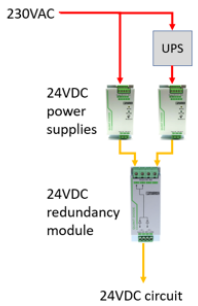
TUPV036

An Evaluation of Schneider M580 HSBY PLC Redundancy in the R744 System A Cooling Unit

D. Teixeira†, University of Cape Town, Cape Town, South Africa
L. Zwalinski, L. Davoine, W. Hulek, CERN European Organization for Nuclear Research, Geneva, Switzerland

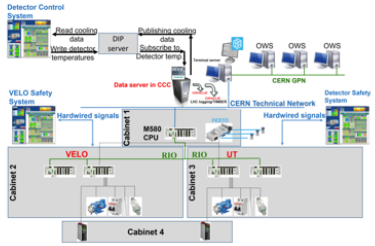
Existing Reliability Solutions in CERN CO_2 Control Systems

24VDC Power Supply Redundancy



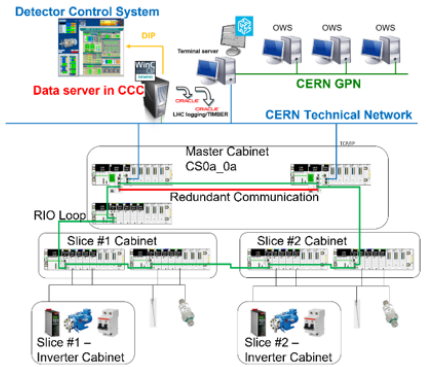
Many systems use 24VDC redundancy to avoid power failures. If either power supply fails, the system still has 24VDC. If the external 230VAC power source fails, there is one power supply connected to UPS and can continue to power the circuit for a limited time

MAUVE Control System RIO loop



MAUVE makes use of RIO loop ring topology to transfer data between external I/O cards and the PLC

Implementation of Schneider M580 HSBY Redundant PLCs



R744 Primary System A - Control System Architecture

- R744 Primary System A uses Schneider M580 HSBY (Hot Standby) Redundant PLCs
- 2 PLCs with redundant communication between them
- One PLC operates the system (Primary PLC) while the other remains ready to take over (Standby PLC)
- Connected to remote I/O cards with RIO loop
- Each PLC has its own redundant 24VDC power supply
- Each PLC has its own connection to the Technical Network

Failure Modes Resulting in PLC Switching

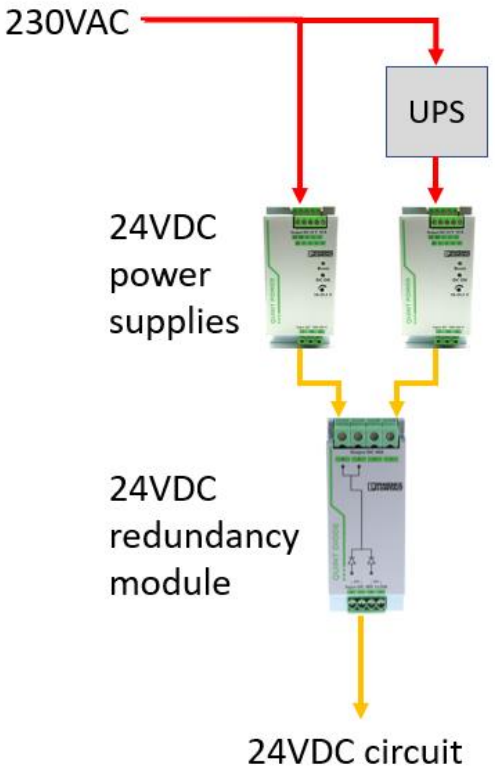
Failure mode	PLC A	PLC B	System Response
1. PLC B failure	Primary	Off	Running
2. PLC A failure	Off	Primary	Running
3. Failure of both PLCs	Off	Off	Not running
4. PLC A loss of network communication	Standby	Primary	Running
5. PLC B failure & PLC A loss of network communication	Primary	Off	Running, no network communication
6. PLC B loss of network communication	Primary	Standby	Running
7. PLC A failure & PLC B loss of network communication	Off	Primary	Running, no network communication

Failure Modes with Complex PLC Response

Failure mode	PLC Behaviour and System Response
8. Logic of PLC A different to PLC B	The PLC which is initially primary remains as such and the other PLC is in wait mode. The system operates without error.
9. Loss of one link between backplanes	The primary and standby PLCs remain as they were, and the system operates as normal
10. Loss of multiple links between backplanes	The primary and standby PLCs remain as they were, but the system runs with loss of functionality. The backplanes which are completely cut off from the PLCs are inoperable.
11. One PLC is completely disconnected from the RIO loop, the other has no connection to the Technical Network, the Hot Standby link is still available	The PLC connected to the Technical Network becomes the primary and the PLC which is still connected to the RIO loop is in standby. In this case the system does not operate as the primary PLC has no communication with the remote backplanes

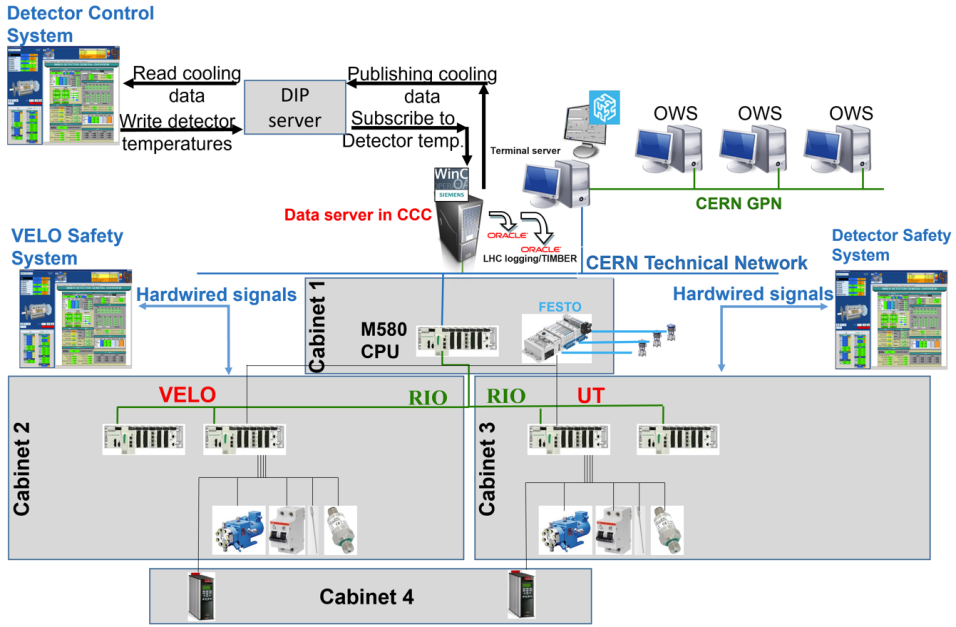
Existing Reliability Solutions in CERN CO_2 Control Systems

24VDC Power Supply Redundancy



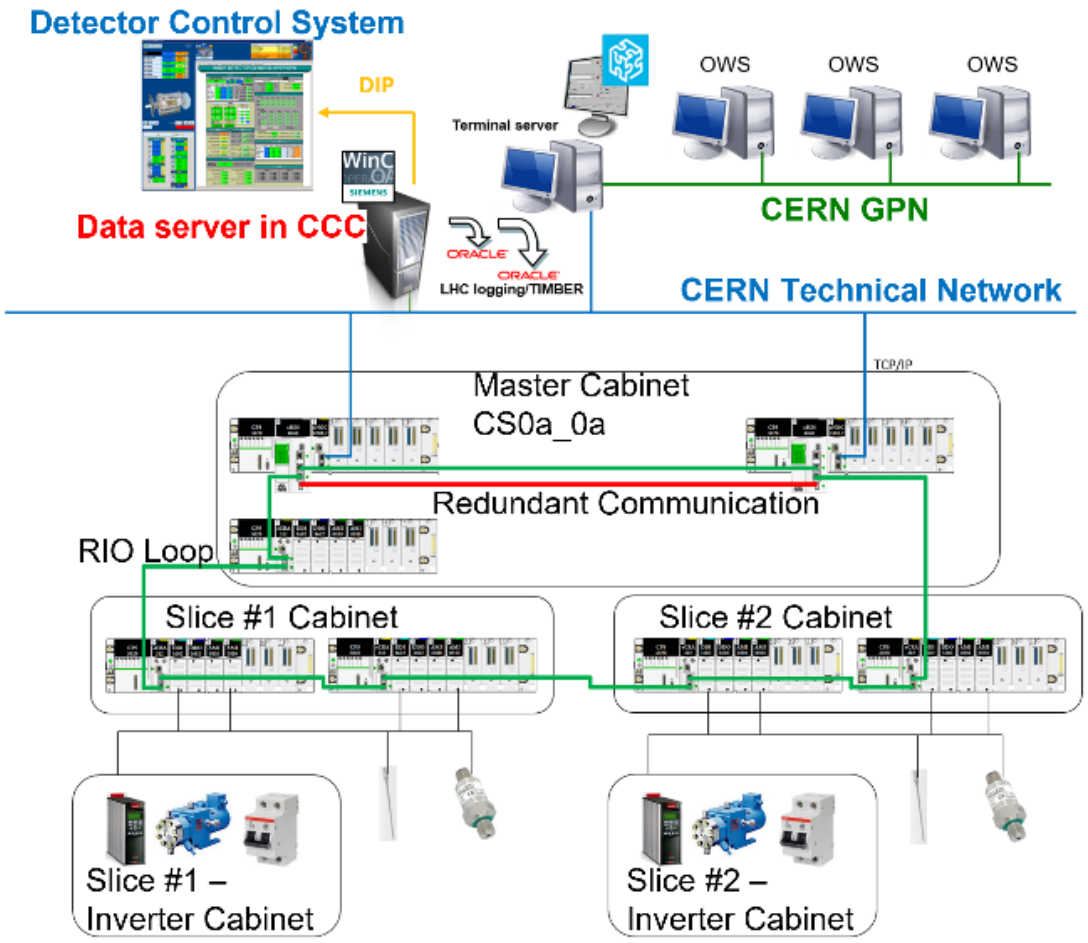
Many systems use 24VDC redundancy to avoid power failures. If either power supply fails, the system still has 24VDC. If the external 230VAC power source fails, there is one power supply connected to UPS and can continue to power the circuit for a limited time

MAUVE Control System RIO loop



MAUVE makes use of RIO loop ring topology to transfer data between external I/O cards and the PLC

Implementation of Schneider M580 HSBY Redundant PLCs



R744 Primary System A - Control System Architecture

- R744 Primary System A uses Schneider M580 HSBY (Hot Standby) Redundant PLCs
- 2 PLCs with redundant communication between them
- One PLC operates the system (Primary PLC) while the other remains ready to take over (Standby PLC)
- Connected to remote I/O cards with RIO loop
- Each PLC has its own redundant 24VDC power supply
- Each PLC has its own connection to the Technical Network

Failure Modes Resulting in PLC Switching

Failure mode	PLC A	PLC B	System Response
1. PLC B failure	Primary	Off	Running
2. PLC A failure	Off	Primary	Running
3. Failure of both PLCs	Off	Off	Not running
4. PLC A loss of network communication	Standby	Primary	Running
5. PLC B failure & PLC A loss of network communication	Primary	Off	Running, no network communication
6. PLC B loss of network communication	Primary	Standby	Running
7. PLC A failure & PLC B loss of network communication	Off	Primary	Running, no network communication

Failure Modes with Complex PLC Response

Failure mode	PLC Behaviour and System Response
8. Logic of PLC A different to PLC B	The PLC which is initially primary remains as such and the other PLC is in wait mode. The system operates without error.
9. Loss of one link between backplanes	The primary and standby PLCs remain as they were, and the system operates as normal
10. Loss of multiple links between backplanes	The primary and standby PLCs remain as they were, but the system runs with loss of functionality. The backplanes which are completely cut off from the PLCs are inoperable.
11. One PLC is completely disconnected from the RIO loop, the other has no connection to the Technical Network, the Hot Standby link is still available	The PLC connected to the Technical Network becomes the primary and the PLC which is still connected to the RIO loop is in standby. In this case the system does not operate as the primary PLC has no communication with the remote backplanes