TRICON
Fault Tolerant Systems
Definizioni

Safety (Sicurezza)

Si definisce Sicurezza la libertà da un rischio inaccettabile, per il Personale, la Collettività, l’Ambiente.
Goal: Safety

Strategy: Fail Operational

Measurement: Reliability

Method: Fault Tolerance
Applications Areas

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

Applications ...
- Safety/ESD Equipment
- Burner Management
- Fire & Gas
- Automotive Presses
- Critical Control
- Rotating
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: 26%
- Petroleum Refining: 23%
- Oil & Gas Production: 24%
- Electric Power Utilities: 11%
- Marine: 8%
- Pulp & Paper: 3%
- Other: 5%
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 worldwide 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

June, 1997
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
• "FAIL SAFE"

MTTF

Spurious trips

Startup phase

t == few years

MTTR

• "FAIL OPERATIONNAL"

MTTF

Spurious trips

t == 100 years

• Statistically, the accidents occurred in transition phases (start-up, shutdown)
Key Issues (Concept)

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

Process lifecycle

Spurious trip
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

PLC

Process

Safety

Availability

Safety

Availability
2°° 3D Voting system

Output = A.B + B.C + A.C

Safety
Availability

Majority state
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:**

- 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!
- No propagation
- Supports 2 faults of different ranks
- Diagnostics are easy to manage
Version 9 High Density Main Chassis
Chassis - Architecture

* Either the left module or right module functions as the active or hot spare at any particular time.
TRIBUS Hardware

- Three Independent Serial Links Transmit Data From Each Main Processor to the Other Two Main Processors
- Serial Links Operate at 4 M Bits/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

- Main Processor
  - NS32GX32
  - NS32381

- Floating Point Processor
  - NS32381

- Debug Comm Port

- Dual Port RAM
  - I/O Processor

- Internal System Bus

- Failure Detect Circuitry

- Status Indicators

- 512K EPROM
  - 2MB SRAM

- Timing Generator

- Interrupt Controller

- Dual Power Regulators

- Vcc

- Dual Power Rails

- Dual Port RAM

- Com Processor

- TriBus

- DMA

- Up Stream
  - Down Stream

- Fault Tolerant Communication Bus

- Fault Tolerant I/O Bus

- Debug Comm Port
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

Power supply #1

- Rectifier
- Filter
- Converter DC/DC
- Fault Detection

Power supply #2

- Rectifier
- Filter
- Converter DC/DC
- Fault Detection

Fault Detection

+V Bus 1
+V Bus 2
OV

REG

Vdc
A
B
C
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
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

Input circuit

Individual opto-isolator

Intelligent I/O CONTROLLERS Triplcated I/O BUS

Threshold Detect Opto-isolator

Microprocessor

Bus Xcvr

Opto-isolator

Dual Port RAM

Short-circuit detection

Microprocessor

Bus Xcvr

Microprocessor

Bus Xcvr

Microprocessor

Bus Xcvr
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
• 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

Signal Conditioning

ADC for each leg

Intelligent I/O Controllers

Triplicated I/O Bus

Mux.

Amp

ADC

Microprocessor

Bus Xcvr

Mux.

Amp

ADC

Microprocessor

Bus Xcvr

Mux.

Amp

ADC

Microprocessor

Bus Xcvr
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
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

* All output switches are opto-isolated
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
* All output switches are galvanically isolated
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 Its 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

<table>
<thead>
<tr>
<th>Main Chassis</th>
<th>Expansion Chassis</th>
<th>RXM Chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>P.S 1</td>
<td>P.S 1</td>
<td>P.S 1</td>
</tr>
<tr>
<td>P.S 2</td>
<td>P.S 2</td>
<td>P.S 2</td>
</tr>
<tr>
<td>CPU</td>
<td>I/O or COM</td>
<td>RXM Prim.</td>
</tr>
<tr>
<td></td>
<td>I/O or COM</td>
<td>I/O</td>
</tr>
<tr>
<td></td>
<td>I/O or COM</td>
<td>I/O</td>
</tr>
<tr>
<td></td>
<td>I/O or COM</td>
<td>I/O</td>
</tr>
<tr>
<td></td>
<td>I/O or COM</td>
<td>I/O</td>
</tr>
<tr>
<td></td>
<td>I/O or COM</td>
<td>I/O</td>
</tr>
</tbody>
</table>

- **Room 1**
  - Remote Room
  - ...up to 12 Kms through Triplicated Fiber Optic

- **30 m max**
Communication Capabilities

ETHERNET 802.3

MODBUS Master

CP U  I/O  I/O  EICM  NCM

-------

ACM

-------

SMM

P.S 1

CPU  I/O  I/O

P.S 1

CPU  I/O  I/O

P.S 2

EICM  NCM

ACM

SMM

P.S 2

Console DCS or PCs

Tristation, SOE, DDE, TCP/IP
## Communication Capabilities (cont..)

**Peer to Peer Communication**

<table>
<thead>
<tr>
<th>PS 1</th>
<th>CPU</th>
<th>I/O</th>
<th>I/O</th>
<th>EICM</th>
<th>NCM</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TSSA, Proprietary protocol**

... 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 Utility through the NCM Module

TCP/IP 802.3 Network

Peer to Peer communication
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 (maximum 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.
Configurazione di rete Ethernet ridondante, con connessioni rame-fibra ottica e Bridge per ottimizzazione del traffico di rete.