Accelerator Reliability Workshop
The ITER Interlock System: Project Status

Antonio Vergara – Ignacio Prieto

Control Systems Division
ITER International Organization

ARW-2015 26th April – 1st May 2015 Knoxville (USA)

The views and opinions expressed herein do not necessarily reflect those of the ITER Organization
The ITER Project

the way to new energy
**Attractions:**
- unlimited fuel
- no CO₂ or air pollution
- intrinsic safety
- no radioactive ash or long-lived nuclear waste,
- cost will be reasonable *if we can get it to work reliably*

**Disadvantages:**
- not yet available
- walls gets activated (but could recycle after 100 years)

A huge global increase in energy use is inevitable.
The idea for ITER originated from the Geneva Superpower Summit in 1985 where Presidents Gorbachev and Reagan proposed international effort to develop fusion energy…

…“as an inexhaustible source of energy for the benefit of mankind”.

China, Europe, India, Japan, Korea, Russian Federation and the United States of America signed the ITER Agreement on 21 November 2006 in the Elysee Palace, Paris
The ITER Domestic Agencies are responsible for implementing the procurement activities under each Member’s responsibility.
Main Sources of Risk at ITER
Superconducting Magnets

10 GJoule: the energy of an A380 at 700 km/hour corresponds to the energy stored in the CERN Large Hadron Collider magnet system. Sufficient to heat up and melt 12 tons of Copper (*)

(*) Rudiger Schmidt (CERN)
Superconducting Magnets

Total Magnetic Energy around 100 GJ

Interaction of strong magnetic fields 5T and up to 17 MA plasma
Plasma Heating & Fuelling Systems
The Plasma

- Energy, Temperature – Internal Components
- Current - Disruptions
Vacuum and Cryogenic Systems
Interlocks at ITER

Cooling (and Heating) Water System
Remote Handling
ITER Interlocks: Particularities
Particularities of ITER interlock systems

1. An eclectic collection of actions

- **Time Response**
  - Slow (> 300 ms)
  - Fast (100 µs to 300 ms)

- **Action Complexity**
  - Low
  - Medium
  - High

- **Four Architectures**
  1. Slow & Medium Complexity → PLC
  2. Fast & Medium Complexity → FPGA
  3. Slow/Fast & Low Complexity → Current loops
  4. Slow/Fast & High Complexity → R&D going on (tbc)
Safety PLC solution - Prototypes
CIS Prototypes in India

Implementation of the Magnet Protection Functions

- DMIS is only triggered if Plasma conditions are met.
- All these events shall be sent to the PCS via PPM.

CIS Progress Meeting - February 2014
CIS V.0 arrival at Seoul
FPGA-based solution – customized COTS
The Hardwired Loop (Discharge Loop and Bypass Loop) allows the coordination of the different elements involved in the protection function, via a common current loop in a 2oo3 (or 1oo2) configuration.

The Interface Boxes (DLIBs/BLIBs) are used to connect the different elements to the loop, providing a reliable interface so the user can either read the DL status or open the loop, to trigger the protection actions.

*The user is defined as the protection equipment: QDS, FDU, PMS, PC.
CERN-based User Interface Box: DLIB

- User status indicators
- Loop status indicators
- Redundant Power supplies
- User input and DL status connectors
- DL input and return connectors
HTS Current Lead Test Bench
Current Lead Control System
From India to China
First Real Case Application - ASIPP
Quench Protection System ASIPP
Particularities of ITER interlock systems

1. An eclectic collection of actions

2. The not-so-safe fail safe states

→ Identification of safe states after a degradation of the interlock components is not always obvious and even impossible sometimes without implying long machine downtimes.

→ Interlocks design shall allow early internal failure detection followed by a controlled sequence of actions

→ Setting the interlock outputs in their fail-safe states is the last option to be taken

→ Intelligent redundancy + self-diagnostics
Particularities of ITER interlock systems

1. An eclectic collection of actions

2. The not-so-safe fail safe states

3. Expensive interlock actions (or when the cure is worse than the disease)

→ Triggering interlocks not only reduces the ITER operation availability but also the tokamak lifetime

→ Example: limited total number of coil fast discharges or unmitigated disruptions

→ ‘Soft’ interlock actions performed in collaboration with conventional controls and always backed-up by ‘hard’ interlocks
Particularities of ITER interlock systems

1. An eclectic collection of actions
2. The not-so-safe fail safe states
3. Expensive interlock actions (or when the cure is worse than the disease)
4. ITER complex procurement strategy
A unique feature of ITER is that almost all of the machine will be constructed through *in kind procurement* from the Members.
In-fund and in-kind procurement
Interlocks Integration
Mitigation of risks related to integration of the interlocks

• Segregation Safety – Interlocks
ITER Defense-in-depth Approach

- Safety
  - Interlocks
  - Plant System I&C
  - Plant Systems

- Interlock Functions
- PCS loss of control
- Change plasma sequence
- Permit / Inhibit
- Regulation & Control
- Plasma Control
- Safety Functions

- Plant System I&C
  - PCS
  - Interlocks
  - Plant Systems
Mitigation of risks related to integration of the interlocks

• Segregation Safety – Interlocks

• Common strategy for interlock identification and classification
### What is an Interlock?

<table>
<thead>
<tr>
<th>Event Likelihood</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Catastrophic</td>
</tr>
<tr>
<td>Frequent</td>
<td>3IL-4</td>
</tr>
<tr>
<td>Probable</td>
<td>3IL-4</td>
</tr>
<tr>
<td>Occasional</td>
<td>3IL-3</td>
</tr>
<tr>
<td>Remote</td>
<td>3IL-3</td>
</tr>
<tr>
<td>Improbable</td>
<td>3IL-3</td>
</tr>
<tr>
<td>Negligible</td>
<td>3IL-2</td>
</tr>
</tbody>
</table>

#### Machine/System Unavailability

<table>
<thead>
<tr>
<th>Cost</th>
<th>&lt; 1h</th>
<th>&lt; 1 day</th>
<th>&lt; 1 week</th>
<th>&lt; 2 month</th>
<th>&lt; 1 year</th>
<th>&lt; 2 year</th>
<th>&gt; 2 year</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 0.1 M€</td>
<td>Mi</td>
<td>Se</td>
<td>Se</td>
<td>Se</td>
<td>Ma</td>
<td>Ma</td>
<td>Ca</td>
</tr>
<tr>
<td>&lt; 1 M€</td>
<td>Se</td>
<td>Se</td>
<td>Se</td>
<td>Se</td>
<td>Ma</td>
<td>Ma</td>
<td>Ca</td>
</tr>
<tr>
<td>&lt; 10 M€</td>
<td>Se</td>
<td>Se</td>
<td>Se</td>
<td>Ma</td>
<td>Ma</td>
<td>Ma</td>
<td>Ca</td>
</tr>
<tr>
<td>&lt; 50 M€</td>
<td>Ma</td>
<td>Ma</td>
<td>Ma</td>
<td>Ma</td>
<td>Ma</td>
<td>Ca</td>
<td>Ca</td>
</tr>
<tr>
<td>&lt;500 M€</td>
<td>Ma</td>
<td>Ma</td>
<td>Ma</td>
<td>Ma</td>
<td>Ca</td>
<td>Ca</td>
<td>Ca</td>
</tr>
<tr>
<td>&gt; 500 M€</td>
<td>Ca</td>
<td>Ca</td>
<td>Ca</td>
<td>Ca</td>
<td>Ca</td>
<td>Ca</td>
<td>Ca</td>
</tr>
</tbody>
</table>

#### Category

- **Frequent**: Event occurs very likely
  - Yearly frequency level: > 5
- **Probable**: Event is likely to occur
  - Yearly frequency level: 0.5 – 5
- **Occasional**: Event possible and expected
  - Yearly frequency level: 0.05 – 0.5
- **Remote**: Event possible but not expected
  - Yearly frequency level: 0.005 – 0.05
- **Improbable**: Event unlikely to occur
  - Yearly frequency level: 0.0005 – 0.005
- **Negligible**: Event extremely unlikely
  - Yearly frequency level: < 0.0005

#### Criteria

- **Disastrous threat to ITER’s mission, abandonment of the project and goals**
- **Loss of a full operational campaign, moderate threat to ITER’s mission**
- **Significant reduction of an operational campaign program**
- **No significant impact on the operational campaign program**
Mitigation of risks related to integration of the interlocks

- Segregation Safety – Interlocks
- Common strategy for interlock identification and classification
- Segregation Central – Local interlocks
Mitigation of risks related to integration of the interlocks

- Segregation Safety – Interlocks
- Common strategy for interlock identification and classification
- Segregation Central – Local interlocks.
- Hardware and software standardisation
Mitigation of risks related to integration of the interlocks

- Segregation Safety – Interlocks
- Common strategy for interlock identification and classification
- Segregation Central – Local interlocks
- Hardware and software standardisation
- Design and configuration guidelines
Mitigation of risks related to integration of the interlocks

- Segregation Safety – Interlocks
- Common strategy for interlock identification and classification
- Segregation Central – Local interlocks
- Hardware and software standardisation
- Design and configuration guidelines
- Mini-CIS
Mitigation of risks related to integration of the interlocks

• Segregation Safety – Interlocks

• Common strategy for interlock identification and classification

• Segregation Central – Local interlocks

• Hardware and software standarisation

• Design and configuration guidelines

• Mini-CIS

• Team spirit and many flight hours
Domestic Agencies
Preliminary Dependability Analysis
**Principle**
Future fusion power plants will be only possible if ITER proves that the reactor and associated systems can run long plasma discharges reliably.

**Consequences**

The ITER interlocks shall:

1. Protect the tokamak integrity
2. Maximise scientific operation time
3. Anticipate and test interlock solutions for future industrial fusion reactors
Interlock Dependability Analysis Strategy

3 Steps

1. What we can control: Central Interlock System

2. What we can coordinate: Plant Interlock Systems

3. All together
Interlock Dependability Analysis Strategy

3 Steps

1. What we can control: Central Interlock System

CIS Integrity Requirements (from Project Baseline):

I. Overall availability (99,9%)
II. Reliability (99,6% over two 8h shifts)
III. Probability of a dangerous failure of less than $10^{-7}$ per hour

Strategy

1. Standard architectures well defined in terms of dependability
   - IEC 61508 Certified equipment whenever possible
   - Non certified equipment with detailed reliability analysis and prototyping
2. Continuous long-term dependability monitoring/assessment
Interlock Dependability Analysis Strategy

3 Steps

1. What we can control: Central Interlock System

2. What we can coordinate: Plant Interlock Systems

Tools for the plant systems currently under design:

i. RAMI
   • Functional Analysis - FMECA
   • Reliability Block Diagrams

ii. HAZOP

iii. 3IL Assessments

Support Life Cycle Management
Interlock Dependability Analysis Strategy

3 Steps

1. What we can control: Central Interlock System

2. What we can coordinate: Plant Interlock Systems

3. All together

- Machine Protection Panel – Qualitative Analysis
- Models for Interlock functions - 17 representative cases analyzed
- Progressive take over of the local plant system interlocks by the CIS team
- R&D: Systems Theoretic Process Analysis (STPA)
The unprecedented technical and managerial complexity of ITER requires an interlock design where the traditional simplicity of tokamak investment protection systems has been replaced by a **4-architecture solution** with different technological choices.

The ITER Interlock System will most likely be the first machine protection system built with most of its components provided **in-kind from up to 36 different countries**.

A strong effort is being put in place to ensure that all actors around the globe design, build and configure the parts of the puzzle to be **properly integrated** with the central system.

While a detailed **dependability analysis** of the Central Interlock System has been already performed, a final strategy has still to be put in place to continuously monitor the progressive growth the overall interlock system.

The ITER interlock system will complete its final design in **March 2016**. Construction of **CIS V.1** will be done in Korea during 2016 and 2017.

CIS V.1 will be tested in the Korean superconducting tokamak KSTAR before being shipped to **Cadarache by 2019**.
Thank you