Spinline 3 E-DCIS Platform Family
ECCS/ESF

- Presenter Jean-Michel Palaric/Neil Midkiff
- Date July 26-27, 2006

SPINLINE 3 E-DCIS Platform Operational Experience

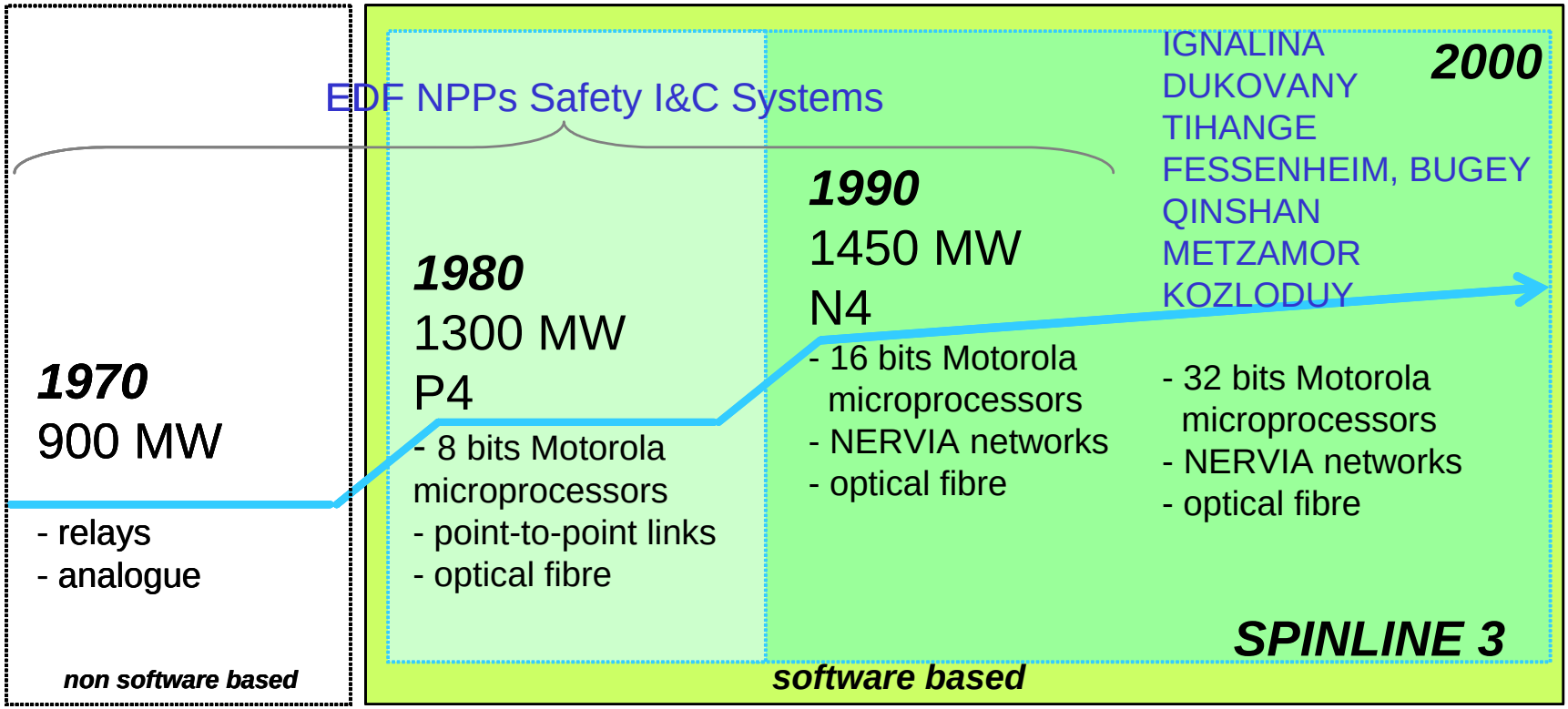
- *SPINLINE 3* is a 3rd generation safety-related E-DCIS platform from DS&S
- This design benefits from the extensive DS&S nuclear I&C installed base:
  - > 613 I&C systems in 97 nuclear units worldwide
  - > 105 safety-related E-DCIS (RTS, ESF, NMS) in 43 nuclear units
- *SPINLINE 3* characteristics fully support the ESBWR design
  - > *SPINLINE 3* was designed from the beginning as a nuclear safety-related platform
  - > Hardware components have no built in redundancy or unnecessary functions
  - > Software is designed and verified according to state of the art nuclear standards
  - > Easily adapted to implement the ECCS – ESF system architecture
  - > Fully diverse from all other platforms, supporting D3 requirements

SPINLINE 3 E-DCIS Platform Operational Experience

- *SPINLINE 3* design conforms to international nuclear licensing standards
  - > Qualification for NRC certification was independently assessed by EPRI/MPR as documented in EPRI TR-1012574, September 2005, in accordance with EPRI TR-107330:
    - – "The SW development process appears to comply with 10CFR50 App B and NUREG0800 Chapter 7, HICB BTP-14" (will comply with ESBWR requirements)
    - – EMC and seismic testing will be supplemented to meet ESBWR requirements
    - – Will comply with ESBWR requirements
  - > DS&S is collaborating with GE to issue a Licensing Topical Report to support SER

- DS&S supports its DCIS customers with Long Term Service Agreements (LTSA's)
  - > DS&S LTSA's have supported all vintages of the DCIS product line for 30 years
  - > DS&S has a unique LTSA to provide DCIS support for all 58 EDF Units

DS&S Safety-Related DCIS History



Reactor units	**20 units**	**4 units**	**17 units**
Cumulated operation (years)	**360 years**	**40 years**	**50 years**

DS&S Safety-Related E-DCIS Reliability

- *SPINLINE 3*
  - > 50 cumulative years operation
  - > 6,000 electronic boards and components

- *SPINLINE family*
  - > EDF P4 & N4 units
  - > 400 cumulative years operation
  - > 41,000 electronic boards and components

- All systems meet their initial safety target
  - > Failure to initiate trip: 0 (typical objective is probability < 10E-5 on demand)
  - > Spurious trips due to DCIS: 0
  - > Operational component reliability (failure rate/hour): 7.0 E-07
  - > (CPU 2.0 E-06, Analog input 2.0 E-06, Binary input 5.0 E-07, Binary output 2.0 E-07)

SPINLINE 3 Overview
The Latest DS&S Nuclear DCIS Platform

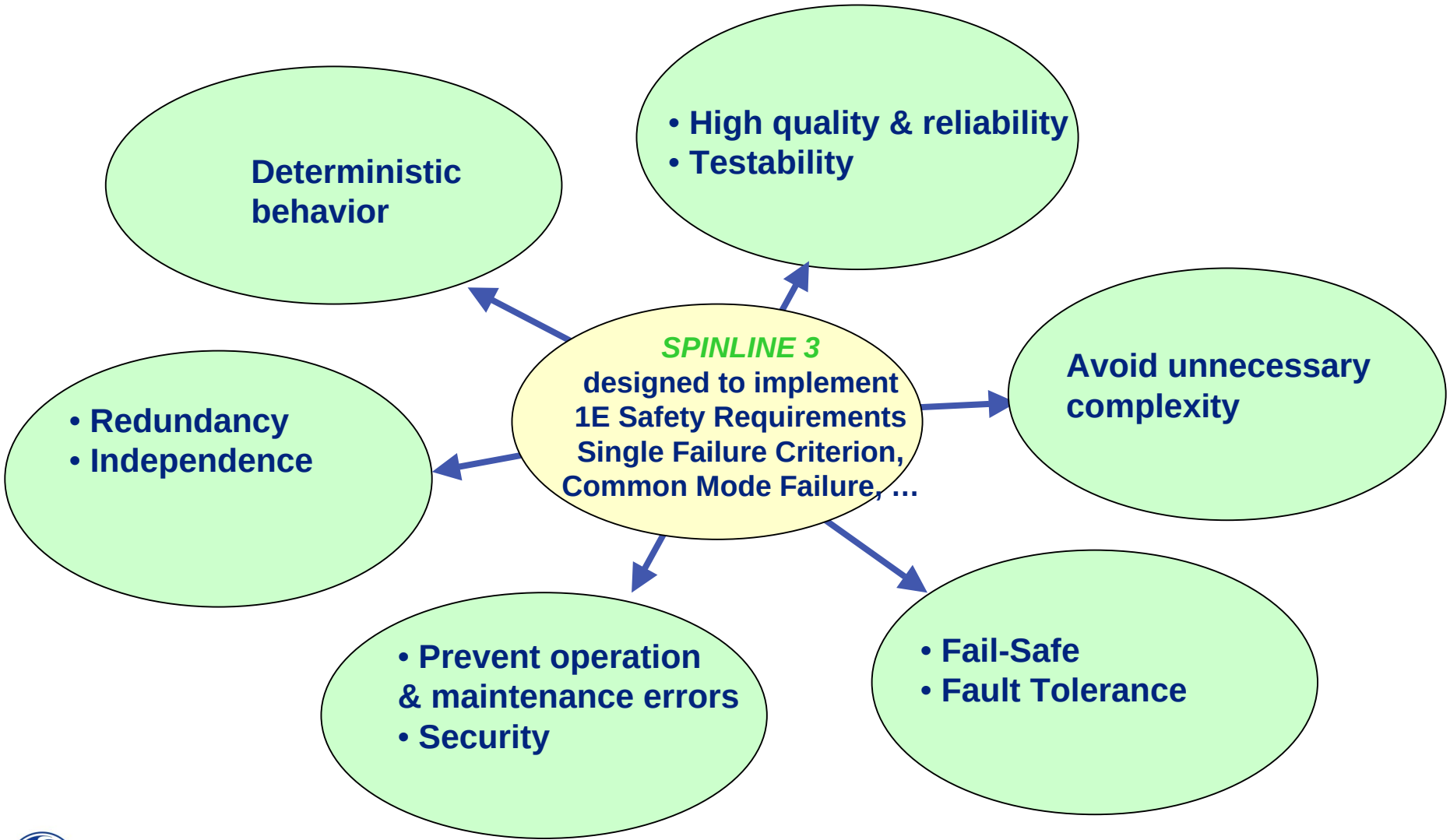
- A Digital Safety-related Instrumentation and Control platform

- Built from the beginning to implement Nuclear Safety Functions

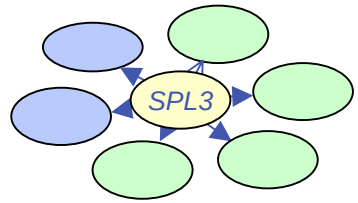
- The result of more than 25 years of DS&S experience in safety-related digital I&C, accumulating 450 reactor years of operation

- Characterized by:
  - > safety-related and availability oriented design criteria
  - > high quality hardware and software components
  - > strict and efficient development methodology

SPINLINE 3
Designed To Nuclear Safety

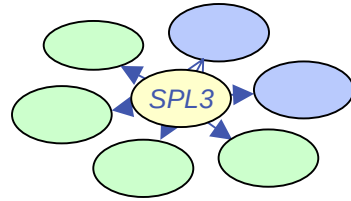


SPINLINE 3
Main Design Criteria (1)



- Deterministic behavior
  - > Cyclical “single loop” processing units and networks
  - > SPINLINE 3 architectures meet response time requirements permanently under any load conditions
- Redundancy is implemented at system level, not at component level
- Independence
  - > The NERVIA network can link processing units from separate divisions while meeting the separation requirements
  - > NERVIA can also interface processing units of safety-related systems to processing units of non safety-related systems

SPINLINE 3
Main Design Criteria (2)

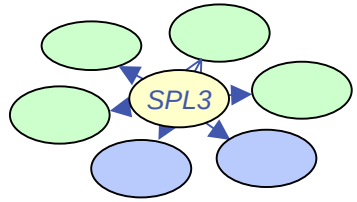


- High quality and reliability
  - > SPINLINE 3 components are designed and implemented to the requirements for safety-related systems

- Testability
  - > The hardware is designed for easy implementation of on-line periodic testing
  - > The processing units and networks include permanent hardware self-supervision

- Avoid unnecessary complexity
  - > Hardware & Software are designed to avoid complexity
  - > Application software is dedicated to the safety-related I&C functions
  - > The operational system software includes only the features needed to implement safety-related I&C functions (no multitasking or interrupts are needed to implement the safety-related functions)

SPINLINE 3
Main Design Criteria (3)



- Fail safe and fault tolerant features
  - > Actuator boards provide defined output in case of hardware failure in the board itself or in the processing unit
  - > Fault tolerant features = fault detection mechanism & ability to design redundant architectures with graceful degradation

- Prevent operation and maintenance errors
  - > Only agreed operating parameters are made adjustable within predefined upper and lower limits
  - > Units under test are physically and logically inhibited

- Security
  - > A physical access to the cabinets and then, to the CPU board is needed to make a change to the software
  - > The software is fully reviewable
  - > Communications within the safety-related system and with other systems are performed, using the NERVIA network

SPINLINE 3
Hardware Components

- 1E Qualified
- Modularity
- Scalability

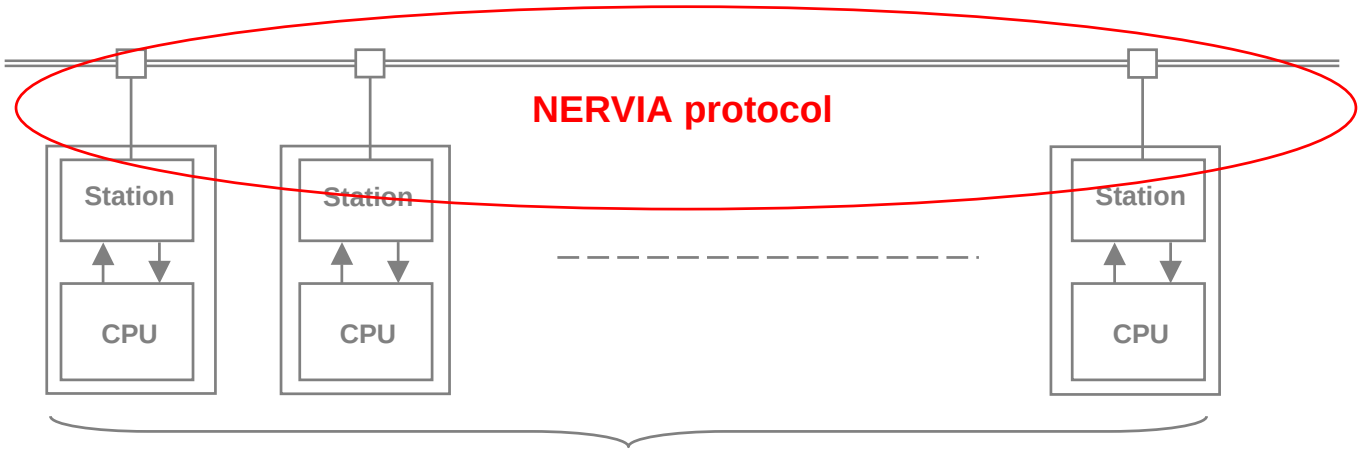
SPINLINE 3
Hardware Qualification

- According to National & International Standards
- IEEE 308 / IEEE 603: - Class 1E Systems
- Qualified class 1E equipment - IEEE 323
- Seismic tests: IEC 60980 (difference with IEEE 344 is the bi-axial testing, instead of tri-axial one, and spectra features)
- EMC - immunity: IEC 61000-4 endorsed by RG 1.180

SPINLINE 3
Software Components

- Application Software
  - > Dedicated to the customer needs
  - > To be developed with 3KEYMASTER/CLARISSE *SPINLINE* 3 dedicated System and Software Development Environment (SSDE)
- Operational System Software
  - > Low complexity : Single loop, No interrupt, Dedicated to I&C needs
  - > 1E qualified : Design and V&V according to IEC 60880
  - > Standardized, Application Independent
- Clarisse SSDE
  - > Description of I&C architecture
  - > Description of I&C functions with formal Functional Block Diagram language (SCADE editor)
  - > Fully automated code generation
  - > Production of design documentation
  - > Configuration management

SPINLINE 3
NERVIA Safety Network



- NERVIA is a class 1E network which provides efficient, safe and secured data communication within the safety-related I&C system.
  - > NERVIA protocol: Token ring, Broadcast implemented on top of a standard 10 Mbits/s Ethernet layer
  - > NERVIA software is compliant with IEC 60880

- NERVIA main features:
  - > Media: shielded cable and optic fibre
  - > Self-tested, fault tolerant
  - > Deterministic: response time is bounded and permanently guaranteed
  - > Physical and logical isolation
  - > No static or dynamic master station
  - > Virus propagation and unintended remote write access to safety-related data not possible

Proposed ECCS Architecture