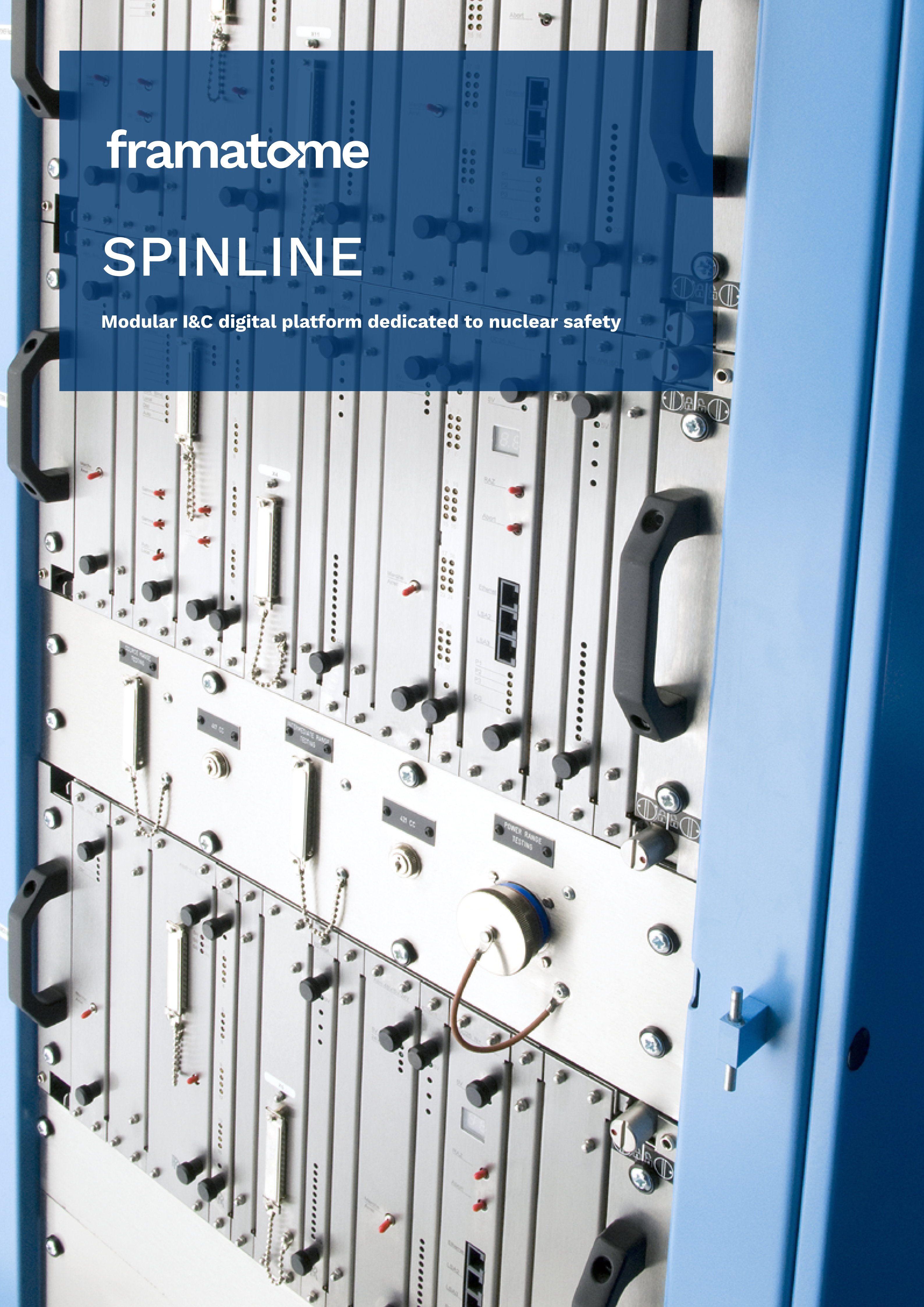
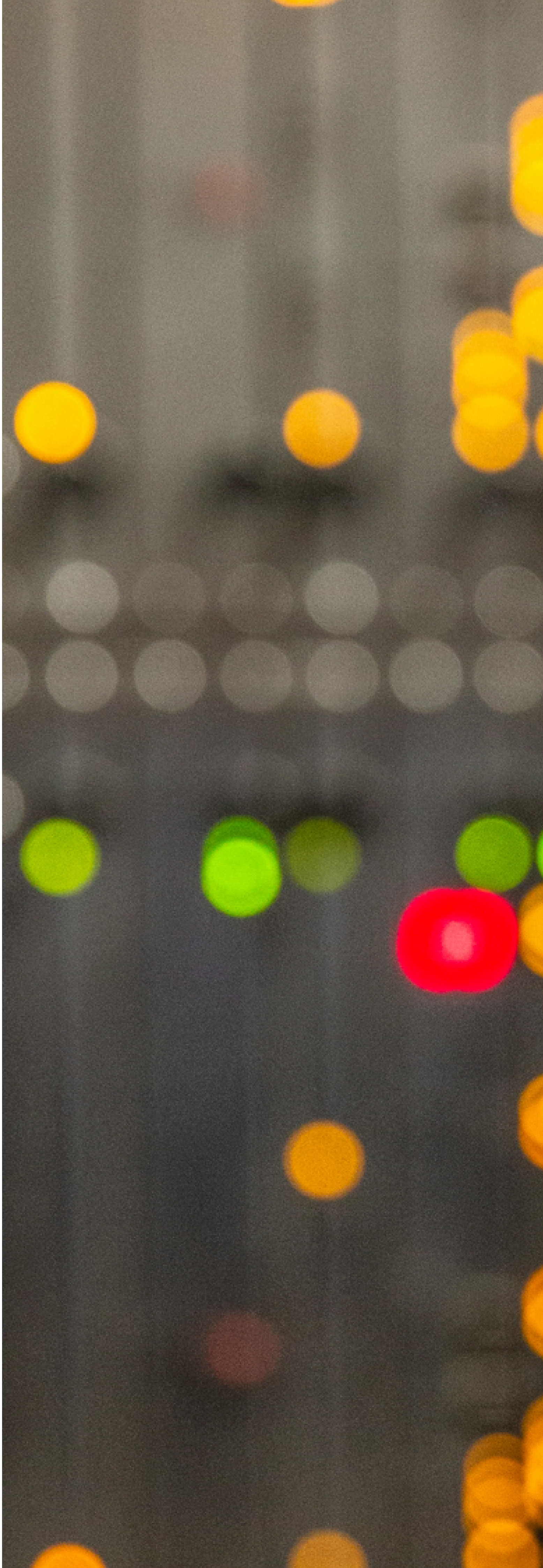
framatome

SPINLINE

Modular I&C digital platform dedicated to nuclear safety



Content



About Spinline

Spinline is one of the latest Framatome digital technology solutions designed specifically for nuclear safety I&C applications.

Spinline is a modular digital solution dedicated to developing or upgrading safety systems used in nuclear reactors.

Spinline is specifically designed to implement any class 1E and category A (IEC-61226) safety I&C functions, at a level of qualification and certification where conventional Distributed Control System (DCS) or Programmable Logic Controllers (PLC) cannot be used.

Safe and available

Spinline enables utilities to improve the safety and availability of nucler power plants (NPPs). The safety-oriented design of Spinline allows and includes specific features such as deterministic behavior, fail-safe, fault tolerance, redundancy, physical and functional separation, functional diversity, online monitoring and automated periodic testing. Availability is improved through self testing, automated periodic testing and fail-safe orientation.

Proven

Based on 50 years of experience, Spinline has been successfully installed in more than 90 nuclear reactors all over the world. This provides Framatome with the largest and longest experience in this field anywhere in the world.

In 2009, Framatome completed the Dukovany plant (Czech Republic) I&C refurbishment, a nine-year project considered as one of the most significant I&C modernization projects in the world.

Spinline is being used to modernize the I&C systems of 20 EDF 1300MW units in France; the largest modernization program in the world, and has been used in 2018 to succesfully modernize key parts of the two Loviisa (Finland) VVER plants.

Framatome offer for safety I&C

Modular

Spinline has been designed to implement I&C digital systems' safety functions in Nuclear Power Plants (NPPs) and Research Reactors.

Spinline can be used in protection systems, such as Reactor Protection System (RPS), Neutron Instrumentation System (NIS), Process Instrumentation System, Engineered Safety Features Actuation System (ESFAS), I&C for Ultimate Diesel Generator / Emergency Diesel Generator (UDG/EDG) and Diesel Load Sequencing System, both in new NPPs and for modernization of existing safety I&C systems in operating plants.

Certified

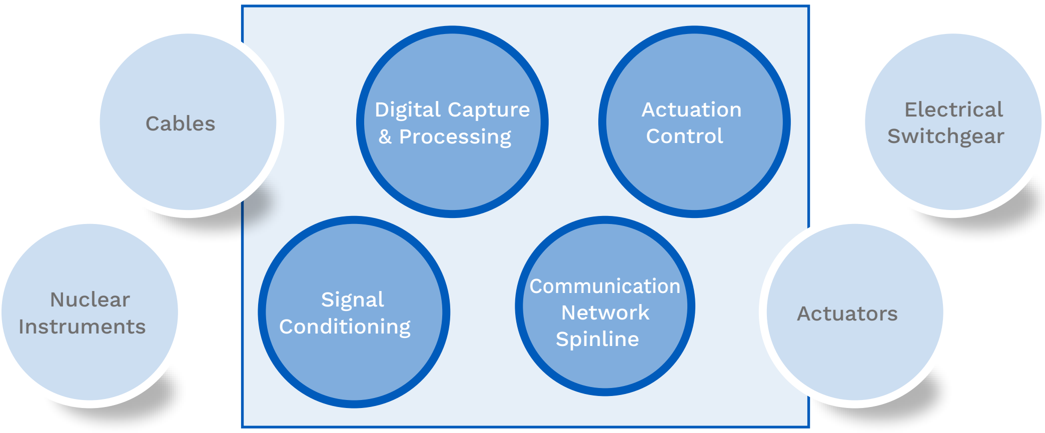
Spinline technology was specifically designed in accordance with the demanding safety requirements inherent to nuclear I&C. Software is developed in strict compliance with International, U.S., European and local standards. Hardware has been qualified for Electromagnetic Compatibility (EMC), environmental, and seismic conditions.

Cost-effective

Spinline is a secure investment. Based on strict and efficient development methodology, Spinline uses up-to-date components ensuring that Framatome customers benefit from the best of the I&C digital technologies and optimize their operational efficiency.

Long-Term Support

Framatome also offers customers the possibility to subscribe to a Long-Term Support Agreement (LTSA) for Spinline and other technologies. Such agreements cover training, maintenance, spare parts and other services for the extent of the contract (up to 25 years after installation). Spinline is included in several of these contracts and therefore will be maintained and updated at least until 2053.



Spinline perimeter: From the sensor to the actuator.

> A modular digital solution to implement any category A and class 1E safety I&C functions.

Design features

Spinline has been designed specifically for nuclear safety applications.

The production of electricity in NPPs must be safe and efficient. The I&C systems, and in particular the safety I&C systems, are key to meeting these objectives.

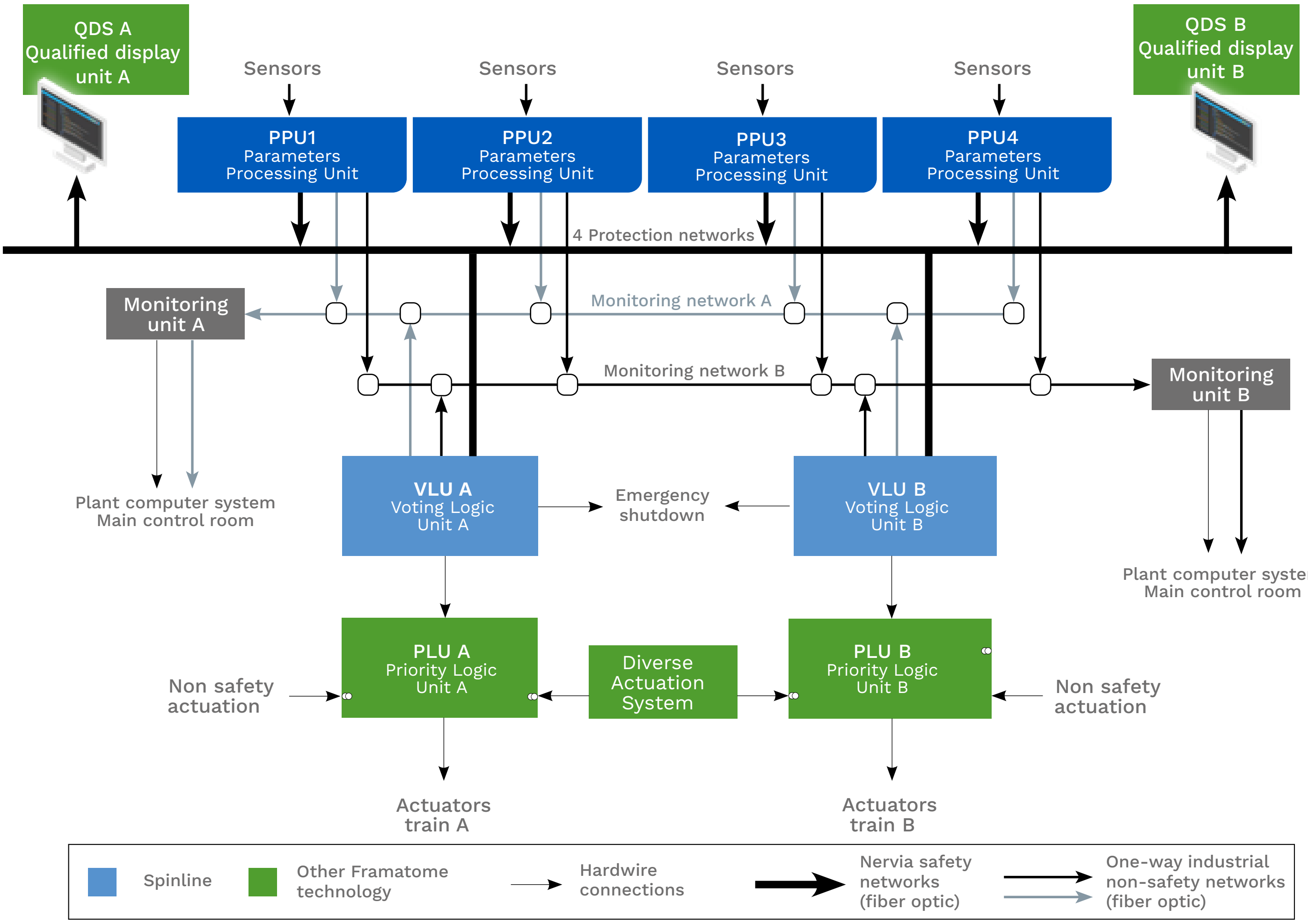
The basic requirements from states, safety authorities, and utilities are:

- High level of safety and availability
- Compliance with international criteria
- Qualification in accordance with nuclear standards
- State-of-the-art technology and performances
- Compliance with NPP lifetime (i.e. availability of spare parts and access to the technology)
- Cost effectiveness

Spinline has been designed to reflect these requirements and offers the following features:

- **Fail-safe architecture :** Spinline assures that, in case of detected failure, the outputs associated to a CPU always go to a predefined state. No detected failure may impair safety.
- **Fault-tolerance** (including single failure criterion): Spinline can meet any redundancy requirement.
- **Functional diversity** can be implemented to defend the system against common cause failures.
- **Functional insulation:** Communication means and insulation devices ensure separation and avoid propagation of failures between redundant parts.
- **Determinism:** For all processing, the same inputs produce the same outputs with a garanteed response time.
- **Easiness of operation and maintenance**
- **Flexibility**: For further evolution without any hardware modification.
- **Modularity:** Spinline can be delivered either as racks to be integrated into existing cabinets (for refurbishment purposes) or as full cabinets.
- **Scalability:** Spinline fits various sizes of I&C systems. It can be used for highly distributed architectures such as a RPS with four channels, distributed processing for acquisition, functional processing and voting; or for more compact architectures such as a NIS with two channels for source and intermediate ranges, four channels for power range, and no separate distribution of the processing.
- **Cost effective:** With its unparalleled reliability and accuracy, Spinline allows utilities to operate plants efficiently with reduced downtime.

Example of reactor protection system based on Spinline



QDS A Qualified display unit A
QDS B Qualified display unit B
Sensors
Sensors
Sensors
Sensors
PPU1 Parameters Processing Unit
PPU2 Parameters Processing Unit
PPU3 Parameters Processing Unit
PPU4 Parameters Processing Unit
4 Protection networks
Monitoring unit A
Monitoring network A
Monitoring network B
Monitoring unit B
Plant computer system Main control room
VLU A Voting Logic Unit A
Emergency shutdown
VLU B Voting Logic Unit B
Plant computer system Main control room
Non safety actuation
PLU A Priority Logic Unit A
Diverse Actuation System
PLU B Priority Logic Unit B
Non safety actuation
Actuators train A
Actuators train B
Spinline
Other Framatome technology
Hardwire connections
Nervia safety networks (fiber optic)
One-way industrial non-safety networks (fiber optic)

History and evolution of the technology

Current Spinline technology is the result of continuous project development to provide customers with the best in class digital technology.

Spinline is one of the latest modular digital technology solutions dedicated to nuclear I&C developed by Framatome.

During its 50 years of accumulated experience, Spinline has been continuously updated to improve reliability/availability and response time performance, make maintenance and operation easier, meet electromagnetic compliance and shorten project development time, thus becoming the world standard for nuclear safety systems digital technology.

Key steps and dates of the Spinline technology

Analog System

Non-software-based

- **France**
  900MW plants

1970

P4 SPIN

8 bits microprocessor

- **France**
  1300MW P4 plants

1980

N4 SPIN

16 bits microprocessor

- **France**
  1450MW N4 plants

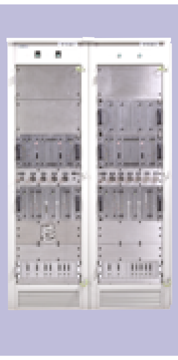
1990

SPINLINE3

32 bits microprocessor

- **Dukovany**
- **Tihange**
- **Metzamor**
- **Qinshan**
- **Kozloduy**
- **Fessenheim**
- **Bugey**

2000



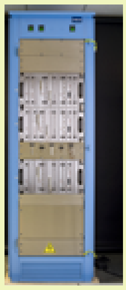
SPINLINE

32 bits microprocessor

- New gateway
- Redesigned CPU board
- Increased signals management capabilities
- Adaptable power supplies
- NERVIA networks
- Optical fiber
- CLARISSE SSDE

- **China**
  CPR1000 program
- **France**
  VD3-1300MW program
- **Finland**
  Loviisa modernization

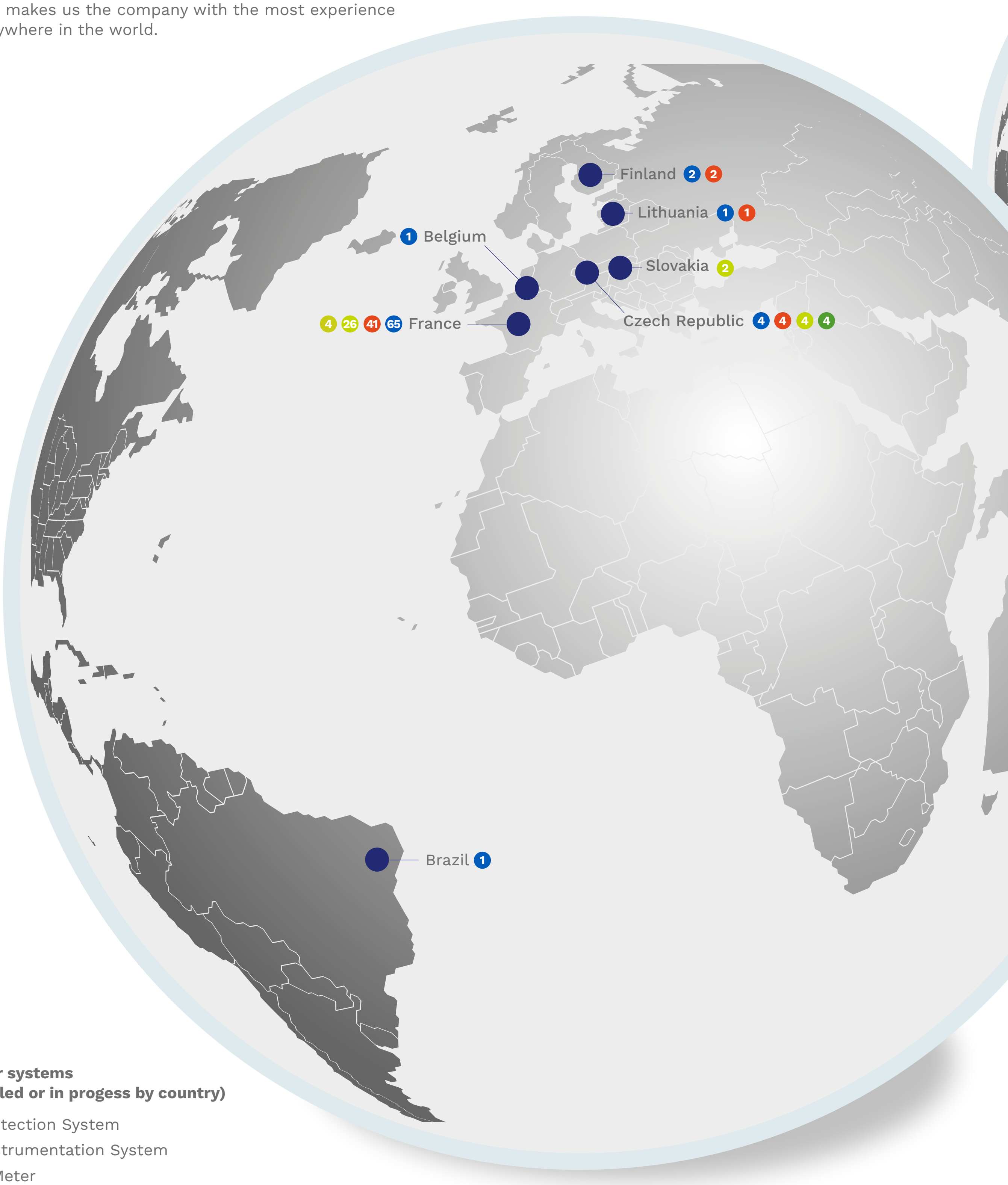
2010



Experience and references

Spinline is based on more than 50 years and 1,840 reactor years of experience worldwide, through multiple retrofit programs and new build projects.

Based on 50 years of experience, Spinline technology has been successfully installed in more than 90 nuclear reactors all over the world. This makes us the company with the most experience in this field anywhere in the world.



References per systems
(number installed or in progess by country)

- ● Reactor Protection System
- ● Neutron Instrumentation System
- ● Reactivity Meter
- ● Diesel Load Sequencing System

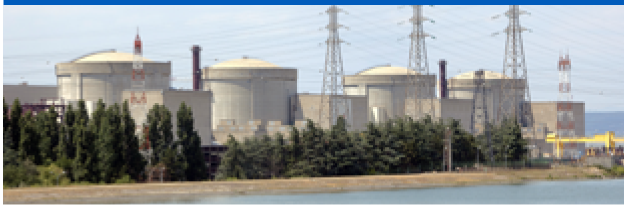
China 40 4
Armenia 1

France

PWR reactors - 58 units

Since the 1970s, Framatome has been the original supplier of EDF for the safety I&C systems of its 58 reactors in France. In 1984, Framatome developed and installed the first digital integrated protection system in the Paluel unit. Spinline, one of the latest of our digital platforms dedicated to nuclear safety I&C, has been developed from this unique experience.

At the end of 2011, EDF renewed its trust in Framatome by choosing Spinline as the technology used for safety I&C systems for the modernization of the 1300MW French nuclear reactors (20 units). For this 14-year project, Framatome is providing the Spinline technology for the Reactor Protection Systems and the Neutron Instrumentation Systems.



Finland

VVER 4400 - 2 units

In 2014, Framatome signed an agreement with Fortum for the modernization of Loviisa NPP I&C systems, which covers mainly the nuclear safety and safety related systems.

The new safety-classified systems delivered by Framatome (including Reactor trip) were based on the Spinline digital safety platform.

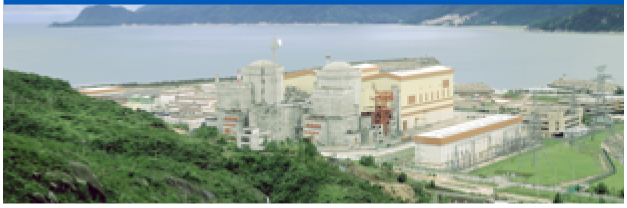
The project, named “ELSA,” was successfully implemented in three phases during 2016-2018.

China

PWR reactors - 35 units

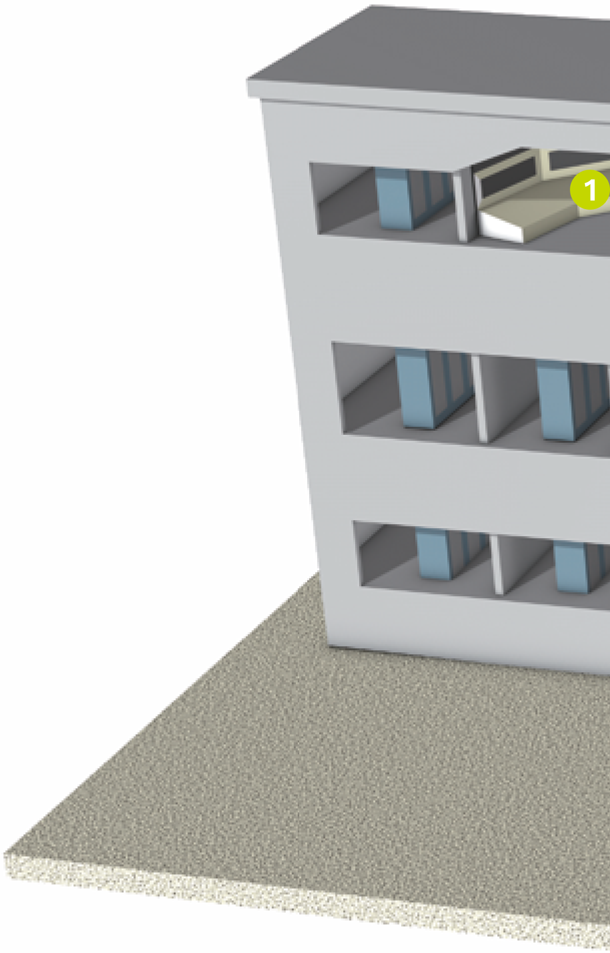
Framatome has supplied safety-critical nuclear instrumentation and core control I&C systems to China since the 1980s. This has involved more than 85% of reactors in operation or under construction in the country – including all the Chinese-designed nuclear power reactors.

The Spinline technology has been chosen by Chinese utilities to be used in Neutron Instrumentation Systems of the CPR1000 fleet (22 reactors).



Main applications

Spinline can be used to implement any nuclear safety I&C.



Designed with flexibility and safety in mind, Spinline meets the most demanding functional and safety requirements of the I&C architectures needed in today's NPPs. This makes Spinline ideally suited for use in systems such as the RPS, ESFAS, I&C for EDG/UDG, Diesel Sequencing System or NIS in both new power plants, and for modernization of existing safety I&C systems in operational plants.

Here are some examples of applications using the Framatome Spinline technology.

Reactor Protection System

It monitors vital reactor operation parameters and in case of emergency, automatically shuts down the reactor and determines the corrective actions to be taken.

All the circuits involved in correcting abnormal situations are activated by the Spinline RPS including:

- Emergency shutdown of the reactor core (which interrupts the nuclear fission reaction by lowering control rods into the reactor core)
- Safety injection
- Start-up of the emergency feed water
- Steam line and feed water line isolation
- Containment spraying and isolation

Neutron Instrumentation System

The Framatome digital NIS uses the neutron flux measured by the excore neutron detectors to permanently monitor:

- Instantaneous nuclear power
- Power fluctuations
- Radial and axial power distribution in the reactor

The Framatome NIS is composed of excore neutron flux detectors (source, intermediate, power and/or wide range, post accident detectors), control and protection processing, ergonomic local or remote Human-Machine Interface (HMI) and actuators.

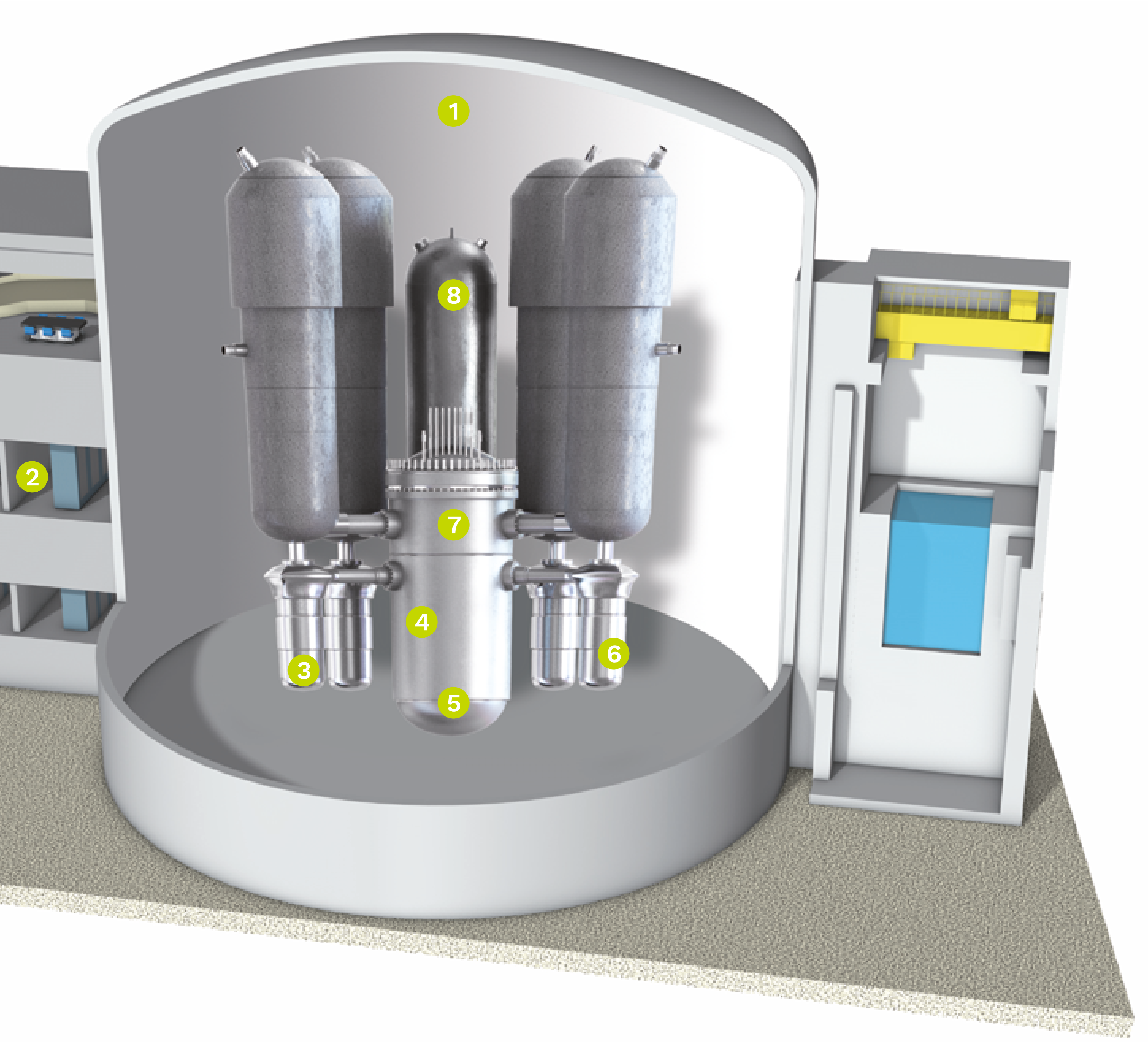
Diesel Sequencing System

The Diesel Sequencing System provides the logic to start the diesel generator set and load the safeguard actions according to pre-established time sequences in the event of loss and subsequent restoration of off-site power. It operates together with the RPS.

The Framatome Diesel Sequencing System is 1E / Cat A qualified and meets international nuclear standards.

When it receives the information about voltage loss, the Framatome Diesel Sequencing System starts the following sequence:

- A command is sent to start up the diesel engine
- When the diesel is ready, the system automatically switches from the mains to the diesel engine
- The power loads are shed
- The power loads are reloaded in a predefined order



1. Reactor Protection System
   Engineered safety features actuation system
   Diesel load sequencing system
   Reactor trip breakers
2. Plant Process Computer
3. Temperature probes Pressure transmitters
4. Neutron Instrumentation System
   Excore neutron detectors
   Reactivity meter
5. Incore instrumentation system
6. Boron meter
7. Rod control system
   Rod position indication system
   Rod position sensors
8. Safety valve control system
   Pressurizer heat control

System development

Framatome has developed Spinline-based application systems considering the overall system life cycle.

Framatome develops Spinline-based nuclear application systems according to high quality processes, consistent with the Framatome Quality Assurance Manual.

These processes comply with international regulations and standards, in particular:

- International Atomic Energy Agency (IAEA) GS-R-3 code (formerly 50-C-QA) and NQSA NSQ -100, for management safety requirements (quality assurance)
- U.S. NRC 10 CFR Part 50, for reporting of defects and non-compliances
- International standards: IEC 61513 (for Systems development), IEC 60880, IEC 60780, IEC 60980

The general principles for managing system development are the following (see diagram below):

- Each system is developed according to a system development lifecycle, embedding software development and equipment development lifecycles
- Lifecycle activities are steered and planned through a project management process
- Safety requirements are taken into account at every development level, implementing suitable specific measures
- Process progress is controlled through scheduled reviews of the development phases (GRSX)
- V&V and Qualification activities are included at all levels of the system development cycle and the technological development
- Rigorous configuration and change management is performed throughout development
- Regulation requirements and contractual standards frameworks are a basis for the system development

Safety system design and V&V life cycle

System requirements specification	System specification	System detailed design & implementation	System integration & validation	System installation & commissioning
• System requirements specification	• System architecture specification	• System detailed design		
	• Preliminary safety analysis	• Safety analysis		
	• Qualification strategy		• Environmental qualification analysis & tests	
	• System validation specification	• System validation development	• System validation	
		• Site test specification	• Site test development	• Site test & commissioning
	• System installation strategy	• Site installation specification	• Site installation design	• Site installation

Equipment design & qualification

Software development and V&V

LSA2
LSA3
P1
P2
P3
CG
Alim.48V/5V-24V
VPP
UC25 N+ LSA
5V
24V

Advanced technology features

Spinline modular features ease the implementation of varied safety functions and architectures.

Spinline provides a set of components suitable to develop better 1E and category A classified I&C systems:

- Software components such as the system software, libraries, the CLARISSE System and Software Development Environment (SSDE)
- Hardware components such as cabinets, racks and boards

These components have been designed according to high-level system requirements in order to easily fulfill customer and regulator's requirements.

State-of-the-art digital technology

Spinline is based on digital technology, making implementation of the functional requirements easier and avoiding the need for specific hardware developments.

The main benefits of the Spinline software-based solution are:

- Functional requirement implementation: Using the Spinline hardware components and the CLARISSE System and Software Development Environment, the development of any kind of I&C function is possible without the need for specific hardware development.
- Stability and accuracy of analog value: once digitized, the analog input signals and triggering thresholds are no longer subject to analog drifts. They do not need further adjustment or calibration.
- Adaptability: Changes in functional requirements can be dealt with at the software level when they do not affect the I/O interface. When I/O changes are needed, the system parameters are adapted accordingly and I/O boards can be added if necessary.
- System supervision: Supervision of the safety I&C system may be achieved without increasing the complexity of the safety classified units. Data available on the safety networks may be used at no additional cost by non-safety classified monitoring stations.
- Automated periodic testing: Spinline provides the suitable features to automate the periodic testing of each function to the largest extent.

Modular and scalable

Spinline hardware and software components are modular and scalable:

- Spinline can fit any size of I&C system, from a simple, one-unit system wtih I/O boards without redundancy, to complex systems having integrated protection system with more than 40 units, redundancy and functional diversity, votes, local and remote testing units.
- Spinline can be delivered either as racks to be integrated into existing cabinets, including in the case of refurbishment, or as full cabinets. The content of the racks and cabinets is adapted to fit the system requirements.

Distributed systems

Spinline components are designed to build distributed systems, i.e. systems where several processing units work together to perform the application functions.

Spinline provides the following types of processing units and communication links:

- Processing units are composed of a rack with a CPU board, input/output boards and network communication interfaces. Processing units may be dedicated: Acquisition Units (AU), Functional Units (FU), and Output Units without vote (OU), or with vote (VU).
- The NERVIA network is the standard communication link within the safety system. It provides safe and efficient data exchange among units. It is deterministic and provides always the same amount of data at the same refresh rate whatever the plant conditions.
- Other links: Gateways are available to Ethernet networks and can be developed to other networks if needed, either on a processing unit or on a standard PC.

Adaptable system architectures

Spinline units and links can combine the two following basic architectural schemes:

- The stream scheme: Units linked by a NERVIA network can work as a stream. For instance, a first unit acquires inputs from sensors and delivers the values to the network. A second unit processes these values and issues results, either directly toward actuators through output boards or on the network toward a third unit (for instance a voting unit).
- The parallel scheme: Units linked by a NERVIA network can work in parallel. For instance, a first unit issues data on the network, and then this data can be processed by two or more units, working in parallel. The parallel scheme is used to split the processing among several units in order to meet diversity requirements. It is also the basic scheme when redundancy is required.

The stream scheme and the parallel scheme are combined, as needed, to build actual system architectures, providing both adequate diversity and redundancy, compliant with the safety I&C requirements.

Redundant systems

Spinline components and distributed capabilities are convenient to build redundant systems.

Spinline provides two kinds of redundancy management:

- Hardware-based active redundancy management: Several separate channels (typically 3 or 4) are composed of one or several units. Output orders from each channel are issued through output boards toward a hardware voting logic.
- Software-based active redundancy management: This is mainly implemented through units receiving data from several channels or divisions, either output units or functional processing units.

Deterministic behavior

Spinline deterministic behavior allows meeting response time requirements and avoiding overload situations:

- Exchange of data among units through networks is pre-defined and systematic (all inter-units data exchanges are configured in fixed tables).
- Due to the asynchronism between the units and the network, the response time is not fixed but capped by a maximum value. The maximum response time for a system is assessed using the max response time of each unit and network.

Spinline determinism guarantees that I&C outputs will always be delivered within the computed maximum response time limit.

Geographical and electrical separation

- The inter-unit communication through NERVIA networks using optical fiber implements electrical and geographical separation within the plant.
- Asynchronous interfaces between the units and networks: The exchanges between units through NERVIA networks are not synchronized at the hardware level or the protocol level. This feature avoids the risk of multiple units hanging due to the failure of a single unit or network. The management of redundant units is easier to achieve as networks work independently of the status of the connected network.
- “1E units / non-1E units” separation: Thanks to the safety properties of the NERVIA network, Spinline allows to totally separate non-1E units from 1E units or, if needed, to permit non-1E units to exchange data with 1E units. Spinline properties ensure that non-1E units can never prevent 1E units from performing their safety function.

Distinct NERVIA networks can be used to have separation of communications according to the safety importance of the data.

Safety-oriented technology

Spinline hardware and software components have been designed to implement safety I&C systems. They include appropriate features to defend (i.e. detect and act) against failures which may occur inside the system due to causes coming from inside or outside the I&C system.

System safety-oriented features:

- For each piece of data processed by Spinline there is an associated validity field which gives the status for this data (“OK” or “Non OK”). Software and hardware components process the data according to this validity information and update its status accordingly.
- Each unit monitors its related units and networks and takes appropriate actions when invalid data is detected. The monitoring is performed according to the expected time-scan of each monitored unit by checking the evolution of specific variables.

Hardware safety-oriented features:

- Output boards provide safety outputs values in case of internal hardware failure, loss of power supply, or detection of CPU scanning disruption (watchdog).
- The CPU clock is monitored against possible frequency drift.

Software safety-oriented features:

- The system software includes appropriate defensive programming to make sure that there are no inconsistencies in the control and data flows. The detection of any inconsistencies would result in a CPU stop. This CPU stop leads to a predefined state of the outputs.
- The application software can include consistency checks and properties assertions in order to defend against possible design or operation faults.

Hardware - Cabinets and racks

Framatome cabinets and racks are designed, manufactured and qualified according to nuclear requirements and standards.

The Spinline hardware is composed of cabinets, racks, electronic boards and cabling, suitable to implement nuclear I&C systems and equipment for new plants or for refurbishment.

The hardware is designed, manufactured and qualified according to nuclear requirements and standards.

Standard cabinets

The cabinets comply with the IEC 60529 standard, protection index IP32 and IK07, and are qualified to withstand seismic stress according to IEC60980. They are designed to be fitted with power supply, racks, cooling fans, input-output cabling interfaces, internal wiring and display devices, and are also designed to withstand temperatures and EMI standards.

Cabinet characteristics:

- Mechanical standard: 19” (38U available)
- Designed to be fitted with 19” racks
- Up to 5 racks per cabinet

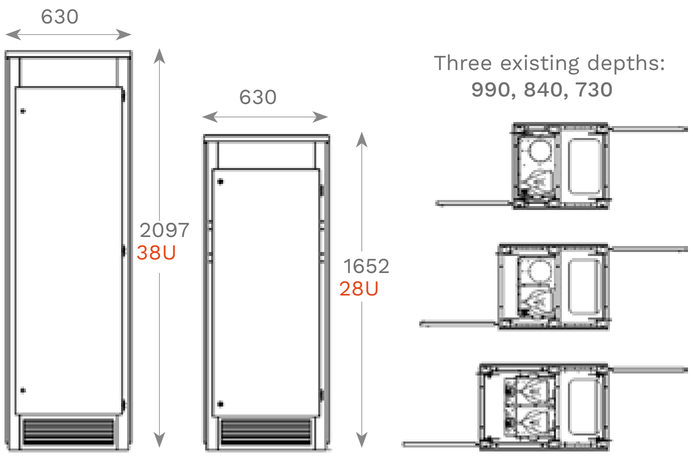
Cabinets can be adapted to specifications:

- Top or bottom wiring
- Mobile terminal block to avoid modifications of wiring in case of modernization
- Retractable lifting rings

A cabinet Includes:

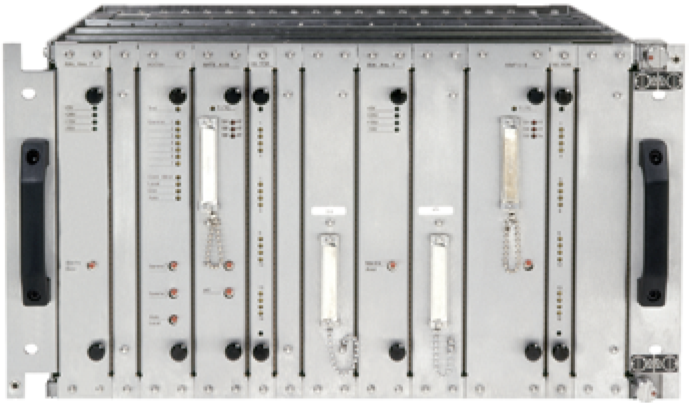
- A frame made of riveted parts
- Side panels and front and rear doors
- The front door is fitted with locks and may be plain or glazed
- Sliding rails for installation of up to 5 racks
- Wiring area accessible through the rear panels
- Roof panel with ventilation slots
- Forced-air ventilation hood with partitioning ceiling panel

The hood is fitted with a high-limit temperature sensor (60°C ±3°C ; 140°F ±5.4°F) and a low-limit rotation fan speed sensor.



Typical dimensions of Spinline cabinet (in mm).

Customized cabinets can also be designed to meet specific customer requirements.



Standard racks

- The 19” 6U racks are designed to withstand the temperatures, EMI, vibrations and earthquakes, defined in applicable standards in force.

They include:

- Frame containing riveted and bolted parts, EMI protection
- One or two printed circuit backplanes with board connectors equipped with keys matching the board type
- Overall dimensions: 482 x 265.5 x 504 mm (W x H x D)

Wiring

The cabinets and racks are designed to facilitate connections with the process, with standard connections and pre-defined customer wires and terminal blocks.

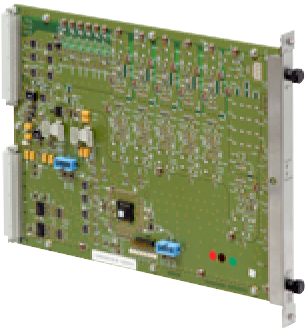
Security and safety

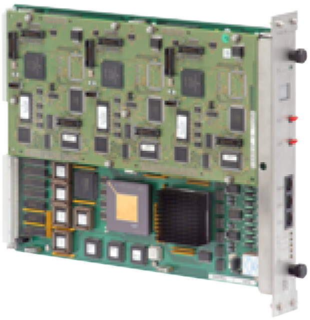
Spinline cabinets feature:

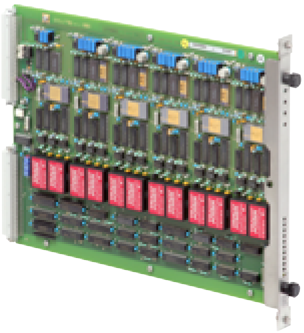
- Door opening detection and alarm mechanisms
- Monitoring of the fan system good health
- Monitoring of the power system good health

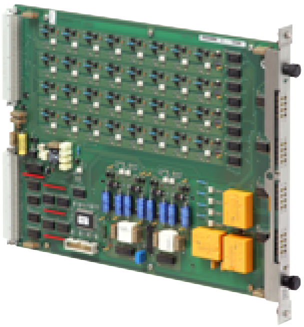
Hardware - Electronic boards

Electronic boards designed for safety.









The systems designed and manufactured by Framatome use:

- Digital processing boards (Spinline)
- Signal acquisition boards
- Signal conditioning boards
- Dedicated electronic boards

The complete range includes additional boards for power supply, output relays, etc. All have been designed to fit in the standard racks and cabinets developed by Framatome for the needs of safety nuclear I&C.

Spinline electronic boards communicate through a dedicated proven parallel communication bus on the backplane boards.

Designed by Framatome for nuclear applications, this bus is a simplified and secured version of the standardized VME bus. Multimaster capability and bus arbitrator have not been implemented to achieve simplicity and deterministic objectives.

Safe behavior on failure detection

Output boards can set their outputs to predefined safe values on detection of failure conditions. Watchdog timers automatically switch outputs when the CPU has failed to issue new values within a predefined time period.

Support for periodic testing

Spinline provides on-boards means to easily switch to signal generated/checked by an extense tester thus increasing the ease of the automatic coverage of periodic testing.

Failure Modes and Effects Analysis (FMEA) and reliability analyses

As Spinline components have been designed to meet nuclear safety requirements; FMEA and reliability analyses have been performed on all electronic boards.

Easy and safe operation

The boards are fitted into the rack which is connected to the wiring at the back of the cabinet.

They can be inserted and removed without interfering with the connections at the back and can be replaced while the system continues to operate. Furthermore, it is impossible to replace one type of board with a different one, thus preventing human error.

Main type of boards

Processor and communication boards

- CPU board UC25, 6 NERVIA ports, 2 LSA
- Nervia gateway boards (NERVIA GW) allow unidirectional transfer from NERVIA network to Ethernet networks (Modbus TCP or UDP, other protocols on demand)
- 10 Mbits Hub board dedicated to a NERVIA use, with 8 Ethernet Ports, 6 twisted pairs & 2 optical fibers
- PCI NERVIA board, installed on a computer with PCI, connecting 4 Ethernet NERVIA points and a PCI bus

Power supply boards

- 24 V power supply board "I.ALIM 24 V": this board generates a regulated DC voltage

Standardized input / output boards

- 32 binary signal acquisition
- 16 analog signal acquisition
- 32 binary output for signaling
- 32 binary signal output for relays & actuators control
- 12 analog signal output

Neutron flux acquisition boards & modules

- Detector acquisition: Source range (pulses), intermediate range (current with gamma correction), power range (only one board for power detectors with 2 or 6 vertical sections), AHT1/B, AHTS4/B
- Wide Range Conditioning module for wide range or post accident (US NRC RG 1.97) channel

Dedicated boards

- Counting rate acquisition
- Temperature acquisition (themocouple & PT100)
- Collectron signal acquisition
- Specific input / output boards

Hardware tools to facilitate operation and maintenance

Spinline has been designed to minimize the operation and maintenance work load of NPP staff.

A set of dedicated tools, operated by standard industrial PCs and offering a user-friendly Human-Machine interface, helps operators to perform system monitoring and maintenance.

Local display unit (LDU)

Using this unit you can check and set processing parameters according to stipulated ranges and through a secured protocol.

Parameters and values may be checked and set individually or loaded as a group for efficient configuration of a new unit.

The LDU is a laptop with dedicated software, loaded with Spinline system data.

Monitoring and maintenance unit (MMU)

The MMU continuously checks that components and data are correct in the Spinline systems. It immediately signals if events requiring attention occur in the system.

Some typical events are:

- Sensor, board or power supply hardware failures
- Spinline cabinet door open
- Signal or parameter values inconsistent between different redundant channels

The system helps locate default causes and starts corrective maintenance. It also maintains an event log file with printing and archiving features.

The MMU is a rack-mounted industrial computer running Windows Server 2019 with a 15" LCD display, keyboard, CD-ROM, NERVIA network ports and digital output for remote alarm signaling.

Automatic testing unit (ATU)

With this unit, maintenance teams can carry out all the testing required on the safety systems, either online during full power operation or off-line during outages.

It includes state-of-the-art functions to:

- Define test sets
- Graphically display data during the test phase
- Analyze and archive the test results

The ATU is available as a rack-mounted unit fitted within the safety system cabinets or as a mobile unit that can be shared by several systems. The ATU includes an industrial computer running Windows with LCD display, keyboard and printer.

Software

Spinline software design is compliant with the safety requirements of the nuclear industry.

The Spinline software is composed of two major components:

- The Operational System Software (OSS) is standard and comes as a software component to be used on the CPU boards of the processing units. It provides the necessary basic functions to ensure communication, data acquisition, data emission and services to be used by the application software.
- The application software is specific and is developed for each project. It implements the I&C application functions fitting the requirements of the I&C system.

The CLARISSE System and Software Development Environment, a dedicated software workshop, provides the software tools and libraries needed to perform the configuration of Spinline Processing Units and Nervia Networks as well as the development of the customer-specific application software.

Operational System Software

The OSS is a minimum complexity software layer that interfaces between the local and remote data delivered by the I/O and communication link boards, and the application software.

It also performs the continuous testing of the hardware, and provides services to the application software.

The system software has been developed and validated according to nuclear standards for software based 1E-safety systems, in particular IEC 60880.

The adaptation of the OSS to the application needs is performed by using the configuration tools of the CLARISSE System and Software Development Environment.

These tools allow the designer to configure the data flowing through the NERVIA networks and the I/O boards of the processing units.

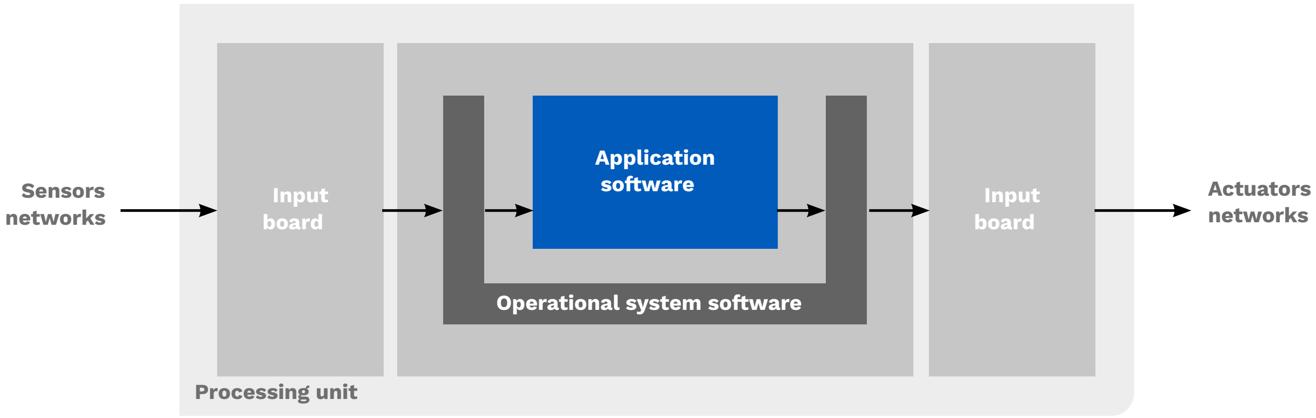
Application software

The application software performs the application functions. Spinline application software is dedicated to safety I&C monitoring, control and protection functions.

Main characteristics:

- Top / down design: The design of the application program starts with an upper level view and proceeds through refinement steps for both the functions and the data. Relevant details are added at the appropriate level (information hiding concept).
- Dataflow organization: The program is entered as a set of function blocks connected by wires, flowing from the input data on the left to the outputs orders on the right. The wires convey data according to data types, the function blocks transform data by means of Boolean operators, numeric operators or by means of functions.
- Single task: The application program associated with the system software runs as a single continuous program loop. One loop execution is called a scan. At each scan, outputs are computed from a fixed image of inputs and from relevant results of the previous scans. There is no processing performed under interruption and no multitasking is possible. This avoids potential deadlocks, resources sharing and overload problems. It helps demonstrate the fulfillment of the response time requirements as well as the simplicity of the software design.
- Synchronous approach: The application program is designed to meet the synchronous hypothesis, i.e., the program reacts to input events within a predefined and controlled time frame.

The Spinline CPU board offers enough computing power to fit the processing needs of typical I&C protection functions in the nuclear field. Moreover, the dataflow organization of the program makes the CPU load quite independent from the actual values of the inputs.



Processing unit: Hardware/Software architecture

The System Software Development Environment (SSDE)

The SSDE is used to automatically configure system software, networks architectures, network stations and information exchange between units.

- **Input of the I&C functions:** I&C functions are described, using a graphic design based tool called SCADE (Safety Critical Application Development Environment). This language provides block diagram formalism based on rigorous textual and graphical syntax and well-defined semantics. SCADE is user-friendly and does not require specialized programming skills.
- **Simulation of SCADE specification:** Simulation is possible from the early stages of the application design.
- Through it, designers can check the actual behavior of their specification.
- It can also be useful during the testing and validation phases, for checking additional functions of the final specification.
- **Automated code generation.**
- **Verification and validation:** Each software design step is checked using appropriate tools.
- **Documentation production:** Most documents are automatically generated.
- **Software configuration management.**

The software development methodology is based on IEC 60880 standard

The development methods comply with the software development cycle of the standard and result in specific documents and reviews at the end of each phase. A separate verification and validation team is setup to:

- Check specifications, design and coding
- Perform the formalized critical component test
- Validate the software

This methodology is aimed at detecting errors early on and obtaining the required quality level without exceeding planned costs and schedules. The number of residual errors observed during software validation is extremely low.

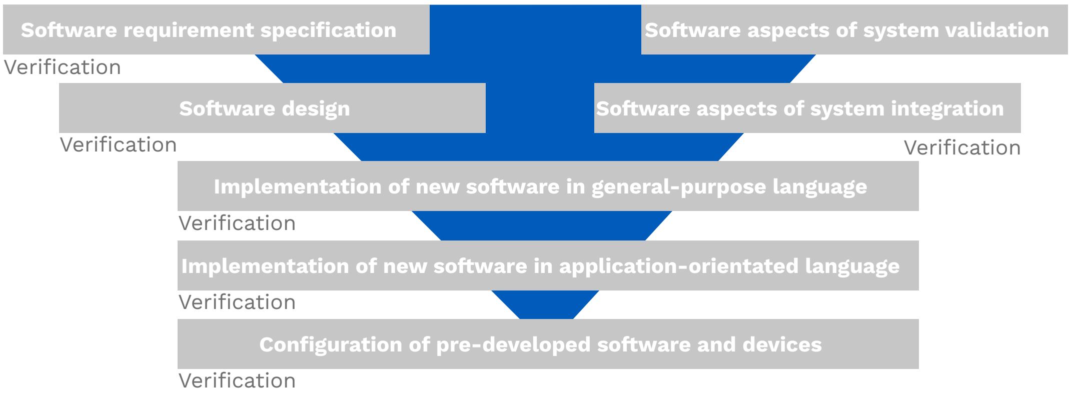
Software engineering tools

Throughout the entire system and software development cycle, Spinline uses a set of tools to ensure software quality.

- **Software development tools:** Guarantee a coherent overall application.
- **Code checking tools:** Measure the quality of the software built complexity, comment rate, etc.
- **Unit test tools:** Use “white box” and “black box” approaches to check coding against specifications as early as possible in the process.
- **Software integration and validation tools on target rack:** Allow developers to test the entire software application in the final environment (each individual element has already been tested).
- **Flash component production tools:** Ensure the consistency between the previously tested software and its storage in REPROM electronic components.

Human-Machine Interface

To ensure maximum safety we mainly offer relay and wire-to-wire based components to control the system (inhibition, manual controls preparation of periodic tests, etc.). A digital classified HMI can be implemented for specific needs.


Software requirement specification
Verification
Software aspects of system validation
Software design
Verification
Software aspects of system integration
Verification
Implementation of new software in general-purpose language
Verification
Implementation of new software in application-orientated language
Verification
Configuration of pre-developed software and devices
Verification

Development activities of the IEC 60880 software safety lifecycle

NERVIA

Communication network for category A and class 1E functions.

NERVIA is a unique safety classified network, providing efficient, safe and secured data communication within the safety I&C system.

NERVIA simplifies and secures wiring

- Saves hundreds of point-to-point wires and dozens of point-to-point communication links
- Uses shielded foiled twisted pairs and optical fibres
- Links racks inside cabinets, cabinets inside safety equipment, safety equipment inside plant I&C and the control room
- Reduces wiring installation and maintenance costs, thanks to much fewer physical links
- Increases wiring reliability, as links which had to be previously tested at periodic intervals are now replaced by full continuously self-tested NERVIA links

NERVIA is a key component in the design of cat. A and class 1E compliant architectures

- Makes safety I&C system design easier:
  - Redundancy adapted to meet the single failure criterion
  - Functional diversity implemented in separate processing units
  - Geographical and electrical isolation between channels
  - Deterministic response time under all plant conditions
  - Communication capabilities with non cat. A and class 1E systems
- The hardware meets the cat. A and class 1E qualification nuclear standards.
- The protocol and software is fully compliant with IEC 60880 requirements.

NERVIA is a secured network

- The protocol is simple and dedicated to I&C systems.
- Processing units cannot write outside their own network memory space.
- Data communication layouts are predefined using the CLARISSE SSDE and burned into the flash memories of the related processing units. No changes to theses layouts are possible during plant operation.
- With NERVIA, virus contamination and remote write access to safety data is impossible.
- Failures within NERVIA networks, whether intentional or unintentional, are instantaneously detected by all active stations, wich may then trigger the appropriate safety actions.

NERVIA is dedicated to safety sritical “hard real time” I&C

- Dataflow driven communication (not event driven): Each station periodically sends the values of a predefined set of variables. Dataflow driven communication is perfectly adapted to the requirements of I&C systems.
- Static data block description (not dynamic data blocks): Application data are organized into coherent blocks, fast for scan by scan transmission, or slow for transmission over several scans. Static data blocks provide steady network traffic, regardless of plant conditions.
- Determinism based on a time-based scheme: Each station has a predefined order in the network scan, with an allocated fixed time window for network access, regardless of the other stations status – ok or not ok. This time-based scheme with static data blocks provides deterministic scan times.
- Broadcast protocol (not point-to-point protocol): Each message transmitted by a station is received by all other stations on the network. A broadcast protocol facilitates redundant architecture design and results in graceful degradation mechanisms.
- Fault tolerant features:
  - NERVIA protocol is fully deterministic and not subject to any interrupt
  - NERVIA protocol is fully distributed, so there is no need for static or dynamic master stations
  - NERVIA stations and media are continuously self-tested
  - NERVIA station behavior is safety oriented in case of internal failure or network abnormal conditions
  - NERVIA station power on/off is smooth and has no influence on the network scan

NERVIA can allow access to non-safety systems

- Safety NERVIA networks may be connected to non-safety equipment such as industrial computers through a NERVIA gateway.
- Communication with other equipment such as PLCs or monitoring system is possible using the Spinline NERVIA gateway board. After a simple configuration, this module allows the transmission of information exchanged on NERVIA networks to other networks based on MODBUS TCP/IP protocol.

Security

Computer security approach for Spinline.

Framatome I&C follows a strict computer and information security program based on general & nuclear specific norms, the Framatome group processes and state-of-the-art technologies.

Spinline is designed specifically for nuclear applications and features secure development and operational environments. It provides protection against unauthorized modifications and implements design requirements that promote integrity and reliability during design, operation and maintenance.

Framatome development environment is protected thanks to general security principles:

- Physical and environmental security: physical access restrictions and monitoring
- Human resource security: employee and contractor references are checked and NDAs must be signed
- IT systems access control: use of networks, applications and IT systems are restricted and monitored

Spinline specific procedures are in place during development, tests and installation:

- Software life cycle processes prevent and detect unauthorized modifications:
  - Strict design control process; configuration management system with traceability; independent V&V and testing
- Spinline software does not include unwanted functions:
  - Proprietary OSS performs only limited functions; the specific application software cannot modify the OSS; the communication network is Framatome proprietary “NERVIA” network
- Integrity of Spinline code is checked upon initialization and each processing cycle:
  - Software loaded on flash memory; checksum regularly verified
- Spinline hardware incorporates failure detection and has a proven high reliability record

During operations, test and maintenance, specific procedures are also implemented:

- Production code alteration requires physical access and removing the main processor board from its rack, which is limited by administrative control, moreover opening cabinet door causes an alarm
- There is no way for remote access to a Spinline system:
  - NERVIA protocol does not allow dynamic modification; adding a machine to modify data or remove one node is immediately detected; one-way communication to external system is implemented with hardware
- Only local access is available for maintenance and testing of a Spinline system:
  - Physical access is required; allowed actions are pre-defined and limited

Framatome I&C computer and information security program is based on ISO 27001, 27002 and nuclear specific guides such as IEC 62645, 62859, IAEA NSS-17 and NRC RG 1.152.

Moreover, continuous training programs are in place to increase the expertise and number of our specialists to be able to provide a specific approach adapted to our customers.

Standards

Spinline is certified by the main international safety authorities (France, China, Finland, US, Czech Republic, etc.).

General safety requirements

International	**IAEA GSR part 2**	Leadership and management for safety (2016)
	IAEA SSG-30	Safety classification of structures, systems and components in nuclear power plants (2014)
	IAEA SSR-2/1	Safety of Nuclear power plants: Design
	IAEA SSG-2	Deterministic safety analysis for nuclear power plants
	IAEA SSG-39	Design of instrumentation and control systems for nuclear power plants
	IEC 60671	Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing
	IEC 60812	Analysis technique for system reliability. Procedure for failure mode and Effect Analysis
	IEC 61226	Nuclear power plants – I&C systems important to safety – Classification of I&C functions
	IEC 61227	Nuclear power plants – Control rooms - Operator controls
	IEC 61500	Nuclear power plants – Instrumentation and control important to safety – Data communication in systems performing category A functions
	IEC 61513	Nuclear power plants – I&C systems important to safety – General requirements for systems
US	**10 CFR 50**	General design criteria for nuclear power plants (appendix A)
	NUREG 800, chap.7	Standard review plan for the review of safety analysis reports for nuclear power plants
	IEEE 338	Standard for criteria for the periodic surveillance testing of nuclear power generating station safety systems
	IEEE 603	Standard criteria for safety systems for nuclear power generating stations
Europe	**RCC-E**	Design and construction rules for electrical and I&C systems and equipment
	RFS	Fundamental safety rules for nuclear reactors
	CRT	Technical rules file (EDF)

Specific hardware design requirements

International	**IEC 60960**	Functional criteria design for a safety parameter display for nuclear power stations
	IEC/IEEE 60780-323	Nuclear power plants – Electrical equipment of the safety system – Qualification
	IEC/IEEE 60980-344	Nuclear Facilities – Equipment Important to safety – Seismic qualification
	IEC 60709	Nuclear power plants – Instrumentation and control systems important to safety – Separation
	IEC 60068-2	Environmental testing
	IEC 60987	Hardware design requirements for computer-based systems
	IEC 62808	Nuclear power plants – Instrumentation and control systems important to safety – Design and qualification of isolation devices
	IEC 62566	Development of HDL-programmed integrated circuits for systems performing category A functions
	IEC 62566-2	Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits for systems performing category B or C functions
	IEC 61000-4 series	Electromagnetic compatibility
US	**IEEE 308**	Standard criteria for class 1E power systems for nuclear power generating stations
	IEEE 379	Standard application of the single-failure criterion to nuclear power generating station safety systems
Europe	**EN 50081-2**	Electromagnetic compatibility – Generic emission standard
	EN 50082-2	Electromagnetic compatibility – Generic immunity standard
	EN 55011	Industrial , scientific and medical (ISM) radio frequency equipment – radio disturbance characteristics – limits and methods of measurement

Specific software design requirements

International	**IEC 60880**	Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions
	IEC 62138	Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions
US	IEEE 7-4.3.2	Standard criteria for digital computers in safety systems of nuclear power generating stations
	NRC 1.152	Criteria for use of computers in safety systems of nuclear power plants
	NRC 1.168	Verification, validation, reviews and audits for digital computer software used in safety systems of nuclear power plants
	NRC 1.169	Configuration management plans for digital computer software used in safety systems of nuclear power plants
	NRC 1.170	Software test documentation for digital computer software used in safety systems of nuclear power plants
	NRC 1.171	Software unit testing for digital computer software used in safety systems of nuclear power plants
	NRC 1.172	Software requirements specifications for digital computer software used in safety systems of nuclear power plants
	NRC 1.173	Developing software life cycle processes for digital computer software used in safety systems of nuclear power plants
Europe	RFS	Software for safety systems

Hardware qualification

Spinline equipment qualification using international standards.

Spinline equipment is tested and validated in accordance with international standards. The following examples correspond to the IEC standards. For any questions regarding the qualification of our equipment with any other standards, do not hesitate to contact Framatome.

Typical environmental tests

Test	Severity
Combined temperature and voltage	min. temp.: 5°C (41°F)
Variation	Maximum board temperature: 55°C (131°F)
Maximum cabinet temperature.	40°C (104°F)
Humidity	93% RH at 40°C (104°F)

Robustness tests

Robustness tests are carried out to evaluate the performance of hardware over a period of time. They are performed in the following order:

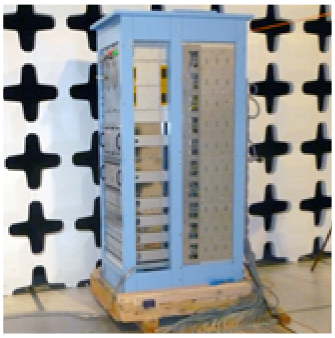
Test	Standard	Severity
Connections & disconnections	CRT 80.C.012.01	Connectors 50 times
Vibrations	IEC 60068-2-6 test Fc 1 g	10 to 500 Hz 10 cycles
Fast temperature variation	IEC 60068-2-14 test Na	-25°C +70°C (-13°F +158°F) 5 cycles
Dry heat	IEC 60068-2-2 test Bb	16 hours 70°C (158°F)
Moist heat	IEC 60068-2-30 test Db	two 24-hour cycles max. temp.: 55°C (131°F)
Cold	IEC 60068 2-1 test Ab	-25°C (-13°F) 16 hours

Seismic qualification

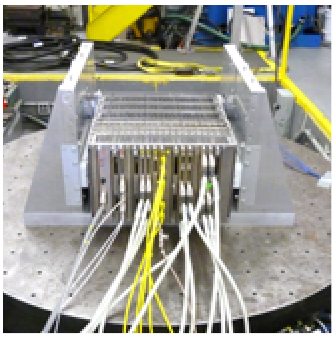
Seismic tests are conducted according to the dual-axes method. The level and spectra of applied accelerations are oversized to cover the required spectrum at the site location.

Test	Standard
Seismic tests	IEC 60980
Recommended practices for seismic qualification	IEC 68-2-6
Seismic tests method and time history method	IEC 68-3-3 or IEC 68-2-57

The analysis is used to validate the configuration. Findings from previous tests performed on similar hardware configurations are examined. These qualifications comply with IEEE 323 and IEEE 344.



Qualification – EMC tests.



Qualification – Seismic tests.

Electromagnetic compatibility

Spinline has been designed to withstand high levels of disturbance which is particularly important when modernizing existing NPPs and Research Reactors.

Spinline complies with the tests and levels in IEC 61000 standards, as far as both immunity and emission are concerned.

Immunity

The generic immunity standard IEC 61000-6-2 applies. This standard includes:

Standard	Field	Level	Criterion
IEC 61000-4-2	Withstand to electrostatic discharge	3	A
IEC 61000-4-3	Electromagnetic fields immunity test	3	A
IEC 61000-4-4	Fast transients immunity test	3	A
IEC 61000-4-5	Surge immunity test	2	A
IEC 61000-4-6	Conducted disturbances induced by radio frequency fields	3	A
IEC 61000-4-8	Power frequency magnetic field	3	A
IEC 61000-4-12	Ring wave immunity test	2	A
IEC 61000-4-18	Damped oscillatory wave	2	A

Level 2: with implemented additional outside protection, level 3 or above is reached.

Emission

The generic immunity standard: EN 50081-2 applies. This standard includes:

Standard	Field	Class
EN 55011/EN 55022/ CISPR 11	Radiated emissions in the frequency range 30-1000 MHz	A
EN 55011/EN 55022/ CISPR 11	Conducted emissions in the frequency range 0.15 – 30 MHz	A

Software qualification

Spinline software strictly adheres to IEC 60880 requirements and recommendations.

Our software is tested and validated in accordance with international standards. The following examples correspond to the IEC standards. For any questions regarding the qualification of our software with any other standards, do not hesitate to contact us.

IEC 60880 is a set of requirements and recommendations applicable to the highly reliable software required for computers to be used in the Safety Systems of Nuclear Plants for Class 1, Category A Safety Functions.

Part 1 of IEC 60880 gives requirements and guidelines on safety, simplicity and maintainability:

- Safety
  - Development process aimed at producing "error free software"
  - Safety-oriented features
  - Defensive programming
  - Deterministic behavior
  - Hardware and software supervision
- Simplicity
  - Avoid unnecessary features and functions
  - Avoid using interrupts
  - Avoid complex operating systems
- Maintainability
  - Prefer application-oriented languages
  - Use software tools
  - Use understandable formalisms

Part 2 of IEC 60880 gives additional requirements:

- Defense against common mode failure
- Software tools
- Qualification of pre-existing software

IEC 60880 mandatory requirements are expressed with "shall" and recommended practices are expressed with "should."

Spinline has been designed not only to comply with all applicable "shall" requirements, but with all applicable "should" recommendations too, thus enforcing safety, simplicity and maintainability within all Spinline software-based components.

Because Spinline strictly adheres to IEC 60880 requirements and recommendations, we provide our customers with the following exclusive safety features:

- Full renewability of all software components
- Unequalled simplicity of the embedded software at system and application level
- Deterministic behavior of safety networks and units
- Ability to meet dedicated safety application function needs with standardized equipment

System functional validation

Independent tests are performed on cabinets and on all systems linked together before being delivered to customers.

The qualification activities including the validation activities are performed on all stages of the system development life cycle. Among these activities, the functional validation of the system is one of the most important phases involving both Framatome and the customer.

After Spinline hardware and software have been individually tested and validated, the whole integrated system is tested and validated in accordance with international standards. As stated in IEC 61513, the objective is to demonstrate compliance with:

- Functional specifications
- Performance requirements
- Interface specifications

During this process, the cabinets to be delivered are incrementally gathered in Framatome premises on an interconnected platform and coupled with test means.

When multiple systems are provided, the functional validations are performed in two stages: first on cabinets of a same system (first test stage), and then on all the systems linked together (second test stage).

For class 1 system or category A & B functions, the so-called interconnected tests are performed by the system V&V team that is not involved in the design and development.

Individual system functional validation

For the first test stage (each system tested individually), the main objectives are:

- Tests of all the system functions defined in the functional diagrams at system level. The tests cover all signal ranges, and the ranges of computed or calculated parameters in a fully representative manner
- Measurement of the system response time (Acquisition – Processing – Vote – System output activation)
- Measurement of the system accuracy (Acquisition – Processing – System output activation)
- Tests of embedded displays and monitoring features
- Test execution of periodic tests procedures
- Test execution of maintenance procedures
- Tests of systems behavior in degraded mode or in case of failure
- Endurance tests

Functional validation of several systems

For the second test stage (all systems linked together), the main objectives are:

- The tests of the electrical and software interface compatibility between each system, which include:
  - – All input / output system interfaces (digital, analog and network) hardware allocation
  - - Electrical range for all digital and analog signals shared between systems
  - - Software compatibility especially for Network protocols
- The tests of functions involving more than one system
- The measure of global response time (Acquisition – Processing – Vote – Actuators interface activation and / or Display / Alarm activation)
- The measurement of the global accuracy (Acquisition – Processing – Actuators interface activation and / or Display / Alarm activation)
- The functional specifications (including behavior in case of failure)

Proven test methods and tools

To achieve all these tests on the first-of-a-kind of the delivered systems, Framatome has developed proven configurable and qualified tests methods and tools that allow the creation of complex test scripts.

Our test benches can exercise the systems under test by static and dynamic simulation of input signals present during normal operation, anticipated operational occurrences and accident conditions.

Each execution of a test script generates an automated logbook which includes the final results and log information necessary to locate malfunctions.

> Framatome has developed proven and qualified test methods and tools to create scripts able to test the most complex configurations

MSA

Long-term services

Spinline technology is supported throughout the life cycle of the I&C systems.

Spinline offers ideal conditions for long-term and low-cost maintenance, both for future extensions and functional improvements to your I&C systems.

Framatome understands the regulatory requirements and commercial pressures faced by utilities.

Utilities need to maximize production efficiency, keep plants operating safely and reliably for longer periods of time, minimize downtime and have reliable support available on short notice.

Framatome is committed to maintaining the capability to manufacture, modify, repair and test at the board, rack and system level over a long time period. This means finding solutions to hardware aging, technology evolution, skills training and tools maintenance.

Framatome's long-term support services for nuclear I&C include:

- Obsolescence management
- On-site maintenance and repairs
- Spare parts management and supply
- Operator training
- Upgrade management
- Modification and retrofit

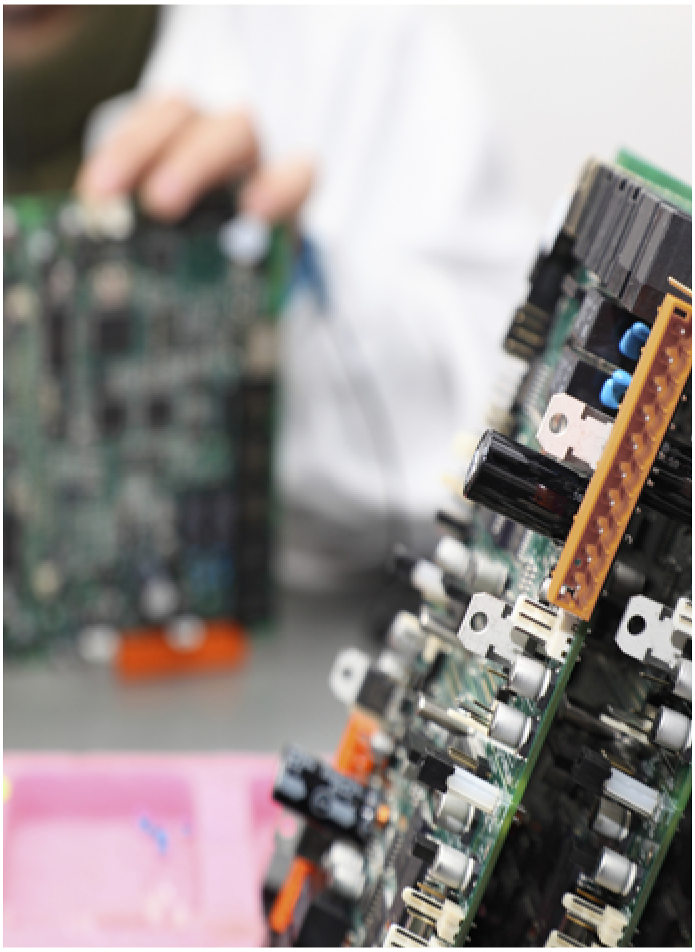
Framatome ensures all these services for its Spinline technology.

Example: Long term maintenance of electronic boards

For 30 years after commissioning, Framatome will continue to provide the same boards or equivalent solutions to replace those in operation and for testing. This means that testing equipment is maintained for the same period of time, along with the knowledge and skills of our testing machine operators.

Since Framatome has been working in the nuclear industry, we have provided NPPs throughout the world with over 2 million boards. We get constant feedback from our customers and our own field engineers, enabling us to constantly update our technology. This feedback associated to our statistical analysis skills, allows us to provide customers with the optimal number of on-site replacement boards.

Finally, our training policy guarantees that skilled engineers will assist and help you when necessary.



Cost effective maintenance for NPPs

Framatome is an international leader in nuclear energy recognized for its innovative solutions and value-added technologies for the global nuclear fleet. With worldwide expertise and a proven track record for reliability and performance, the company designs, services and installs components, fuel, and instrumentation and control systems for nuclear power plants. Its more than 15,000 employees work every day to help Framatome's customers supply ever cleaner, safer and more economical low-carbon energy. Visit us at: www.framatome.com, and follow us on Twitter: @Framatome_ and LinkedIn: Framatome.

Framatome is owned by the EDF Group (75.5%), Mitsubishi Heavy Industries (MHI – 19.5%) and Assystem (5%).

Scan the QR code to browse our solutions by market area.

framatome

Framatome
Tour AREVA. 1 Place Jean Millier
92400 Courbevoie, France

ic@framatome.com
www.framatome.com