Data Systems
& Solutions

protect perform predict

SPINLINE 3 ECCS architecture and IEEE 603 compliance

Presenter Jean-Michel Palaric/Dominique Moulin

The information in this document is the property of Data Systems & Solutions and may not be copied, or communicated to a third party, or used for any purpose other than that for which it is supplied, without the express written consent of Data Systems & Solutions. While the content of this document is given in good faith, based on the latest information available to Data Systems & Solutions, no warranty or representation is given concerning it. This content does not establish any contractual or other commitment binding on Data Systems & Solutions or any of its subsidiary or associated companies.

Content

- Architecture description
- Compliance with IEEE 603 main criteria
  - 4. Safety system design basis
  - 5.1 and 5.15 SFC and reliability
  - 5.6 Independence
  - 5.8 Information displays
  - 6. Sense and command features
  - 6.2 manual control
  - 6.7 maintenance bypasses

Architecture description

The information in this document is the property of Data Systems & Solutions and may not be copied, or communicated to a third party, or used for any purpose other than that for which it is supplied, without the express written consent of Data Systems & Solutions. While the content of this document is given in good faith, based on the latest information available to Data Systems & Solutions, no warranty or representation is given concerning it. This content does not establish any contractual or other commitment binding on Data Systems & Solutions or any of its subsidiary or associated companies.

Data Systems & Solutions

Echelons of defense according to NUREG/CR-6303 and NEDO 33251

		LAYER 1 NON SAFETY RELATED SYSTEMS	LAYER 2 SAFETY RELATED SYSTEMS	LAYER 3 DIVERSE NON SAFETY RELATED SYSTEMS
CONTROL ECHELON		NE-ECCS (PIP A, PIP B, BOP)		
REACTOR TRIP ECHELON			E-ECCS RTIF SSLC (RTIF – RPS, NMS, LD&IS, ATWS/SSLC)	Diverse Protection System (DPS – some RPS, some LD&IS)
ESF ACTUATION ECHELON			E-ECCS ESF SSLC (ECCS – IC, ADS, GDCS, suppression pool equalizing, isolation, SLCS)	Diverse Protection System (DPS – IC, ADS, GDCS, SLCS, some LD&IS) Severe Accident (deluge system)
MONITORING AND INDICATION ECHELON		NE-ECCS Plant Computer Function	E-ECCS ESF SSLC	Diverse Protection System (DPS)

HW/SW platform diversity

Safety	Safety Related		Non-Safety Related				
Category	E - DCIS		NE - DCIS				
System Families	RPS NMS	ECCS ESF	DPS	NUCLEAR CONTROL SYSTEMS	Balance of any NE-DCIS Systems	PCS	severe accident
Architecture	NUMAC derived	SPINLINE 3 redundant	triple redundant	triple redundant	dual redundant	workstations **	PLCs
Systems	RPS LD&IS (MSIV) NMS ATWS/SLCS*	IC SRV/DPV GDCS LD&IS	RPS ECCS backup	FWC, PAS (automation) SB&PC, T/G control	PIP A, PIP B balance of plant (power generation)	HMI, alarms, SPDS, historian, 3D-Monicore	deluge system

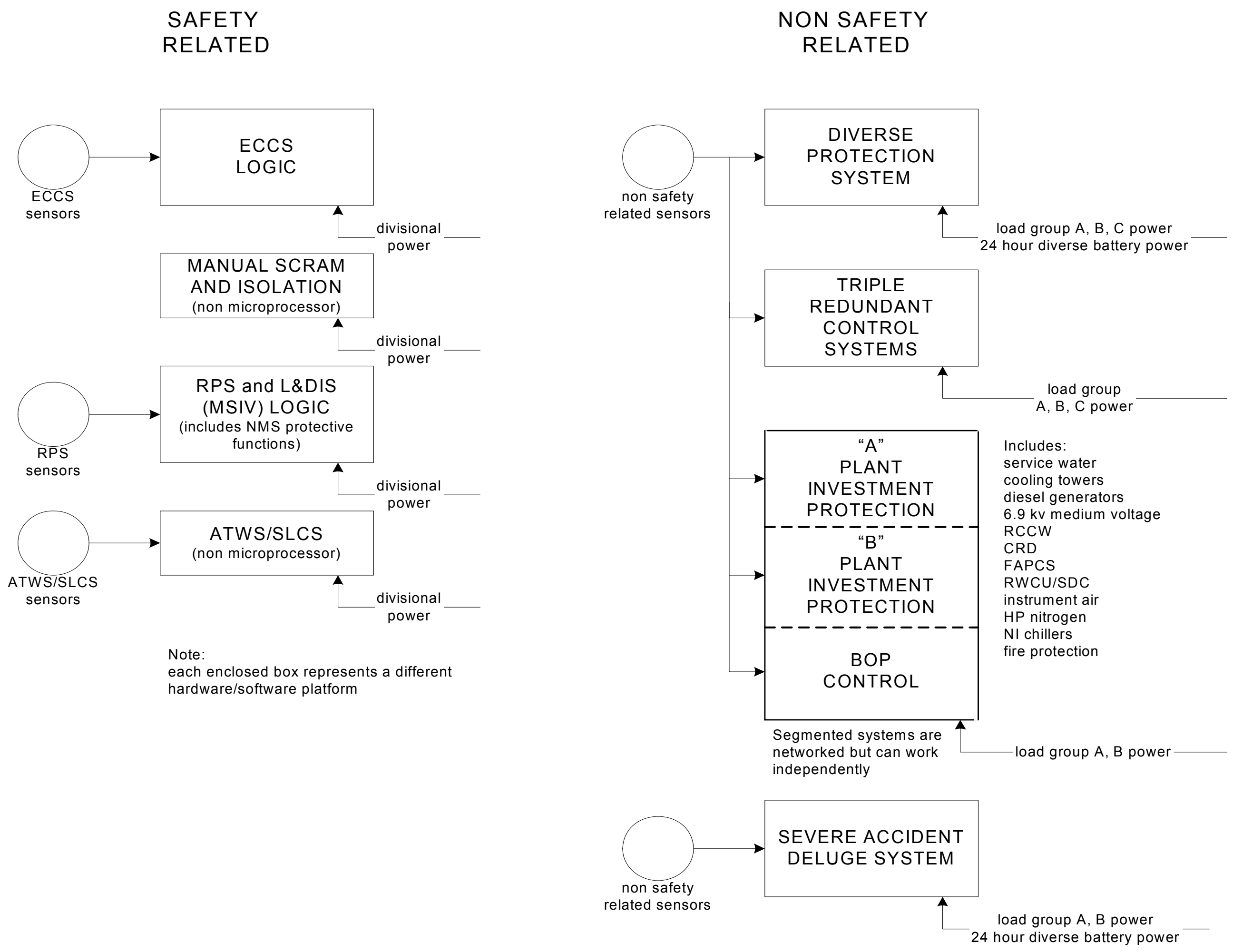
* non microprocessor based

** dual redundant as necessary

Diversity Strategy

Within Essential Controls (NRC)	▥	▤					
Essential -vs- DPS (NRC)	■	■	▤				
Essential -vs- Non-E (GE DCD PRA)	▤	▤	▥	▥	▥		▨

Sensor and power diversity



SAFETY RELATED

ECCS sensors → ECCS LOGIC ← divisional power

MANUAL SCRAM AND ISOLATION (non microprocessor) ← divisional power

RPS sensors → RPS and L&DIS (MSIV) LOGIC (includes NMS protective functions) ← divisional power

ATWS/SLCS sensors → ATWS/SLCS (non microprocessor) ← divisional power

Note:
each enclosed box represents a different hardware/software platform

NON SAFETY RELATED

non safety related sensors → DIVERSE PROTECTION SYSTEM ← load group A, B, C power, 24 hour diverse battery power

non safety related sensors → TRIPLE REDUNDANT CONTROL SYSTEMS ← load group A, B, C power

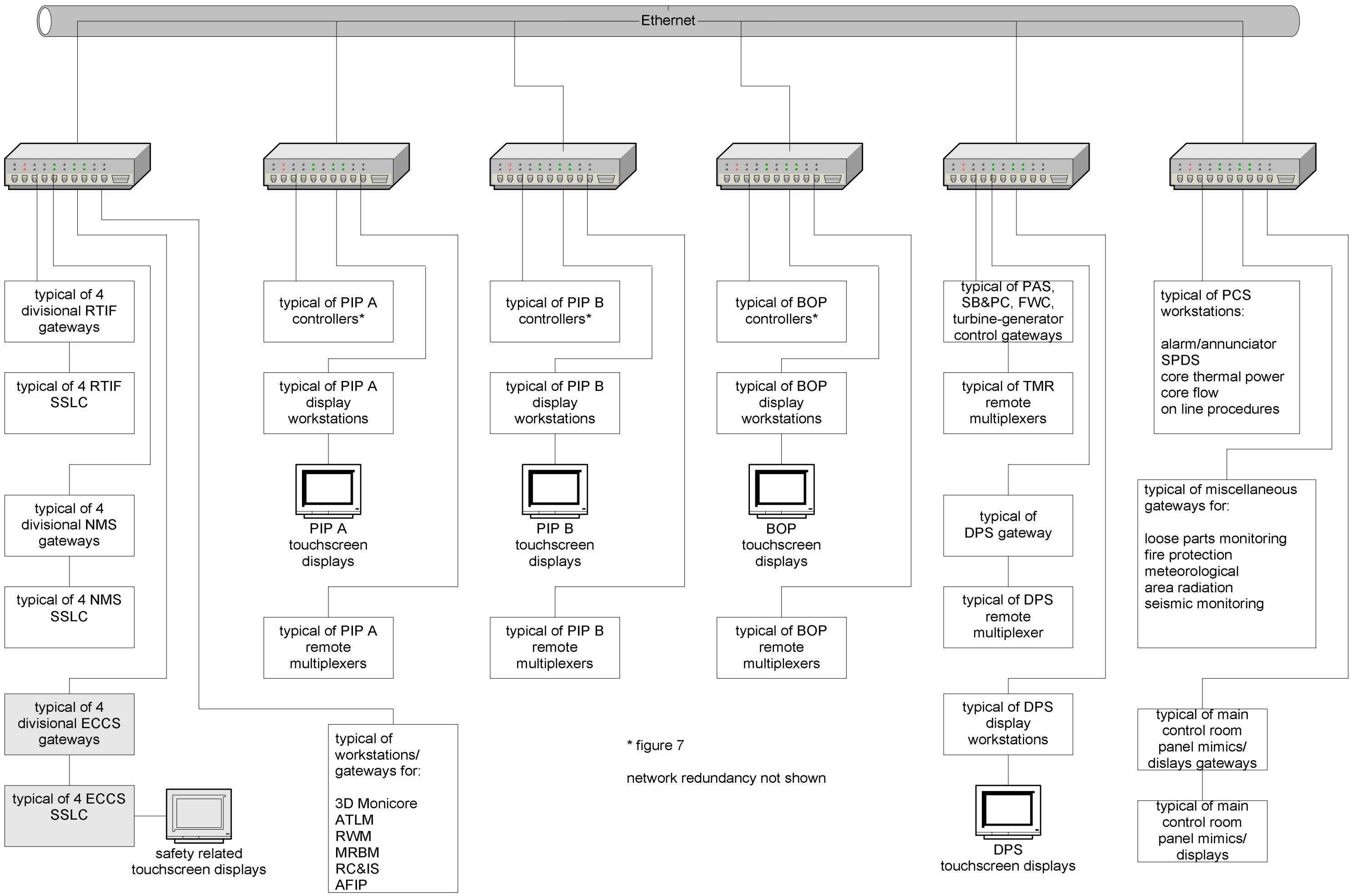
non safety related sensors → "A" PLANT INVESTMENT PROTECTION; "B" PLANT INVESTMENT PROTECTION; BOP CONTROL ← load group A, B power

Includes:
service water
cooling towers
diesel generators
6.9 kv medium voltage
RCCW
CRD
FAPCS
RWCU/SDC
instrument air
HP nitrogen
NI chillers
fire protection

Segmented systems are networked but can work independently

non safety related sensors → SEVERE ACCIDENT DELUGE SYSTEM ← load group A, B power, 24 hour diverse battery power

General ECCS architecture/SPINLINE 3 SCOPE



Ethernet

typical of 4 divisional RTIF gateways

typical of 4 RTIF SSLC

typical of 4 divisional NMS gateways

typical of 4 NMS SSLC

typical of 4 divisional ECCS gateways

typical of 4 ECCS SSLC

safety related touchscreen displays

typical of PIP A controllers*

typical of PIP A display workstations

PIP A touchscreen displays

typical of PIP A remote multiplexers

typical of workstations/ gateways for:

3D Monicore
ATLM
RWM
MRBM
RC&IS
AFIP

typical of PIP B controllers*

typical of PIP B display workstations

PIP B touchscreen displays

typical of PIP B remote multiplexers

typical of BOP controllers*

typical of BOP display workstations

BOP touchscreen displays

typical of BOP remote multiplexers

* figure 7

network redundancy not shown

typical of PAS, SB&PC, FWC, turbine-generator control gateways

typical of TMR remote multiplexers

typical of DPS gateway

typical of DPS remote multiplexer

typical of DPS display workstations

DPS touchscreen displays

typical of PCS workstations:

alarm/annunciator
SPDS
core thermal power
core flow
on line procedures

typical of miscellaneous gateways for:

loose parts monitoring
fire protection
meteorological
area radiation
seismic monitoring

typical of main control room panel mimics/ dislays gateways

typical of main control room panel mimics/ displays

ECCS/***SPINLINE 3*** scope

❑ The ECCS includes three sets of technological systems to perform the functions

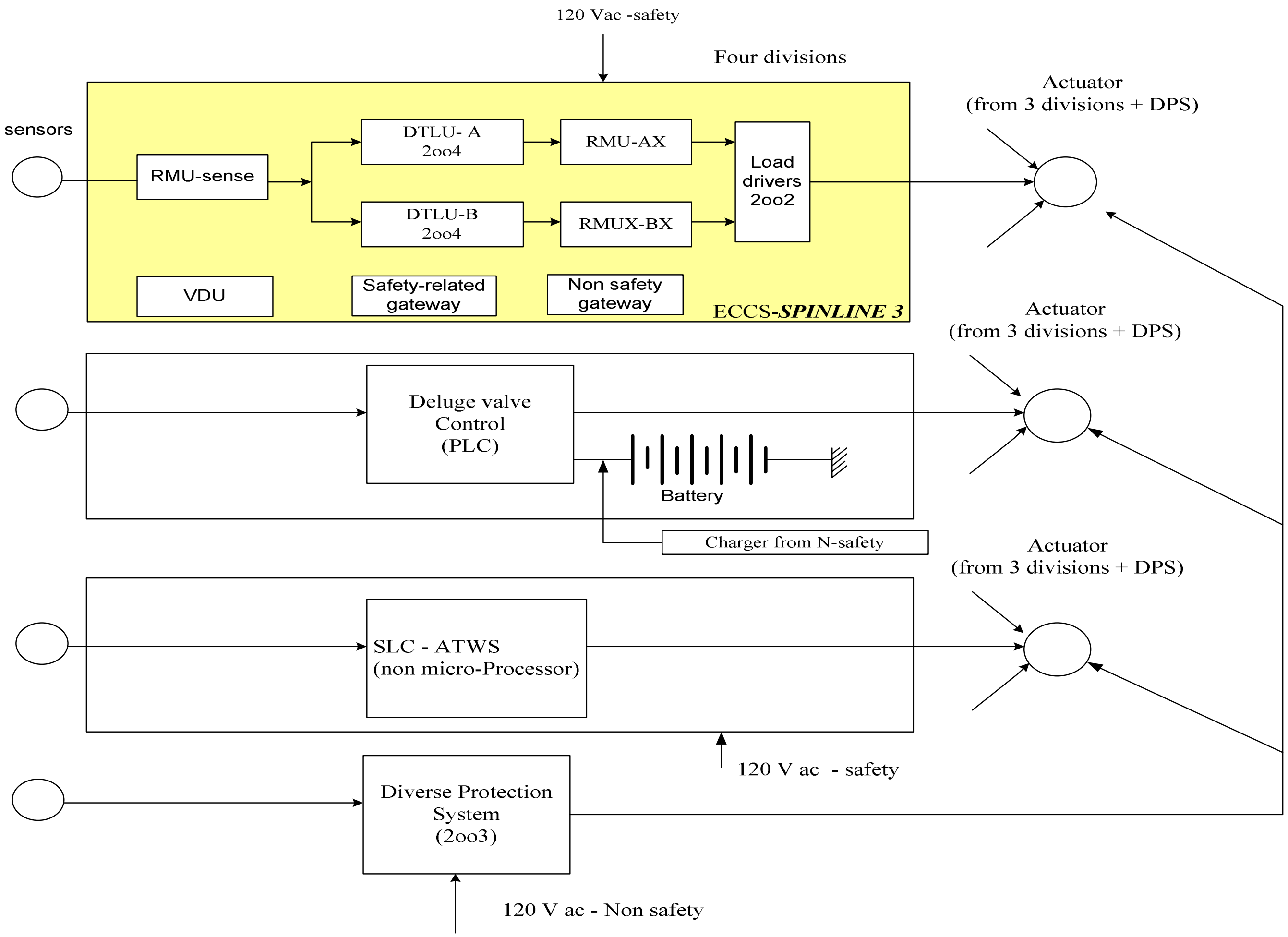
- The SSLC/ESF, built with SPINLINE 3, corresponds to the logic for :
  - Automatic Depressurization System (ADS)
  - Gravity-Driven Cooling System (GDCS)
  - Leak Detection & Isolation System (LD & IS)., except the MSIV actuation control
  - Isolation Condenser System (ICS), portion of the function
  - Standby Liquid Control System (SLCS) boron injection initiation logic for LOCA

- The deluge line system , diverse from SSLC/ESF

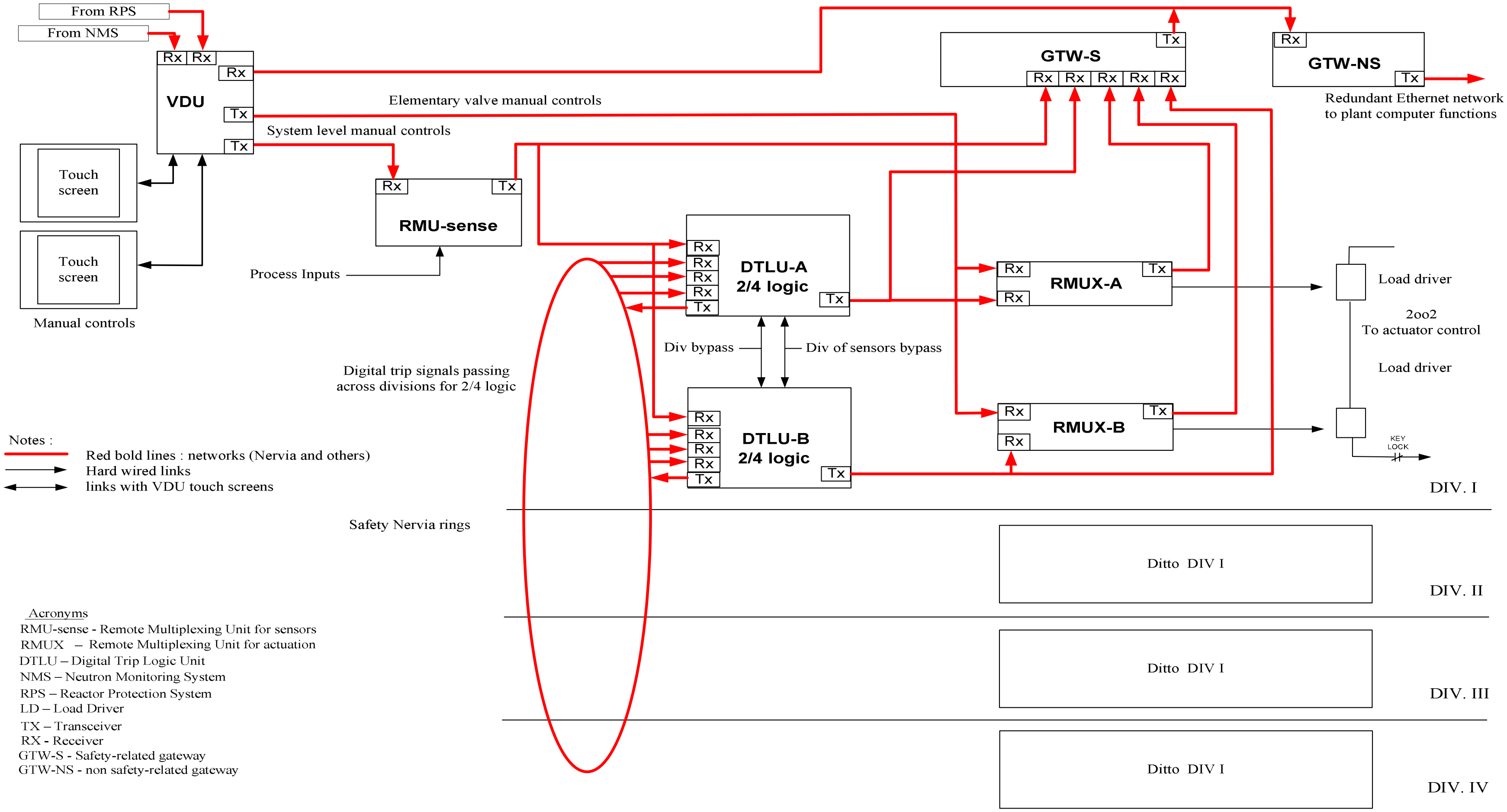
- The SLC/ATWS , based on a non microprocessor technology.

Data Systems & Solutions

ECCS/***SPINLINE 3*** scope



ECCS-***SPINLINE 3*** general architecture



Notes :

- Red bold lines : networks (Nervia and others)
- Hard wired links
- links with VDU touch screens

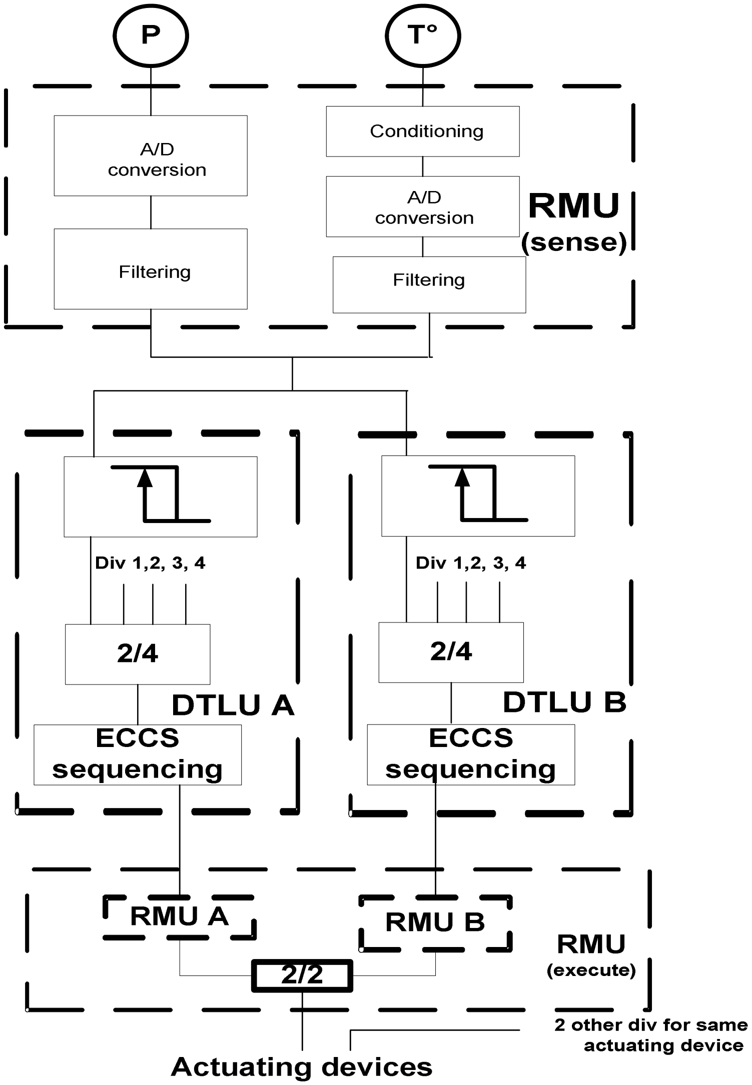
Acronyms

RMU-sense - Remote Multiplexing Unit for sensors
RMUX – Remote Multiplexing Unit for actuation
DTLU – Digital Trip Logic Unit
NMS – Neutron Monitoring System
RPS – Reactor Protection System
LD – Load Driver
TX – Transceiver
RX - Receiver
GTW-S - Safety-related gateway
GTW-NS - non safety-related gateway

Main Inputs/outputs

Processing Unit	Main Inputs	Main Outputs
RMU-sense	System level manual controls sensors	results of measurement of physical values system level manual controls results of self tests
DTLU	results of measurement of physical values Partial trips of other divisions system level manual controls division-of-sensors bypass results of self-test of the upstream units	Partial trips to DTLU of other divisions individual automatic controls for all the actuators Self test results
RMU-X	individual automatic controls for all the actuators individual manual controls for each actuator signals monitoring the continuity down to load drivers	hard-wired control signals to the corresponding load drivers Self tests results
Safety gateway	All data coming from the digital units of the division	Data to VDU and NS-Gateway for plant monitoring
Non safety gateway	Data coming from the safety gateway of the division	Data to plant computer
VDU	Data from safety gateway (system status & alarms) Manual controls from operator	Manual controls

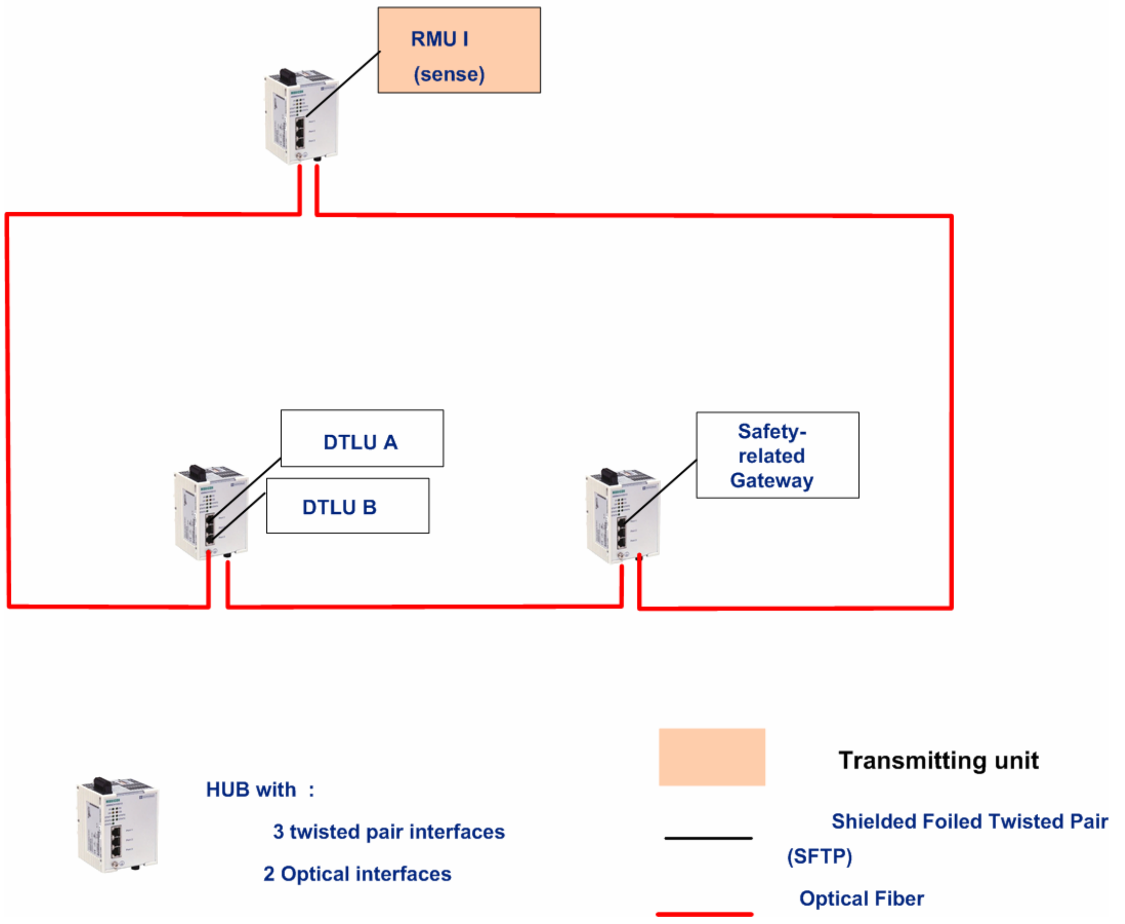
Distribution of processings



RMU-sense network architecture

The four RMU safety Nervia networks have the same architecture

The hereunder scheme represents the network of the first Division



RMU I (sense)

DTLU A

DTLU B

Safety-related Gateway

HUB with :

3 twisted pair interfaces

2 Optical interfaces

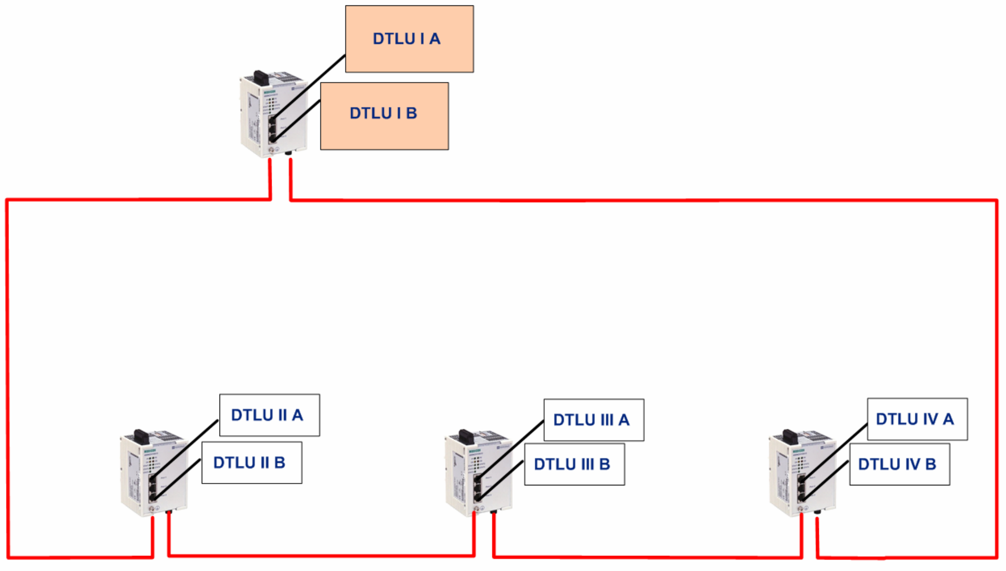
🟧 Transmitting unit

— Shielded Foiled Twisted Pair (SFTP)

— Optical Fiber

DTLU network architecture

**The four DTLU safety networks have the same architecture.
The hereunder scheme represents the network of the first Division**



DTLU I A

DTLU I B

DTLU II A

DTLU II B

DTLU III A

DTLU III B

DTLU IV A

DTLU IV B

HUB with :
3 twisted pair interfaces
2 Optical interfaces

🟧 **Transmitting unit**

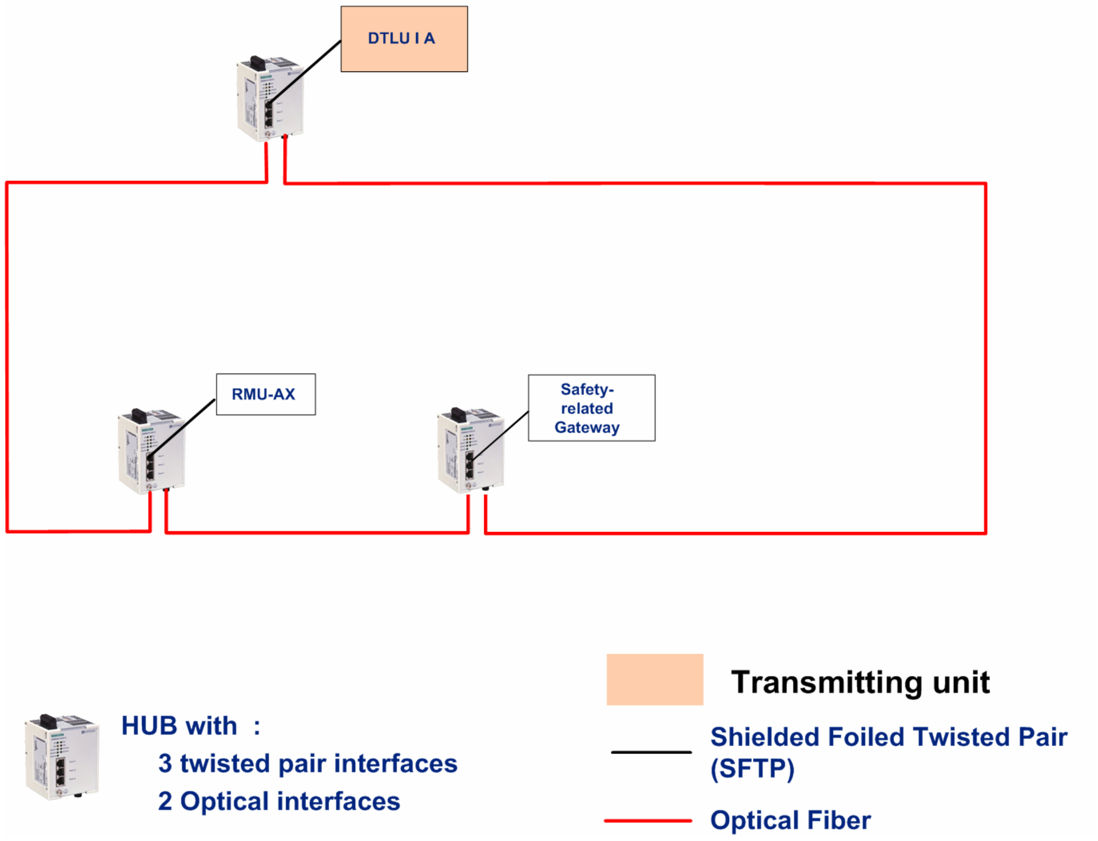
— **Shielded Foiled Twisted Pair (SFTP)**

— **Optical Fiber**

DTLU-RMU network architecture

All DTLU-RMU-X safety networks have the same architecture. There are four networks for DTLU A- RMU-AX and 4 others for DTLU B- RMU-BX

The hereunder scheme represents the network of the first Division



HUB with :

3 twisted pair interfaces

2 Optical interfaces

🟧 **Transmitting unit**

— **Shielded Foiled Twisted Pair (SFTP)**

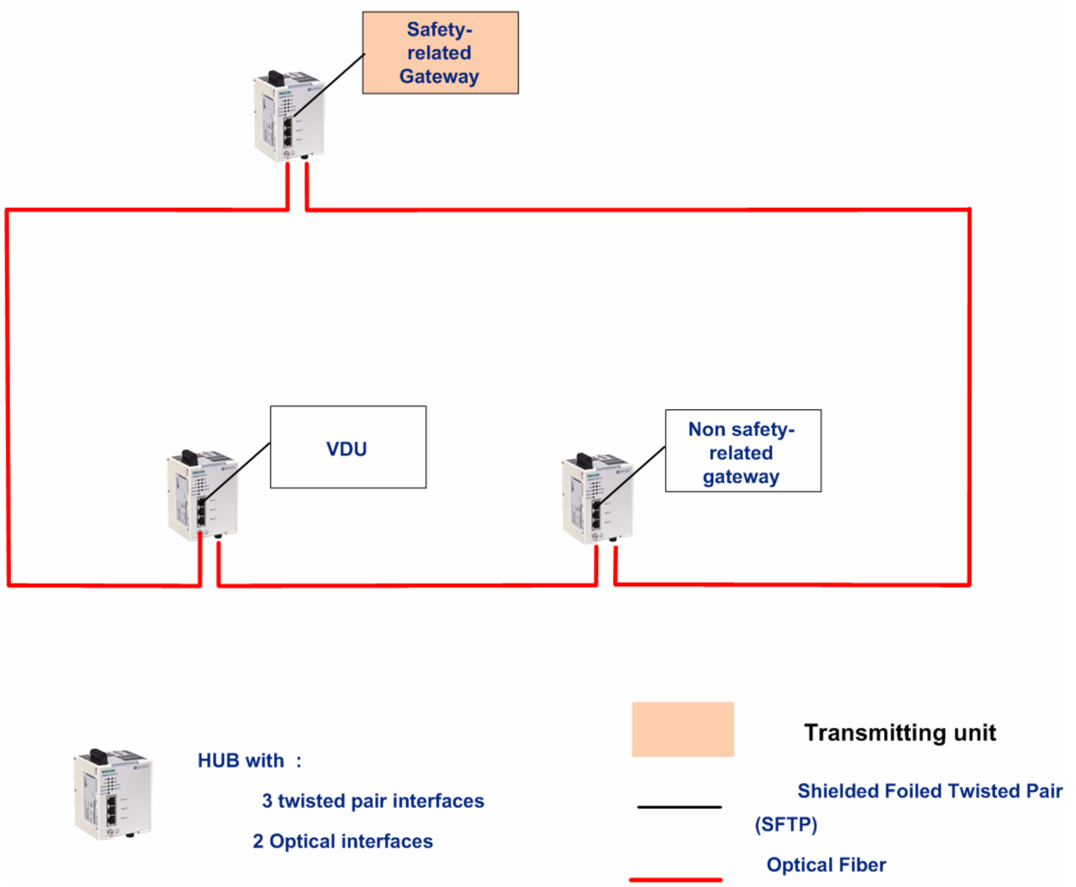
🟥 **Optical Fiber**

Data Systems & Solutions

safety-related gateway network architecture

The four safety-related gateway Nervia networks have the same architecture

The hereunder scheme represents the network of the first Division



Safety-related Gateway

VDU

Non safety-related gateway

HUB with :

3 twisted pair interfaces

2 Optical interfaces

🟧 Transmitting unit

— Shielded Foiled Twisted Pair (SFTP)

🟥 Optical Fiber

Compliance with IEEE 603 requirements

IEEE 603 4. Safety System design basis

- IEEE 603 4.

Item from IEEE 603 section 4		
a	Design basis events	Not under DSS responsibility
b	Safety functions and protective actions	
c	Permissive conditions	
d	Specification of variables to be monitored (automatic and manual)	
e	Manual control requirements	
F	Location of sensors	
g	Environmental condition	Qualification of ECCS/SPINLINE 3 according to specified environmental conditions (see DCD)
h	Provisions for avoidance of functional degradation of safety system performance	According DSS scope of supply this is limited to potential influence of systems connected to ECCS/SPINLINE 3. This is described in section independence
i	Reliability	Described in section reliability
j	Critical point in time or the plant conditions after the onset of a DBE.	Not under DSS responsibility
k	Equipment protective provisions that prevent the safety system from accomplishing their safety functions.	Not relevant.
l	Any other design basis.	N/A.

IEEE 603 5.1 and 5.15 Safety and availability : requirements

- Basically there are 2 kinds of requirements : deterministic and probabilistic :
  - Deterministic : compliance with SFC according to IEEE 379. This compliance includes a special care on “potential for system actuation” (§6.3.3)
  - probabilistic : often expressed in terms of probability to fail to initiate a safety actuation on demand and in terms of frequency of spurious actuations
- Of course the goal of the regulatory body and plant operator is to get the best possible figures
- In fact the final design is a trade-off and a balance between safety and availability : an increase of safety will decrease availability and vice-versa
- The system PRA is based on SPINLINE 3 boards and components failure rates:
  - Each SPINLINE 3 board is designed in parallel with its FMEA to include safety features at the outset of the design
  - In particular the design is such that the undetected part of the failure rate is lowered as much as possible

Approach of FMEA/PRA

- How can these requirements be reached ?
  - 1- Build an architecture according to design criteria of IEEE Std 603
  - 2- Perform a deterministic analysis to prove that SFC is fulfilled. This analysis will determine the major principles of behavior in case of failure and will initiate the fault-trees needed for probabilistic analysis (R/A)
  - 3- Complete this deterministic analysis with cases of multiple failures and their consequences on the performance of actuations i.e. if they can be blocked or spuriously initiated. The results can be presented in several forms
  - 4- This gives to the Designer, the Operator and the Regulatory body a better understanding and confidence in the system. Later the results of this analysis can be included in OMMs to guide the maintenance
  - 5- Perform the probabilistic analysis using the above results. Check that the targets are hit. Else go back to step 1 and adapt the architecture
  - 6- the final result is the architecture validation

Evolution margin

- 3 main possibilities to influence safety and availability :
  - The technology : design of basic components (boards) include a R/A to lower the failure rate and the undetected failure rate. Extensive self tests are included in the system SW
  - The architecture : modify the redundancy inside divisions
  - The flexibility of the architecture : adapt the behavior in case of failure thanks to configurable votes

ECCS voting configuration

- ECCS is energized-to-operate and fail as is for ADS and GDCS. This is the case dealt with in the following
- 3 levels of vote :
  - DTLU
    - Normal operation : 2/4
    - 1st fault (or invalid signal) : 2/4 becomes 2/3
    - 2nd fault : 2/3 becomes 2/2
    - 3rd or 4th fault : 2/2 becomes NO ACTUATION
  - RMU-X
    - Normal operation : 2/2
    - 1st or 2nd fault upstream hardwired 2/2 vote; the 2/2 vote becomes NO ACTUATION
  - Valve
    - Normal operation : 1/3 (each valve is controlled by 3 different divisions)

ECCS voting configuration

- SFC compliance as per IEEE 603 5.1 and IEEE 379 means that :
  - No single failure (and its consequences) leads to a failure to initiate a safety actuation
  - Potential for system actuation must be examined from the point of view of safety consequences. For ESBWR it will be examined in the sense of inadvertent valve opening

- SFC is met because :
  - 4 divisions
  - Each valve can be controlled by one division out of three (generic assumption)
  - Case considered : single failure + periodic test (division is bypassed before periodic test)

Results

		DTLU vote	RMU HW vote	Valve	Comments
Normal situation		**2oo4**	**2oo2**	**1oo3**	**Assume that valve is controlled by div i and div j for all following cases**
Under periodic test	Test of RMU-s, or DTLU or RMU-X of Div i	2oo3 In other div	2oo2 In other div	1oo2	3 divisions still controls actuators. Each valve can still be controlled by 2 div Div i outputs are switched off before testing

Results

		DTLU vote	RMU HW vote	Valve	Comments
In case of detected failure(s). Note : by far, the most likely situation in case of failure(s)					
In case of failure, normal operation	failure of RMU-s of Div i	2oo3 in all div	2oo2 in all div	1oo3	4 divisions still controls valves. Each valve can still be controlled by 3 div
	failure of DTLU of Div i	2oo3 in other div	NA in div i 2oo2 in other div	1oo2	3 divisions still controls valves. Each valve can still be controlled by 2 div
	failure of RMU-X or HW vote of div i	2oo4	NA in div i 2oo2 in other div	1oo2	3 divisions still controls actuators. Each valve can still be controlled by 2 div
In case of failure, units under test	Test of Div i and failure of RMU-s of Div j	2oo2 in div not under test	NA in div under test 2oo2 in div not under test	1oo2	The valve is controlled by the div not subject to test. Each valve can still be controlled by 2 div
	Test of Div i and failure of DTLU-s of Div j	2oo2 in other 2 div	NA in div i and j 2oo2 in other div	1oo1	The valve is controlled by the div not subject to test or failure
	Test of Div i and failure of RMU-X or HW vote of Div j	2oo3 in div not under test	NA in div i And j 2oo2 in other div	1oo1	The valve is controlled by the div not subject to test or failure

NA : No Actuation

Results – case of Nervia

Potential failure mode	System effect	Detection
Loss of a RMU-s communication board	Included in RMU-s failure	Detected
Loss of a DTLU communication board	Included in RMU-s failure and DTLU failure	Detected
Loss of a RMU-X communication board	Included in RMU-X failure	Detected
Loss of a hub	In the worst case, loss of only one safety network (e.g. communication network between a given RMU and DTLU of the same division)	Detected
Optic fibre cut (10baseFL)	None thanks to the virtual optic fibre ring providing a medium redundancy	Detected
Shielded twisted pair cut (10baseT)	In the worst case, loss of only one safety network (e.g. communication network between a given RMU and DTLU of the same division)	Detected
Loss of power supply	None thanks to the power supply redundancy	Detected

Compliance with IEEE Std. 603

Section 5.6 – Independence

Independence Assessment – Overview

- Compliance with IEEE Std. 603 Section 5.6 – Independence Assessment – Overview:
    - The evaluation of the ECCS is based on the guidance in the Standard Review Plan in NUREG 0800 Appendix 7.1-C:
  - The evaluation shows that the ECCS has been designed to meet the requirements and will perform its safety functions in the event of:
    - faults in redundant portions of the ECCS,
    - design basis events,
    - faults in other systems connected to or in proximity to the ECCS.
  - Independence considerations:
    - Physical independence – the effects of physical damage, e.g. mechanical, chemical, electromagnetic, radiation damage, will not affect other systems that are physically independent.
    - Electrical independence – the effects of electrical faults, e.g. surge, will not affect other systems that are electrically independent.
    - Communicational independence – the effects of communication faults, e.g. message corruption, will not adversely affect other systems that are communicationally independent.

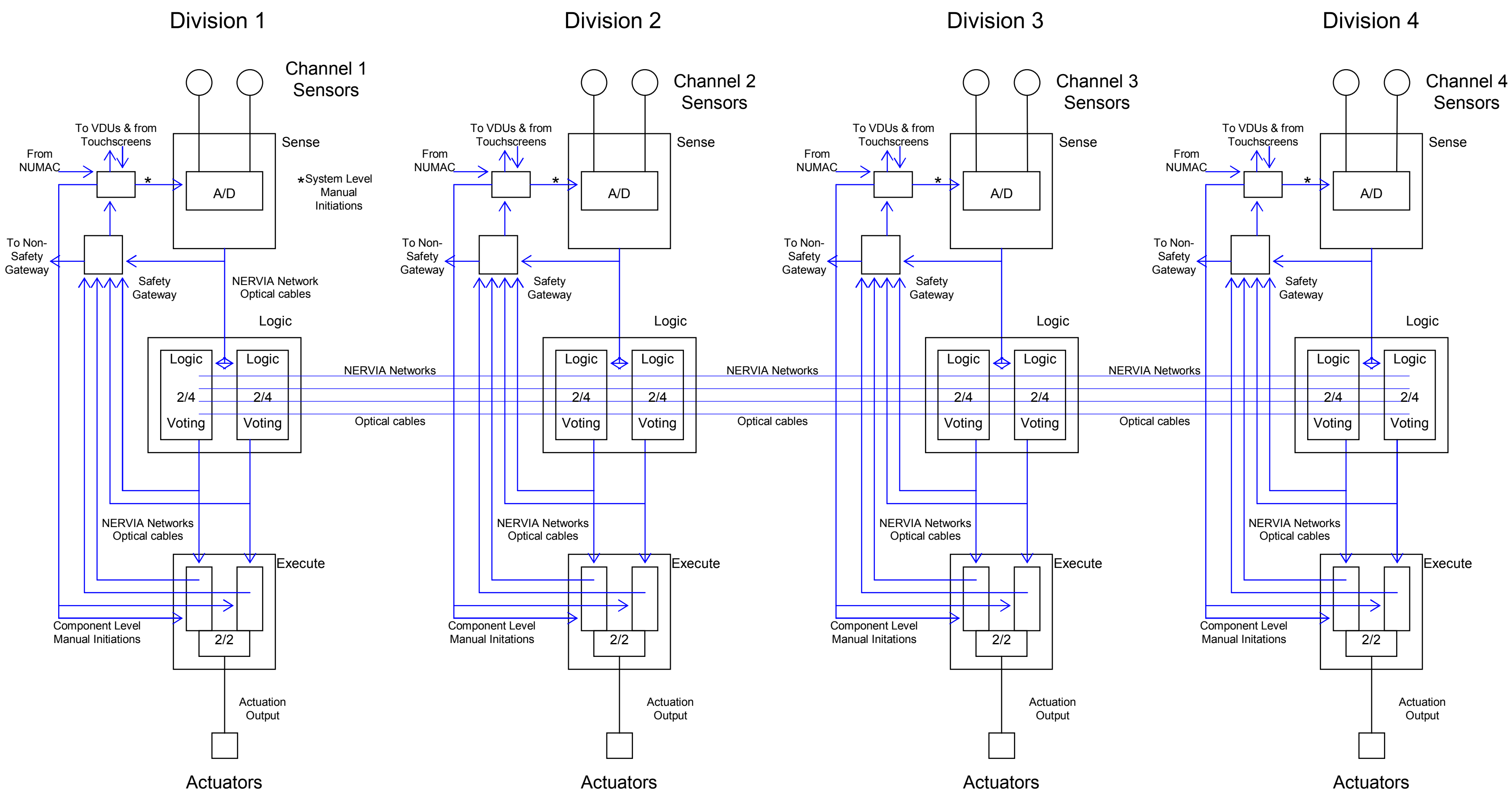
Independence Assessment – Overview

- Independence Considerations for the ECCS:
  - Independence between redundant portions of the ECCS:
    - A physical, electrical or communication fault in one redundant portion will not prevent the ECCS from performing its safety functions.
    - Redundant portions of the ECCS are the four divisions and also some redundant sub-systems within a division.
  - Independence between the ECCS and the effects of a design basis event:
    - Design basis events will not prevent the ECCS from performing its safety functions.
  - Independence between the ECCS and other systems:
    - A physical, electrical or communication fault in other systems either connected or in proximity will not prevent the ECCS from performing its safety functions.
    - Other systems are the Class 1E supporting systems, such as power supplies which are connected on a divisional basis and non-safety systems such as plant data acquisition systems.
    - Other systems are those that are connected in some way to the ECCS or in proximity to it.

Independence between redundant portions of the ECCS

- Independence between redundant portions of the ECCS
  - Overview of the ECCS divisional architecture:
    - The ECCS comprises four redundant and independent divisions each able to perform sufficient plant actuations to maintain the safety of the plant.
    - Four sensors are provided for each plant parameter measured (four channels), one channel provides the input to its associated ECCS division.
    - Four sets of control room touchscreens enable the system and component level manual initiations to be input to the division logic.
    - Four sets of control room VDUs provide the system and plant indications derived from the ECCS divisions.
    - Each division processes inputs, performs logical calculations including 2oo4 voting to generate actuation outputs to plant actuators.
    - A simplified representation of the architecture is shown on the following slide.

ECCS Divisional Architecture



Independence between redundant portions of the ECCS

- Physical faults in one division will not affect other divisions
  - Divisions are physically independent and separated by distance and physical barriers, e.g. walls.
  - Divisions are located in separate rooms, have separate cable runs, separate containment penetrations, etc.
  - Where equipment from different divisions are in close proximity, e.g. in the control room, the design ensures that there is no potential to cause effects across divisions.
  - The four sensors and input channels for each plant parameter, one to each division, are independent and physically separated from one another.
  - Supporting Class 1E systems, electrical supplies and HVAC, are also in four independent divisions separated by distance, physical barriers, etc. and these support the ECCS on a divisional basis.

Independence between redundant portions of the ECCS (cont'd)

- Electrical faults in one division will not propagate to other divisions of the ECCS:
  - Each division is powered from divisional essential electrical supply, a Class 1E safety grade supply that is a battery-backed non-interruptible power supply.
  - There are no electrical connections between divisions – connections are via opto-electrical isolation devices.
  - Communication between divisions is limited to the minimum necessary, channel trip and bypass status, required for voting.
  - All inter-division communication takes place via the NERVIA networks which use only fibre-optic cables between divisions ensuring electrical isolation.
  - There are no common switches shared by divisions.
  - All connections to and from the control rooms are electrically isolated as they are via NERVIA networks using optical data links.

Independence between redundant portions of the ECCS (cont'd)

- Communications faults between divisions will not prevent the ECCS from performing its safety functions:
  - Independence is achieved largely as a result of features of the NERVIA networks (see next slides)
  - The only inter-divisional communication is via four NERVIA networks providing the partial actuate and bypass status data required for the 2oo4 voting.
  - A division always transmits on the same inter-divisional network and reads data from the other three of these networks.
  - All inter-division communication is one-way and asynchronous, i.e. the transmitting division simply makes the data available on its network for all other divisions to read.
  - A corrupted message or no communication is detected by the extensive NERVIA network and message checking algorithms.
  - Failure to transmit data will not prevent that division from continuing to function normally as it does not wait for any response from receiving stations.
  - If data is corrupted or unavailable on a network, pre-defined safe actions will be taken by all stations and the failure will also be annunciated to the control room.
  - The safe action results in the voting logic in the other divisions going from 2oo4 to 2oo3.
  - Faults are revealed immediately allowing the system to be repaired.

NERVIA Networks

- NERVIA networks are –
  - Hardware is Class 1E qualified.
  - Compliant with IEC 61226 for systems implementing Category A functions, such as reactor trip, ESFAS actuation, in nuclear power plants
  - NERVIA protocol and software development is fully compliant with IEC 60880 requirements.
- NERVIA networks are used in the ECCS to provide data communication;
  - between divisions – four networks all linking the four divisions, each division transmits its trip and bypass data on one network and reads similar data from the other three allowing the 2oo4 voting to take place.
  - between subsystems within a division – each sensing and actuation subsystem has its own NERVIA network which transmits data to the safety-related gateway.
  - touch screen control units transmit manual system level and components level initiation inputs using NERVIA network technology.
  - to the safety-related gateway and on to the control room VDUs and the non-safety-related gateway.

Features of NERVIA Networks Important to Independence

- ❑ Features of NERVIA Networks Important to Independence –
  - Fault tolerant – the protocol is designed for safety, self-testing and data is continuously validated. Failures are instantly reported to all receiving stations so that safe actions can be taken.
  - The non-safety related gateway is configured as read only ensuring data from non-safety systems cannot enter the ECCS.
  - Uses optical links between hubs ensuring electrical isolation between divisions and also between subsystems.
  - Determinism by token ring technique – a fixed cycle time is guaranteed, receiving stations know when the next data is due, how much to expect, what type it should be and take safe action if the data fails to arrive or is not as expected.
  - Broadcast transmission – data transmitted by one station is received and stored by all other stations on the network - there is no handshaking.
  - Network station operation is asynchronous with unit operation – each has independent cyclical processing – provides tolerance to synchronisation faults.

Independence from the effects of design basis events

- Independence from the effects of design basis events:
  - Overview of the effects of design basis events on the ECCS:
    - Design basis events are those for which the plant is designed to withstand without any loss of capability to perform safety functions.
    - They include certain severities of steam leak, fire, flooding, seismic event, aircraft impact, lightning strike, loss of off-site power, etc.
    - Design basis events have the potential to subject parts of the ECCS, plant sensors and actuators, to extreme environmental conditions.
    - The effects of design basis events on the ECCS are mitigated by the protection afforded by equipment qualification, location and enclosure.

Independence from the effects of design basis events

- Physical independence from the effects of design basis events:
  - All components are qualified for continued functional capability for the worst environmental conditions that may occur at its location during and following design basis events.
  - Components and equipment are qualified for the extremes of temperature, humidity, vibration, electromagnetic conditions and acceleration forces, etc. that may be encountered for their plant location and enclosure type.
  - Spacial separation, physical barriers and equipment locations are designed to limit the effects of design basis events on the ECCS equipment.

Independence from the effects of design basis events

- Electrical independence from the effects of design basis events:
  - The electrical supplies to the divisions are divisional essential supplies which are Class 1E supplies and are uninterruptible supplies.
  - A secondary source of divisionalised power is available in the Instrument and Control Power system.
  - The ECCS is not dependent on off-site power.
  - The electrical isolation between division equipment limits the effects of electrical abnormalities such as a surge caused by a single lightning strike to one division only.
  - Electrical isolation and protection features within a division limit spurious actuations in the event of electrical abnomalities.

Independence from the effects of design basis events (cont'd)

- Communicational independence form the effects of design basis events:
  - The system is designed to be tolerant of communication faults and to be independent between divisions.
  - All communications within the ECCS and to and from other systems are one-way, and only use NERVIA networks which are fault tolerant and ensure the highest integrity of data (see earlier slides).
  - If communications problems are experienced, the data will be invalidated by consistency algorithms and the divisions will take safe default action resulting in the voting going from 2oo4 to 2oo3 enabling the ECCS to continue to maintain the plant in a safe state.
  - The system will continue to perform its safety functions in the event of data corruption or loss of communications – a single event will not prevent the ECCS from performing its safety function.
  - Data corruption in a logic unit will not lead to spurious actuations, outputs from duplicated logic trains within a division are voted in 2oo2 hardwired voting - an actuate demand will not be generated by the division if only one logic train requests an actuation demand.

Independence from other systems

- ❑ Independence between the ECCS and other systems:
  - ▪ Overview
    - Single faults in a Class 1E system supporting the ECCS will not prevent it from performing its safety functions.
    - Class 1E Systems connected to the ECCS are:
      - – power supplies, HVAC systems, pneumatic actuation systems,
      - – actuated plant systems, valves, etc.
      - – control room systems.
    - Any faults and failures in any non-safety systems, whether connected or not, will not prevent the ECCS from performing its safety functions.
      - – any non-safety systems.
    - The effects of faults in other systems in proximity to the ECCS will not prevent it from performing its safety functions :
      - – systems which could generate missiles or harsh environments, e.g. steam pipes fractures, fires, rotating machinery,
      - – spurious operation of fire suppression systems,
      - – faults in non-safety-related systems,
      - – faults in the diverse protection system.

Independence from other systems (cont'd)

- Physical independence from effects caused by other systems:
  - The ECCS is protected from physical damage caused by other systems, e.g. missile generation from rotating plant or pressurised systems, by its location, walls and barriers.
  - Any single incident of localised damage will not affect more than one division of the ECCS as a result of spacial separation.
  - The ECCS does not share its locations with any non-safety equipment that could cause physical damage to it.
  - Only those supporting Class 1E systems, such as power systems and HVAC systems, share locations with the ECCS and then only the associated division of those systems.

Independence from other systems (cont'd)

- Electrical independence from the effects caused by supporting Class 1E systems:
  - The ECCS uses power from divisionalised essential non-interuptible power supplies – single malfunctions in electrical supplies will not affect more than one division.
  - A secondary source of power to the ECCS is available in the divisionalised instrument and control power supply which can be used in the event of loss of the normal power.
  - The SRV solenoid and DPV squib initiator power is supplied from corresponding divisional 250VDC batteries.
  - HVAC systems are division based using divisional power supplies, each division serves the locations for one division of the ECCS.
- Electrical independence from non-safety systems:
  - Non-safety systems are connected to the ECCS only via electrical isolation devices, e.g. opto-isolators, to prevent propagation of faults from non-safety systems to the ECCS.

Independence from other systems (cont'd)

- Communicational independence from other systems:
  - The ECCS receives no data from non-safety systems.
  - Data received from other safety systems is from NUMAC, i.e. RPS and NMS data for display on the VDUs in the control room, which is handled by networks featuring fibre-optic cable, one-way data transfer, display only restrictions and communications failure detection.
  - Division based manual actuation data from the control room touch screens enters the division subsystems via NERVIA type network connections – these commands are all 'Arm and Fire' requiring two deliberate actions to actuate.
  - Bypass status is sent from the control room via fibre-optic cable to the divisions.
  - Data sent from the ECCS to other safety systems is via one-way safety related NERVIA networks (one network per division).
  - Each of these NERVIA safety-related networks has two data path gateways, one safety related, the other non-safety related.
  - Data from divisional subsystems is transmitted by the safety-related gateway via a NERVIA network to the control room VDUs and the non-safety-related gateway.
  - The safety related gateway is the only transmitter on the network - it simply places data on the network for other stations to read.
  - Non-safety systems acquire data via the non-safety related gateway, a receiving station which simply reads data from the network and cannot alter it.

Summary – Independence Compliance

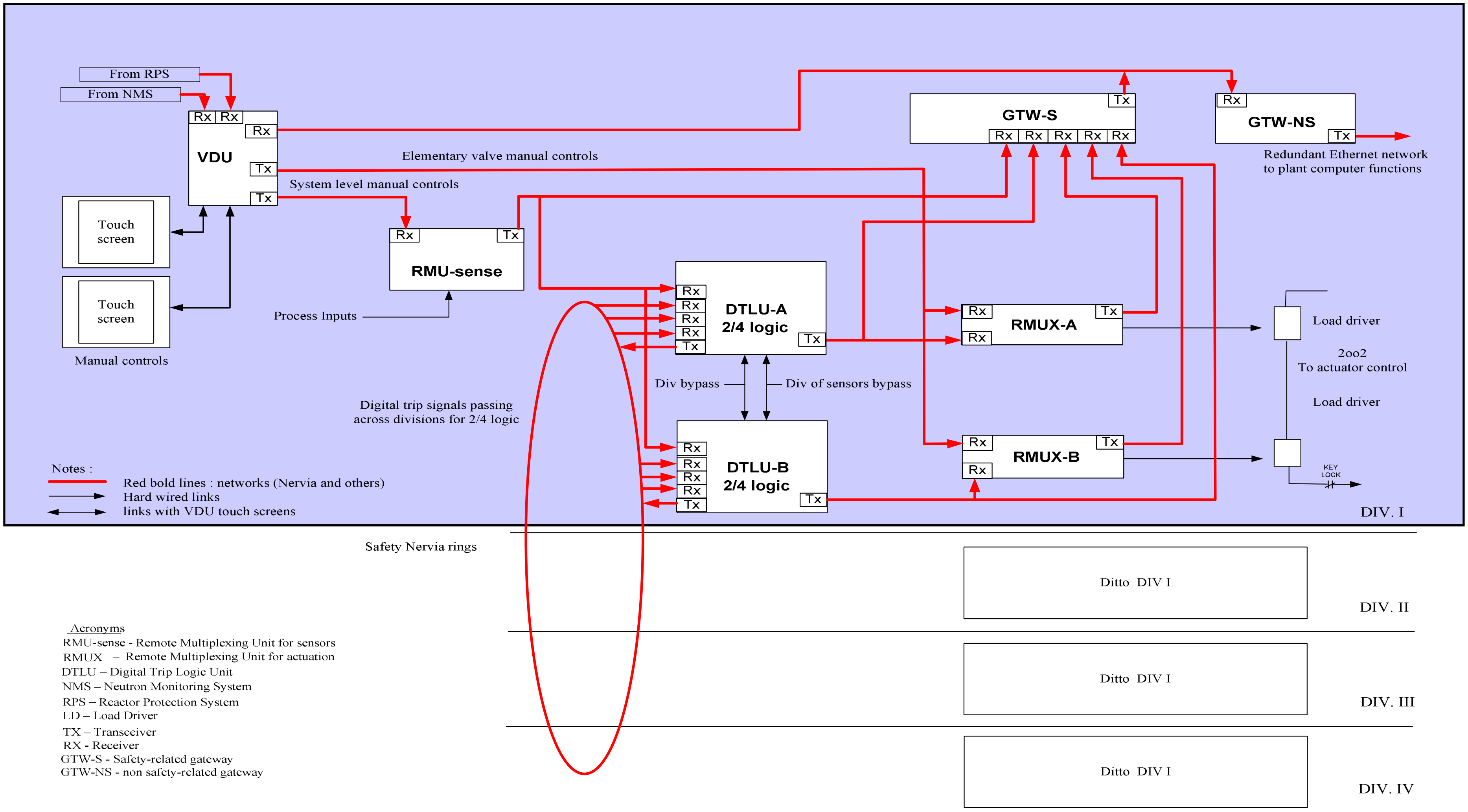
- Summary – Independence Compliance of the ECCS:
  - The ECCS is:
    - Divisionally independent throughout, physically, electrically and communicationally.
    - Independent of the effects of design basis events:
      - equipment qualification, physical barriers, separation, location and electrical isolation and communicational independence.
    - Independent of the faults and failures in other systems:
      - other systems which are connected to it – for Class 1E systems, e.g. power supplies, connected to the ECCS on a divisional basis – secondary power source available.
      - non-safety systems are not directly connected, connections are via non-safety data gateways and optical data links.
      - other systems in proximity to it - barriers, enclosure and location protect the ECCS.
  - A key factor in the independence is the use of NERVIA data networks.
    - Cummunicational independence – fault tolerant, one-way data transfer between divisons and to non-safety systems, self-checking, data validation, safe default actions.
    - Electrical independence – use of optical data links.
    - Physical independence - hardware qualification to Class 1E nuclear standards.

IEEE 603 5.8 Information displays

- IEEE 603 5.8.1 : the display instrumentation for safety systems (NMS, RPS, ECCS) is performed by VDU. There is one VDU per division
- IEEE 5.8.2 : system display indication
  - Two levels of display :
    - VDU in control room (e.g. see DCD 7.3.1.1.5 for ADS). Safety related gateway elaborates data to be displayed : system status and alarms
    - Local display at non safety related gateways for diagnosis and corrective maintenance (e.g. SPINLINE 3 HW failures)
- IEEE 5.8.3 indication of bypasses :
  - Bypasses of sensors and division are displayed by VDU in the control room
- IEEE 5.8.4 location
  - All displays of system status and alarms are available on VDU in the Control room. There is one VDU per division.

IEEE 603 6. Sense and command features

- ***SPINLINE 3*** scope only comprises sense and command features:
  - Process sensors : out of scope
  - Signal conditioning : RMU-sense
  - Decision logic : DTLU
  - Manual switches : VDU manual controls, bypass (sensor and division)
  - Process controls : RMU-execute
  - Indicators for operator action : VDU
  - Limit switches and control circuitry : load drivers
- Execute features are the valves and are out of scope



Notes :

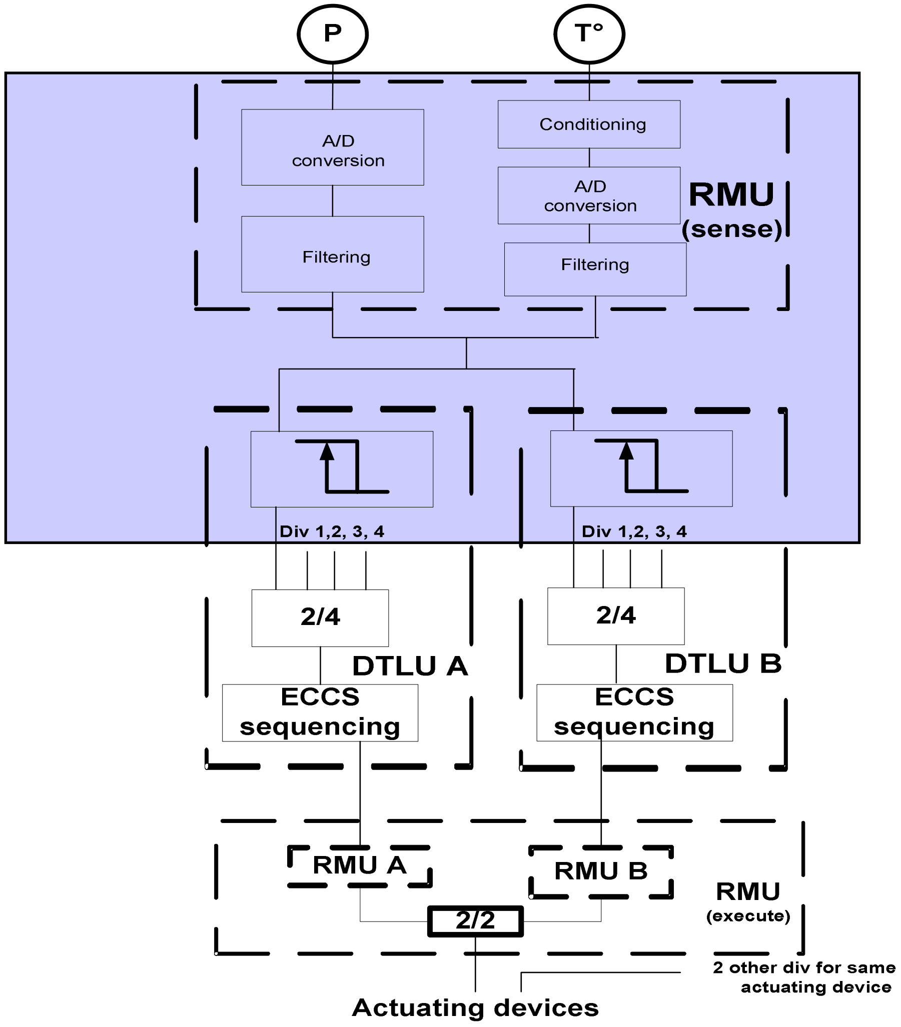
🟥 Red bold lines : networks (Nervia and others)
→ Hard wired links
↔ links with VDU touch screens

Acronyms

RMU-sense - Remote Multiplexing Unit for sensors
RMUX – Remote Multiplexing Unit for actuation
DTLU – Digital Trip Logic Unit
NMS – Neutron Monitoring System
RPS – Reactor Protection System
LD – Load Driver
TX – Transceiver
RX - Receiver
GTW-S - Safety-related gateway
GTW-NS - non safety-related gateway

Channel

- ❑ Loses its identity when single protective action signals are combined
- ❑ For manual controls : VDU + RMU-execute is a channel

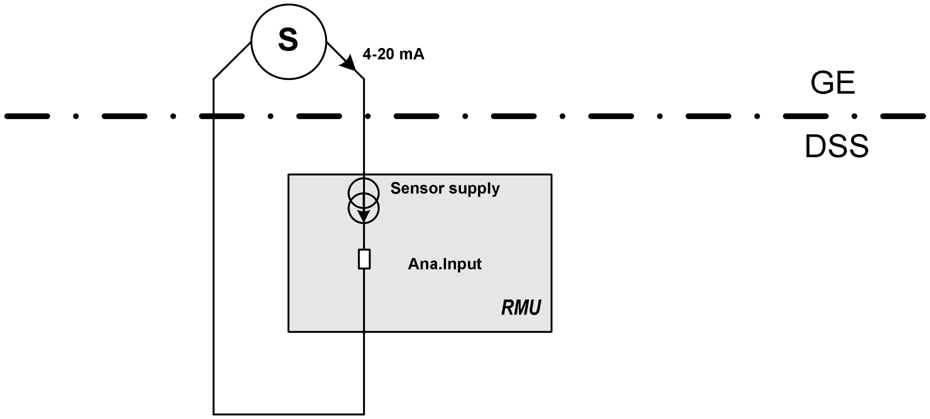


Channel/division borders

- There is no guidance or recommendation in IEEE 603 about the borders of channels and division
- The ECCS Design follows the spirit of the overall ESBWR design which is “divisional”:
  - Exchanges between divisions are done after elaboration of partial trips in each division
  - in terms of functional blocks the border is in DTLU, at the output of threshold comparison

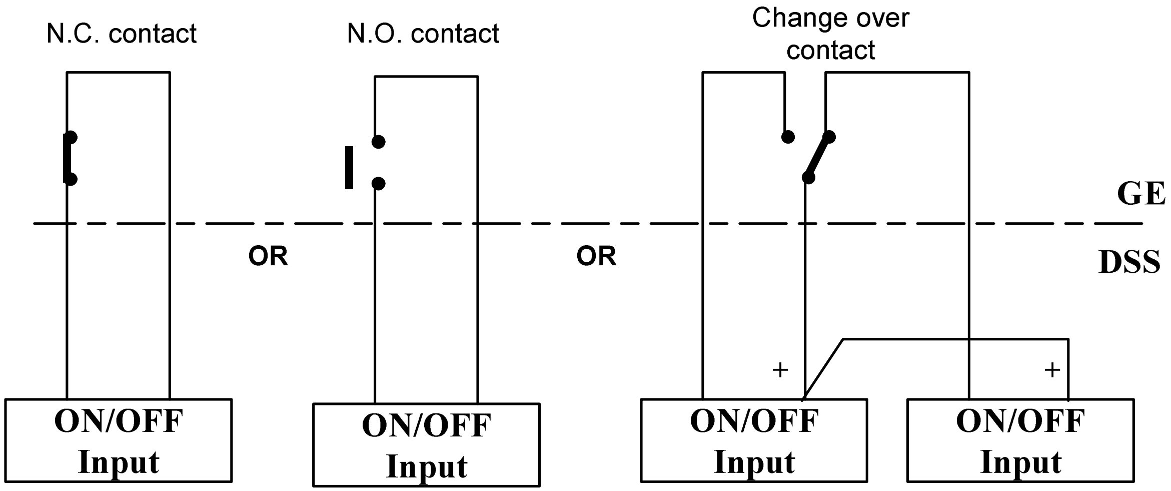
Input/output devices

- ❑ Refer to SPINLINE 3 data sheets for electrical features
- ❑ Case of analogue sensor (typical of 4-20mA for pressure – absolute or differential, level) acquired by 16EANA board



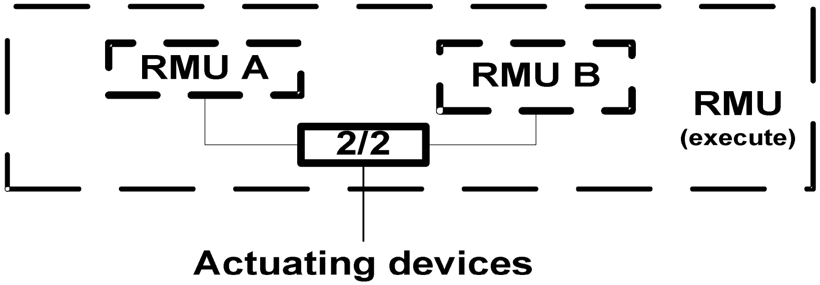
Input/output devices

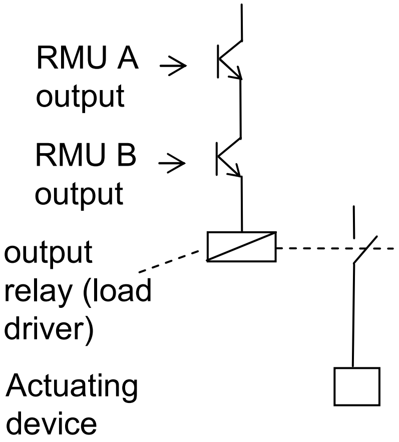
- Case of binary inputs (typical of U = 15VDC, I= 9 mA) acquired by 32ETOR board



Input/output devices

- The 2/2 vote is a hardwired logic based on AND-ed transistors :
  - each RMU controls transistors on its 32 ACT board
  - The AND is hardwired through MV16 boards





IEEE 603 6.2 Manual control

- Requirements IEEE 603 :
  - 6.2 a) Implement manual initiation at division level. Minimize number of operator manipulations and number of equipment consistent with 5.6.1 (independence between redundant portions of a safety system):
    - Each division has independent individual manual controls per valve initiated by operator through VDU directly to RMU-X. These manual controls are independent and physically separated (see discussion on independence)
    - Each division has independent system level (e.g. ADS, GDCS) manual controls initiated by operator through VDU to RMU-sense, DTLU and RMU-X to execute properly the time-phased system sequence.
    - For each division the above provides different manual controls on actuators
    - in case of failure of a part common to manual and automatic control, there are 3 other divisions to mitigate the failure
    - In case of CCF, the DPS is credited
    - Note : 6.2 a) is in the same spirit as RG1.62 items 4 and 5. RG1.62 is not considered here since it is based on IEEE 279, now withdrawn and replaced by IEEE 603

IEEE 603 6.2 Manual control

- 6.2 b) and 6.2 c) relates to design basis beyond the scope of ECCS/ ***SPINLINE 3.*** The implementation of manual controls in this system assumes that Clauses 4 e) and j) have been fulfilled by GE overall I&C design

IEEE 603 6.7 Bypasses - sensors

- **Division of Sensors bypass**
  - The goal of division-of-sensors bypasses is to allow the maintenance of sensors.
  - Bypassing any single division of sensors is accomplished from each divisional SSLC cabinet by manual switch control.
  - This bypass disables the DTLU A and B in the four divisions. Interlocks are provided so that only one division of sensors at a time can be placed in bypass.
  - When such a bypass is made, all four divisions of 2-out-of-4 logic become 2-out-of-3 logic while bypass is maintained.
  - Bypass permits calibration and repair of sensors or the DTLU function.
  - the remaining three divisions furnish sufficient redundant sensor data for safe operation and the logic is such that all four divisions can still perform 2-out-of-3 trip decisions even if sensors are bypassed
  - Bypass status is indicated to the operator until the bypass condition is removed. An interlock rejects attempts to bypass simultaneously more than one SSLC division.

IEEE 603 6.7 Bypasses - division

- **Division-out-of-service bypass**
  - The goal of division-out-of-service bypass is to allow the maintenance of the division. Only one division at a time can be bypassed.
  - When such a bypass is made :
    - The power supply of all RMU outputs of the related division is switched off for all systems being energized-to-operate.
    - The power supply of all RMU outputs of the related division is maintained for all systems being de-energized-to-operate. The only one in this case for ECCS is ICS.