other projects. To eliminate any such problems, the safety authority has now requested that system software be only dedicated to 1E class systems.
- the engineering process, which, in the specific context of an analog-to-digital upgrade, must be formalized to suitably clarify the system specification-to-software document interface. More generally, the NPP operator must present his engineering process at the start of the project, to facilitate identification of documents relevant to project development. These documents must cover every single phase from formulating requirements and defining specifications right up to the various types of testing. It must be possible to correctly situate them in the engineering process at each phase in development, so that their links with upstream and downstream documents can be identified and their content accurately appraised. Use of this approach is a guarantee that the process will comply with prevailing rules for development and that system safety requirements take shape gradually yet remain traceable as the project unfolds. It is then easier to relate the tests used in verifying compliance, to the original set of requirements. Right from the start, there must be a consensus with the NPP operator on the required content of each development stage. Correct progression and observance of the different engineering phases then contribute positively to the safety demonstration, particularly where the system might evolve toward new versions.
- inclusion by the NPP operator, in the project schedule, of enough time for the safety authority and its technical support organization to conduct the safety assessment; and provision for timely forwarding to these entities of the relevant documentation.

#### **5. CONCLUSION**

In 1996, the NPP operator launched feasibility studies for the refurbishment of the nuclear instrumentation system (RPN) installed in its CP0-series (900 MWe) units. All six of these units have

now been equipped with the new digital RPN. IRSN considers that the upgrade to digital technology facilitates both operation and maintenance of the system without regression of the safety level.

The assessment method applied by IRSN enabled crediting of all aspects impacted by the revamp, in a relatively short time. Its assessment was based on documentation supplied by the Operator and dealt primarily with system design (reliability, architecture, interconnected tests), hardware (periodic tests, qualification), software (compliance with IEC standard 60880 for programmed systems, evaluation of the development process and its by-products, test coverage), operation, requalification, health physics, fire protection and human factors.

The upgrade from analog to digital technology had organizational impact (changes in periodic test and parameter setting procedures, etc.) as well as human implications (on operator training and mastery of the digital system), both of which must be considered in safety analysis. In general, this experience revealed that a few areas – such as engineering process and interface dynamics – required special emphasis in future update assessments. For a major update impacting numerous technical fields, the Operator also needs to make better provision, in scheduling project development activities, for the time required by the safety authority to perform its assessment.

Given the speed of technological advances and of changes in the industrial environment, use of digital I&C system means that, from the outset of the project, the Operator must take whatever measures are necessary to guarantee long-life system operation, as protection from potential loss of industry expertise and the risk of component obsolescence.

## REFERENCES

1. Basic Safety Rule I.3.a Principes généraux de conception et d'installation (General design and installation principles).
2. Basic Safety Rule IV.1.a Classement des équipements (Equipment classification).
3. Basic Safety Rule IV.2.b Exigences à prendre en compte dans la conception, la qualification, la mise en œuvre et l'exploitation des matériels électriques appartenant aux systèmes électriques classés de sûreté (Requirements for design, qualification, installation and operation of electrical equipment for safety class electrical systems).
4. Basic Safety Rule V.2.d Règles générales applicables à la réalisation des matériels électriques (General rules applicable to electrical equipment manufacture).
5. IEC 60231A, General principles of reactor nuclear instrumentation.
6. IEC 60671, Periodic tests and monitoring of the protection system of nuclear reactors.
7. IEC 60709, Separation within the reactor protection system.
8. IEC 60780, Nuclear power plants – Electrical equipment of the safety system – Qualification.
9. IEC 60880, Software for computers in the safety systems of nuclear power stations, 1986.
10. IEC 60980, Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations.
11. Elsensohn, Henry, Soubiès, "Contribution to the safety assessment of instrumentation and control software for nuclear power plants," 22<sup>nd</sup> Water Reactor Safety Information Meeting (WRSM), Washington D.C., 24-26 October 1994.
12. Henry, Régnier, "Methods and tools used at the IPSN for the safety assessment of critical software," IAEA Specialists' Meeting on Design and Assessment of Instrumentation and Control Systems in NPPs Coping with Rapid Technological Change, Garching, Germany, 6-8 October 1998.

13. Péron, Régnier, Soubiès, "IPSN's experience with new generation tools for static analysis of safety critical software," International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000), Washington D.C., November 2000.

---

# German Experiences on Renewing of I&C Systems in NPPs

E. Piljugin, H. Heinsohn

*Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH*

---

## **Abstract:**

Software-based digital instrumentation and control (I&C) systems are going to substitute the conventional hard-wired I&C systems not only in common technology but also increasingly in nuclear power plants. In German nuclear power plants, software-based digital I&C equipment is up to now mainly used in process control systems but more and more also in limitation systems, emergency systems as well as partially also in reactor protection systems.

Since the nineties they have been only four reportable events according to the German notification criteria which concerned faults in software-based digital equipment in German nuclear power plants were reported. This paper highlights the impact of I&C on two of these events.

Additionally, the approach of GRS to develop methods for quantitative reliability assessment of digital I&C systems including the software is presented.

---

## 1. INTRODUCTION

Instrumentation and control systems in nuclear installations constitute are vital for safety and reliability. I&C systems mainly perform the following tasks:

- recording of process variables,
- generate and processing of signals (set points, monitoring, voting logic, etc.),
- control of actuators (drives of pumps and valves, etc.).

For the process I&C and especially for information and communication systems of German nuclear installations, software-based systems and devices were employed rather early. The range of devices has been extended from programmable logic controllers to network systems and main frame computers for recording, processing, monitoring and storage of process data.

Originally safety related I&C systems in German nuclear power plants exclusively consisted of analogue modules. Meanwhile, software-based digital I&C systems supersede analogous I&C systems in non-nuclear power plants and increasingly also in nuclear power plants. In German nuclear power plants, software-based digital I&C equipment are not only used in process systems but also more and more in limitation systems, emergency systems and as well as partially in reactor protection systems.

Table 1 presents a selection of software-based digital I&C equipment in safety systems and safety related systems in German nuclear power plants evaluated during the Y2K-research in German nuclear power plants.

**Table 1: Selection of software-based digital I&C equipment in German NPP's (status as of 1999/2000)**

Concerned measures or function	I&C components or system
Emergency alarm: Flooding of the reactor building	Instrumentation
Protection equipment of the emergency diesel generator with priority against the signals of the safety system: overspeed and cooling water temperature monitoring	Instrumentation
Speed monitoring of main coolant pumps	Instrumentation
Low frequency monitoring of emergency power trains	Instrumentation
Converter for uninterruptible power supply	Control logic
Correction of RPV level measurement	Instrumentation
Reactor in-core instrumentation	Instrumentation
Neutron flux measurement	Instrumentation
Monitoring of the steam activity downstream steam generator	Instrumentation
Pressure and pressure difference monitoring	Instrumentation
Control and monitoring equipment for electrical power supply	Control and monitoring equipment
Safety relevant limitation system	Digital control system Teleperm XS
Emergency safety system: independent safety and accident management system	Digital control system Teleperm XS
Automation of the pumps switch-over by cooling water	Control logic
Vibration monitoring of forced circulation pumps	Instrumentation
Control of the power supply converter for forced circulation pumps	Control logic

## 2. GERMAN OPERATIONAL EXPERIENCE WITH DIGITAL I&C SYSTEMS

Based upon the national notification criteria 4 events (s. Table 2) with software-based digital I&C systems in German nuclear power plants were reported since the nineties. This relatively low number of reported events is explained by the fact that - according to the notification criteria for I&C systems - incidents must be reported only

- if they cannot be corrected within 24 hours or
- if the failure has some potential for on a common cause failure.

**Table 2: Reported events with software-based digital I&C**

Date of event	Event
23.05.1990	Sporadic disturbances of rotation speed recording of MCP
19.02.1992	Faulty function of the control of the reactor hall crane
10.05.2000	Faulty secondary load reduction and failure to insert control rod
06.04.2001	Drop of a fuel assembly after erroneous lift

Hereinafter, I&C technical aspects of the events in 2000 and 2001 are addressed.

### 2.1 Event of 10.05.2001

The „reactor power limitation system“, concerned in this event, has been upgraded in 1998 from hard-wired logic to software-based digital I&C (TELEPERM XS). The design of the new I&C does not consider the case of withdrawing for maintenance the four power range ionisation chambers of one chain of the neutron flux core external instrumentation.

In order to repair a faulty ionisation chamber of the neutron flux instrumentation, the affected component of the core external instrumentation was withdrawn during power operation. In this case simulations were performed in the I&C of the limitation system. This caused a disturbance which led to fast reduction of generator power and simultaneously disabled the drive and the drop function of the control rods actuated by the safety relevant limitation system (safety level 2). Additionally, due to the simulation, the automatic control of the operational boron injection, of the demineralised water injection, and of one high-pressure pump were inoperable. This equipment, however, could have been activated by manual operation.

The reactor protection set points of the primary circuit for the activating the reactor scram were not reached during this incident. If challenged, the automatic scram would have been actuated by the self-sufficient hard-wired reactor protection system. A protective scram by manual action was possible at any time, too.

During the tests and checks while planning, developing and commissioning (also by validation & verification) the digital I&C, the deficiency in the logic was not recognized. For the repair of ionisation chambers the simulation for only one single ionisation chamber was checked. A simulation procedure for the exchange of the entire chain with all installed ionisation chambers was not designed and consequently not checked.

In order to prevent disturbances by spurious signals during the withdrawal of the chain of elements during power operation, the signals of the chamber chain in four redundancies of the digital I&C were neutralized via simulation. This was done by entering a specific signal command sequence on the service unit. The command sequence changes the status of the signal into „error“, while the signal value remains unchanged.

The propagation of „error“ signals within the logic was not sufficiently investigated and tested during the planning of maintenance measure for the chamber chain.

Root-causes of the event were:

- errors in the specification and requirements, and

- insufficient tests of specification including commissioning tests,
- furthermore, signal monitoring (signal value and error status) was not comprehensive within the system documentation or at the service device during the simulation.

Measures to fix the problem:

After the event, the utility revised the I&C instruction for the simulation and entered additional components to block the signals with the status „error“ in the digital I&C. Also, the system documentation was revised taking into account the processing of the error status.

## **2.2 Event on 06.04.2001**

During the refuelling of the reactor a fuel assembly dropped. When it was lifted, its structure erroneously fastened to the adjacent assembly in such way that both assemblies were drawn out of the reactor core. Due to an overload indication the operator stopped shortly after lifting of the assembly. Since there was no previous automatic stop of the hoisting gear above the load limiting value, the operator continued unloading the fuel assemblies at slow-speed.

When the intended hoisting level was reached (the foot of the fuel assembly being about 80 cm above the core upper grid), the hoisting procedure was finished. One minute later the erroneously caught second fuel assembly slipped down, dropped on the core upper grid and stuck there in an inclined position. No damage of the fuel assembly with release of radionuclides was noticed.

Two independent faults contributed to the simultaneous lift of both fuel assemblies:

- failure of the automatic load stop and
- the operator ignored the overload indication

The refuelling machine is protected by two overload limiting values, one for handling the control rods and one for handling the fuel assemblies. The load monitoring is designed as two-channel software-based digital system.

The refuelling machine is to be stopped when handling fuel assemblies in a single channel exceeding the value 3850 N (a single fuel assembly weighs about 2800 N). In the event described this stop did not occur because the process logic for limiting load was not ready for operation. There was no indication of this state.

Root-causes of the event:

After renewing the two-channel software-based load measurement, commissioning tests were performed, which did not consider all operational modes of the measurement equipment. Above all, the newly installed data interface of the external service device was not systematically tested for possible impacts of measurement equipment.

As root-cause of the failure a synchronisation problem of the firmware of the equipment was identified. In the opinion of experts, an unidentified and unrecognised state up to the blockade of the overload stop can occur while using the PC interface.

Measures to fix the problem:

Among other things an indication limiting value was superposed to the upper overload limiting value. The indication range of the analogous indication display was extended and the limiting values were marked.

After work at the load measurement equipment which could lead to changes of parameters a final functional test has to be carried out.

## **2.3 Summary**

The experience with digital I&C in German nuclear power plants shows that the reportable events are attributed to deficiencies in the specification, the development and qualification of software, the system structure, the commissioning tests, and the planning and performance of maintenance. Three of the four events are related to software-based I&C systems taken from the manufacturing for non-nuclear installations. Therefore, it is necessary to define rules and requirements for the equipment in a proper way to ensure the quality of safety relevant components in NPP.

In view of the increasing importance of software-based digital I&C for safety relevant systems in nuclear power plants it is necessary to collect the operational experience on a wider basis compared to the current notification criteria.

## **3. RELIABILITY ASSESSMENT OF DIGITAL I&C SYSTEMS**

The practice of GRS with the quantitative reliability assessments of the traditional I&C is applied to develop approaches for quantitative reliability assessment of digital I&C systems including the software in compliance with the needs of PSA. The assessment of software reliability needs to be integrated into the overall assessment of the system taking into account impacts of I&C on the process protected.

In the framework of current investigations, the following work is carried out:

- evaluation of operational experience in view of reliability of digital I&C including international experiences where available,
- assessment of reliability data relevant for PSA,
- evaluation of the state-of-the-art for the reliability assessment of digital I&C,
- adaptation of the methods to the needs of the reliability assessment,
- development of a pilot PSA-model for an emergency system upgraded by digital I&C.

On the basis of these investigations it will be verified if the traditional fault-tree modelling of digital I&C can provide useful results or if specific adaptations are necessary.