TRICON
Fault Tolerant Systems

Definizioni

Safety

(Sicurezza)

Si definisce Sicurezza la libertà da un rischio inaccettabile, per il Personale, la Collettività, l'Ambiente.

TRICONEX Systems

- Goal : Safety
- Strategy : Fail Operationnal
- Measurement: Reliability
- Method: Fault Tolerance

Applications Areas

Industries ...

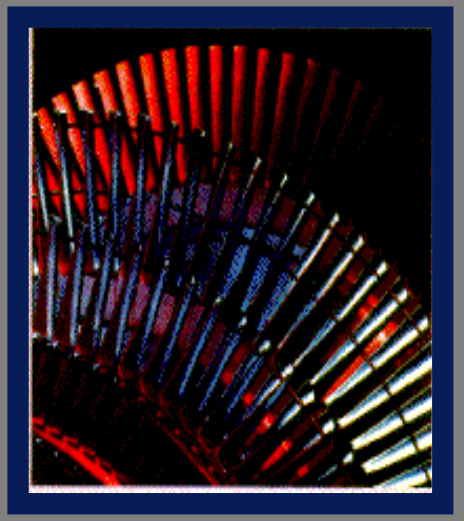
Oil & Gas	Hydrocarbon Processing	Utility
Pulp & Paper	Marine	Nuclear
Textile	Rubber and Plastics	Cement
Food	Pharmaceutical	Metals

Applications ...

Safety / ESD	Burner Management	Rotating Equipment
Fire & Gas	Automotive Presses	Critical Control

Expertise in Major Safety and Critical Control Areas:

TRI-SEN SYSTEMS

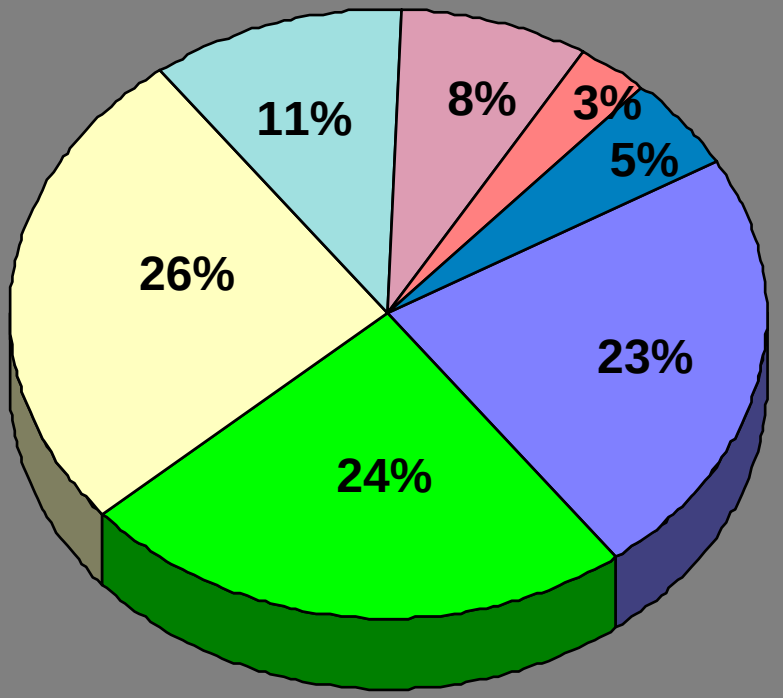


- Gas Turbine Control
- Steam Turbine Control
- Integrated Turbine Compressor / Anti-Surge
- Integrated Turbine Generator / Voltage Regulation

TRICON TMR SYSTEMS

- Safety / Emergency Shutdown
- Critical Control
- Burner Management
- Fire & Gas Detection
- New applications Nuclear & Transportation

Markets Served



- Chemical Manufacturing
- Petroleum Refining
- Oil & Gas Production
- Electric Power Utilities
- Marine
- Pulp & Paper
- Other

Technology and Quality

- TRICON TMR (Triplicated Modular Redundant) system is viewed as the standard for safety and critical control
- Triconex is the leading supplier of fault tolerant control systems worldwide:

  - Over 2 500 TMR and 4 200 Turbine Solutions installed worlwide and over 500 in Europe and Africa

  -62% market share (1996 Frost Sullican PLC study)
- Our TMR Products are designed to meet the highest levels of safety certification - IEC 1508 class 3, DIN VDE 0801, 19250 level 6 (TÜV clas 6), FM Class 1 Div. 2
- We continually certify our products to International standards - DIN, CSA, FM, IEC, UL, CE Mark, ABS

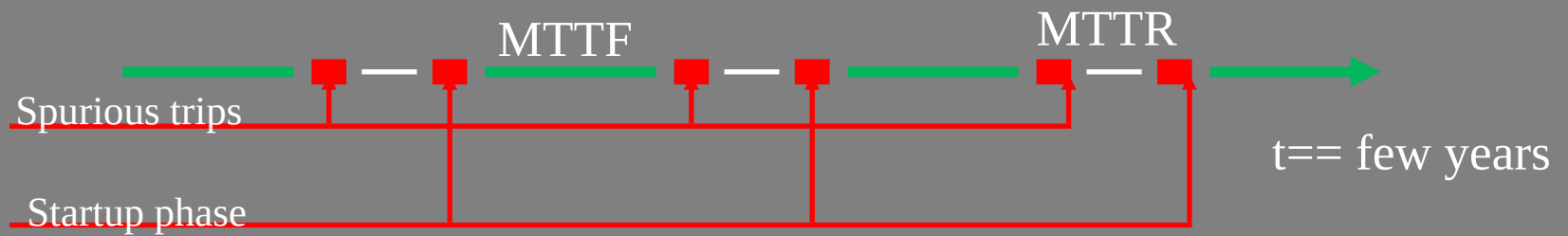
Strategy to fulfill safety requirements

- **" Fail Safe"** strategy: A failure inside a sub-system must shutdown the safety system

- **"Fail operationnal"** strategy: A failure inside a subsystem do not lead to a shutdown

Safety Application Lifecycle

- **"FAIL SAFE"**

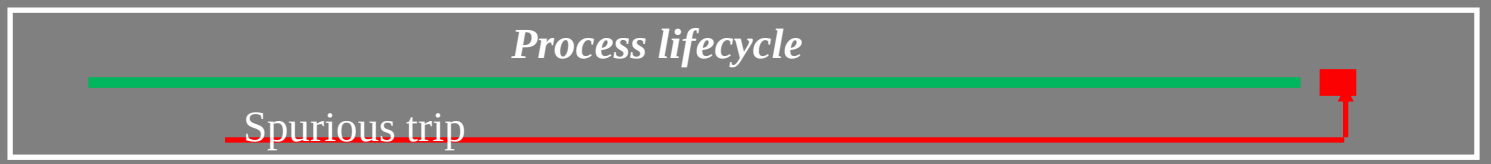


- **"FAIL OPERATIONNAL"**

- *Statistically, the accidents occured in transition phases (start-up, shutdown)*

Key Issues (Concept)

- Reliability = To avoid spurious trips
- Maintenance = To decrease downtime
- Availibility = To decrease production costs
- Safety = To control failures



Strategy to become reliable

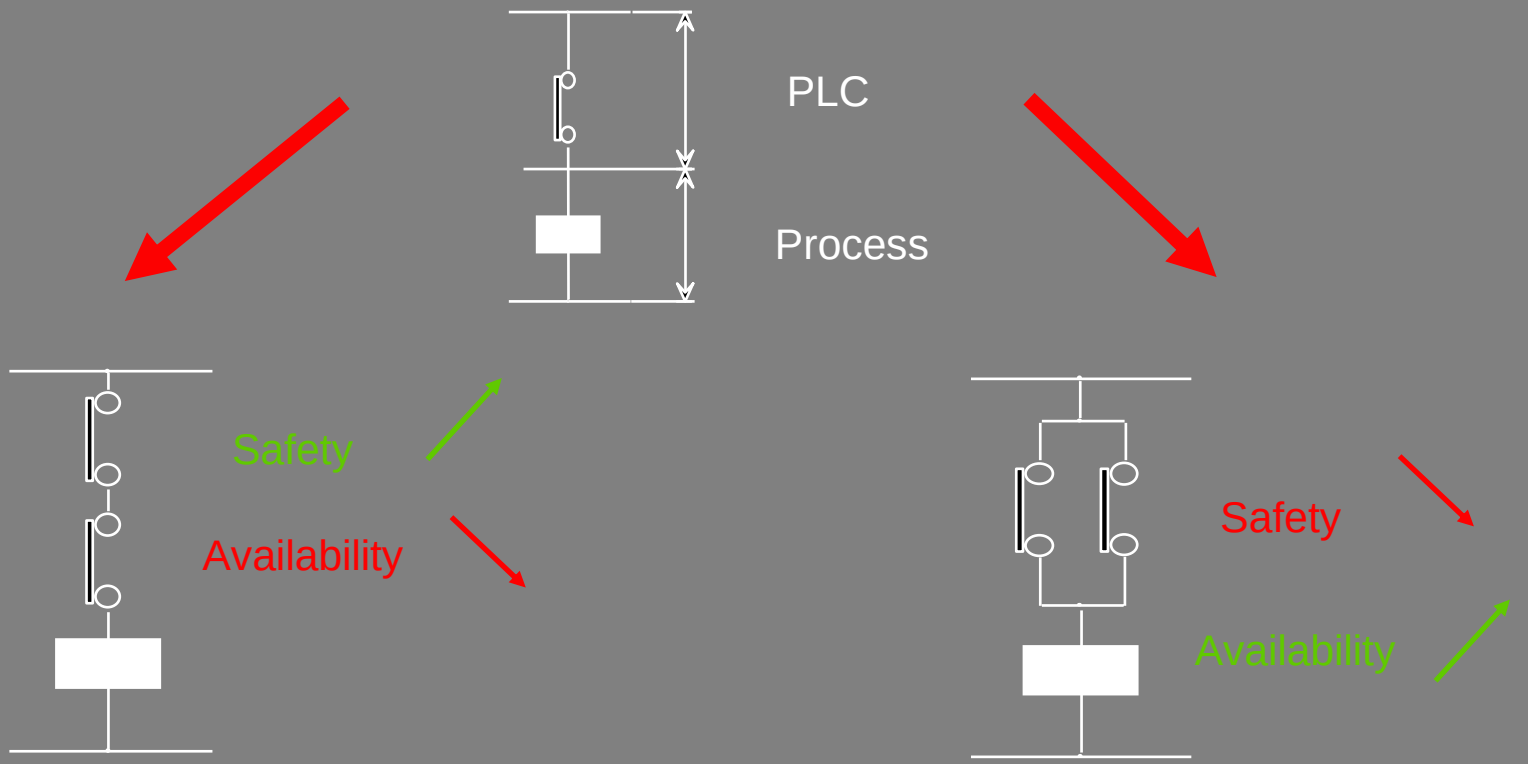
- Avoid Failure

  -Internal failures of the system (quality plan)
  -Exploitation failures (Programming tools, diagnostics, maintenance, training)

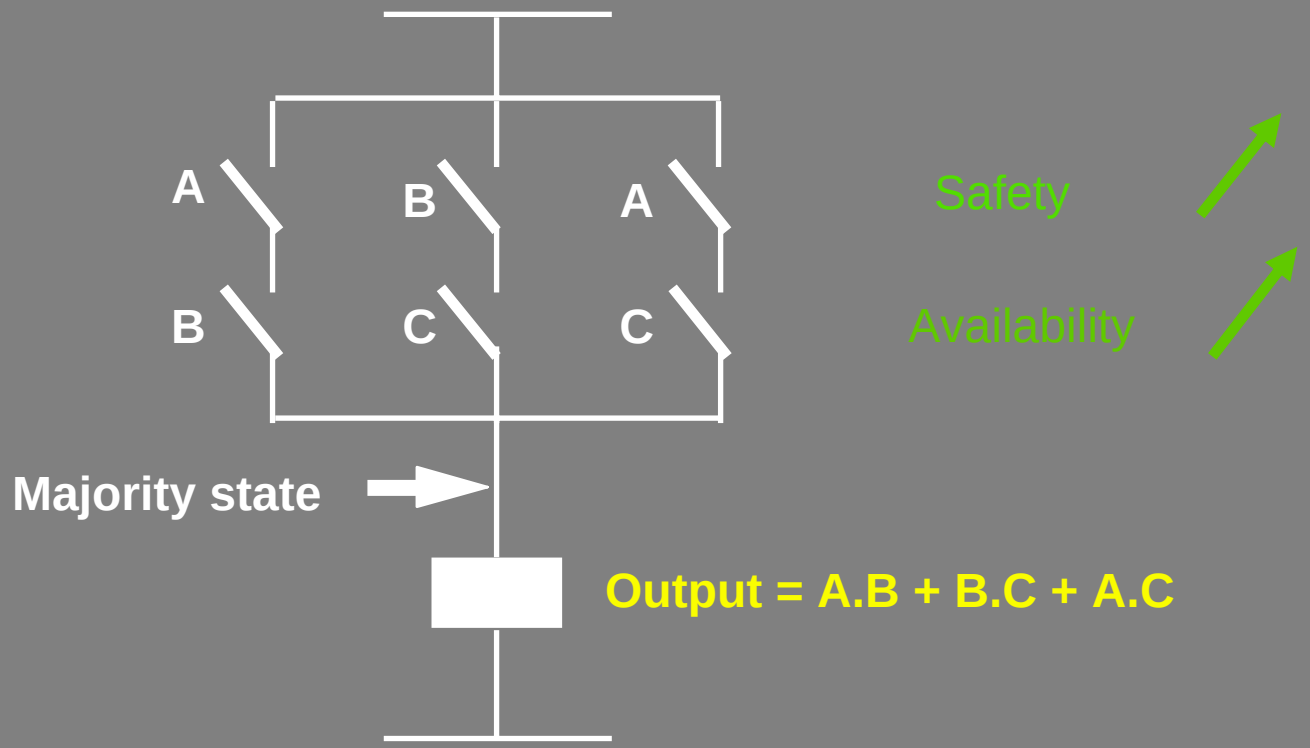
- Support failures

  -Electronic component failures
  -Mechanical component failures
  -No single point of failure
  -Redundancy
  -On line replacement

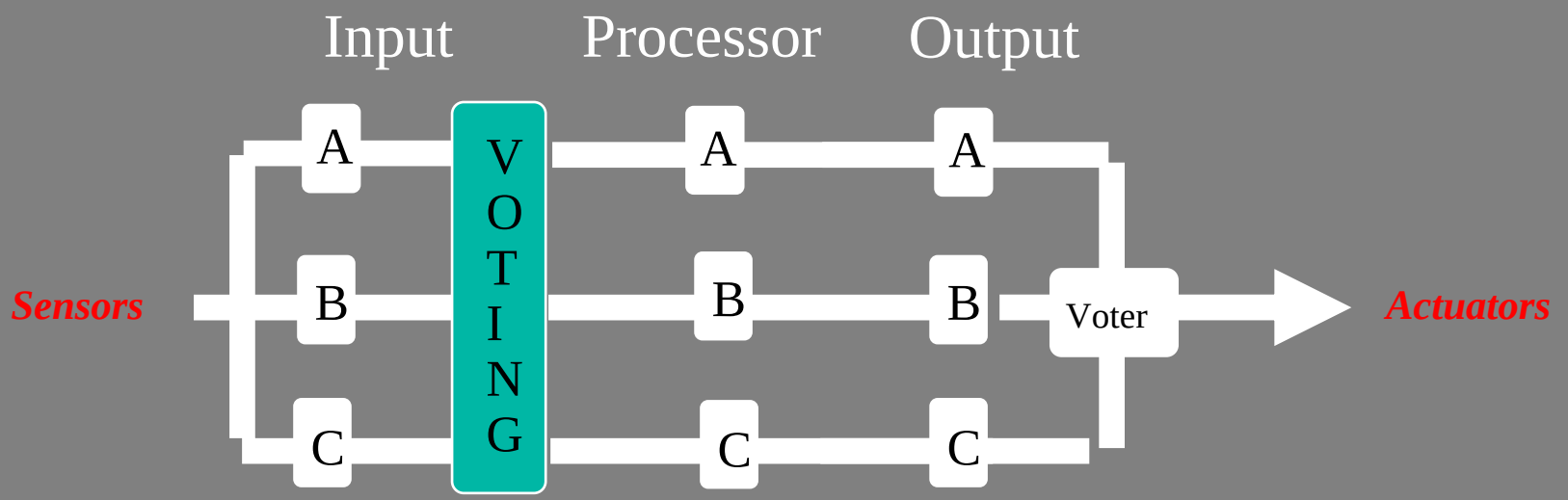
Dual Architectures



2°°3D Voting system



TMR Architecture



- No propagation
- Supports 2 faults of different ranks
- Diagnostics are easy to manage

TRICON - TMR Fault Tolerant Controller

Utilizes Triple Modular Redundant Architecture from Input Termination to Output Termination

❖ Definition of Triconex Fault Tolerance:

❖ *Identifies and Compensates for Failed Control System Elements and Allows On-Line Repair while Continuing its Assigned Task Without Process Interruption.*

- **High Safety Integrity - High Safety Availability Due to TMR Architecture, Diagnostics, and On-Line Repair**
- **High Availability - Eliminates Spurious (False) Trips**

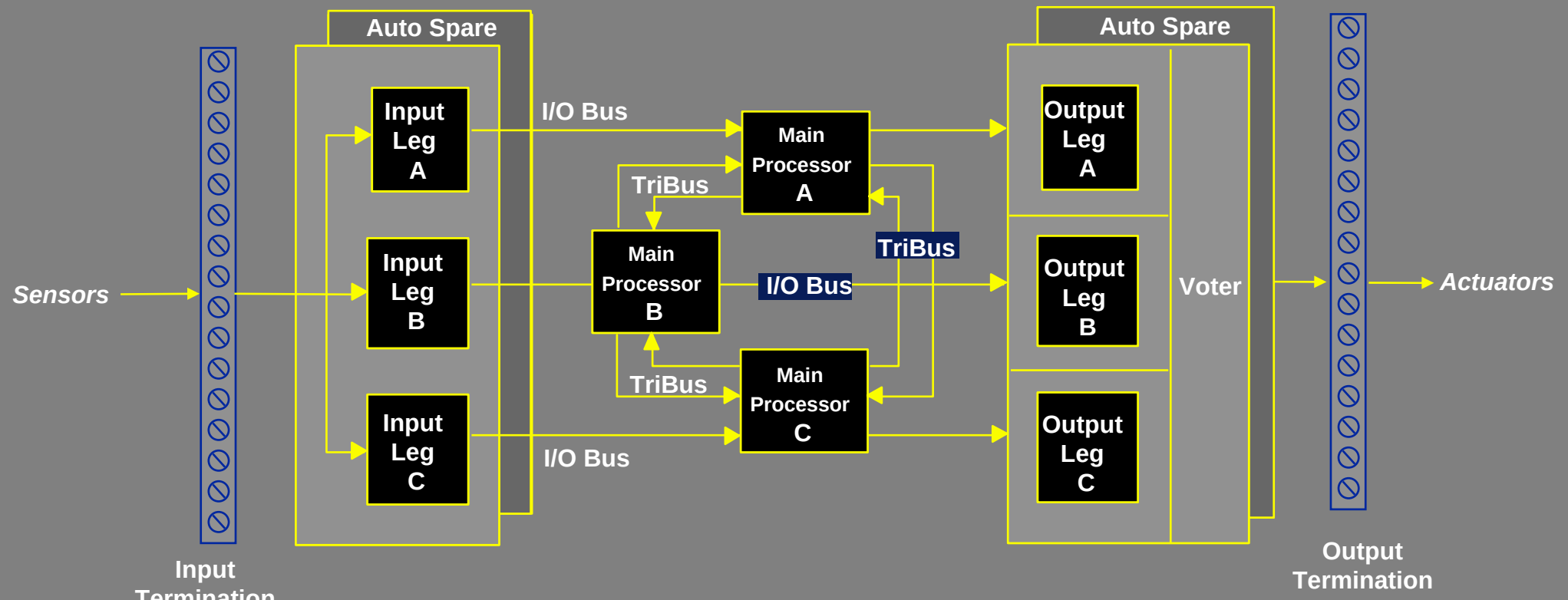
Triconex TMR vs. All Other PLC Technologies

1. **No Single Point of Failure**
2. **Diagnostics**
3. **On - Line Repair**

The Difference Between Long Term and Short Term Availability and Reliability ---- Diagnostics

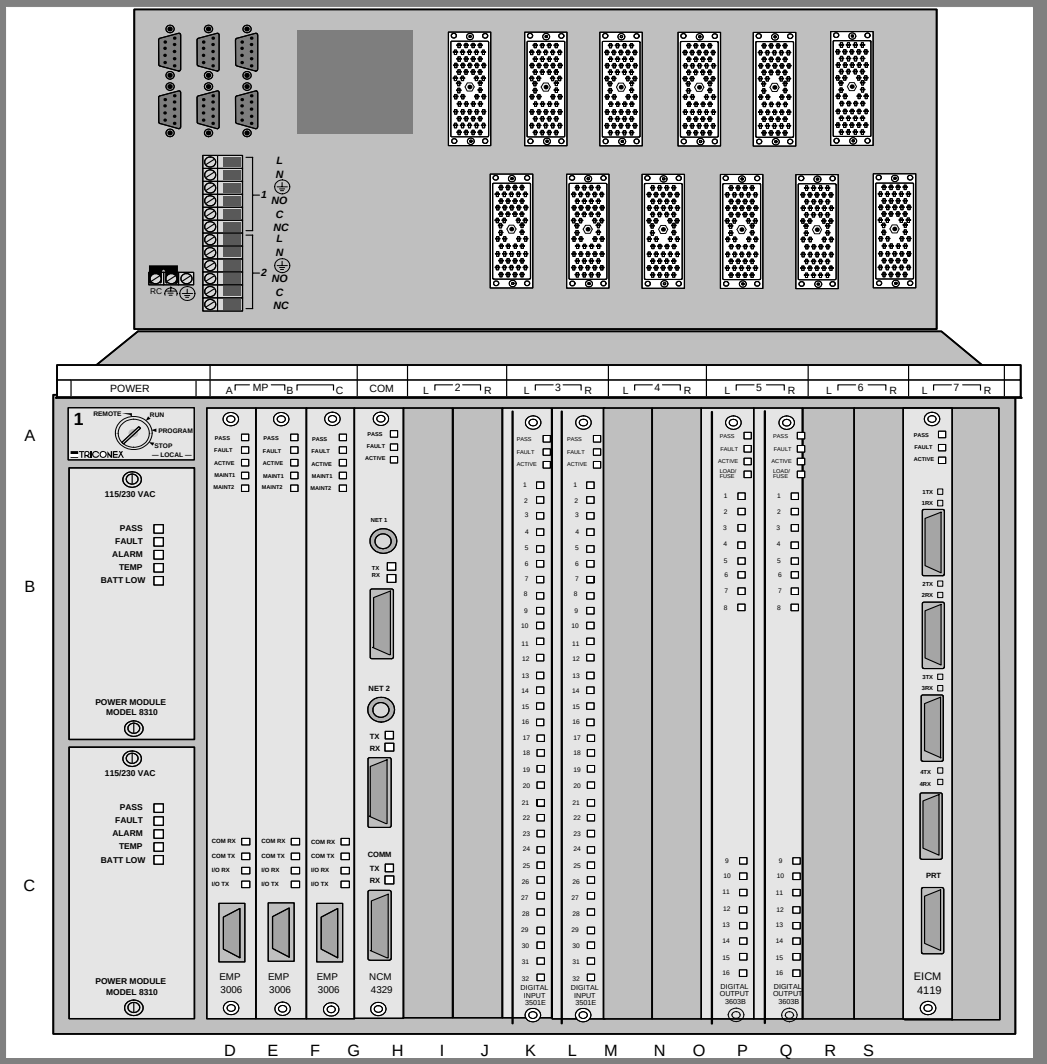
Diagnostics are Embedded in the System - Independent of User Written Application Programming!

Fully Triplicated Architecture

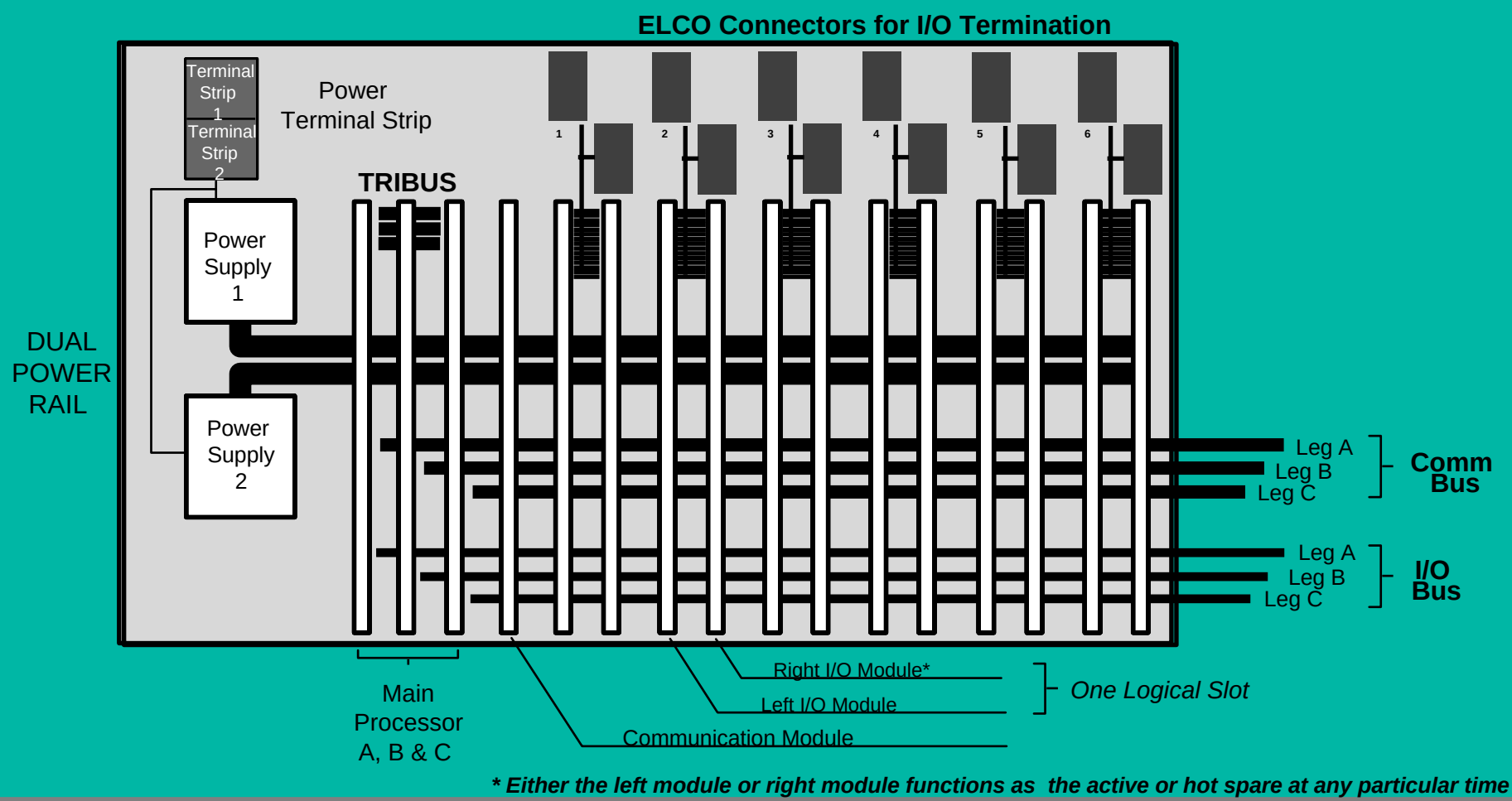


- No propagation
- Supports 2 faults of different ranks
- Diagnostics are easy to manage

Version 9 High Density Main Chassis



Chassis - Architecture



TRIBUS Hardware

- Three Independent Serial Links Transmit Data From Each Main Processor to the Other Two Main Processors
- Serial Links Operate at 4 MBits/Second
- Utilizes a Fault-tolerant Clock (Tri-Clock) Consisting of Three Independent Clocks and Associated Selection Circuitry

TRIBUS Functions

- **Synchronizes MPs at the Beginning of Each Scan**
- **Votes DI Data Between MPs and Flags Disagreements**
- **Transfers AI Data Between MPs**
- **Compares DO and AO Between MPs and Flags Disagreements**
- **Transfers Diagnostic and Program Data Between MPs**
- **Transfers Incoming Communication Messages Between MPs**
- **Communication Bus for Automatic Re-education of MP**

Main Processor Module

- **32 Bit Microprocessor Operating at 25 MHz**
- **Floating Point Co-Processor**
- **1800 Kbytes of User Memory**
- **I/O and Communication Co-Processors**
- **Fault Tolerant Interprocessor Bus (TRIBUS)**
- **Hardware Voting and Comparison Circuits**
- **Supports the Collection of Sequence of Events (SOE) Data**
- **Extensive Background Diagnostics**
- **On-Line Replacement**

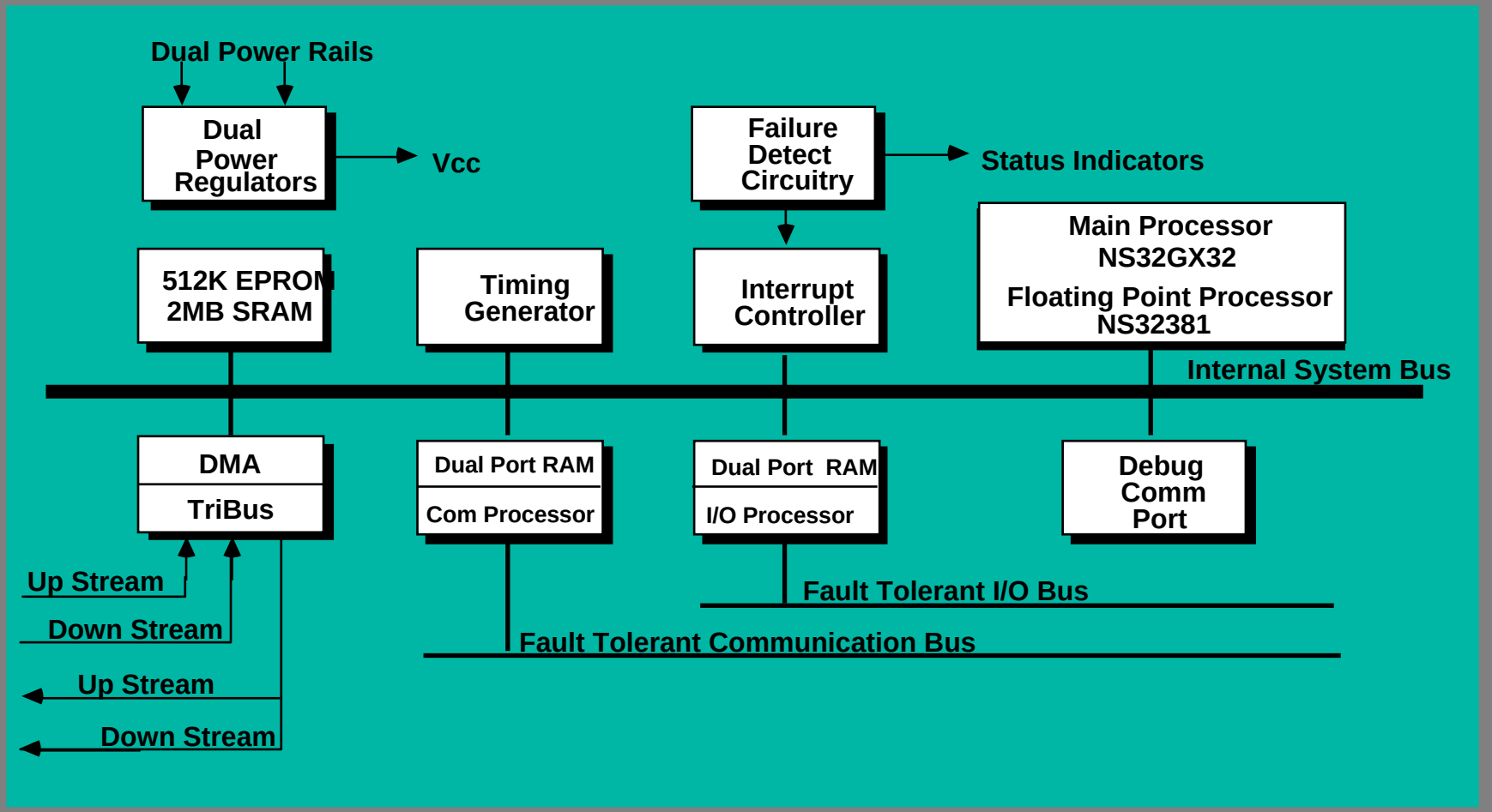
Diagnostics - Hardware

- **MPs Inspect the Chassis Layout for Proper Cards and Installed Cards**
- **Any Download Commands Will Create a System Inspection Query**
- **Application Program File Compared with Installed I/O Boards Firmware**

If a Board is Missing or Improperly Installed, The MPs Flag a System Alarm

During Downloads, TRISTATION Displays all Disagreements

Main Processor - Architecture



Fault Tolerant Power Subsystem

- **Dual High Density Power Supplies - Each Capable of Powering Entire Chassis Load (175 Watts Each)**
- **Dual Voltage Regulators - Two per Leg on Each Module**
- **Full Noise Isolation on Inputs and Outputs**
- **Over-Temperature Alarm**
- **On-Line Replacement**
- **Batteries for Memory Back-up on Main Chassis Backplane**

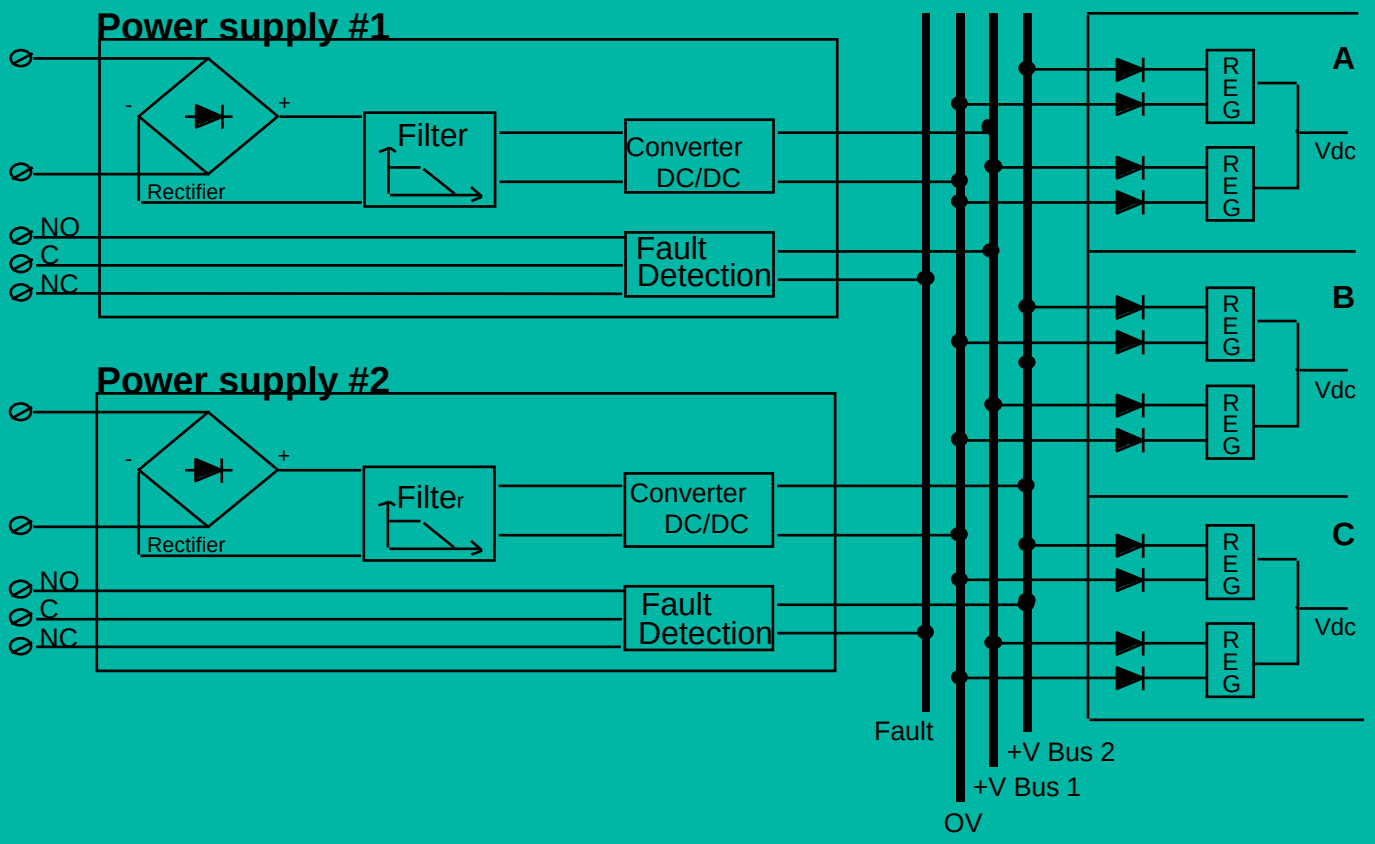
Diagnostics - Power Subsystem

Power Supplies, Batteries and Power Regulators are Fully Redundant and Tested Frequently

- **Output Voltage is Measure**
- **Main Chassis Batteries are Tested**
- **Each MP, I/O and Communication Module's On-board**
- **Power Regulators are Toggled Off to Test the Redundant Power Regulator**

If Fault is Detected by MPs 2oo3 Vote, Power Supply Fault Light is Energized and a System Alarm is Generated

Power Supplies - Architecture



Enhanced TMR Digital Input Module

- **Independent Signal Conditioning, Power Sources and Communications Paths**
- **No Single Point of Failure**
- **Tests for Stuck "ON" Circuits**
- **Full Isolation Between Channels**
- **Full Noise Immunity**
- **On-Line Replacement**

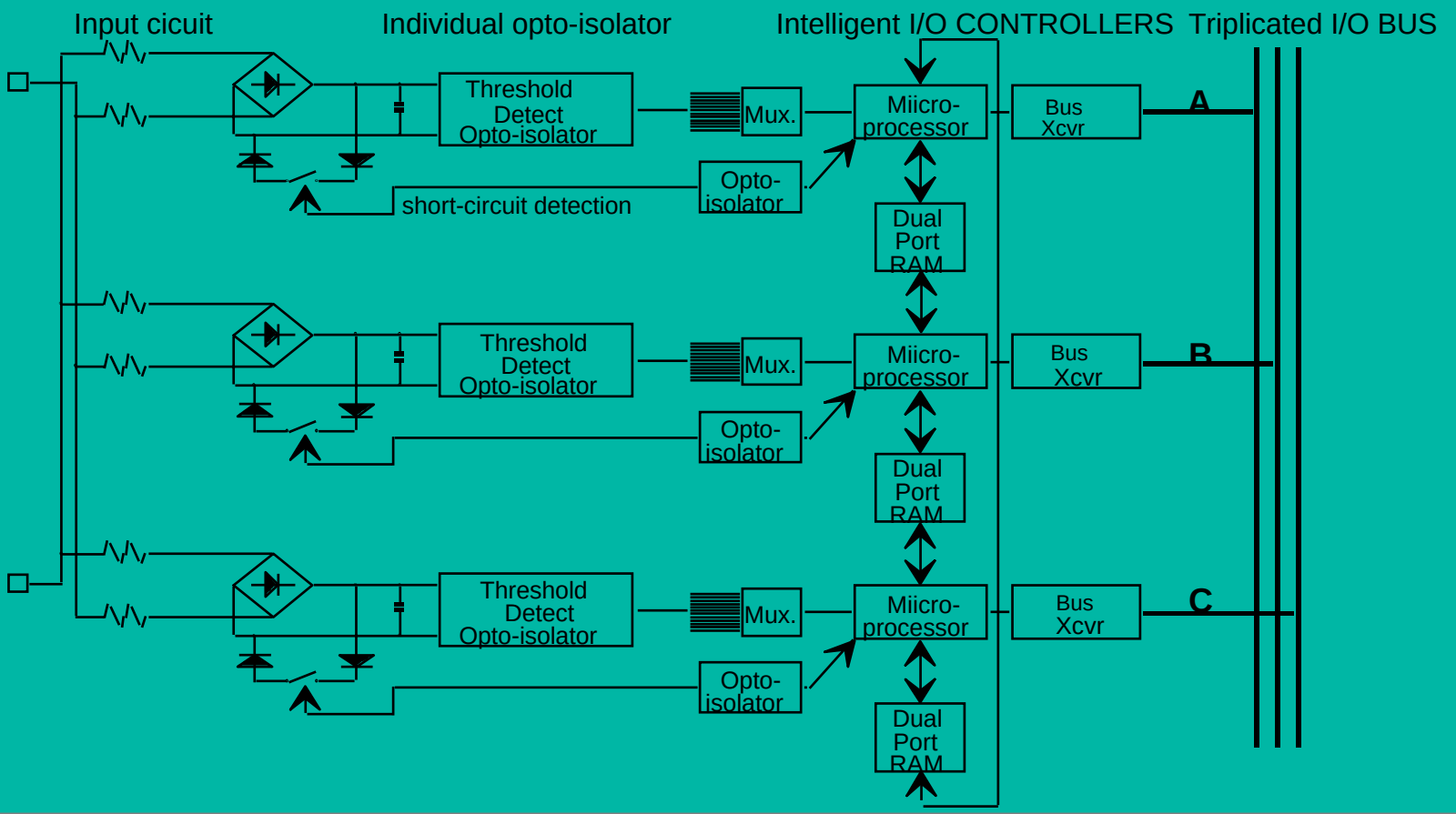
Diagnostics - TMR EDI Module

Continuous On Board Testing for Stuck - On Circuits

- **Each of Three Input Circuits Per Point are Tested for "Stuck-ON " Condition**
- **Status of Circuit Sent to MPs for Alarming**

If Circuitry is Found to be Stuck-On, MPs Vote to Activate DI Module Fault LED and Generate a System Alarm.

EDI Module - Architecture



TMR Analog Input Module

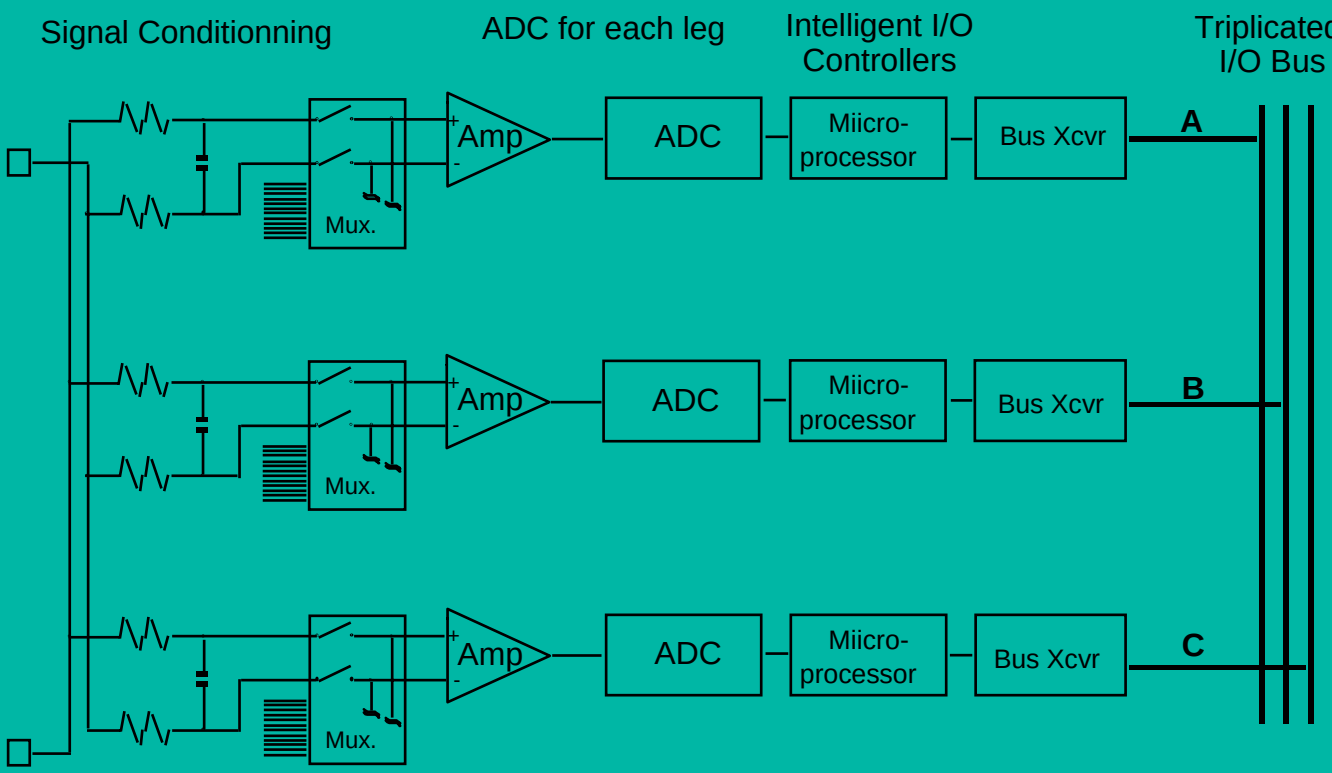
- **Triplicated A/D Converters and Multiplexors**
- **Automatic Calibration Using Built-in Reference Voltages**
- **0.15% Full Scale Range Accuracy**
- **No Single Point of Failure**
- **Isolated Input Channels**
- **On-Line Replacement**

Diagnostics - TMR AI Module

- *Mid-Value Select Algorithm with Measurement Deviation Testing*
  - **> 2% Standard Deviation from Mid-Value after 40 Deviations - Leg is Faulted**

Main Processors Vote to Energize Fault LED

TMR AI Module - Architecture



TMR Enhanced Digital Output Module

- **Fault Tolerant Hardware Voter for Each Output Point**
- **Series / Parallel Quad Output Circuits**
- **No Single Point of Failure**
- **Field Loopback Sensing**
- **Latent Fault Detection**
- **Fully Isolated Output Channels**
- **On-Line Replacement**

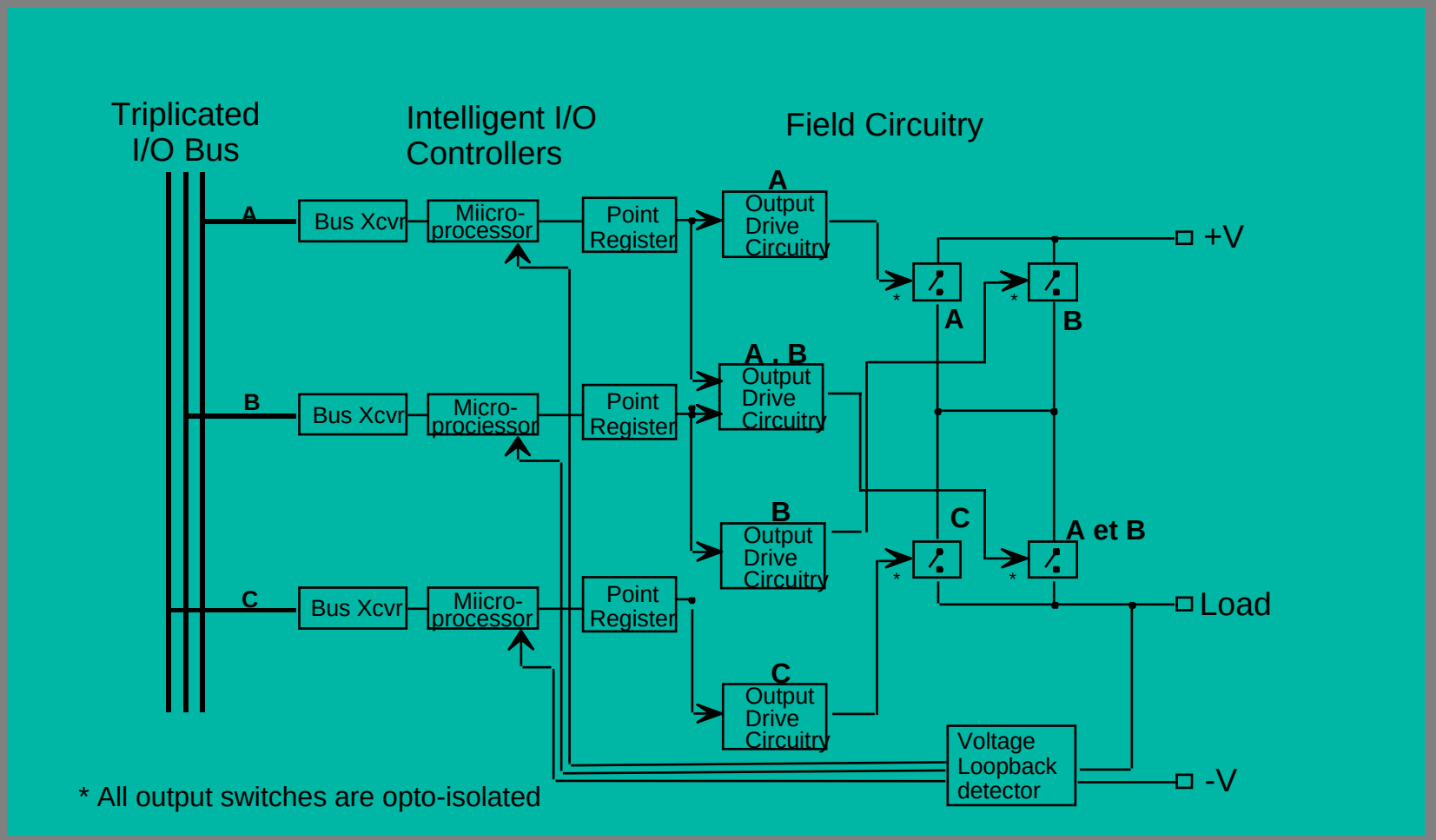
Diagnostics - TMR EDO Module

Stuck-On and Stuck-Off Tests are Performed Continuously

- **Both Tests Are Performed on All Output Circuits Regardless of Power Status. (NE or ND)**
- **Output Switches are Closed then Opened, Voltage Loopback Verifies Proper Operation**

If Switch is Found Faulty, MPs Vote to Activate DO Module Fault Light and Generate a System Alarm

TMR EDO Module : Architecture



Supervised Digital Output Module

- **Fault Tolerant Hardware Voter for Each Output Point**
- **Series / Parallel Quad Output Circuits**
- **24 VDC Version Uses Smart FETs That Require No Fusing**
- **No Single Point of Failure**
- **Field Loopback Sensing**
- **Latent Fault Detection**
- **Fully Isolated Output Channels**
- **Blown Fuse Detection**
- **Line Monitoring of Field Load (Open or Short)**
- **On-Line Replacement**

Diagnostics - Supervised DO

Stuck-On and Stuck-Off Tests are Performed Continuously

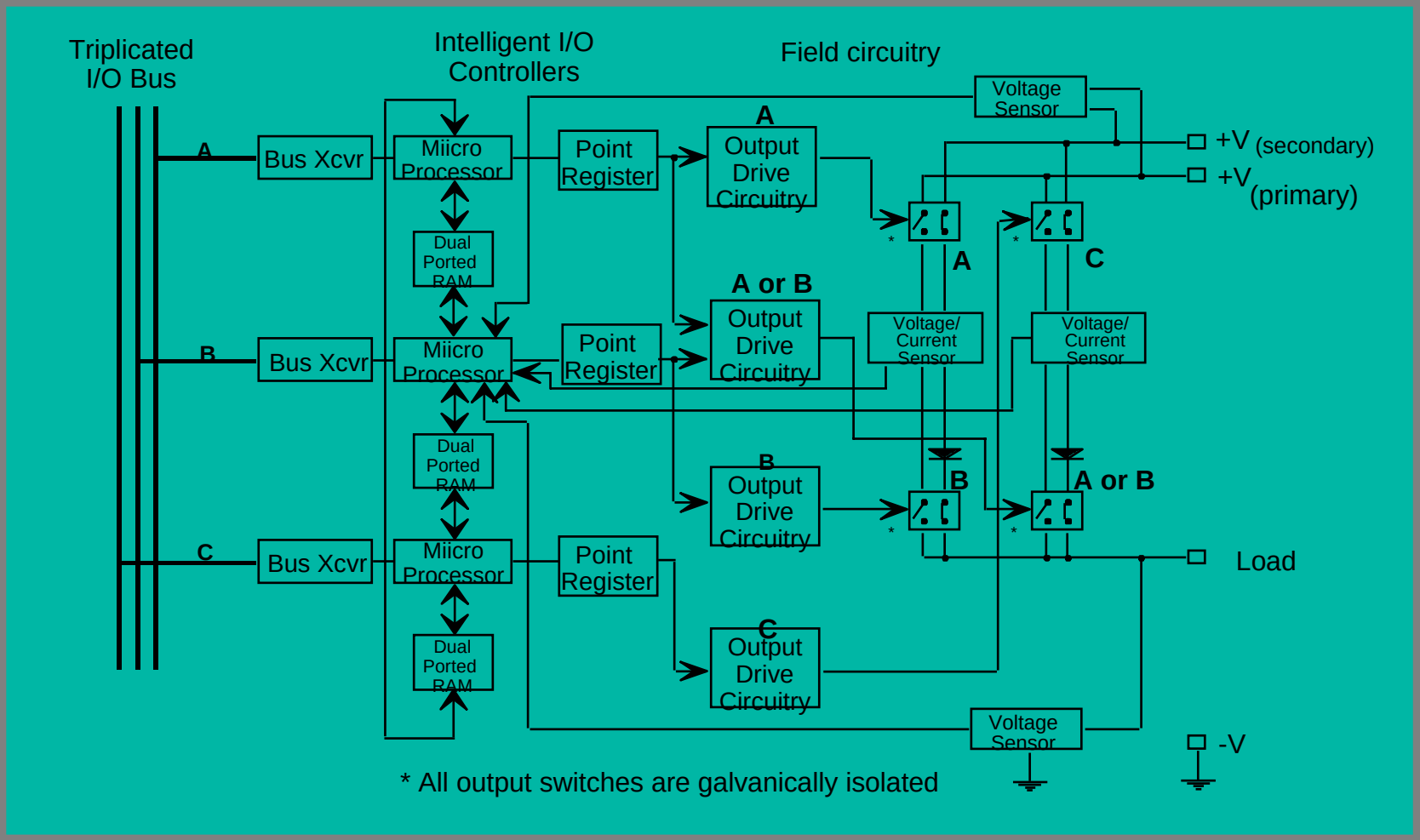
Both Tests Occur on All Output Circuits Regardless of Power Status (NE or ND)

- **Output Circuits are Toggled, Voltage Loopback Circuits Verify Proper Operation**
- **Field Load Monitored by Use of Voltage Loopback Circuits**

If Output Switch is Found Faulty, MPs Vote to Energize Fault LED and Generate a System Alarm

If Load is Missing, MPs Vote to Energize Load LED - Field Device Failure, NOT TMR System Fault

SDO Module -Architecture



TMR Analog Output Module

- **Triplicated D/A Converters for Each of the 8 Output Points**
- **2oo3 Selection Circuit Selects Correctly Operating DAC for Each Point and Periodically Selects Each DAC to Check It's Correct Operation**
- **Loopback Checking of All Analog Output Channels**
- **Automatic Calibration Using Built-in Reference Voltages**
- **0.15% Full Scale Accuracy**
- **No Single Point of Failure**
- **On-Line Replacement**

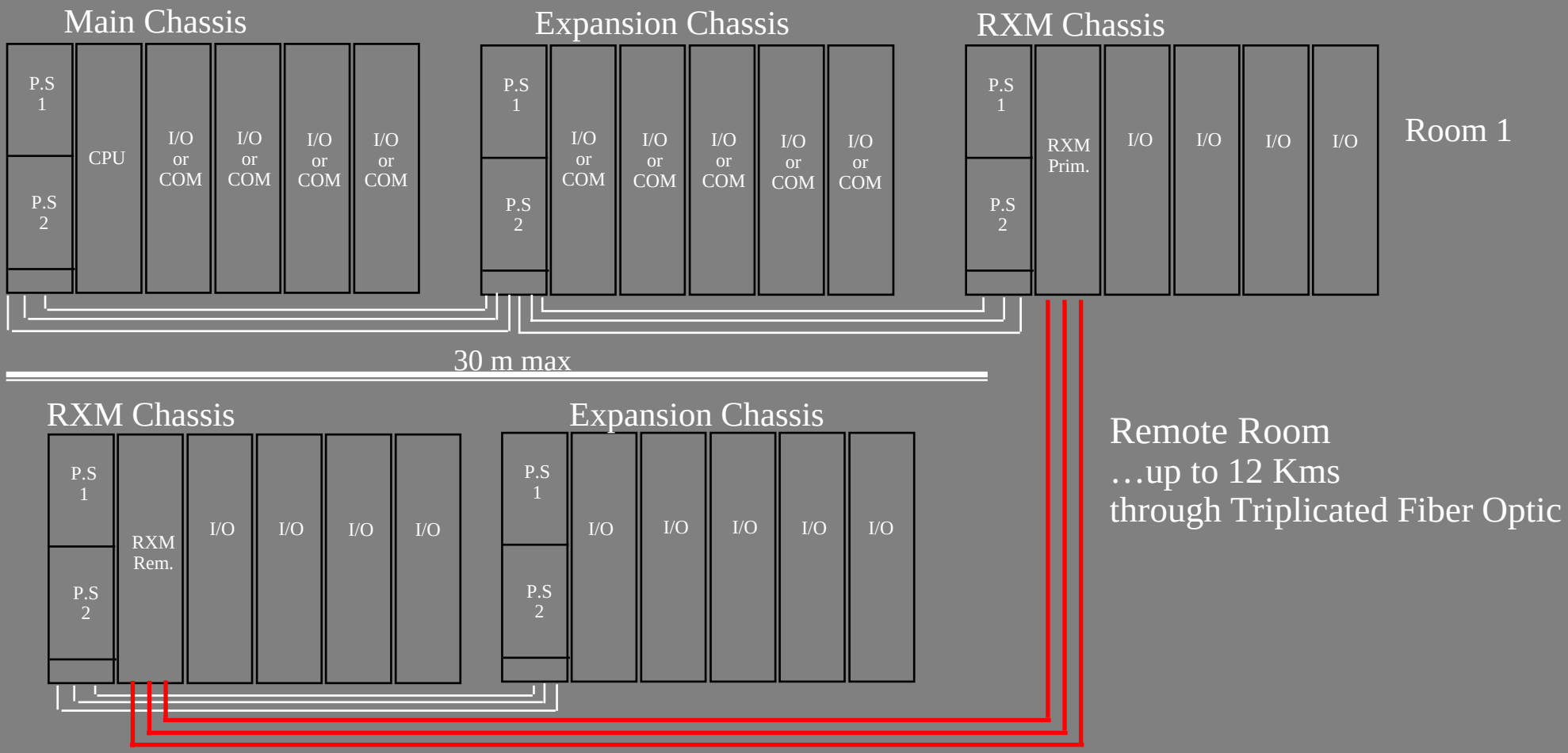
TMR Pulse Input Module

- **Triplicated Pulse Counter for Each of the 8 Input Points**
- **Accurate Timers Are Used on Each Point to Determine Time Required to Accumulate the Required Number of Pulses (1 Microsecond Accuracy)**
- **Measures Speed (RPM) to an Accuracy of 0.01% at Normal Operating Speeds**
- **No Single Point of Failure**
- **On-Line Replacement**

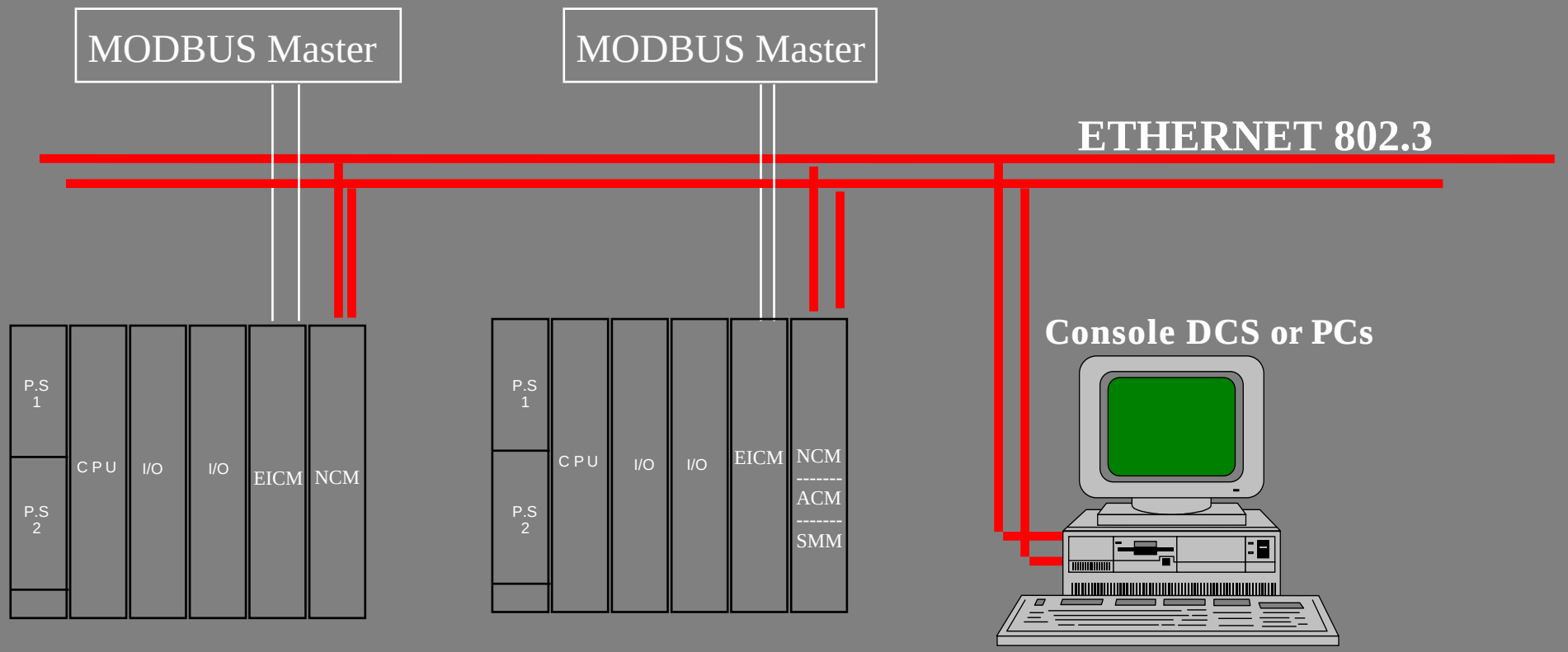
TMR Thermocouple Input Module

- **Triplicated A/D Converters and Multiplexors**
- **Automatic Calibration Using Built-in Reference Voltages**
- **Supports Thermocouple Types J, K, and T**
- **Provides 32 Differential, Non-commoned Inputs**
- **No Single Point of Failure**
- **On-Line Replacement**

Typical Architecture



Communication Capabilities

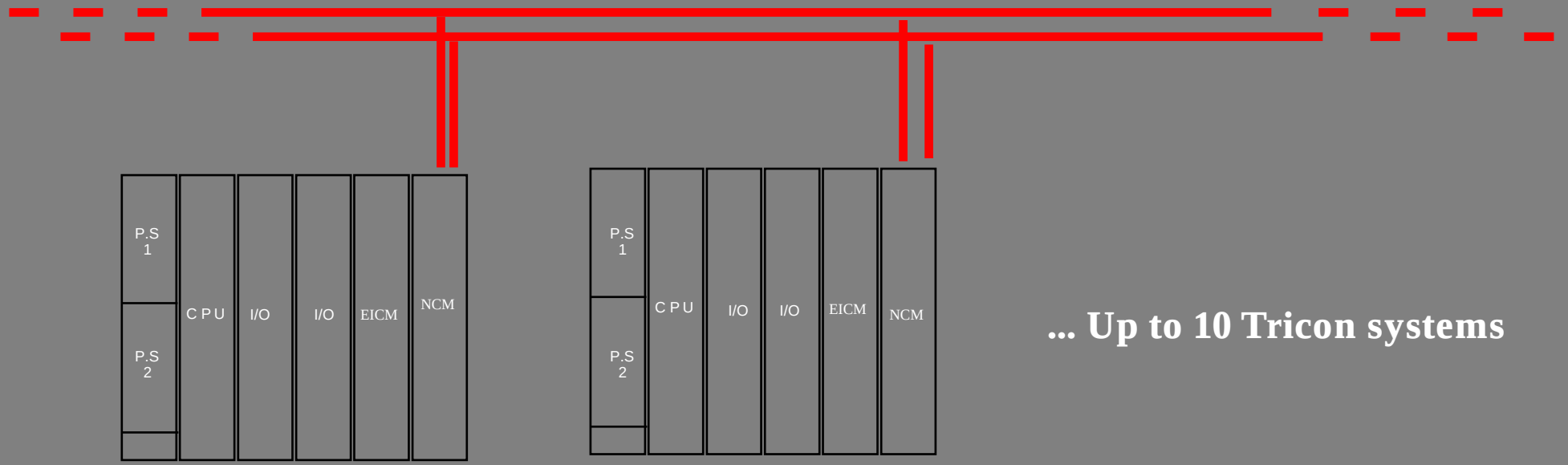


Tristation, SOE, DDE,TCP/IP

Communication Capabilities (cont..)

Peer to Peer Communication

TSSA, *Proprietery protocal*

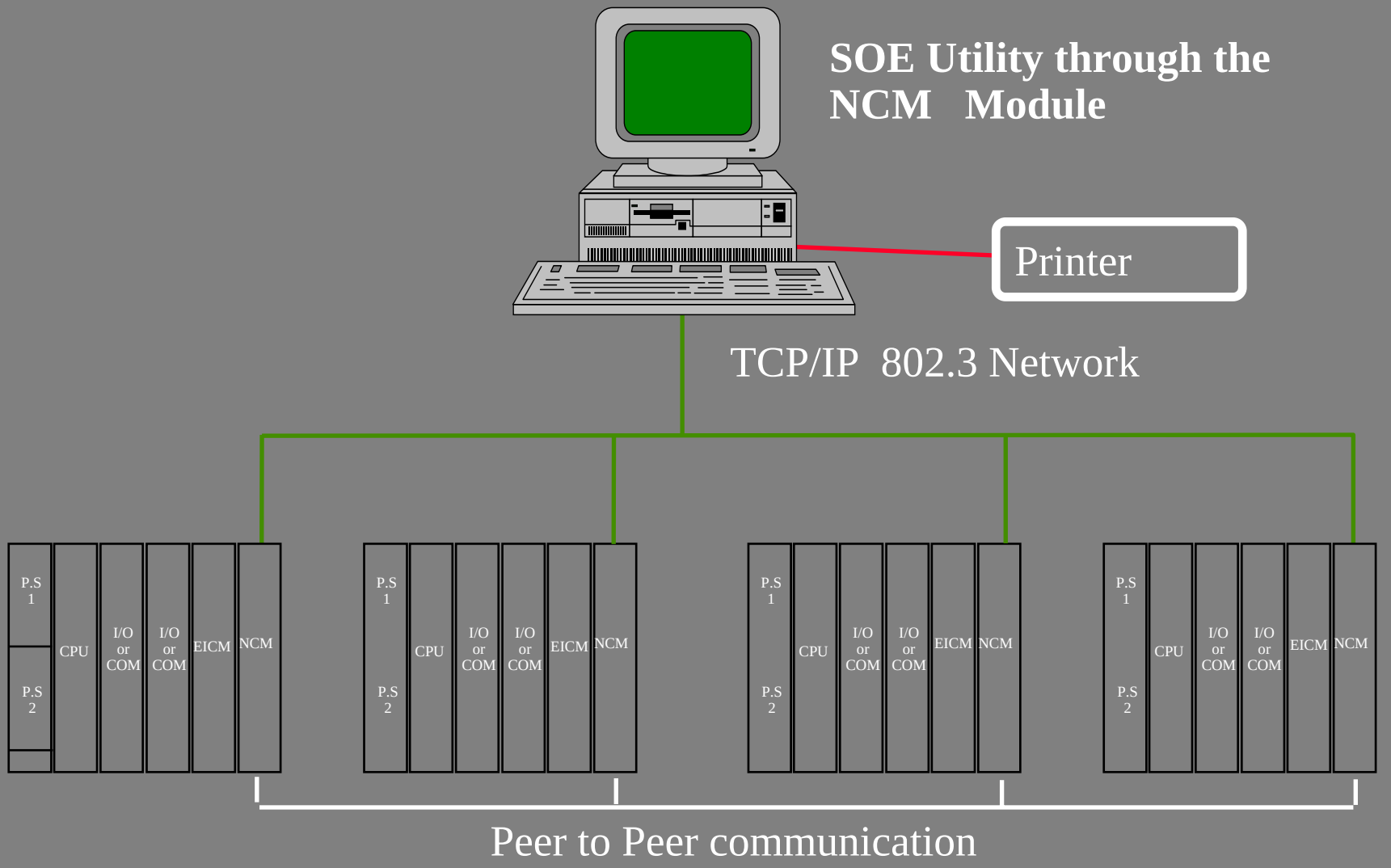


... Up to 10 Tricon systems

Triconex Communication Modules

- **Network Communication Module (NCM)**
  - Supports Two IEEE 802.3 Ports
- **Intelligent Communications Module (EICM)**
  - Four Isolated RS-232 / 422 Serial Ports (One Port Used for TriStation and Others Typically Used for MODBUS Communication to DCSs and Other Computer or SubSystems)
  - One Parallel Printer Port
- **Safety Manager Module (SMM)- Honeywell TDC 3000**
  - Connects to TDC 3000 Universal Control Network (UCN)
- **Advanced Communication Module (ACM)- Foxboro I/A Series**
  - Connects to Foxboro I / A Series Nodebus
  - Supports Additional 802.3 Port and Two RS-232 / 422 Serial Ports

Sequence of Events : SOE



SOE - Features

- All the variables are recorded and time stamped in the memory of the TRICON
- Accuracy : scan time
- SOE block are setting up within Tristation (maximun of 14 SOE
- The control program manages event collection by means of functions that the user includes in his program
- All the informations can be retrieved through the different communication modules
- SOE Data Retrieval utility program is available through the Network Communication Module NCM.

Raffineria di Priolo

Configurazione di rete Ethernet ridondante, con connessioni rame-fibra ottica e Bridge per ottimizzazione del traffico di rete

TRICONEX

NCM-2
Node 6

NCM-1
Node 5

CAVO IN RAME
CAVO COASSIALE IN RAME
FIBRA OTTICA

C | F O

F O | B | C
FIBRA OTTICA | BRIDGE | COAX

C | B | F O
COAX | BRIDGE | FIBRA OTTICA

C | F O

Printer1_1

F O | C

C | F O

Printer2_1

F O | C

PR1_2

P1

PR1_1

SG10_1

P2

SG10_2

FIX 32