Paper Presentation:
“COMPLETE AND SIMULTANEOUS DCS FAILURE IN TWO 500MW UNITS”

K C Tripathy, DGM (C&I)
Anoop K, Dy Manager (C&I)
B K Rathore, Dy Manager (C&I)
ROLE OF DCS IN POWER PLANTS

INTRODUCTION

ANALYSIS

LEARNINGS

CONCLUSION

DCS

Protections

Controls

Operations

Monitoring

Reporting

Analysis

Alarms
DCS ARCHITECTURE FOR CASE-STUDY

**TOTAL:**
- 214 processors, 46 workstations, 50 Ethernet switches

**Domain-1 for 1st Unit**
- 103 processors, 21 workstations

**Domain-2 for 2nd Unit**
- 103 processors, 21 workstations

**Domain-3 for Common plant**
- 8 processors, 4 workstations

**Network-A (Ethernet)**
- 22 Layer-2 switches, 3 Layer-3 switches

**Network-B (Ethernet)**
- 22 Layer-2 switches, 3 Layer-3 switches

Each functional group has:
- 2 redundant processors & 2 redundant networks

**TOTAL:**
- 214 processors, 46 workstations, 50 Ethernet switches
INCIDENT NO. 1 REPORT

 Bá both units initially @ full load

<table>
<thead>
<tr>
<th>Maintenance Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>• An Ethernet switch in network-B common domain was found to be non-communicating.</td>
</tr>
<tr>
<td>• This switch (common to both units DCS) was restarted as per site procedure.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Both units all DCS processors simultaneously rebooted &amp; lost all logic configurations.</strong></td>
</tr>
<tr>
<td>• Both units boiler and TG tripped on <strong>hardwired backup protections</strong> outside DCS control.</td>
</tr>
<tr>
<td>• No indications/alarms available for operation. No SOE/event logs for troubleshooting.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operational Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Emergency auxiliary drives were started directly from LT switchgear.</td>
</tr>
<tr>
<td>• DG incomer breaker was manually closed in one unit from switchgear.</td>
</tr>
<tr>
<td>• ECW pumps (that tripped in one unit) were directly started from HT switchgear.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Restoration</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Workstations were inoperative after the incident until network-B was temporarily switched off.</td>
</tr>
<tr>
<td>• Full download was done in DCS panels, taking <strong>3-4 hours for complete restoration.</strong></td>
</tr>
<tr>
<td>• Suspected switch was replaced with proper IP address and port settings.</td>
</tr>
</tbody>
</table>
PLANT SAFETY HAZARDS

**BOILER** (tripped via hardwired MFT to all firing equipment)
- Furnace pressure of one unit was found near high trip limit after DCS restoration.
- Boiler drums were emptied, BCW pumps ran dry without any protection.
- ID-FD fans ran without any control or protection for over an hour.
- Safety relief valves floated for 15 minutes in both units, as bypass was unavailable.
- **POTENTIAL RISK**: Furnace explosion / Tube failures (if backups also fail)

**TURBINE** (tripped via hardwired inter-trip from MFT)
- Turbine of one unit crash-halted, 2 days before hand-barring is possible.
- TG lub oil temperature control unavailable: low temperatures persisted.
- All TDBFP ran without any protection, one had exhaust diaphragm rupture.
- Hotwell of one unit emptied & CEPs ran dry without any protection.
- **POTENTIAL RISK**: Water ingress / Bearing failures (if backups also fail)

**GENERATOR** (tripped via low fwd power delayed backup)
- Seal oil system of one unit out of service for a few minutes (due to UT-ST changeover failure & delay in DC SOP starting)
- Hydrogen leakage in one unit observed in TG floor.
- **POTENTIAL RISK**: Fire hazard
INCIDENTS NO. 2 & 3 REPORT

Work before 2\textsuperscript{nd} incident
- DCS vendor representative was at site in order to troubleshoot the 1\textsuperscript{st} incident.
- While restoring uplink connection to another common Ethernet switch in network-B, similar complete DCS failure occurred (one unit tripped at full load, other boiler tripped)

Activities after 2\textsuperscript{nd} incident
- The uplink connection that caused the 2\textsuperscript{nd} failure was removed.
- Operational actions and system restoration done similar to 1\textsuperscript{st} incident.
- Both units kept under safe shutdown for further testing.

Work before 3\textsuperscript{rd} failure (test)
- All Ethernet switch port settings and connections in the network checked thoroughly.
- Double physical connections between same set of switches were removed, wherever found.
- On reconnecting the uplink that caused 2\textsuperscript{nd} failure, complete DCS of both units failed again.

Activities after 3\textsuperscript{rd} failure
- The net-B uplink connection that caused the 2\textsuperscript{nd} and 3\textsuperscript{rd} failures was taped and kept removed.
- System restoration done similar to 1\textsuperscript{st} and 2\textsuperscript{nd} incidents & both units taken to full load.
- Threat still exists in network-A, BUT solution is pending from supplier for 2 ½ months.
INITIATING CAUSE (DCS NETWORK)

(Representative diagram for network-B, similar for redundant network-A)

5 SWITCHES IN LOOP

(Broadcast storm initiated by restart / uplink initialization of any one switch in the loop)
Single network overload caused working memory overflow and application crash of communication handler utility inside DCS processor firmware (incidentally common to both networks).

All processors (active and redundant) abruptly rebooted at once. Thereby both redundant network & redundant processor concepts of DCS design were defeated.

Since the particular version of DCS processor does not keep a backup copy of logics in non-volatile flash, all logic programs were lost. This resulted in a huge downtime of 3-4 hours.

Indicative DCS processor volatile memory (RAM) allocation table

<table>
<thead>
<tr>
<th>Real-time OS</th>
<th>Input /Output Scan</th>
<th>Logic Execution</th>
<th>External Communications</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS</td>
<td>AI, AO, DI, DO</td>
<td>Special, Fast, Medium, Slow</td>
<td>Net-A, Net-B, Backup link</td>
</tr>
</tbody>
</table>

**REBOOT**
### DESIGN CONSIDERATIONS - PROCESSOR

<table>
<thead>
<tr>
<th>Network failure or overload</th>
<th>• Loss of ALL network communications or complete communication overload (in any or both of the redundant networks) should NOT lead to complete loss of control in ANY functional group – in line with Functional Grouping Concept of DCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup copy of logics</td>
<td>• DCS processors always must keep a backup copy of logics in non-volatile flash memory, in order to avoid complete loss of logics and huge downtime of 3-4 hours for logic download and restoration.</td>
</tr>
</tbody>
</table>
| Processor memory allocation | • DCS processor functions of RTOS, I/O Scans, Logic execution and External communications have to be protected by dedicated memory allocation.  
• The communication handler utilities inside processor firmware for either redundant network and hot backup link also should be completely independent. |
| DCS safety compliance       | • Internationally accepted safety certifications and standards (TÜV, SIL3 – IEC 61508) must be mandatory for all DCS contract technical specifications.  
• DCS vendor to certify total network safety compliance for its processors. |
| Vendor solution tieup       | • All DCS vendors must to be contractually mandated to provide prompt support and permanent solutions (within one month) in the unlikely event of complete DCS control failure with potential catastrophic consequences, throughout plant lifespan. |
### Broadcast storms

- All sources of **broadcast storms causing network overload** must be identified and addressed through appropriate checks and balances (in architecture and configurations).

### Parallel double connections

- **Parallel double connections (port redundancy)** between any two adjacent pairs of switches must be prevented by design.

### Inadvertent ring or loop

- Multiple (> 2) switches must not form a **closed physical path** (ring or loop). Special attention needed at the **highest level of network hierarchy** where multiple domains or units of same DCS connect.

### Firewall safety

- **Hardware Firewalls** must be installed in the DCS network at appropriate interfaces and configured to prevent **Denial-of-service (DoS) attacks** from outside the plant network. Typical firewall interfaces: for offsite PLCs, PADO, intranet, ERP etc.
A detailed backup design document (for all systems independent of DCS) that ensure basic minimum plant safety needs to be issued for every project.

- The list may include hardwired systems for automatic action & start/stop provisions and indications for manual intervention during DCS failure.

• **2/3 MFT Processors fail** must initiate hardwired MFT, and trip all firing equipment
  - DC/emergency scanner air system auto-start, closing spray main block valves
  - Direct indication for furnace pressure and excess oxygen independent of DCS

• **Hardwired MFT or control failure of both turbine protection functional groups** (monitored through watchdog relays) must directly energize turbine trip solenoids.
  - Direct indication for turbine speed, vacuum, lub oil pressure & seal oil-H$_2$ DP.
  - Direct pressure-switch auto-start, manual start buttons and status for emergency drives

• **Enabling signal from DCS for UT-ST fast changeover electrical circuit** must be ensured available through set-reset latch relay, to prevent loss of unit supply.
  - Manual closing provision for DG incomer breaker & critical auxiliary drives on the electrical module at LT switchgear.

• **The backup protections for boiler and turbine** must use redundant power sources, both independent of normal power sources to protection panel. Failure of both backup supplies must initiate machine trip through DCS. Desk EPBs must trip machine through backup path.

(Detailed list in technical paper)
<table>
<thead>
<tr>
<th>Need to test</th>
<th>Avalanche crash tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>• To ensure safety in control systems: “First introspect, then inspect, thus protect”</td>
<td></td>
</tr>
<tr>
<td>• Complex network architecture makes DCS based protection systems vulnerable.</td>
<td></td>
</tr>
<tr>
<td>• To be done from inside DCS network, directly upon its processors.</td>
<td></td>
</tr>
<tr>
<td>• During Factory Acceptance Test (FAT) at vendors’ shop-floor by Engineering Group.</td>
<td></td>
</tr>
<tr>
<td>• During Site Acceptance Test (SAT) at project site by Commissioning Group.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sample tests for FAT/SAT</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Creation of port redundancy, loop of multiple Ethernet switches followed by restart / uplink re-initialization of any one switch, in a fully networked system.</td>
<td></td>
</tr>
<tr>
<td>• Creation of a Denial-of-service (DoS) attack from inside the DCS network.</td>
<td></td>
</tr>
<tr>
<td>• The tests may be carried out on either network first, then both together.</td>
<td></td>
</tr>
</tbody>
</table>
PLANT O&M CONSIDERATIONS

Online DCS maintenance

• Comprehensive DCS online maintenance procedure to be mandatorily submitted by DCS vendor & approved by Engineering, to be strictly followed at site.
• Typical procedures to be included: Logic backups/changes, network settings, single-point failure & restoration, complete MMI restoration, complete DCS restoration

Backup healthiness

• Healthiness of all backup systems (independent of DCS) also to be ensured by C&I maintenance (check) and operation (witness) departments periodically during protection checking, typically after unit overhauls. Joint protocol to be recorded.

Emergency operation

• Site-specific emergency handling operation procedures to be prepared to handle complete DCS failure situation, with assigned responsibilities.

(Detailed list in technical paper)
CONCLUSION POINTS

During the complete DCS failures, all major equipment in power plant faced high risk of catastrophic damage due to loss of all protections and controls.

DCS Processors must retain primary control tasks of logic execution and I/O scan even under complete network failure or overload.

DCS design contract specifications, vendor support tie-up, network crash-tests, and site O&M procedures need to be strengthened further.
“DCS Processors must be pre-designed & crash-tested against all network failures & overloads to ensure human & plant safety”

THANK YOU