Influence of highly integrated systems on Chips on the FDIR concepts and practices: the example of SCoC3 within OSCAR computer (AS250 OBC)

Laurence Meredith // 04th October 2011

All the space you need

ASTRIUM
AN EADS COMPANY

Outline

- FDIR (Failure Detection Isolation and Recovery) general principles
- Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3 microprocessor
  - AS250: generic platform for **L**ow **E**arth **O**rbit Earth observation & science satellites
  - SCoC3: Spacecraft Controller on a Chip 3: Integrated microprocessor using a LEON 3 chip
- CONCLUSION

FDIR: General principles (1/2)

- Answer to customer's autonomy, availability and survivability requirements
- Based on general principles which define the FDIR concept
  - Hierarchy,
  - Required reaction time,
  - Recovery actions….
- Relies on design resources (redundancies…), robustness features and on failure management (FDIR function)

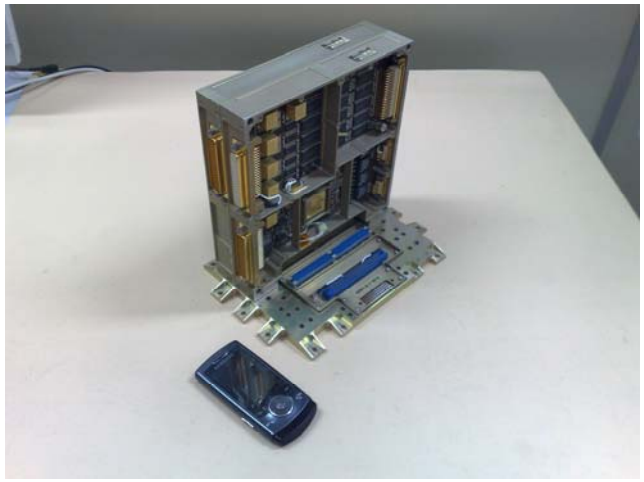
➔ Independent from processor choice

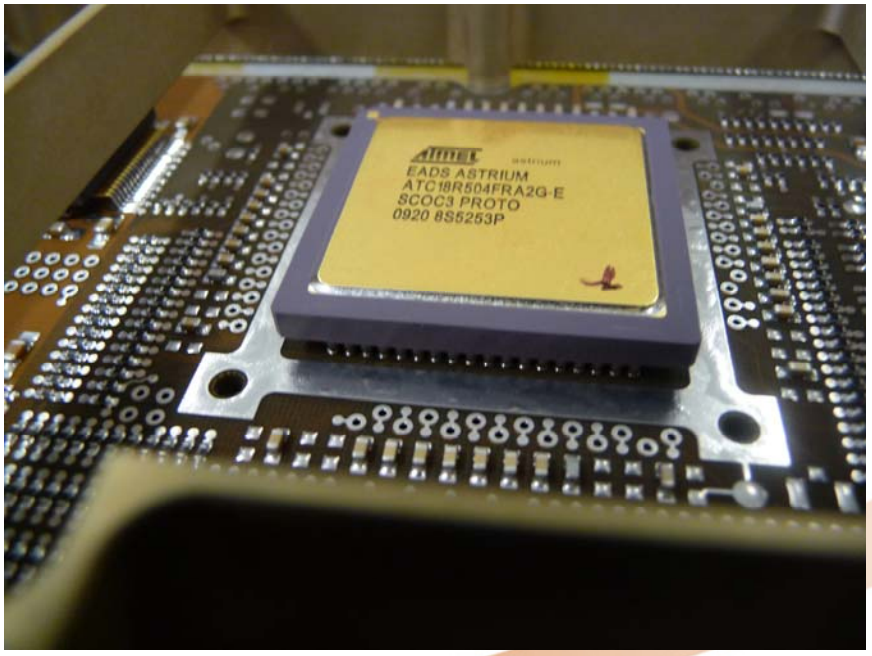
FDIR: General principles (2/2)

- The FDIR principles do not depend on the processor performances and internal architecture
- Conversely some processor features such as:
  - Self test capability,
  - Processing performance,
  - Cross strapping between nominal and redundant processor modules

Constitute added-value characteristics supporting the FDIR implementation

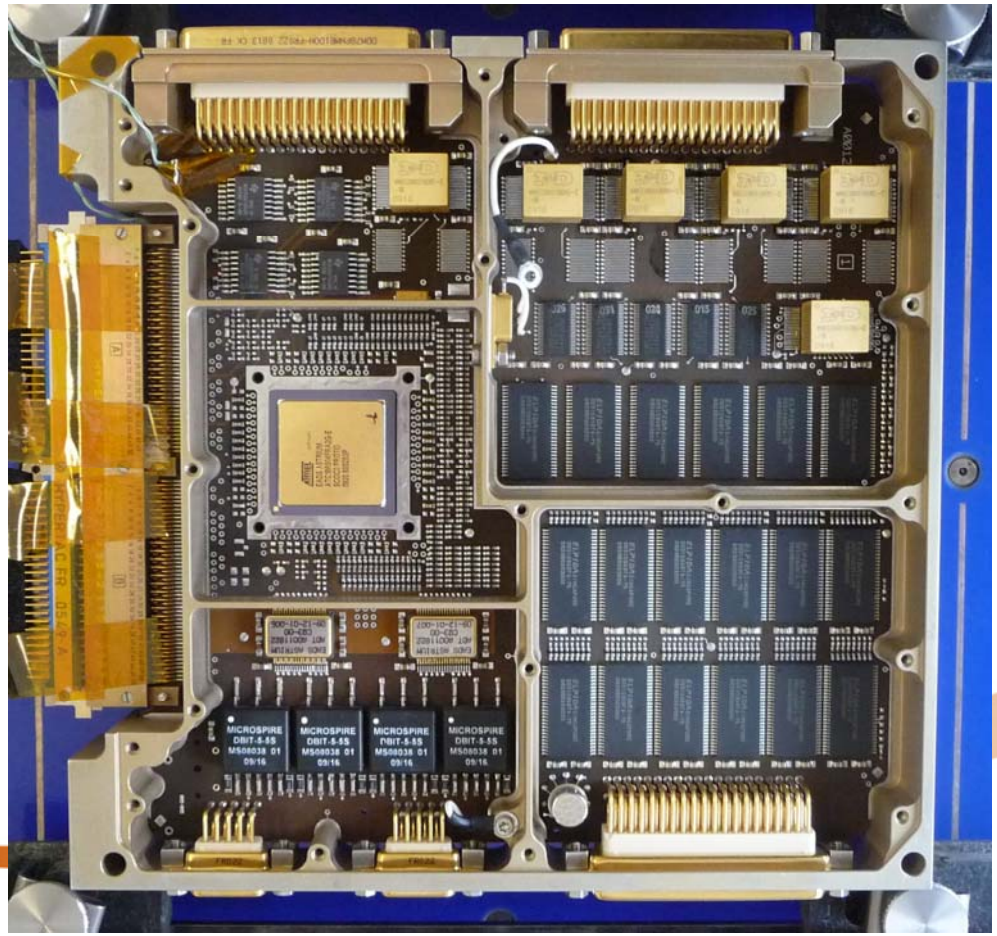
Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3





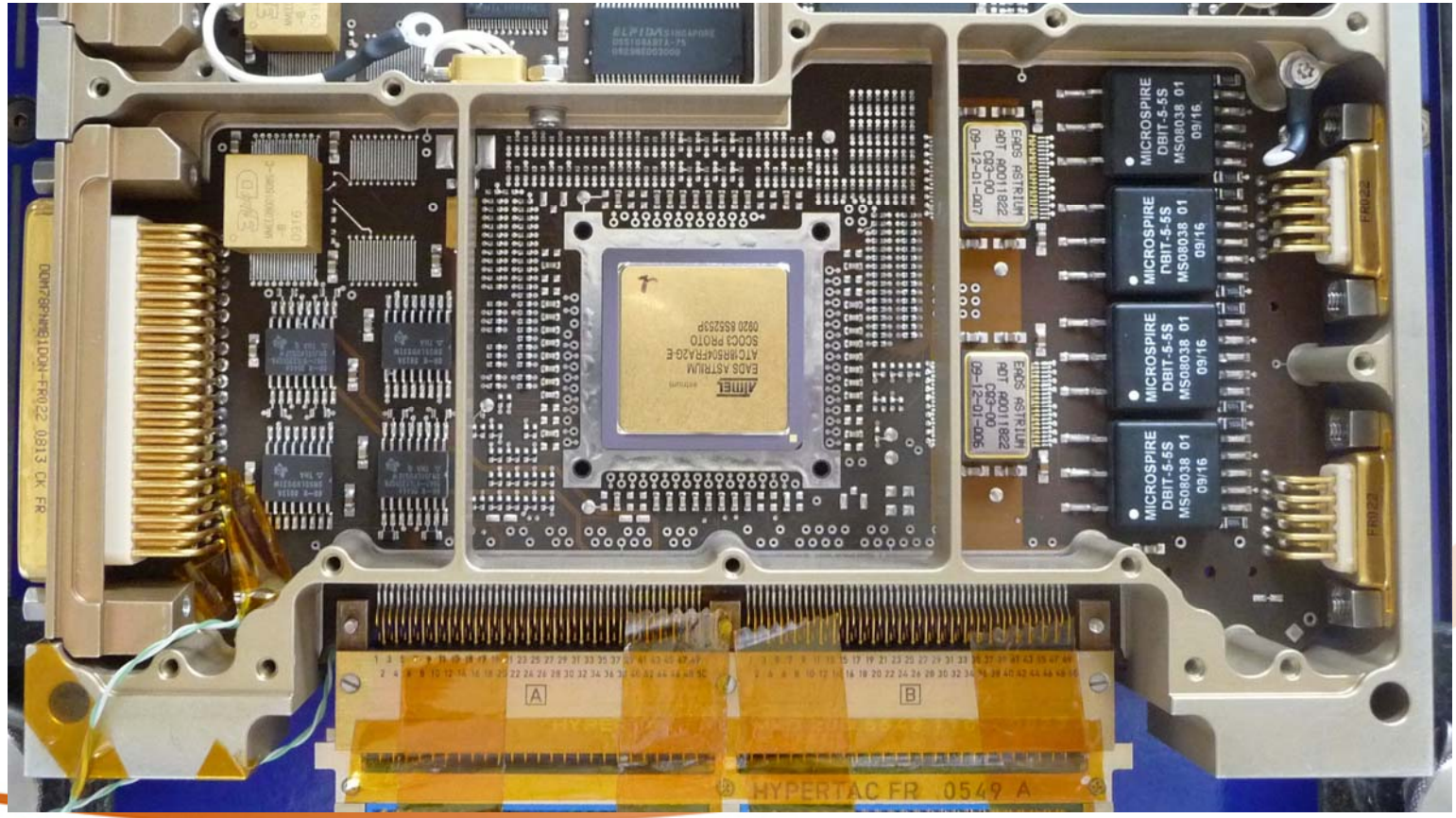
Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

- Kerops 1 (processor board of nominal OBC)



Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

- Kerops 2 (processor board of redundant OBC)



Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

- SCoC3 auto-test capability:

  1) Addition of « very early error detection » mechanisms as the result of co-enginering betwwen HW and SW teams:
  - All the IPs registers of the IPs connected to the AMDA buses (internal buses) are almost instantaneously accessible by the processor
    - IP: Instruction Pointer: bus suscribers (modules)
  - Additionnal diagnostics register are implemented

    - All failures are individually and accurately identified

    - Compared to a processor with non-integrated (discret) components, the failures are precisely identified: processor acces to all information thanks to all IPs registers acces instead of only 1 « error report» available for each interface which does not provides failure details

  2) The 2 SDRAM areas scrubbing is performed automatically by HW (done by SW on previous generations - 1750 or ERC32): 1 less task for the SW.

Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

- SCoC3: processing performances for a few frequencies

Mhz	Dhrystone MIPS	Whetstone MIPS
32	31	17.2
48	38.3	25.8
80	68	42

Note 1:Dhrystone MIPS gives the performance for integer unit and whestone MIPS for floating point unit

Note 2:ERC32 performance was 18MIPS at 25Mhz and MA3 1750 performance was between 1 and 3 depending on the frequency

Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

3 main objectives of the AS250 FDIR:

1) **Guarantee the satellite integrity in case of failure leading to the irreversible loss of the nominal mission**
   - ➔ *definition of a satellite safe mode and associated transition criteria*
2) **Optimize the mission operational availability**
   - ➔ *implementation of fault tolerant design with reactive and accurate FDIR thus reducing mission outages* (✶)
3) **Simple and generic actions sequence for anomaly recovery**
   - ➔ *local reconfiguration when failure is well identified* (✶)
   - ➔ *switch off payload when mission continuity is no longer possible*
   - ➔ *survivability of the satellite through unique fall back sequence or safe mode when failure is complex or critical*

✶ *Requires high processing performance, a processor with high self test coverage capability and the possibility to use processor and inputs/outputs management independently with cross strapping between nominal and redundant functions for more robustness – as featured by SCoC3*

Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

- Hierarchical anomaly management depending on the Time To React

Reaction time	FDIR type	Detection / Isolation	Reconfiguration
< 30s	1 - Immediate reaction By on board hardware protection function	On-board	Performed on- board
30s <T< 96h	2 - On board software Implementing SW monitorings	On-board	Performed on-board or by Ground Control Centre depending on the failure
T > 96h	3 - Ground Control Centre Through monitorings and housekeeping telemetries	Ground Control Centre	Performed by Ground Control Centre

Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

1 – Immediate on-board protections:

- The associated action consists in a immediate passivation of the monitored function and a transition in stable state ensuring the satellite integrity or mission continuity. The Ground Control Center is in charge of satellite final configuration.
- There are:
  - Local hardware protections: The PCDU implements LCLs switching OFF the failed equipments to avoid electrical or thermal failure propagation. The continuation of the failure management is handled by the CSW Functional Monitorings dedicated to the failed equipment.
  - System software alarm: As soon as the watch dogs implemented in the OBC are triggering, a transition in safe mode is initiated in order to put the satellite in a stable safe state.

➔ ***SCoC3 very high self failure detection coverage allows identification and passivation of the failure with a very high level of confidence: mission disturbance minimised.***

➔ ***A higher processor self failure detection coverage and thus a more appropriate reaction in case of processor failure: self correction or reset or processor reconfiguration to the redundant unit.***

Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

2 – On board software monitoring (or Functional Monitoring):

- Four different actions are performed by the on-board software depending on the anomaly detected:
- Emission of an anomaly message to the Ground Control Centre without any modification of satellite configuration or mode,
- Local reconfiguration remaining in operational mode,
- Payload switch off and transition in payload safe mode,
- Transition in acquisition or safe mode,

➔ *SCoC3 has a higher processing capability which allows implementing monitoring (at equipment or global functional chain or system level) that require processing (less limitation than for other processors which processing capability is almost all dedicated to nominal functions),*

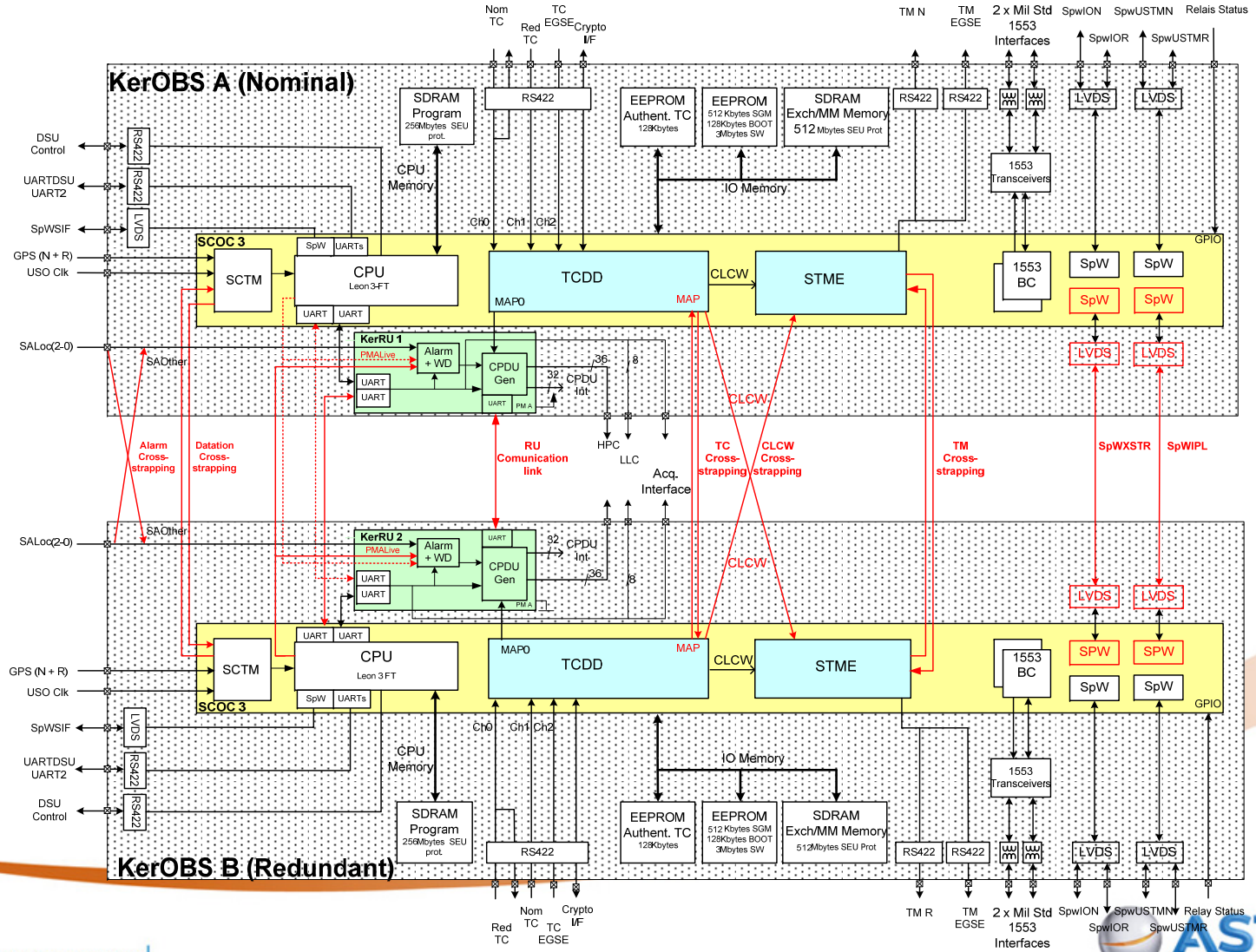
➔ *Independent KerRU (reconfiguration unit) cross strapped with SCoC3 to generate a reconfiguration of the OBC in case of internal failure.*

3 – Ground Control Centre monitoring:

- The detection and the whole recovery process is supported by the ground.

Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

Cross-strappings between SCoC3 functions

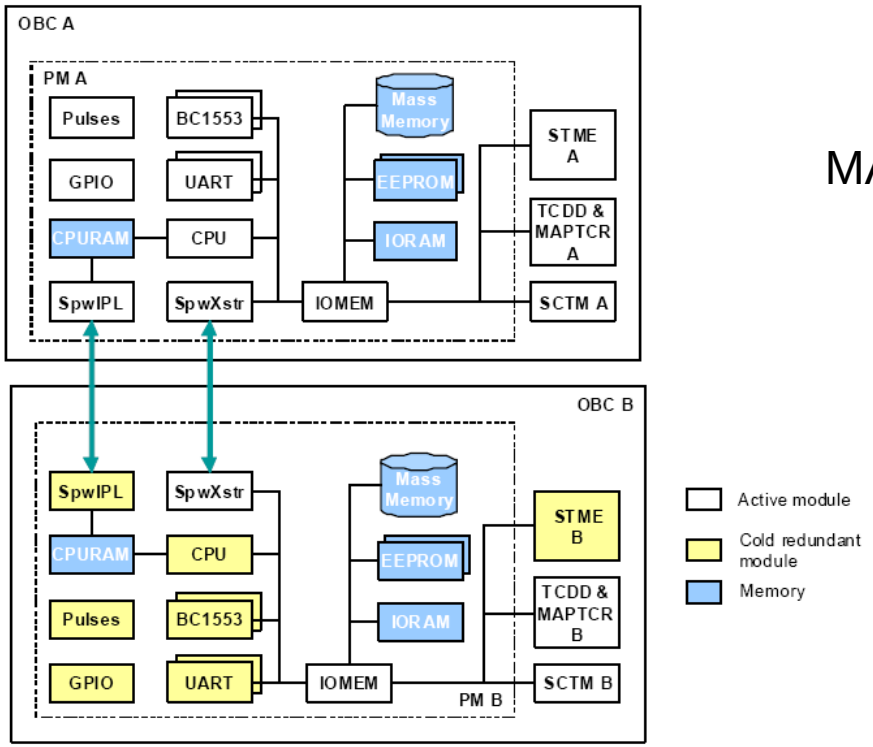


Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

- Cross strapping between the OBC core are the following:
  - The PM and the mass memories (SDRAM area)
  - The PM and the safeguards memories (EEPROM area)
  - The PM and the decoders
  - The PM and the reconfiguration unit
  - The PM and the datation modules
  - The PM and the transfer frame generators
  - ➢ Increase of system reliability and failure tolerance (design robustness)
- It has been proven that no single failure can possibly propagate from one OBC to the other (analyse performed in the Failure Mode Effect and Criticality Analysis – FMECA - physical HW implementation taken into account + thermal analysis)

Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

- Hot/cold redundant architecture



MASTER OBC

SLAVE OBC

Example of AstroSat 250 FDIR: AS250 OBC based on a SCoC3

- The cross-strappings between SCoC3 modules allows more failure tolerance and higher reliability for the OBC function (nominal + redundant)
  - SCoC3 failure rate = 118fits at 45°C
- The integration of the processor functions within 1 chip instead of having discrete components decreases the failure rate of the processor function and increase the reliability of the equipment
  - Reliability of OBC function (2 OBC) over 10 years = 0.984

CONCLUSION

- Use of SCoC3 does not impact the FDIR principles and definition but allows:

1) High detection capacity of its own failures (for immediate reaction and accurate failure identification and isolation)

2) High processing capability available for SW monitoring's

3) High reliability thanks to cross strapping's and high integration

4) No failure potential propagation identified between nominal and redundant units