CLS Safety Systems

Robby Tanner, Elder Matias & Hao Zhang
Controls & Instrumentation Dept (CID)

Safety System Development.

150+ Employees

Saskatoon, SK, Canada, Earth
Ahh, Saskatoon...

Where’s that?
Access Control and Interlock System (ACIS)

Organization: Regulatory and Internal

Development Process and Testing

Industrial Software and Equipment (spec. BMIT)
Regulated by the Canadian Nuclear Safety Commission (CNSC)

Licensed as a Class 1B Facility

CLS Health, Safety and Environment Department is Independent

Controls and Instrumentation Dept. (CID) Produces Systems for HSE.

Validation and Verification Testing Performed by HSE.
System Development Process

- Development
  - Hazard Analysis
  - Requirements Specification
  - Design

- Testing
  - Validation
  - Integration Testing
  - Unit Testing

- Implementation
  - Development/Installation

Flowchart: Development to Testing to Implementation
Breast Tumours

Conventional Digital Imaging

Synchrotron Digital Imaging gives more detail regarding the shape of the tumour – this information may lead to better, earlier diagnostics.

Christopher Parham, UNC, 2003
Slide courtesy Dean Chapman, UofS
Hazard Analysis: Radiation Exposure is Primary Hazard

Requirements:
- Use both quantitative and qualitative definitions
- Secure an enclosure,
- Search an enclosure.

An example of a formal definition:
Specification

State Diagram of the Search/Secure Procedure

Initialization (Reset)
[Reset = False]/

Enclosure Open

Beam Ready
[All Clear Timer = Expired]/

All-Clear Interval

[Doors <> Closed OR EOS=False]/

Locking Up
[EOS=True AND All Perimeter Doors = Closed AND LUS1 = Pressed]/
[Exit Door = Closed] OR [All Clear Timer = Start]

[Area Timer = Start]

[LUS2 to LUSn = Pressed]/
Critical Functions (SIFs)

H/W chain monitors critical states

PLC chain provides all features.
PLC System w/ HW Backup

Shielding

Simple relay chain to monitor critical functions.

Emergency Off Station(s)

SSH Open Command

PLC chain provides all features.

PLC

Shielding

Lockup Stations

SSH Controls
- Office and Controls network
- Engineering Station
- Plantbus
- Remote I/O (ProfiSAFE)
• Siemens PCS 7 v 7.0 SP 1

• Failsafe Libraries

• PLCSIM
Programming Environment
### Code Organization

The page contains a screenshot of a software interface, likely a configuration or programming tool, with various code elements and properties. The interface includes sections for code editing and properties settings.

#### Code Elements
- **Contents of '0B35/1605_1_LOCKUP'**
  - List of code elements with type, position, duration, and comment.
  - The code elements include:
    - `BMIT/ACIS/POE-11605_1_LOCKUP/F_1605_1_ES` - A BAR 12/1 100 ms
    - `BMIT/ACIS/POE-11605_1_LOCKUP/F_1605_1_ES` - F.CH.DO 12/14 100 ms
    - `BMIT/ACIS/POE-11605_1_LOCKUP/F_1605_1_ES` - F.OR 12/15 100 ms
    - `BMIT/ACIS/POE-11605_1_LOCKUP/F_1605_1_ES` - F.OR 12/15 100 ms

#### Properties - Runtime Group
- **Task:** 0B35
- **Name:** 1605_1_LOCKUP
- **Comment:**
- **Reduction ratio:** 1
- **Phase offset:** 0
- **Optimize run sequence:**
- **Active:**

The screenshot also shows a section titled **Properties - Runtime Group** with a properties window open, showing the task and name with various settings.
Testing/Debugging

- In Situ
- Test bed
- PLCSIM
Hardware Configuration diagnostics VERY handy.
Lessons Learned – Grandfathering

EOSs, LUSs, Timers, etc

24 V (H/W)

H/W Logic

LED Relay (H/W)

24 V

LED Relay (PLC)

PLC

F-DO
Lessons Learned – Self-Diagnostics

24 V (H/W)

A

B

C

PLC

F-DO
Dark Periods (SIL-2/SIL-3)

“Dark periods occur during switch-off tests and during complete bit pattern tests. This involves test-related 0 signals being switched to the output by the fail-safe output module while the output is active. The output is then switched off briefly (dark period). A sufficiently slow actuator does not respond to this and remains switched on.”

Light Periods (SIL-3)

“Light periods occur during complete bit pattern tests. This involves test-related “1” signals being switched to the output by the fail-safe output module while the output is deactivated (output signal “0”). The output is then switched on briefly (light period). A sufficiently slow actuator does not respond to this and remains switched off.”

“SIMATIC – Automation System S7-300 Fail-Safe Signal Modules”,

Edition 02/2001, Page 3-14
Lessons Learned – Design Process

Some Kind of Permissive

Door 1
Door 2
Door 3

H/W Permits

PLC Permissive

Door 1
Door 2
Door 3

PLC
Lessons Learned – Design Process

• Requirement Specification

Critical Errors Can be Introduced at the Top of the Design Process

Secure Searched

Shutters Closed

Common-Mode Failure

Secure Searched

Shutters Closed
Conclusion

• Siemens Failsafe Offerings Are Impressive
• User Needs to be Familiar with Environment
• CLS will continue to use H/W
• Focus on Process to Enhance Safety AND Efficiency
Final Thought

• Personal Observation

• Workplace Safety Crime

- Lightning Arrestors
- Really Cool Cape
- Helmet
- Asbestos-Lined Fire-Rated Coveralls
- Eye Protection
- Elbow Pads & Gloves
- Kneepads & Shinguards
- Steel-Toed Boots