CLS Safety Systems

Robby Tanner, Elder Matias & Hao Zhang

www.lightsource.ca

2008 PCaPAC

Canadian Light Source

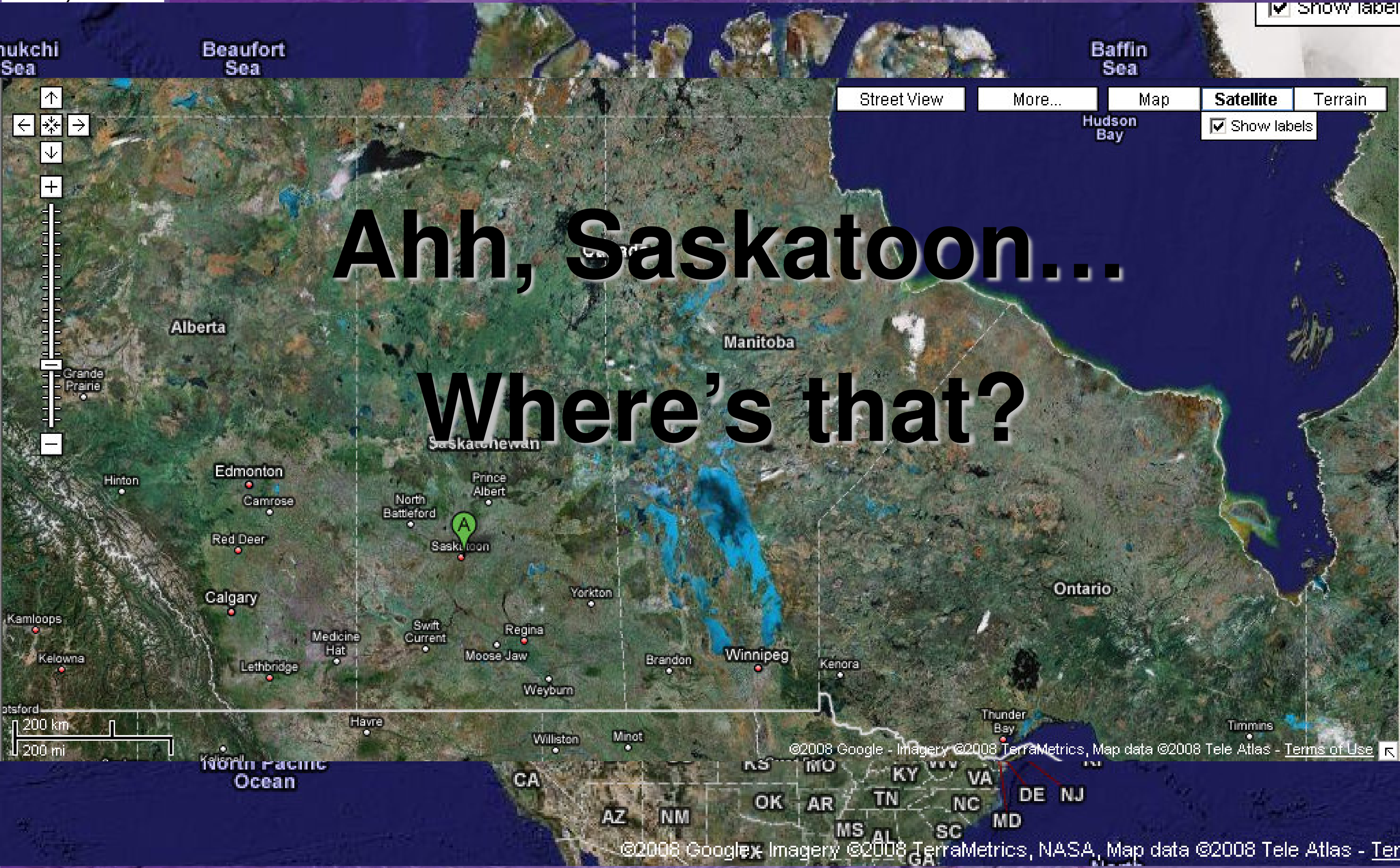
❑Controls & Instrumentation Dept (CID)

❑Safety System Development.

❑150+ Employees

❑Saskatoon, SK, Canada, Earth

Location



Ahh, Saskatoon…

Where’s that?

Canadian Light Source
Centre canadien de rayonnement synchrotron

Experimental Hall & Beamline

Overview

- ❑Access Control and Interlock System (ACIS)
- ❑Organization: Regulatory and Internal
- ❑Development Process and Testing
- ❑Industrial Software and Equipment (spec. BMIT)

Organization

❑Regulated by the Canadian Nuclear Safety Commission (CNSC)

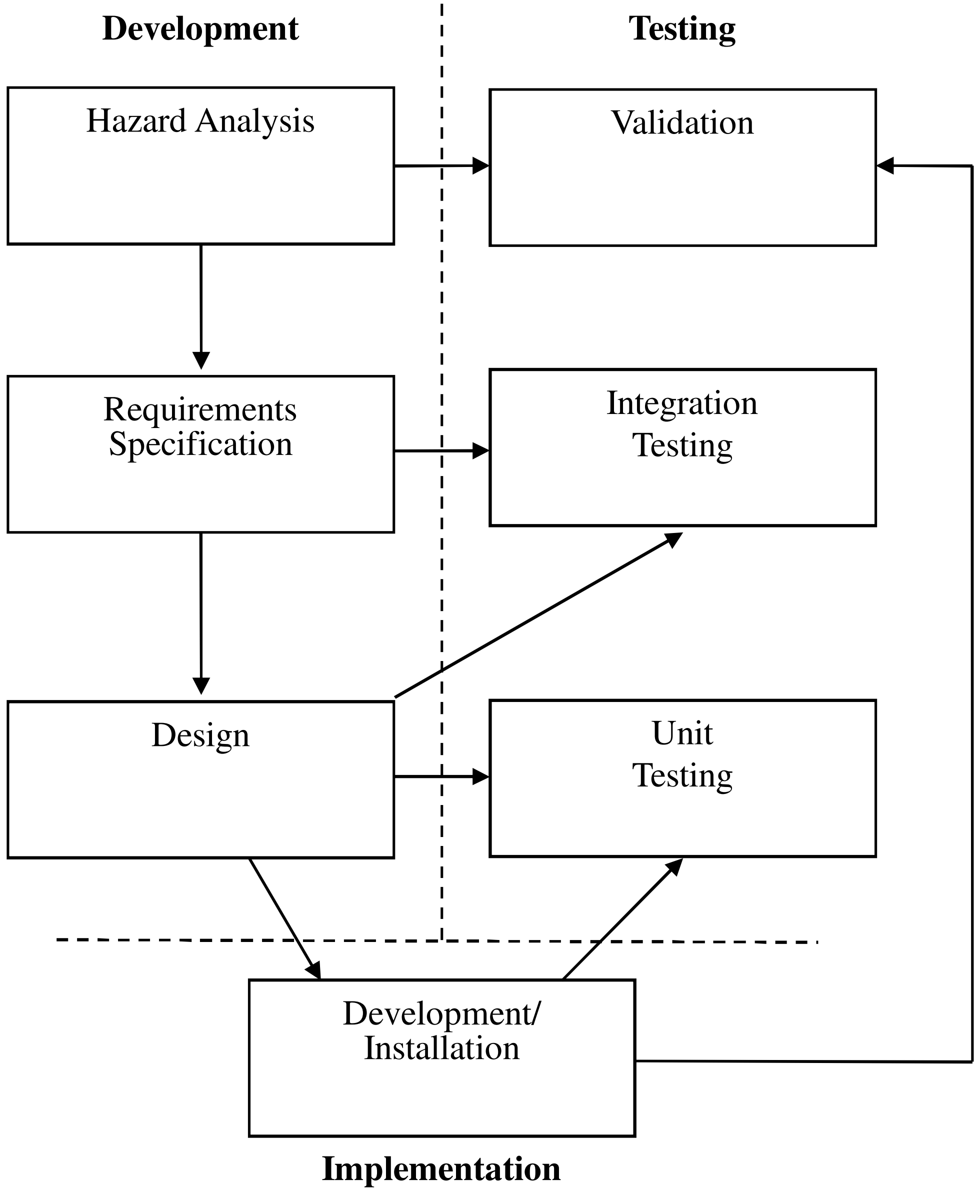
❑Licensed as a Class 1B Facility

❑CLS Health, Safety and Environment Department is Independent

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

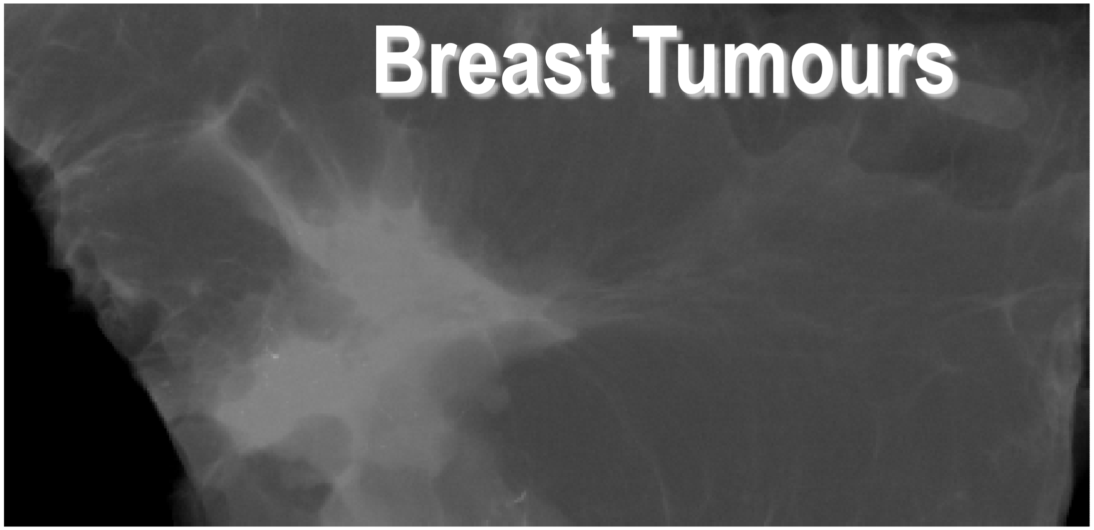
❑Validation and Verification Testing Performed by HSE.

System Development Process

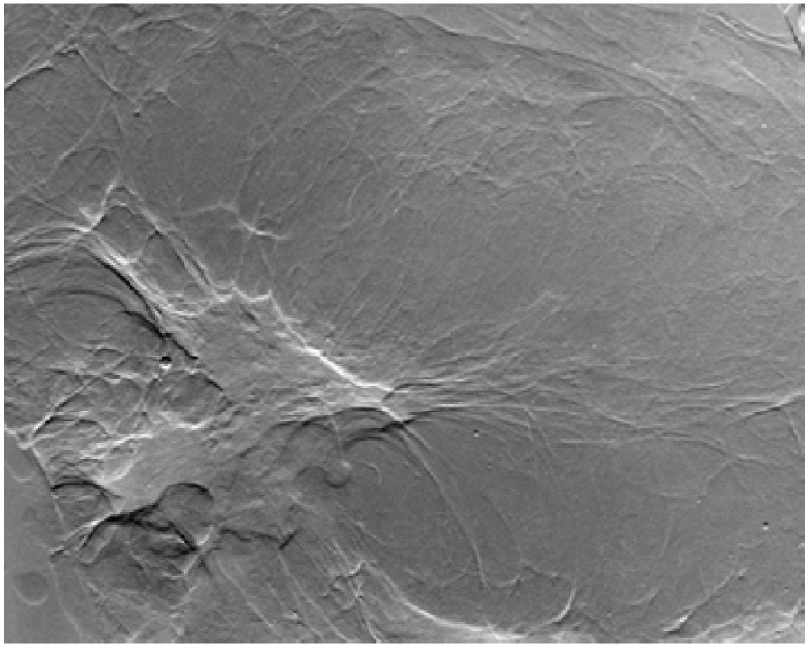


Bio-Medical Imaging & Therapy (BMIT)

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

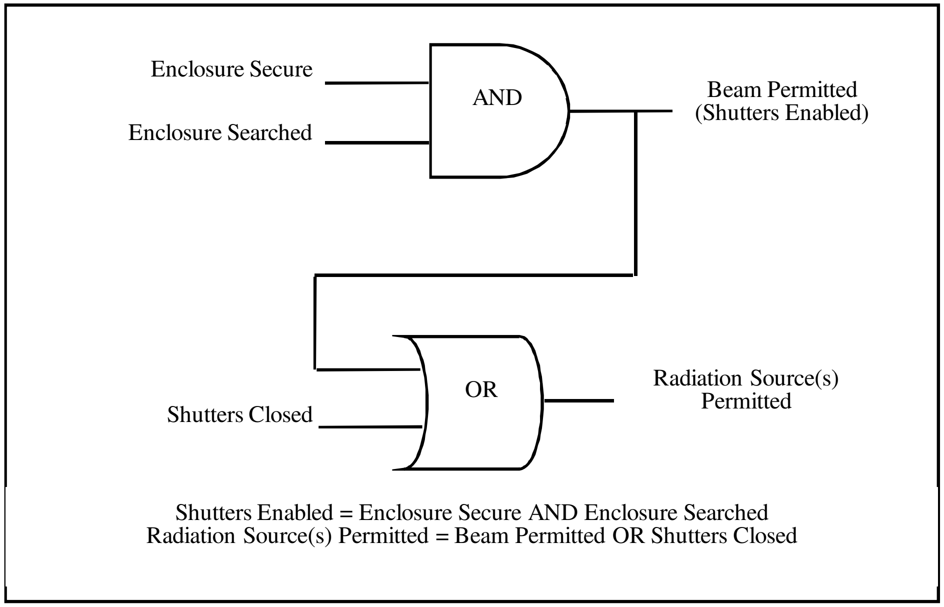
Specification

❑Hazard Analysis: Radiation Exposure is Primary Hazard

❑Requirements:

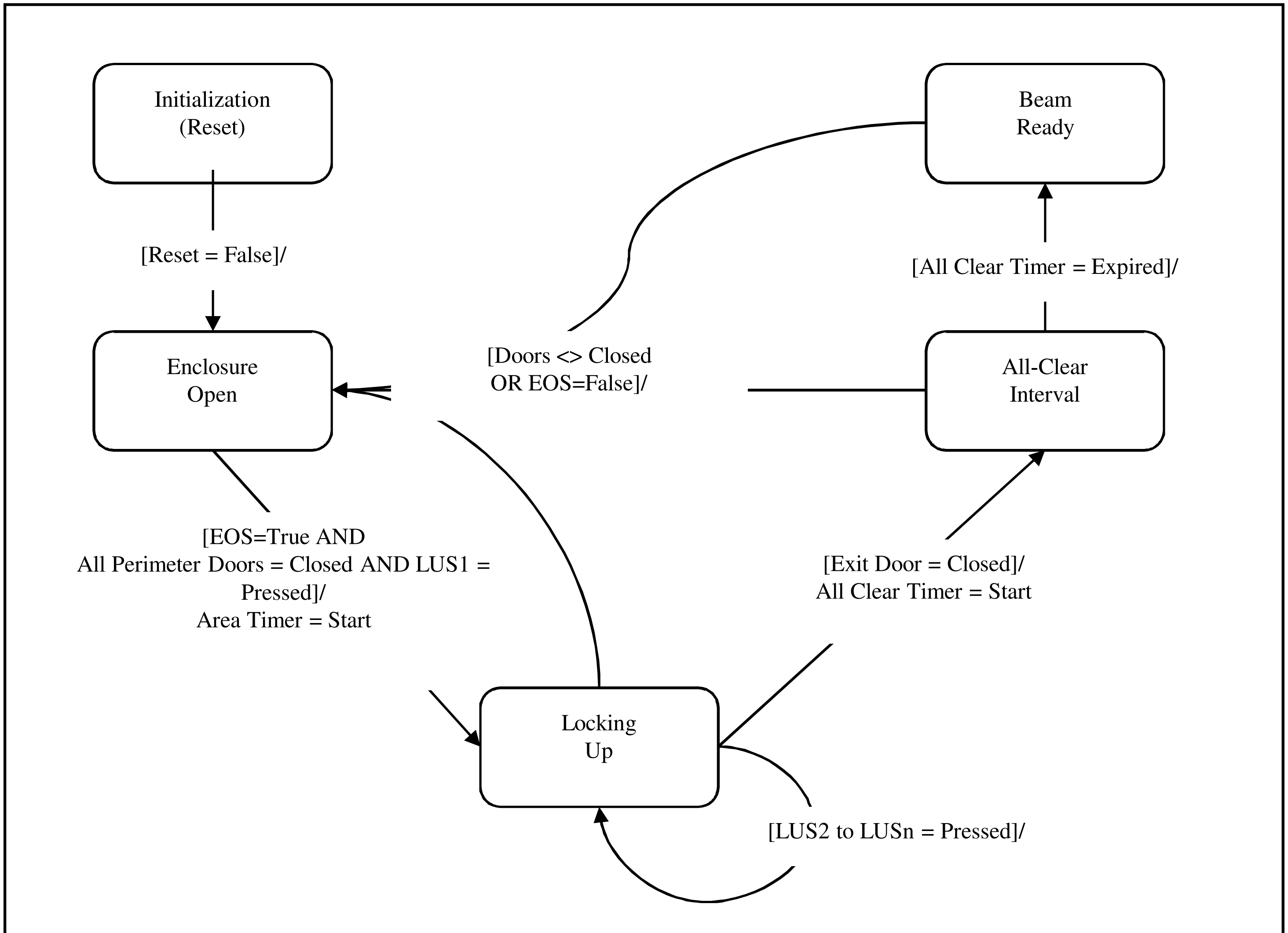
- ❑Use both quantitative and qualitative definitions
- ❑Secure an enclosure,
- ❑Search an enclosure.

❑An example of a formal definition:



Shutters Enabled = Enclosure Secure AND Enclosure Searched
Radiation Source(s) Permitted = Beam Permitted OR Shutters Closed

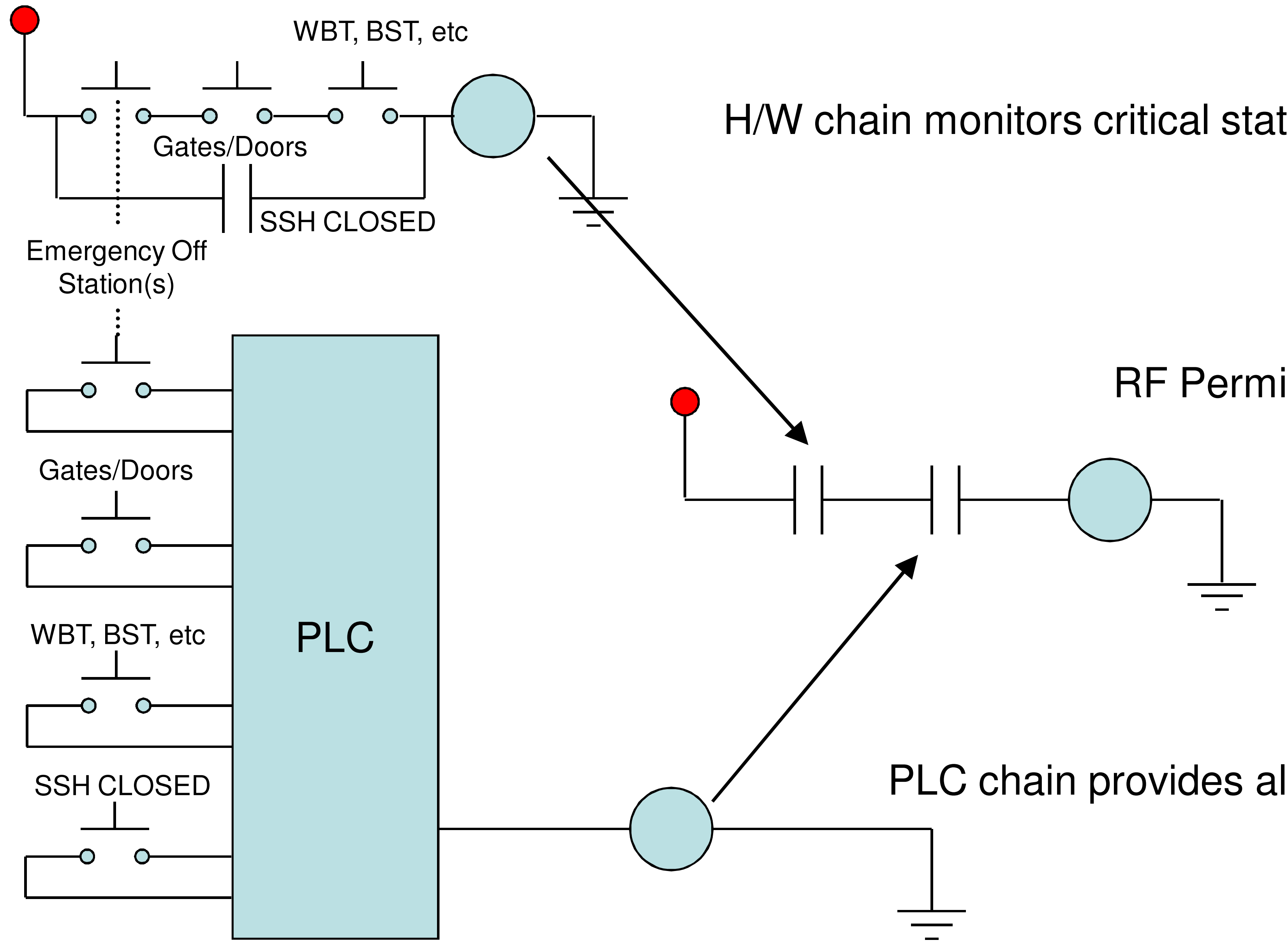
Specification



State Diagram of the Search/Secure Procedure

Canadian Light Source Centre canadien de rayonnement synchrotron

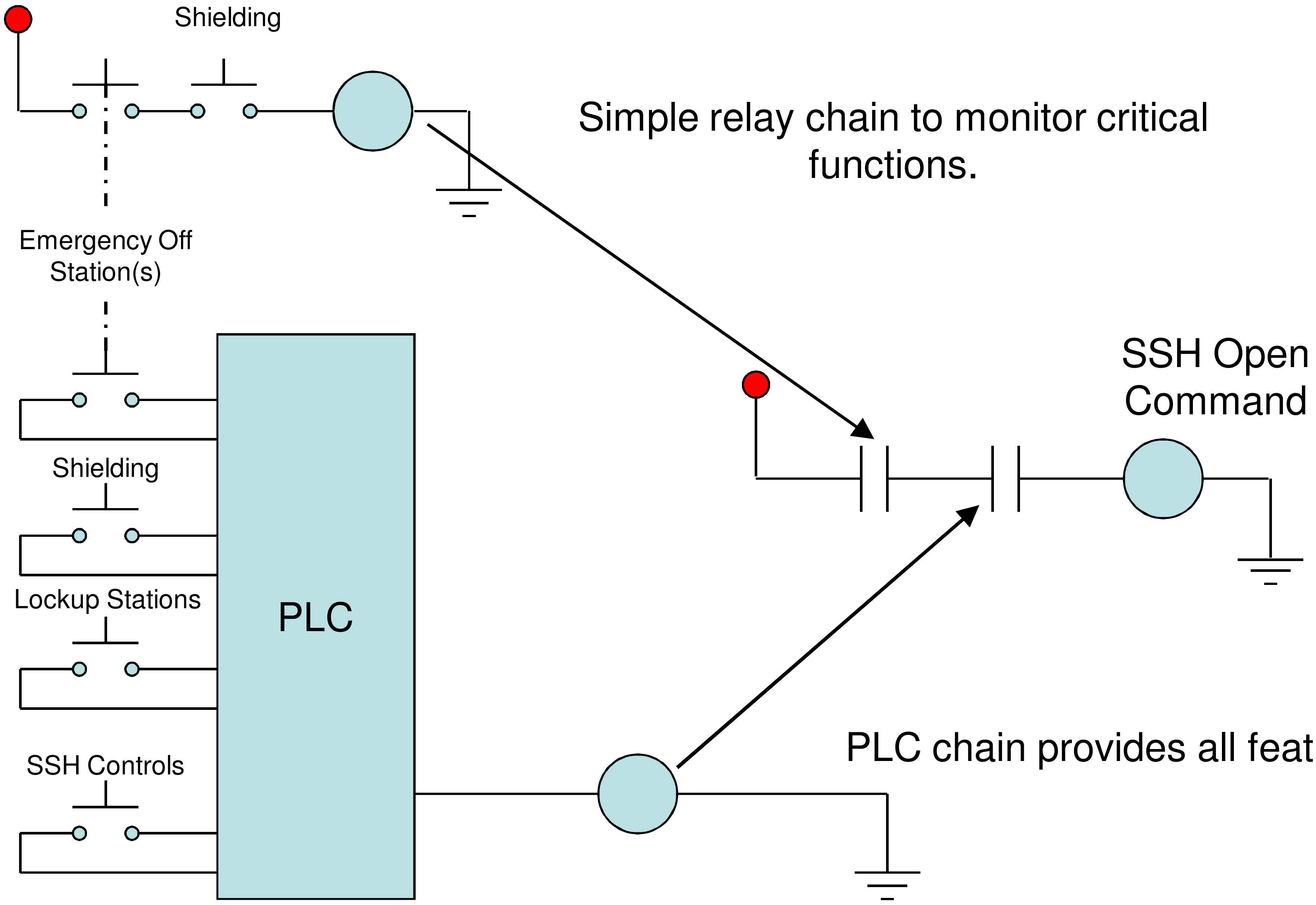
Critical Functions (SIFs)



H/W chain monitors critical states

PLC chain provides all features.

PLC System w/ HW Backup

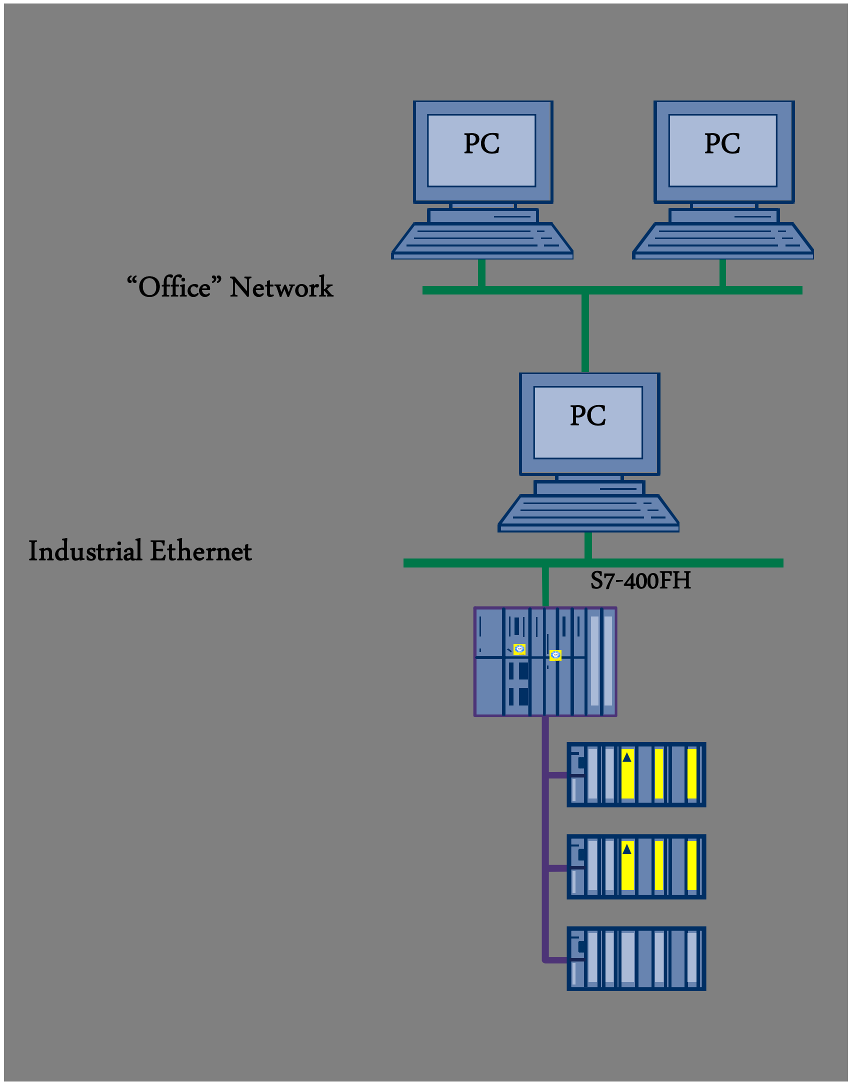


Simple relay chain to monitor critical functions.

PLC chain provides all features.

Hardware

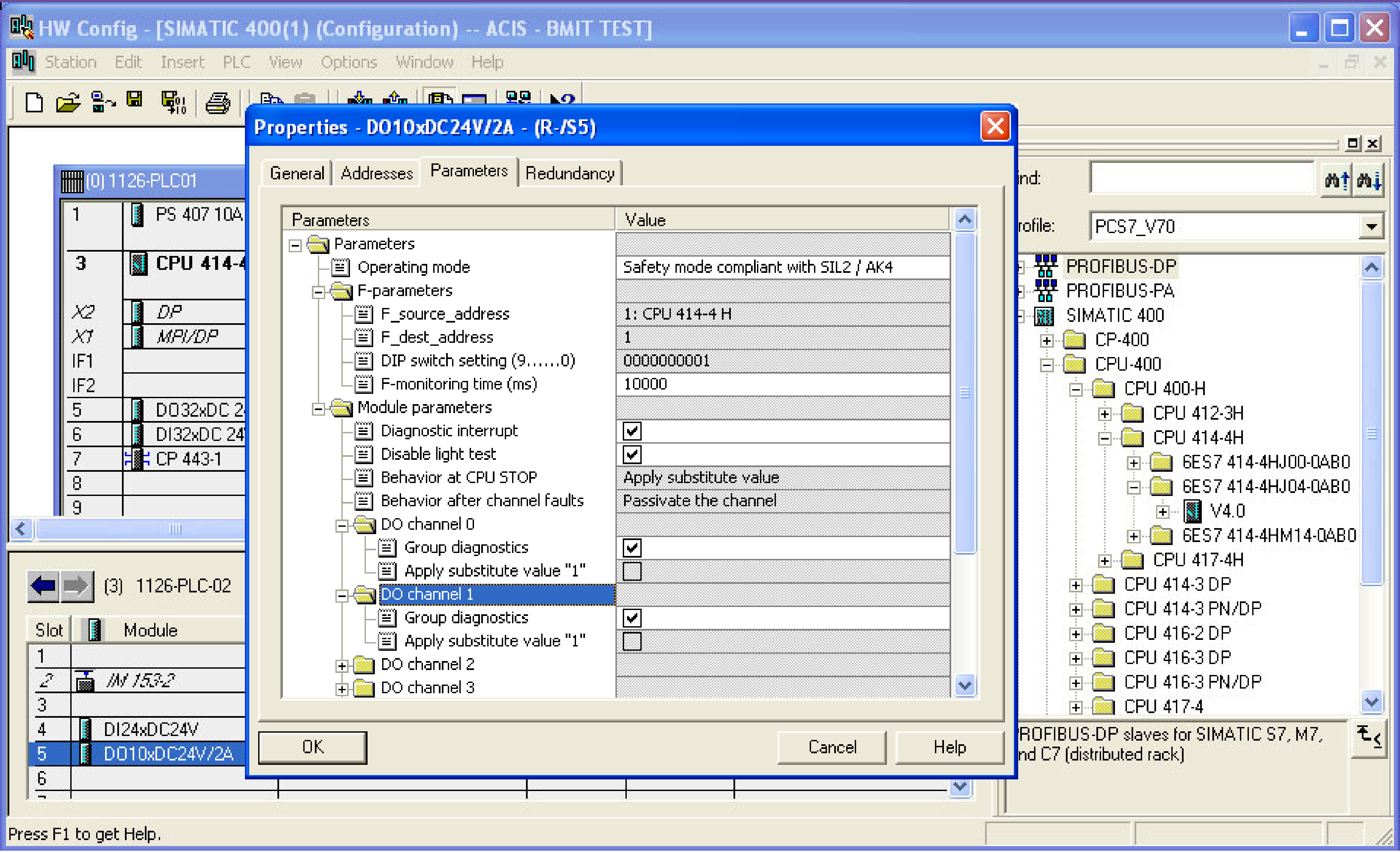
- ❑Office and Controls network
- ❑Engineering Station
- ❑Plantbus
- ❑Remote I/O (ProfiSAFE)



Software

- Siemens PCS 7 v 7.0 SP 1
- Failsafe Libraries
- PLCSIM

Hardware Configuration



HW Config - [SIMATIC 400(1) (Configuration) -- ACIS - BMIT TEST]

(0) 1126-PLC01

1	PS 407 10A
3	CPU 414-4
X2	DP
X1	MPI/DP
IF1	
IF2	
5	DO32xDC 2
6	DI32xDC 24
7	CP 443-1
8	
9	

(3) 1126-PLC-02

Slot	Module
1	
2	IM 153-2
3	
4	DI24xDC24V
5	DO10xDC24V/2A
6	

Properties - DO10xDC24V/2A - (R-/S5)

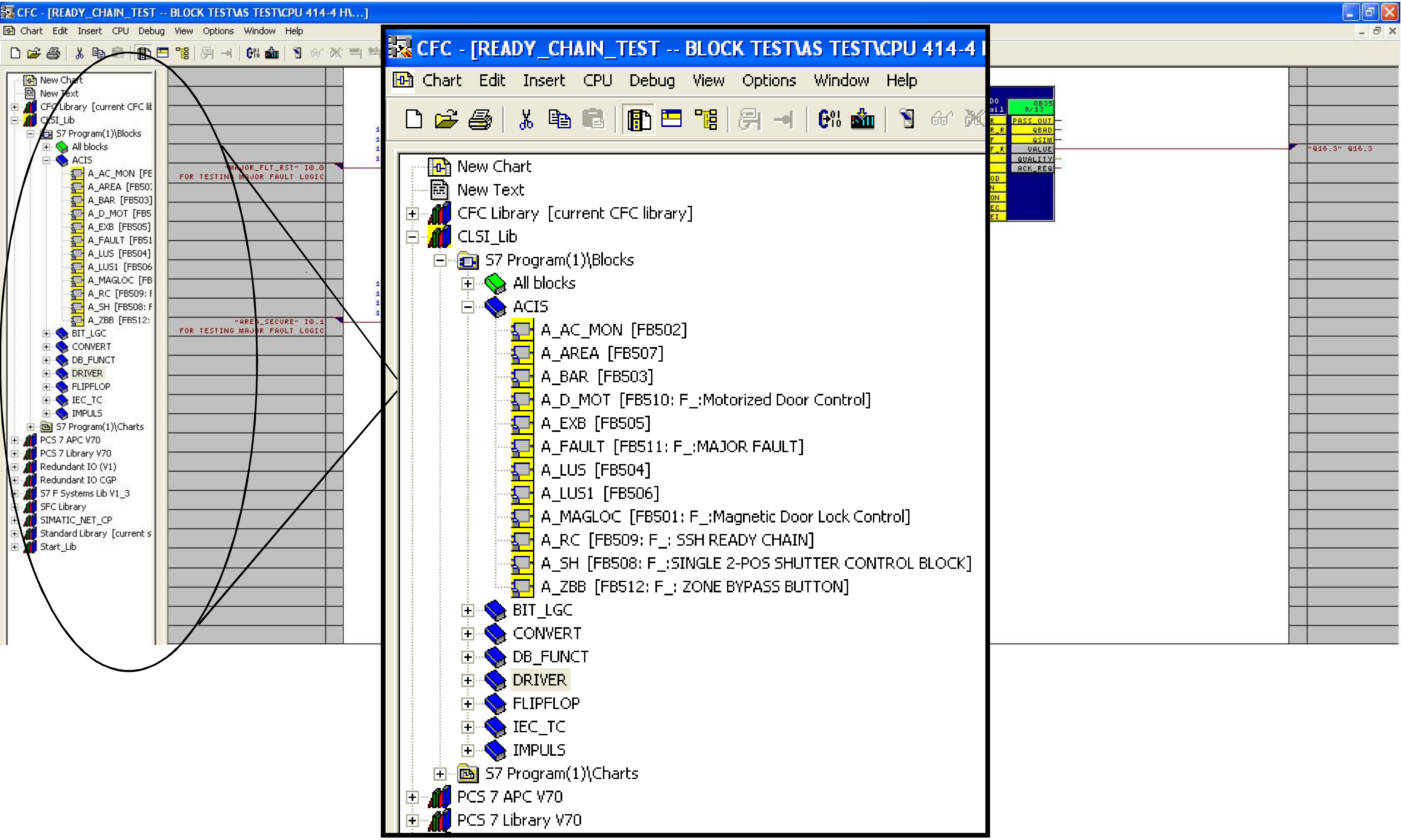
Parameters	Value
Parameters	
Operating mode	Safety mode compliant with SIL2 / AK4
F-parameters	
F_source_address	1: CPU 414-4 H
F_dest_address	1
DIP switch setting (9......0)	0000000001
F-monitoring time (ms)	10000
Module parameters	
Diagnostic interrupt	☑
Disable light test	☑
Behavior at CPU STOP	Apply substitute value
Behavior after channel faults	Passivate the channel
DO channel 0	
Group diagnostics	☑
Apply substitute value "1"	☐
DO channel 1	
Group diagnostics	☑
Apply substitute value "1"	☐
DO channel 2	
DO channel 3	

Profile: PCS7_V70

- PROFIBUS-DP
- PROFIBUS-PA
- SIMATIC 400
  - CP-400
  - CPU-400
    - CPU 400-H
      - CPU 412-3H
      - CPU 414-4H
        - 6ES7 414-4HJ00-0AB0
        - 6ES7 414-4HJ04-0AB0
          - V4.0
        - 6ES7 414-4HM14-0AB0
      - CPU 417-4H
    - CPU 414-3 DP
    - CPU 414-3 PN/DP
    - CPU 416-2 DP
    - CPU 416-3 DP
    - CPU 416-3 PN/DP
    - CPU 417-4

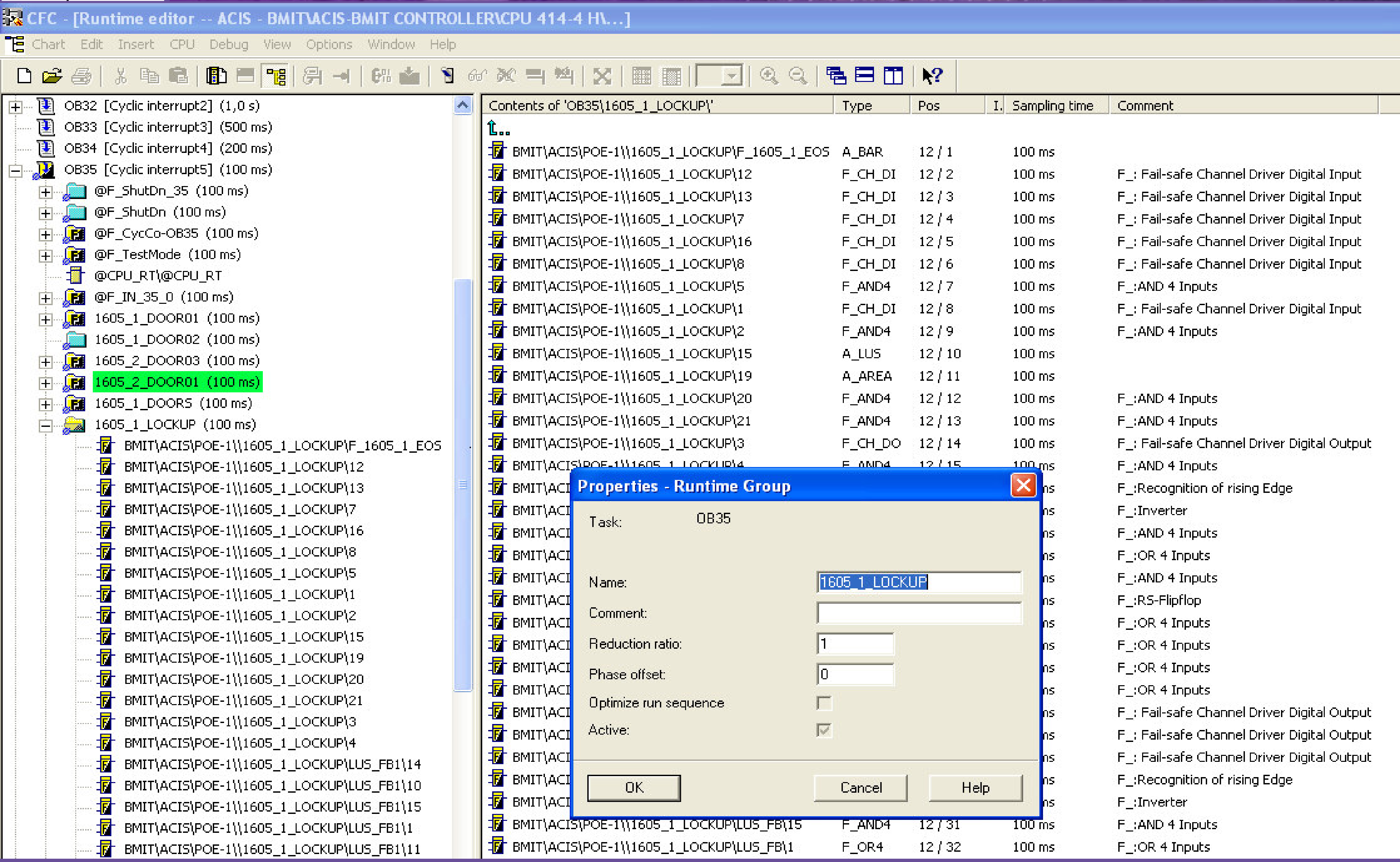
ROFIBUS-DP slaves for SIMATIC S7, M7, nd C7 (distributed rack)

Programming Environment


CFC - [READY_CHAIN_TEST -- BLOCK TEST\AS TEST\CPU 414-4 H\...]
Chart Edit Insert CPU Debug View Options Window Help
"MAJOR_FLT_RST" I0.0
FOR TESTING MAJOR FAULT LOGIC
"AREA_SECURE" I0.1
FOR TESTING MAJOR FAULT LOGIC
OB35
9/13
PASS_OUT
QBAD
QSIM
VALUE
QUALITY
ACK_REQ
"Q16.3" Q16.3

```
New Chart
New Text
+ CFC Library  [current CFC library]
- CLSI_Lib
    - S7 Program(1)\Blocks
        + All blocks
        - ACIS
            A_AC_MON  [FB502]
            A_AREA  [FB507]
            A_BAR  [FB503]
            A_D_MOT  [FB510: F_:Motorized Door Control]
            A_EXB  [FB505]
            A_FAULT  [FB511: F_:MAJOR FAULT]
            A_LUS  [FB504]
            A_LUS1  [FB506]
            A_MAGLOC  [FB501: F_:Magnetic Door Lock Control]
            A_RC  [FB509: F_: SSH READY CHAIN]
            A_SH  [FB508: F_:SINGLE 2-POS SHUTTER CONTROL BLOCK]
            A_ZBB  [FB512: F_: ZONE BYPASS BUTTON]
        + BIT_LGC
        + CONVERT
        + DB_FUNCT
        + DRIVER
        + FLIPFLOP
        + IEC_TC
        + IMPULS
    + S7 Program(1)\Charts
+ PCS 7 APC V70
+ PCS 7 Library V70
+ Redundant IO (V1)
+ Redundant IO CGP
+ S7 F Systems Lib V1_3
+ SFC Library
+ SIMATIC_NET_CP
+ Standard Library  [current s
+ Start_Lib
```

Code Organization



CFC - [Runtime editor -- ACIS - BMIT\ACIS-BMIT CONTROLLER\CPU 414-4 H\...]

- OB32 [Cyclic interrupt2] (1,0 s)
- OB33 [Cyclic interrupt3] (500 ms)
- OB34 [Cyclic interrupt4] (200 ms)
- OB35 [Cyclic interrupt5] (100 ms)
  - @F_ShutDn_35 (100 ms)
  - @F_ShutDn (100 ms)
  - @F_CycCo-OB35 (100 ms)
  - @F_TestMode (100 ms)
  - @CPU_RT\@CPU_RT
  - @F_IN_35_0 (100 ms)
  - 1605_1_DOOR01 (100 ms)
  - 1605_1_DOOR02 (100 ms)
  - 1605_2_DOOR03 (100 ms)
  - 1605_2_DOOR01 (100 ms)
  - 1605_1_DOORS (100 ms)
  - 1605_1_LOCKUP (100 ms)
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\F_1605_1_EOS
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\12
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\13
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\7
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\16
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\8
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\5
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\1
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\2
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\15
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\19
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\20
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\21
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\3
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\4
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\LUS_FB1\14
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\LUS_FB1\10
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\LUS_FB1\15
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\LUS_FB1\1
    - BMIT\ACIS\POE-1\\1605_1_LOCKUP\LUS_FB1\11

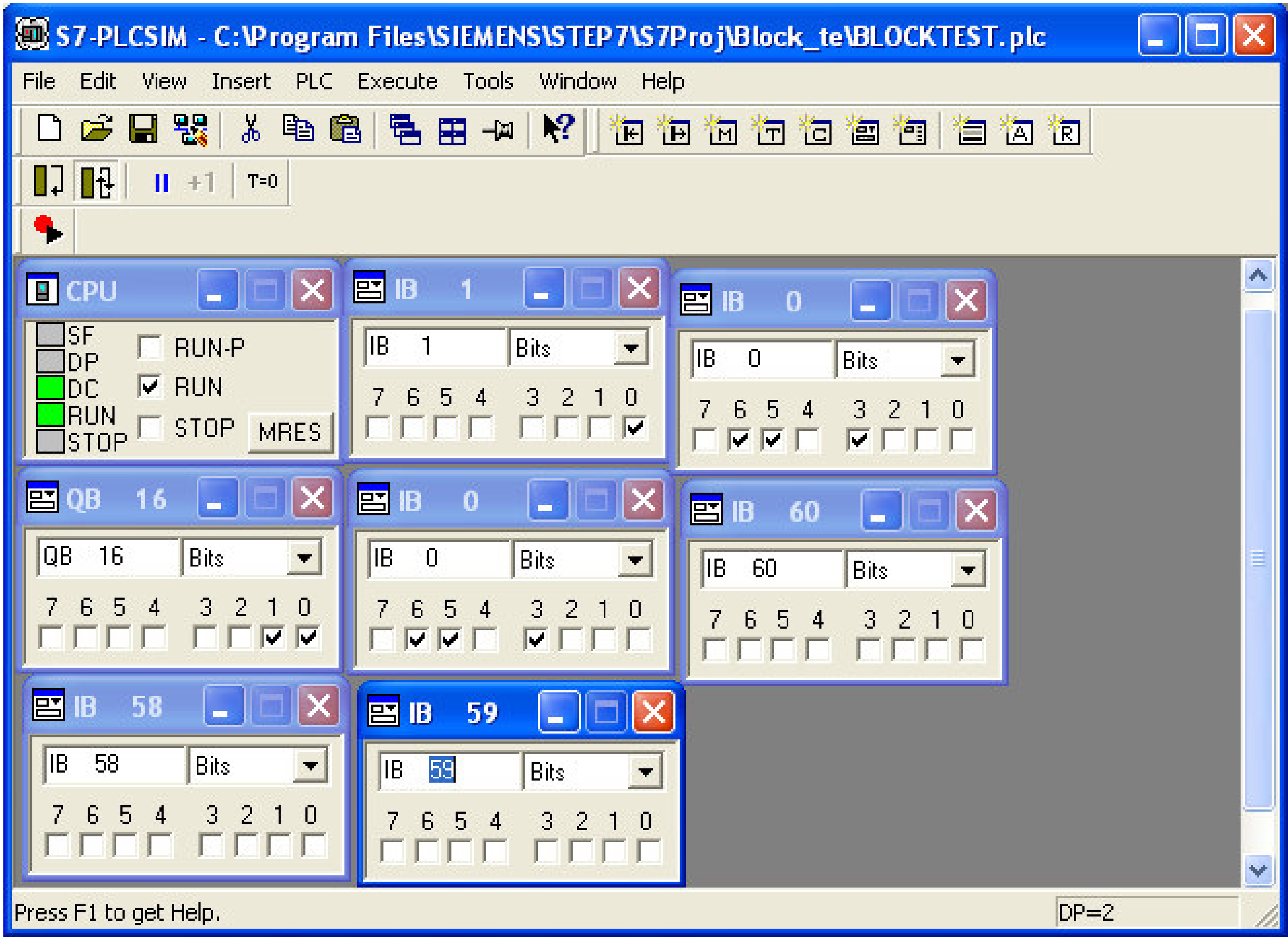
Contents of 'OB35\1605_1_LOCKUP\'	Type	Pos	I.	Sampling time	Comment
..					
BMIT\ACIS\POE-1\\1605_1_LOCKUP\F_1605_1_EOS	A_BAR	12 / 1		100 ms	
BMIT\ACIS\POE-1\\1605_1_LOCKUP\12	F_CH_DI	12 / 2		100 ms	F_: Fail-safe Channel Driver Digital Input
BMIT\ACIS\POE-1\\1605_1_LOCKUP\13	F_CH_DI	12 / 3		100 ms	F_: Fail-safe Channel Driver Digital Input
BMIT\ACIS\POE-1\\1605_1_LOCKUP\7	F_CH_DI	12 / 4		100 ms	F_: Fail-safe Channel Driver Digital Input
BMIT\ACIS\POE-1\\1605_1_LOCKUP\16	F_CH_DI	12 / 5		100 ms	F_: Fail-safe Channel Driver Digital Input
BMIT\ACIS\POE-1\\1605_1_LOCKUP\8	F_CH_DI	12 / 6		100 ms	F_: Fail-safe Channel Driver Digital Input
BMIT\ACIS\POE-1\\1605_1_LOCKUP\5	F_AND4	12 / 7		100 ms	F_:AND 4 Inputs
BMIT\ACIS\POE-1\\1605_1_LOCKUP\1	F_CH_DI	12 / 8		100 ms	F_: Fail-safe Channel Driver Digital Input
BMIT\ACIS\POE-1\\1605_1_LOCKUP\2	F_AND4	12 / 9		100 ms	F_:AND 4 Inputs
BMIT\ACIS\POE-1\\1605_1_LOCKUP\15	A_LUS	12 / 10		100 ms	
BMIT\ACIS\POE-1\\1605_1_LOCKUP\19	A_AREA	12 / 11		100 ms	
BMIT\ACIS\POE-1\\1605_1_LOCKUP\20	F_AND4	12 / 12		100 ms	F_:AND 4 Inputs
BMIT\ACIS\POE-1\\1605_1_LOCKUP\21	F_AND4	12 / 13		100 ms	F_:AND 4 Inputs
BMIT\ACIS\POE-1\\1605_1_LOCKUP\3	F_CH_DO	12 / 14		100 ms	F_: Fail-safe Channel Driver Digital Output
BMIT\ACIS\POE-1\\1605_1_LOCKUP\4	F_AND4	12 / 15		100 ms	F_:AND 4 Inputs
BMIT\ACI				ns	F_:Recognition of rising Edge
BMIT\ACI				ns	F_:Inverter
BMIT\ACI				ns	F_:AND 4 Inputs
BMIT\ACI				ns	F_:OR 4 Inputs
BMIT\ACI				ns	F_:AND 4 Inputs
BMIT\ACI				ns	F_:RS-Flipflop
BMIT\ACI				ns	F_:OR 4 Inputs
BMIT\ACI				ns	F_:OR 4 Inputs
BMIT\ACI				ns	F_:OR 4 Inputs
BMIT\ACI				ns	F_:OR 4 Inputs
BMIT\ACI				ns	F_: Fail-safe Channel Driver Digital Output
BMIT\ACI				ns	F_: Fail-safe Channel Driver Digital Output
BMIT\ACI				ns	F_: Fail-safe Channel Driver Digital Output
BMIT\ACI				ns	F_:Recognition of rising Edge
BMIT\ACI				ns	F_:Inverter
BMIT\ACIS\POE-1\\1605_1_LOCKUP\LUS_FB\15	F_AND4	12 / 31		100 ms	F_:AND 4 Inputs
BMIT\ACIS\POE-1\\1605_1_LOCKUP\LUS_FB\1	F_OR4	12 / 32		100 ms	F_:OR 4 Inputs

Properties - Runtime Group

Task:	OB35
Name:	1605_1_LOCKUP
Comment:	
Reduction ratio:	1
Phase offset:	0
Optimize run sequence	☐
Active:	☑

Testing/Debugging

- In Situ
- Test bed
- PLCSIM



S7-PLCSIM - C:\Program Files\SIEMENS\STEP 7\S7Proj\Block_te\BLOCKTEST.plc

CPU

SF	☐ RUN-P
DP	☑ RUN
DC	☐ STOP
RUN	MRES
STOP	

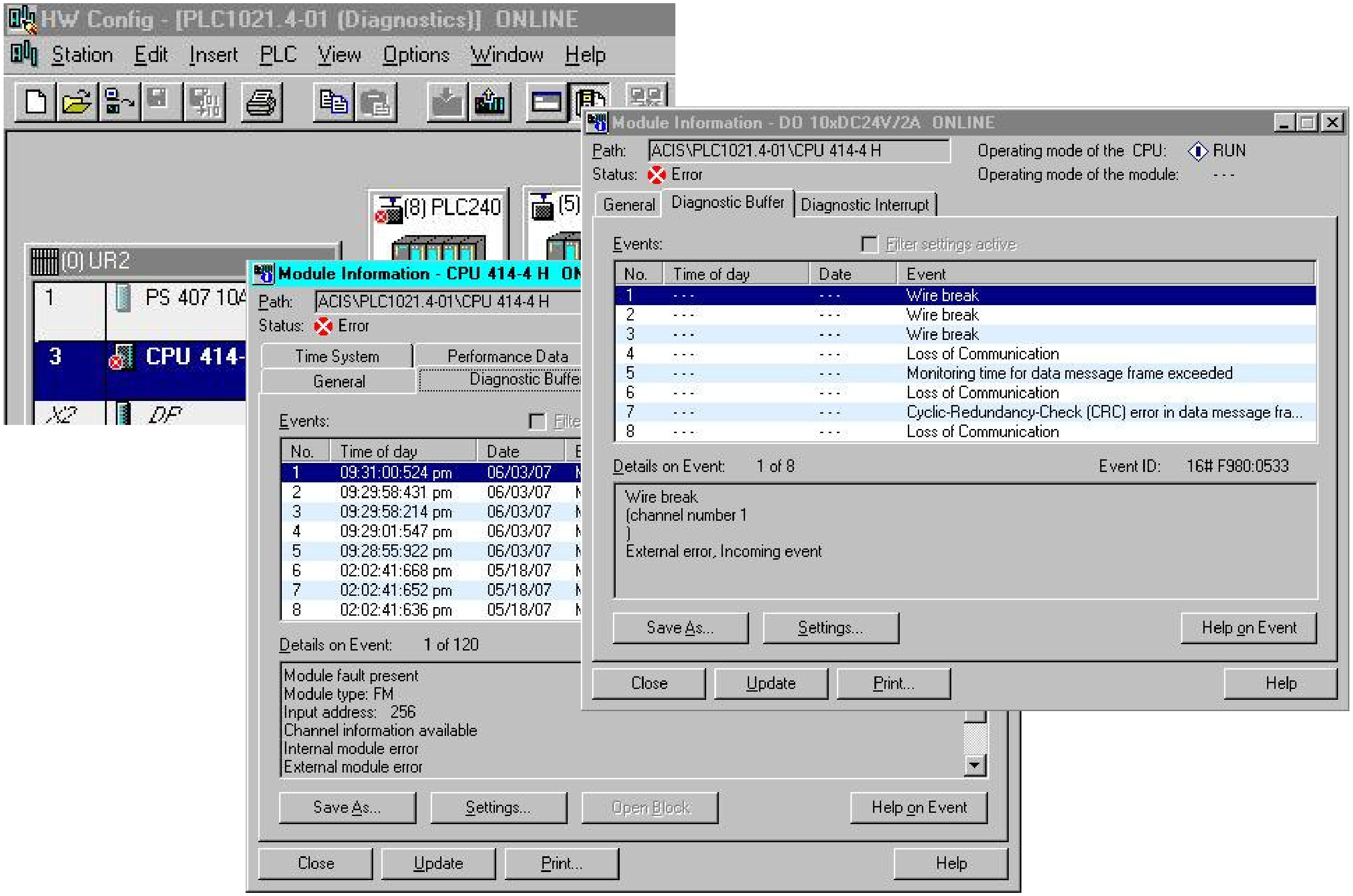
Window	Format	7	6	5	4	3	2	1	0
IB 1	Bits	☐	☐	☐	☐	☐	☐	☐	☑
IB 0	Bits	☐	☑	☑	☐	☑	☐	☐	☐
QB 16	Bits	☐	☐	☐	☐	☐	☐	☑	☑
IB 0	Bits	☐	☑	☑	☐	☑	☐	☐	☐
IB 60	Bits	☐	☐	☐	☐	☐	☐	☐	☐
IB 58	Bits	☐	☐	☐	☐	☐	☐	☐	☐
IB 59	Bits	☐	☐	☐	☐	☐	☐	☐	☐

Press F1 to get Help.

DP=2

Testing/Debugging

- ❑Hardware Configuration diagnostics VERY handy.



Module Information - CPU 414-4 H ON

Path: ACIS\PLC1021.4-01\CPU 414-4 H
Status: ☒ Error

Events: □ Filte

No.	Time of day	Date	E
1	09:31:00:524 pm	06/03/07	M
2	09:29:58:431 pm	06/03/07	M
3	09:29:58:214 pm	06/03/07	M
4	09:29:01:547 pm	06/03/07	M
5	09:28:55:922 pm	06/03/07	M
6	02:02:41:668 pm	05/18/07	M
7	02:02:41:652 pm	05/18/07	M
8	02:02:41:636 pm	05/18/07	M

Details on Event: 1 of 120

Module fault present
Module type: FM
Input address: 256
Channel information available
Internal module error
External module error

Module Information - DO 10xDC24V/2A ONLINE

Path: ACIS\PLC1021.4-01\CPU 414-4 H
Status: ☒ Error
Operating mode of the CPU: RUN
Operating mode of the module: - - -

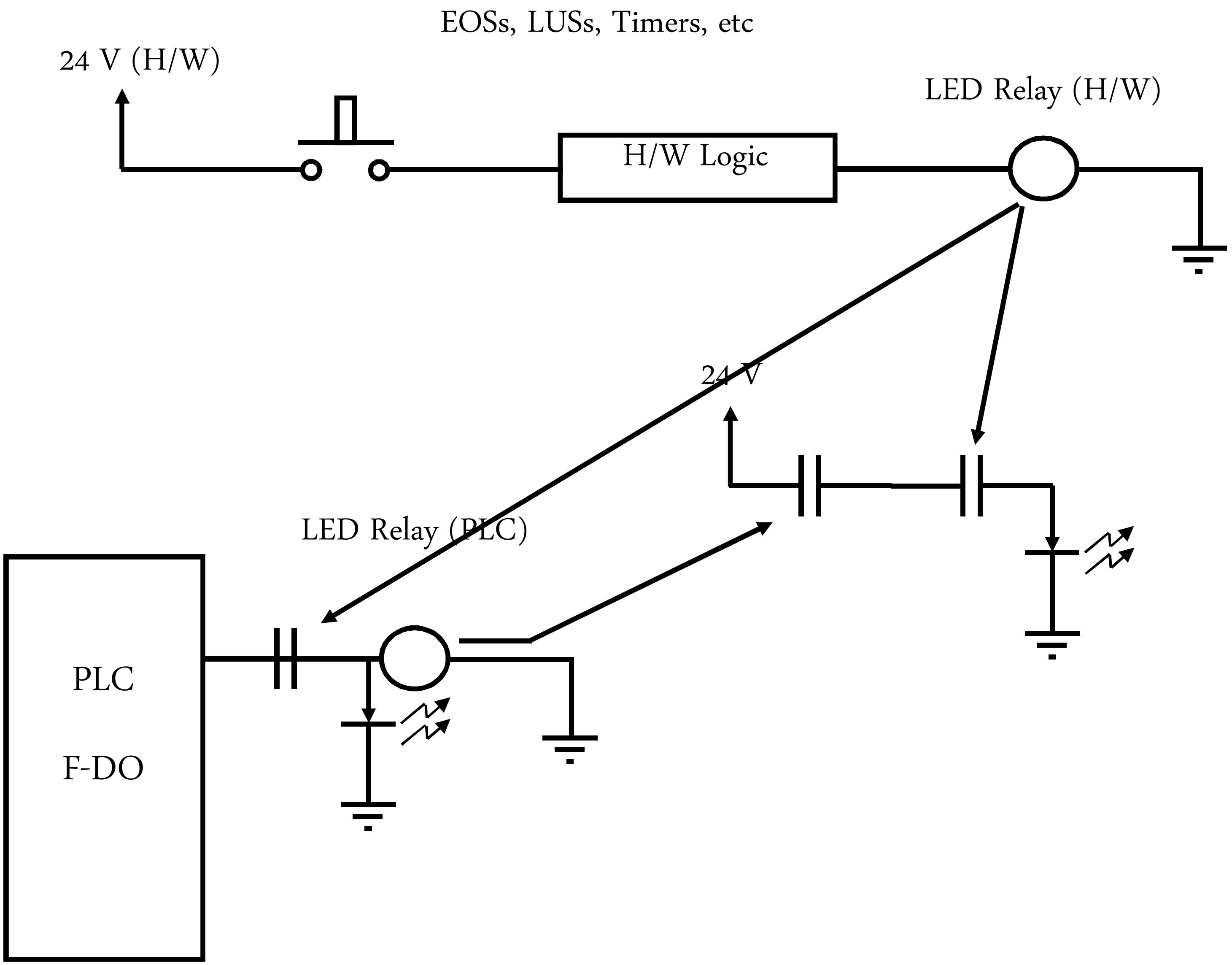
Events: □ Filter settings active

No.	Time of day	Date	Event
1	- - -	- - -	Wire break
2	- - -	- - -	Wire break
3	- - -	- - -	Wire break
4	- - -	- - -	Loss of Communication
5	- - -	- - -	Monitoring time for data message frame exceeded
6	- - -	- - -	Loss of Communication
7	- - -	- - -	Cyclic-Redundancy-Check (CRC) error in data message fra...
8	- - -	- - -	Loss of Communication

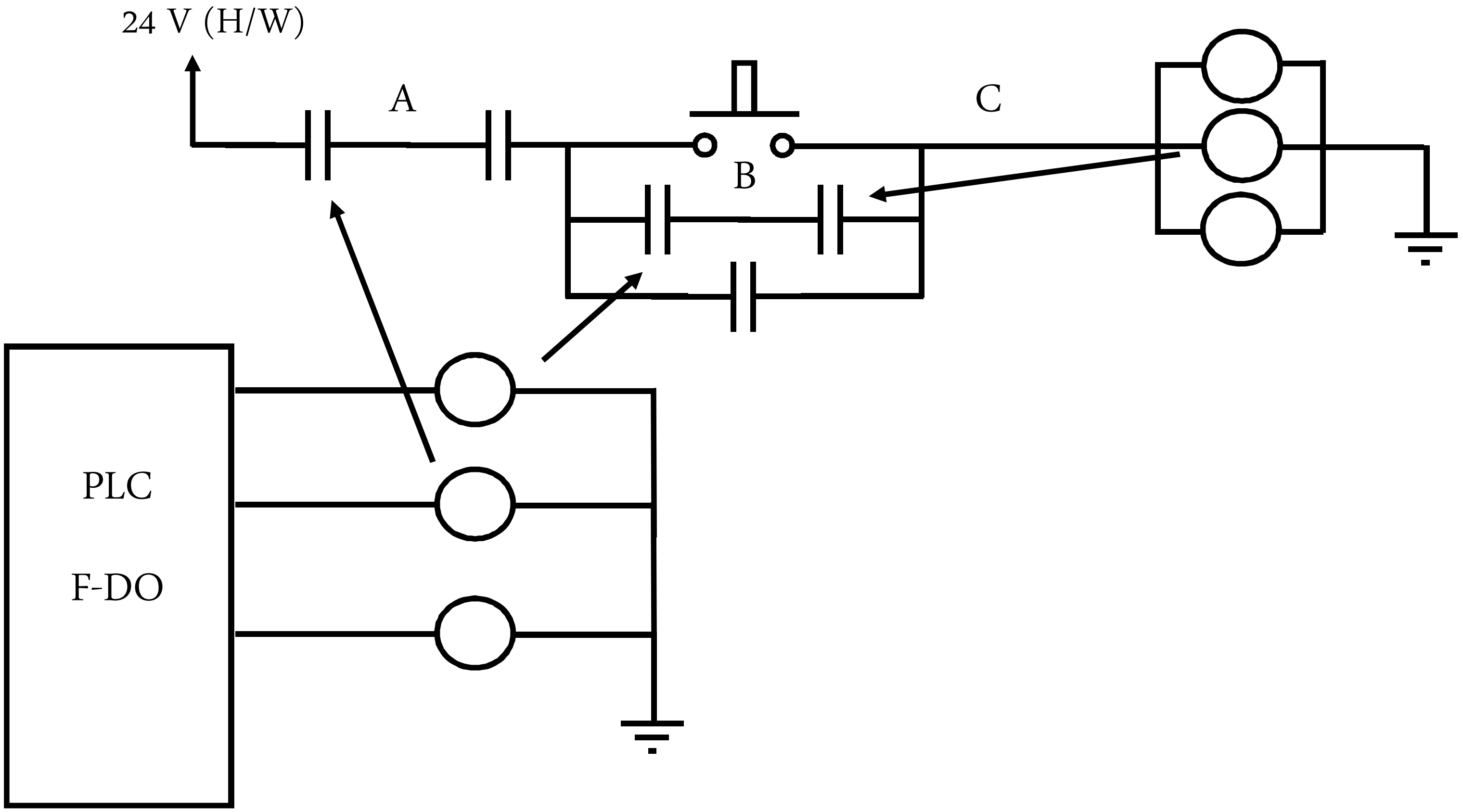
Details on Event: 1 of 8 Event ID: 16# F980:0533

Wire break
(channel number 1
)
External error, Incoming event

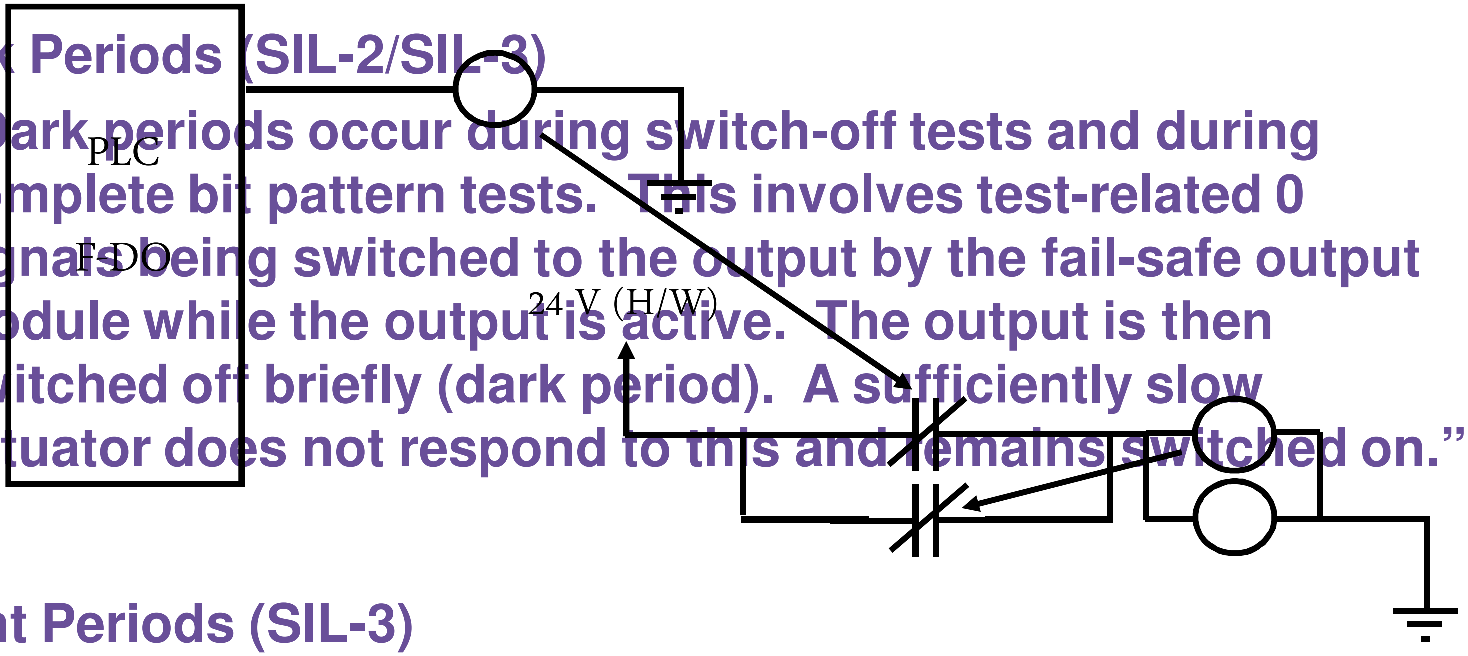
Lessons Learned – Grandfathering



Lessons Learned – Self-Diagnostics



Lessons Learned – Self-Diagnostics



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.”

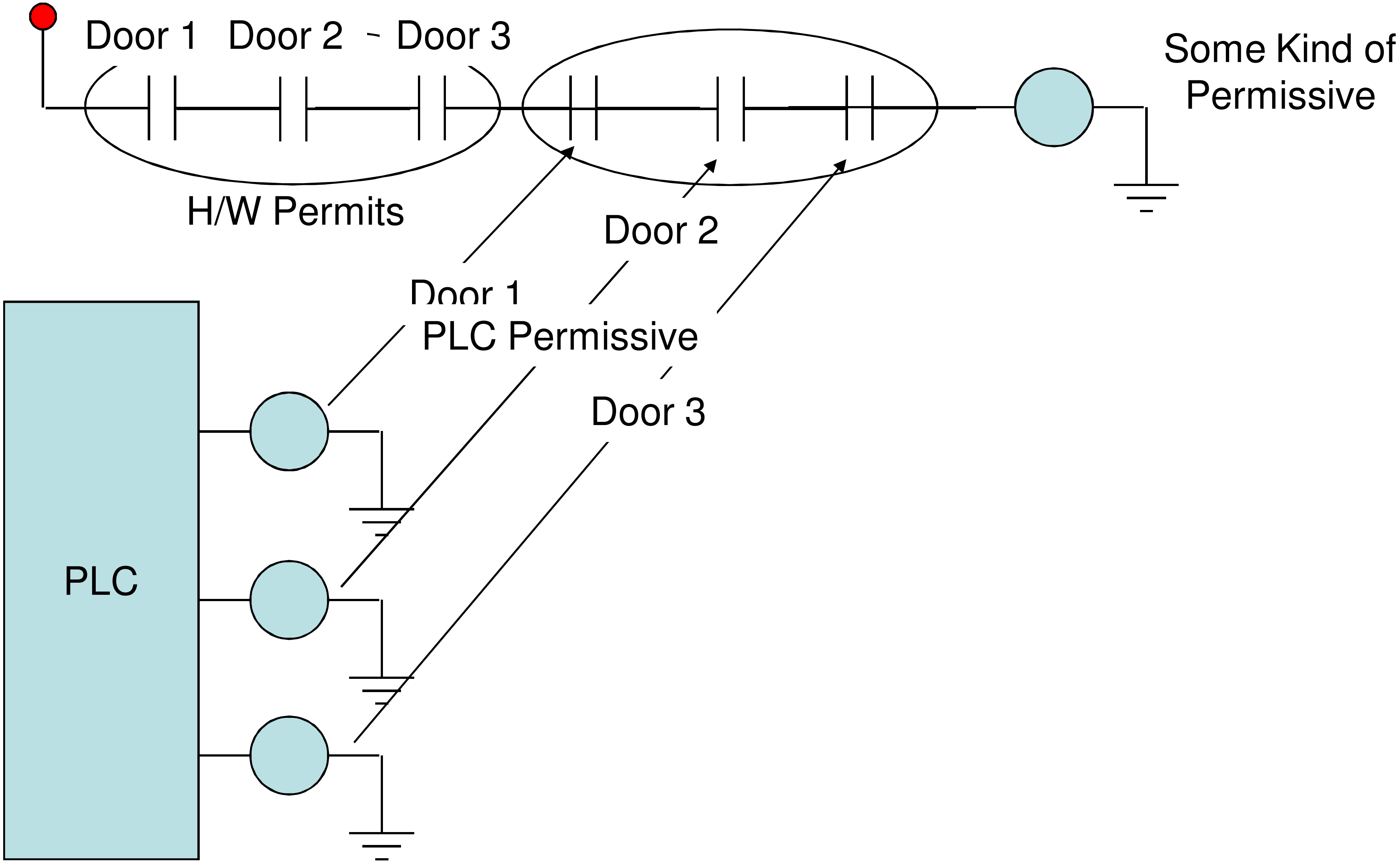
Light Periods (SIL-3)

❑“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 de-activated (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

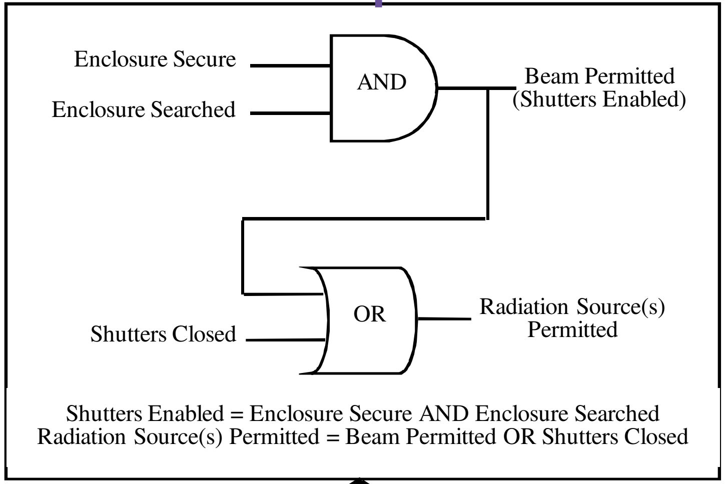
Lessons Learned – Design Process



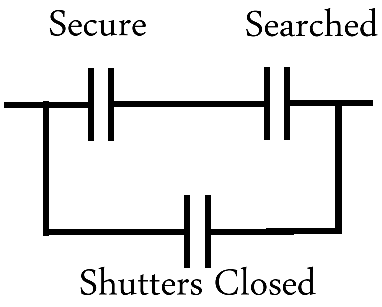
Lessons Learned – Design Process

•Requirement Specification

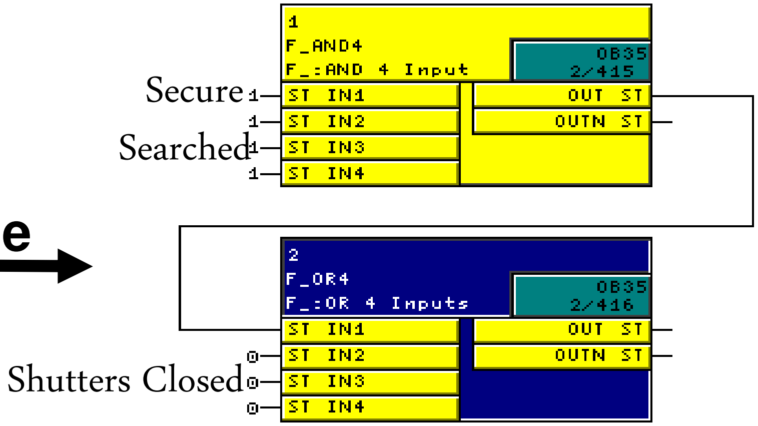
Critical Errors Can be Introduced at the Top of the Design Process



Shutters Enabled = Enclosure Secure AND Enclosure Searched
Radiation Source(s) Permitted = Beam Permitted OR Shutters Closed



Common-Mode Failure



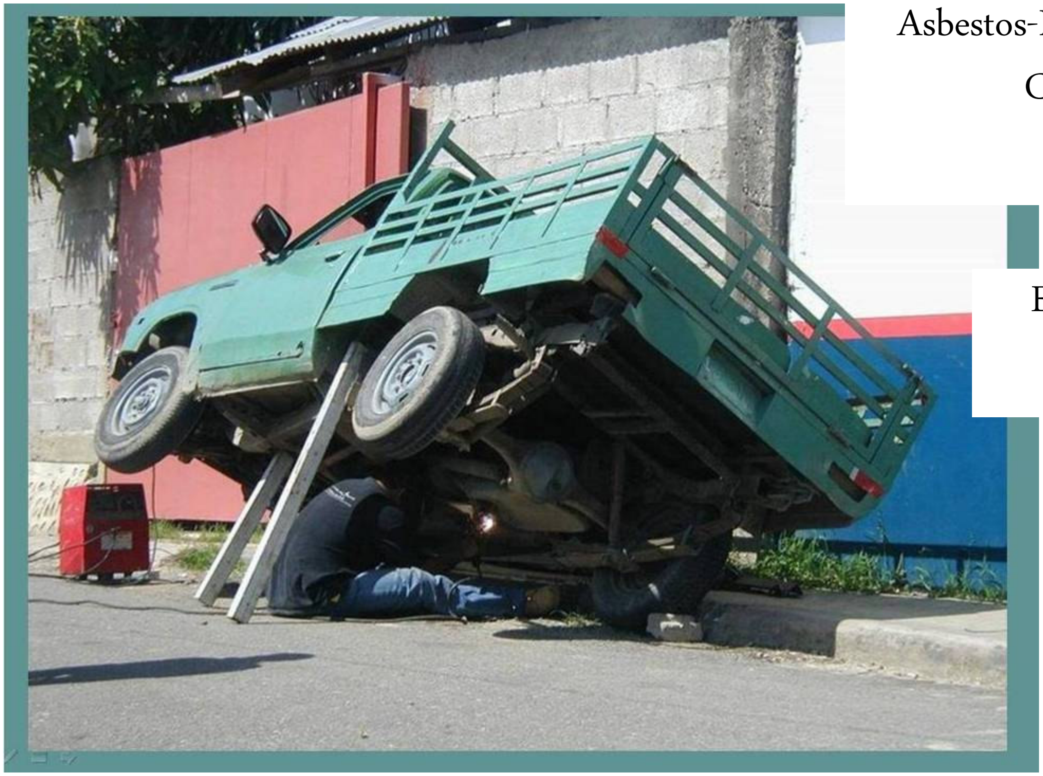
Canadian Light Source Centre canadien de rayonnement synchrotron

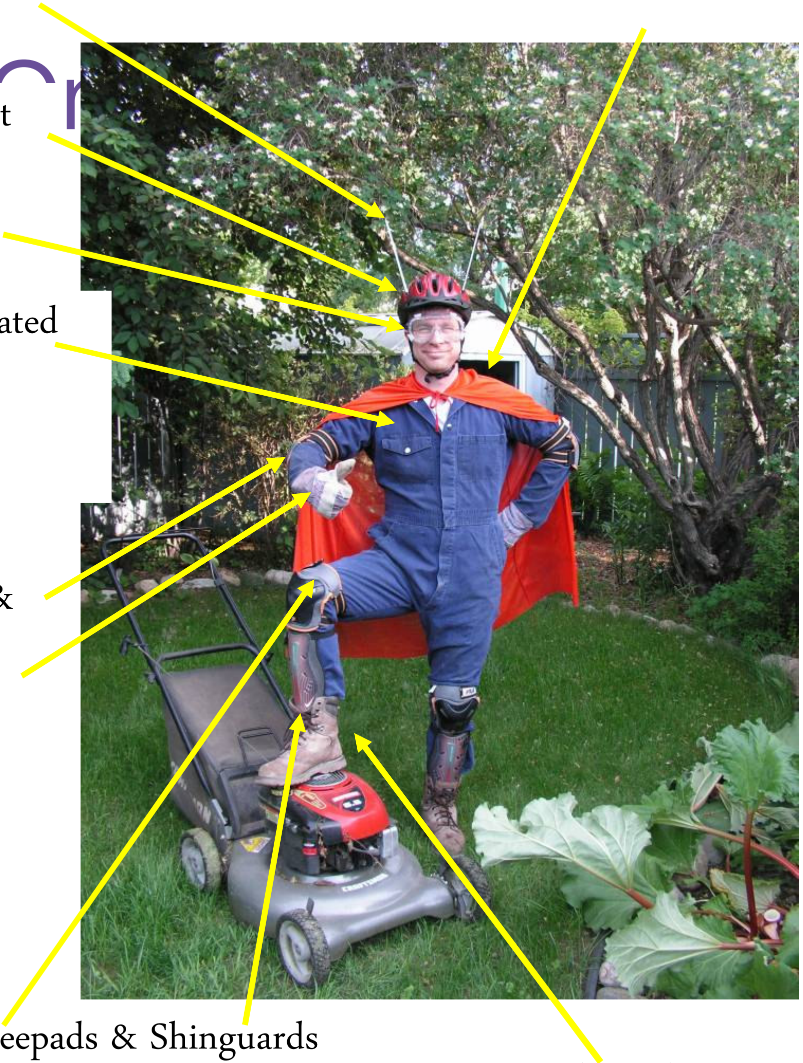
Conclusion

- 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 Saf





Lightning Arrestors

Really Cool Cape

Helmet

Eye Protection

Asbestos-Lined Fire-Rated Coveralls

Elbow Pads & Gloves

Kneepads & Shinguards

Steel-Toed Boots