

# **SPS Access Safety System**

Reliability assessment and  
Risk Analysis of one safety  
function

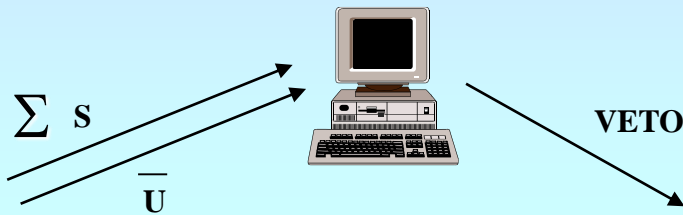
# SPS Access System reliability assessment

Safety function:

Send inhibition command to SPS machine equipment involved in personnel protection when a door is forced in ECX5

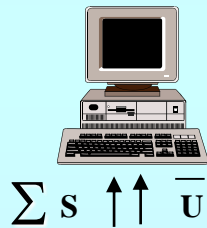
Safety chain:

PCR



**IEC 61508**

CCR



CCR

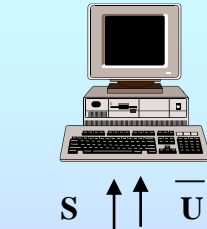
**&**



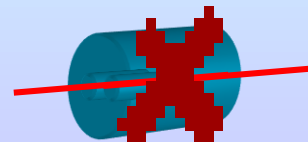
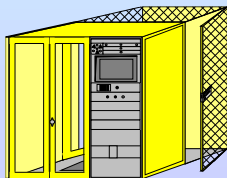
- **Availability?**
- **SIL?**
- **Risk?**

**INB**

Site  
ECX5



Site  
EIS-beam



# Data collection

The screenshot displays the Reliability Workbench interface. The main window shows a prediction summary for a project titled "Prediction for SPS.wkb". The prediction results are as follows:

- PREDICTION : FR=663
- Magnetic switch (reed): FR=0.00954
- Relay (MIL): FR=0.0551
- Coil: FR=0.000112
- Relay (Telecordia): FR=0.175
- Connective...
- Connective...
- Connective...
- Connective...
- Solenoid...
- Battery, I...

A dialog box titled "MIL-217 Switch : 1" is open, showing the following parameters:

- Quantity: 1
- Environment: Ground,benign
- Quality,Other: Low Quality
- Load Type: Inductive
- Elec Stress Calc Mode: Calculated
- Current Stress Ratio: 0.5
- Operating Current (A): 0.5
- Contact Form: Single Pole,Single Throw
- Connection Type: Reflow Solder
- Adjustment Factor: 1
- Type,SW \*: Reed
- No of Contacts \*: 2
- Rated Current (A) \*: 1
- No of Pins \*: 2

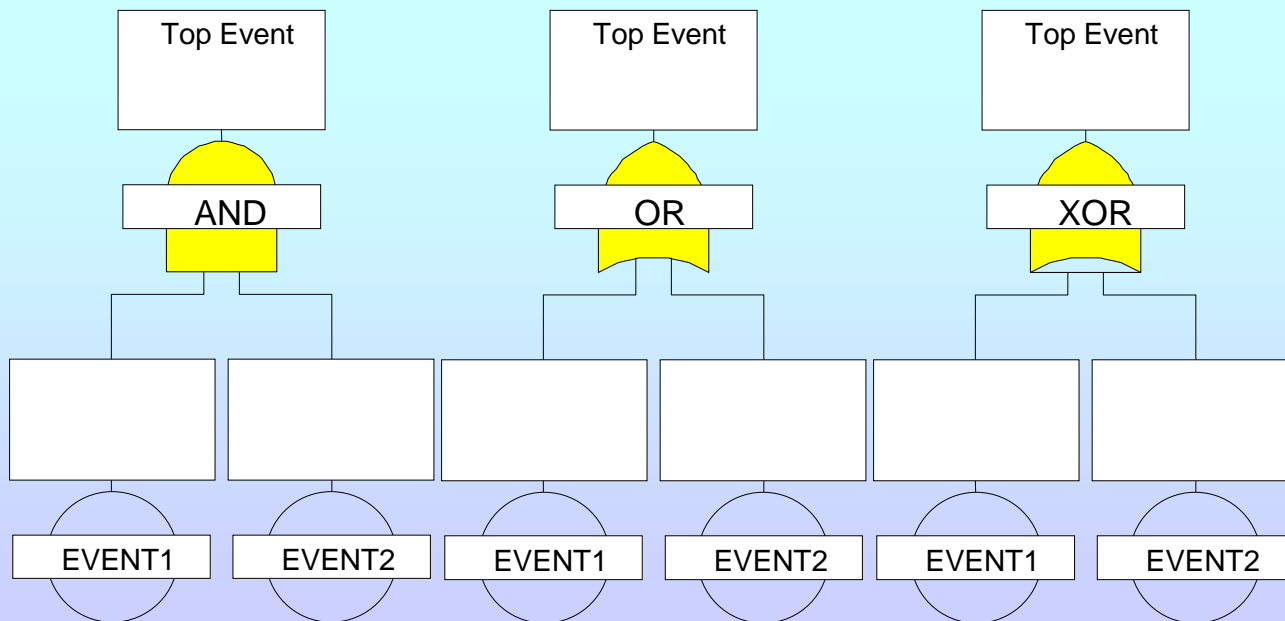
A "View Dialog" window is also open, displaying the following data:

Total Failure rate (fpmh)	0.00954
Base Failure Rate (fpmh) (1_BASE)	0.001
Environment (pi_E)	1
Quality (pi_Q)	2
Contact Configuration (pi_CT)	1
Load Stress (pi_LS)	4.77

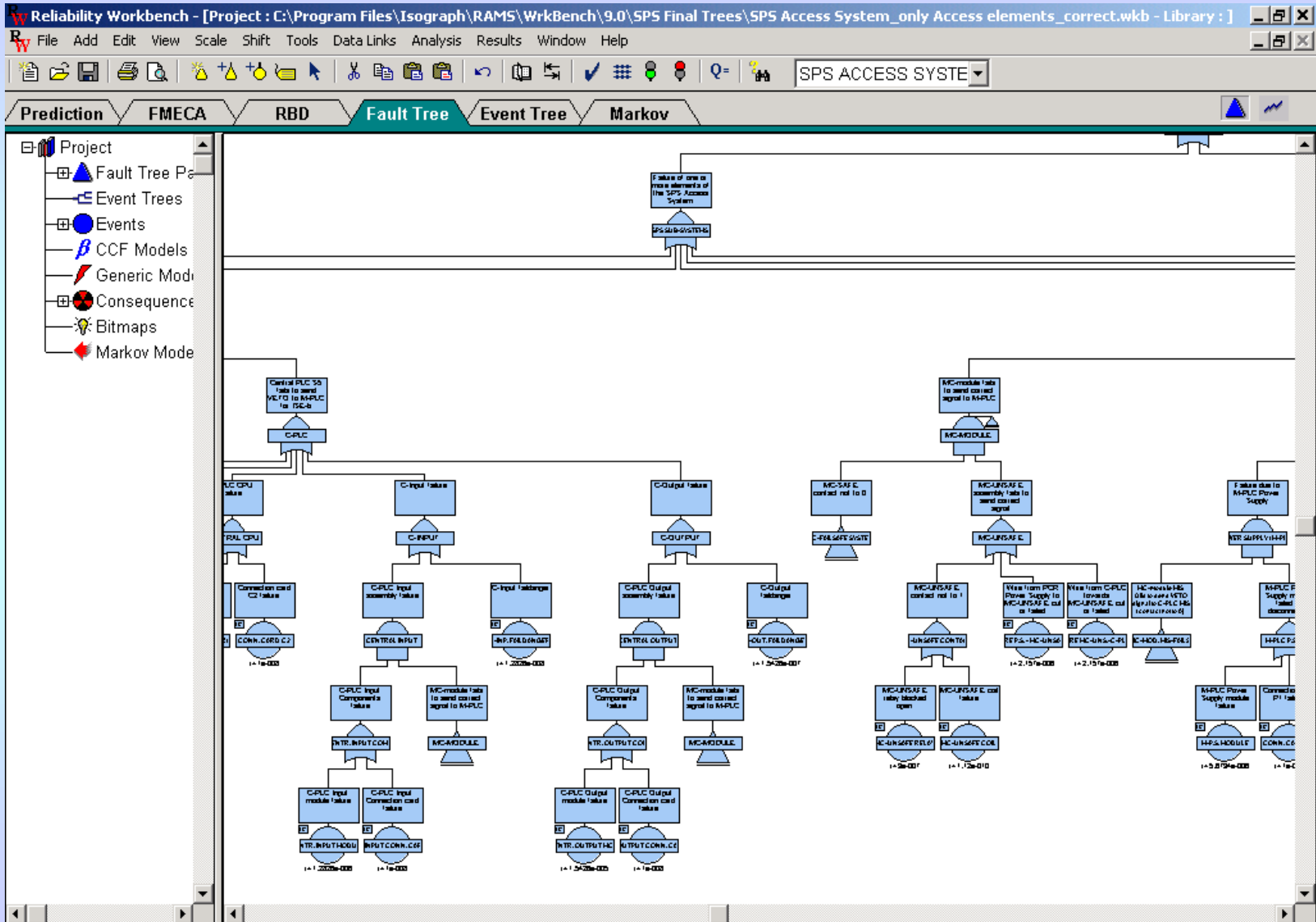
The Windows taskbar at the bottom shows the system time as 19:50 PM on P:10 L:0.

# Fault Tree analysis

- Top-down modeling of failure modes of components
- Boolean logic scheme (OR, AND, XOR, etc.)
- Failure, repair and inspection data
- Dependencies between sub-system



# Fault Tree analysis



# Event Tree analysis – Fault Tree Linking

Reliability Workbench - [Project : C:\Program Files\Isograph\RAMS\WrkBench\9.0\SPS - results and changes\SPS Access System\_all\_for Event Tree.wkb - Library : ]

File Add Edit View Scale Shift Tools DataLinks Analysis Results Window Help

Prediction FMECA RBD Fault Tree **Event Tree** Markov

Initiating Event: Door forced in ECX5	CERN General Power Supply	SPS Access Safety System + external events	Beam Dump System	Consequence	Frequency
<pre> graph LR     A[Door forced in ECX5] -- Failure --&gt; B1[ ]     A -- Success --&gt; B2[ ]     B1 -- Failure --&gt; C1[ ]     B1 -- Success --&gt; B2     B2 -- Failure --&gt; C2[ ]     B2 -- Success --&gt; C3[ ]     C1 -- Failure --&gt; D1[ ]     C1 -- Success --&gt; C3     C2 -- Failure --&gt; D2[ ]     C2 -- Success --&gt; C3     D1 -- Failure --&gt; E1[ ]     D1 -- Success --&gt; C3     D2 -- Failure --&gt; E2[ ]     D2 -- Success --&gt; C3     E1 -- Failure --&gt; F1[No consequences]     E1 -- Success --&gt; F2[1 or more fatalities]     E2 -- Failure --&gt; F2     E2 -- Success --&gt; F3[1 or more fatalities]     E3 -- Failure --&gt; F3     E3 -- Success --&gt; F4[No consequences]                     </pre>					
<p>Attach Fault Trees (if independent)</p>					

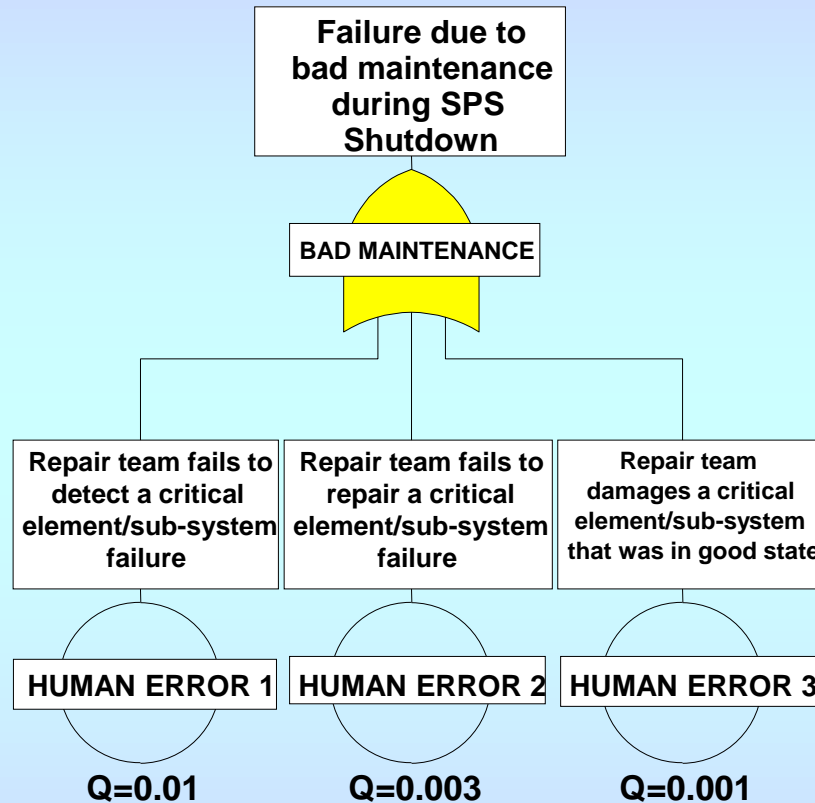
Project

- Fault Tree Pa
- Event Trees
  - ET1
- Events
  - AIRCRA
  - BEAM D
  - C-BOTT
  - C-BOTT
  - C-BOTT
  - C-INP. C
  - C-INP. F
  - C-INP. M
  - C-INPUT
  - C-OUT.
  - C-OUT.
  - C-OUT.
  - C-OUTP
  - C-P. S. M
  - C-P. S. M
  - C-PLC A
  - C-PLC E
  - C-PLC M
  - C-TOP -
  - C-TOP A
  - C-TOP M
  - C. INPU
  - C. OUTP
  - C1: GEN
  - C2: BAT

Ready B:10 E:267

Start | Inbox - Microsoft Outlook | Slides\_presentation | Reliability Workbench ... | 15:47 PM

# Human error



# Maintenance and repair

Reliability Workbench - [Project : C:\Program Files\Isograph\RAMS\WrkBench\9.0\SP5 Final Trees\Opzioni\Final Results\SP5 Access System\_only faildanger\_correct]

File Add Edit View Scale Shift Tools Data Links Analysis Results Window Help

Prediction FMECA RBD **Fault Tree** Event Tree Markov

Project

- Fault Tree Pages
- Event Trees
- Events
- CCF Models
- Generic Models
- Consequences
- Bitmaps
- Markov Models

**Edit Local Model**

Model Type : Dormant

Failure Rate : 2.11e-006

Standard Deviation : 0 Normal

MTTR : 24

Standard Deviation : 0 Normal

Inspection Interval : 0.167

OK Cancel

Failure due to LC Power Supply

L-PLC Power Supply module failed or disconnected

L-PLC POWER SUPPLY ASS. Q=0.0505

Connection Failure of wire

Failure

LOCAL MICRO PROC.  $r=2.11e-006 \tau=0.167$  Q=5.08e-5

CONNECTION CARD I2  $r=1e-008 \tau=0.167$  Q=2.41e-7

L-INP. FAILDANGER  $r=1.2826e-008$  Q=8.46e-5

L-OUTPUT FAILDANGER  $r=1.5426e-007$  Q=0.00102

LC-SAFE RELAY  $r=2.6307e-007$  Q=0.00173

Input failure L-Output failure LC-SAFE contact failure

INPUT Q=4.8e-5 L-OUTPUT Q=0.00102 LC-FAILSAFE Q=0

Input danger L-Output faildanger LC-SAFE relay blocked close

Ready G:106 E:252

Start Reliability AvSim+ Inbox - Microsoft... Grafici v... Reliability 15:41 PM



# **Likelihood** of Initiating Event (data from SL/OP)

- A door is forced at SPS almost once per year (***Probable***)
- Considering 15 access points, a door is forced at ECX5 about 0.05 times/year (***Occasional***)

# Consequence (data from TIS/RP)

**Major** (best case):

- dose exceeding lower limits for a Prohibited Radiation Area at CERN  
(Loss of  $\sim 10^8$  particles per pulse, typical at ECX5)
- temporary sterility to a man (0.15 Gy) at 1 m distance  
(Loss of  $\sim 10^{10}$  protons,  $1.5 \cdot 10^{-4}$  of a single full beam, typical at SPS ring)

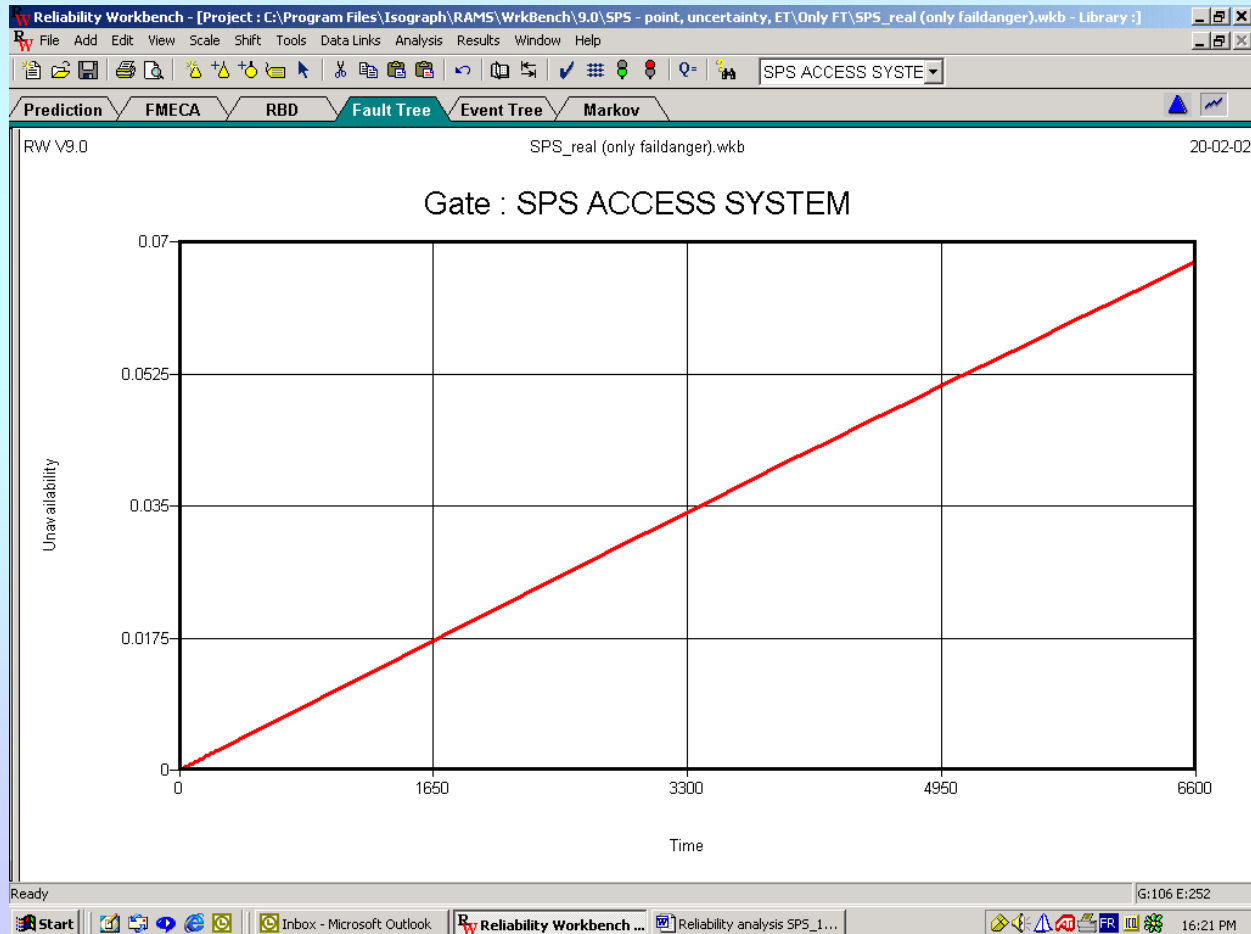


**Catastrophic** (worst case): death in a few hours or days ( $\geq 5$  Gy)

(Loss of  $\sim 2 \cdot 10^{12}$  protons for a man at 1 m, or loss of a single pulse ( $6 \cdot 10^{13}$  protons) in a 450 GeV/cycle beam, for a man at 5 m)

# Results of today's SPS safety system function

Availability: **93.26 %**



# Results of today's SPS safety system function

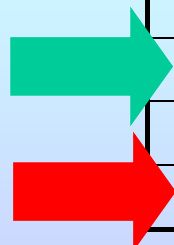
*(Low Demand mode of operation)*

*(IEC 61508 classification)*

Safety Integrity Level: **SIL 1**

Req. by  
IEC 61508

Current



SIL	Average probability of failure to perform its design function on demand (FPPD <sub>ave</sub> )
4	$10^{-5} < Pr < 10^{-4}$
3	$10^{-4} < Pr < 10^{-3}$
2	$10^{-3} < Pr < 10^{-2}$
1	$10^{-2} < Pr < 10^{-1}$

# Results of today's SPS safety system function

Risk Class: **II (Tolerable Risk)**

Frequency	Consequence			
	Catastrophic	Major	Severe	Minor
Frequent	<b>I</b>	<b>I</b>	<b>I</b>	<b>II</b>
Probable	<b>I</b>	<b>I</b>	<b>II</b>	<b>III</b>
Occasional	<b>I</b>	<b>II</b>	<b>III</b>	<b>III</b>
Remote	<b>II</b>	<b>II</b>	<b>III</b>	<b>IV</b>
Improbable	<b>II</b>	<b>III</b>	<b>IV</b>	<b>IV</b>
Negligible / Not Credible	<b>III</b>	<b>IV</b>	<b>IV</b>	<b>IV</b>

Aggregate risk for all SPS access points:  
Risk Class: **I (Intolerable Risk)**

# Confidence, Sensitivity and Importance analysis

- **Confidence analysis:**

- **Lognormal distribution (where possible)**
- **Upper Confidence limit: 99%**

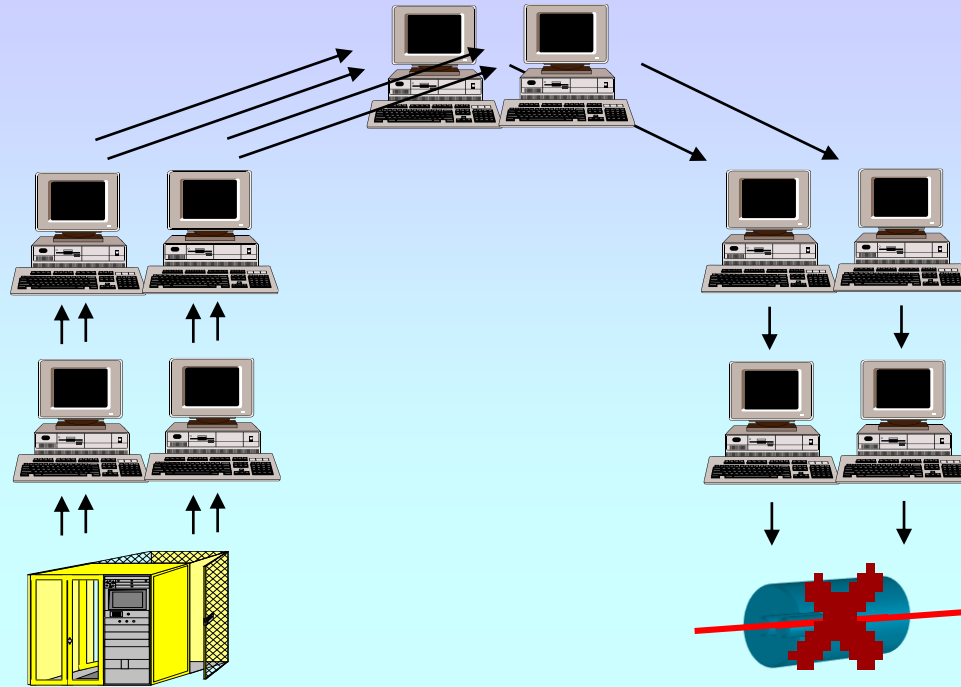
- **Sensitivity analysis:**

- **Components' unavailability should be  $\sim 1\%$  of actual  $Q$  to reach a SIL 3 without changing the architecture**
- **If components'  $Q$  is 50% higher,  $Q_{\text{tot}} > 0.1 \rightarrow$  out of SIL classification**

- **Importance analysis:**

- **Finds out "critical" components**
- **Optimizes changes' efficiency with respect to  $Q$**

# Improvement option 1: full redundancy



Availability: **99.52 %**

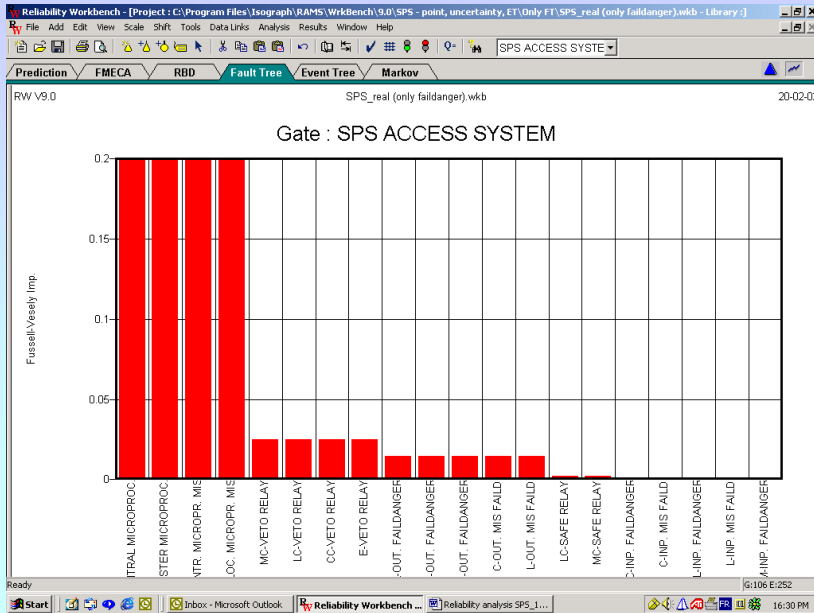


Safety Integrity Level **SIL 2**

Risk Class: **II (Tolerable Risk)**

**Better but ... expensive !!!**

# Improvement option 2: critical components



- 9 relays doubled
- All PLC CPUs checked
- Junction boxes checked
- PLC Output modules doubled
- Maintenance improved

Availability: **99.93 %**



Safety Integrity Level: **SIL 3**

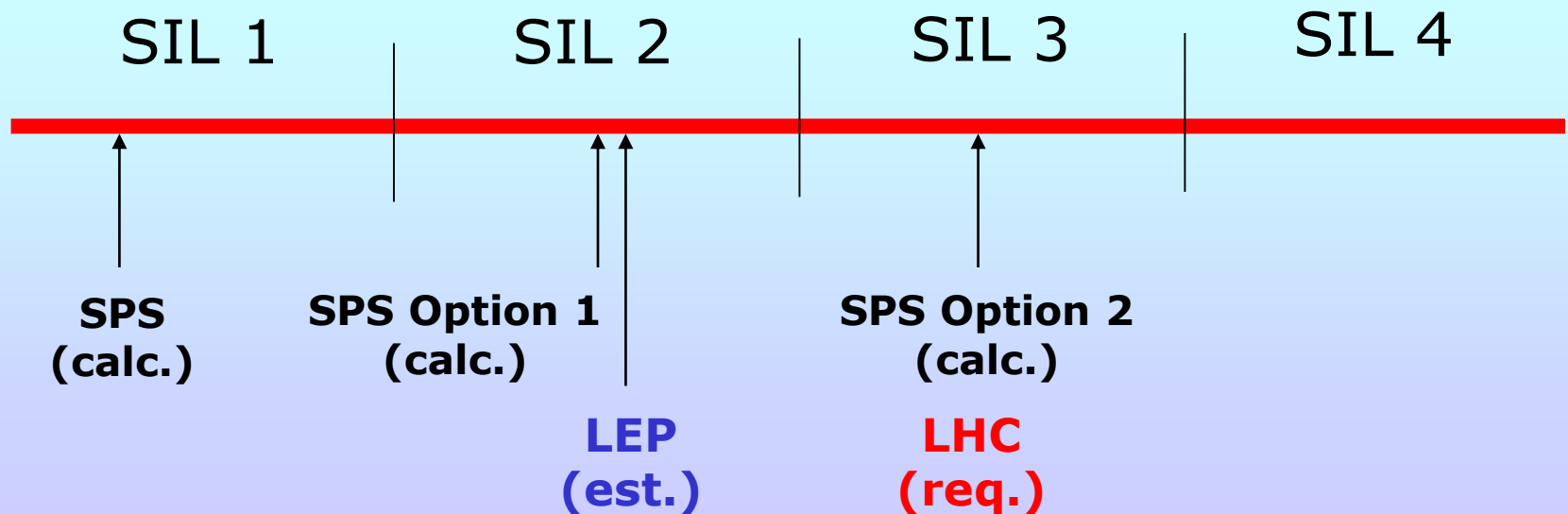
Risk Class: **III (Acceptable Risk)**

**Much better and ... cheaper !!!**



# Summary

	Availability	SIL	Risk Class
Today's SPS safety function	93.26 %	<b>SIL 1</b>	II (Tolerable)
Option 1 (full redundancy)	99.52 %	<b>SIL 2</b>	II (Tolerable)
Option 2 (critical components)	99.93 %	<b>SIL 3</b>	III (Acceptable)



# Conclusions



- Satisfactory quantitative results
- Good software performance
- Not satisfactory reliability parameters for the analyzed function **even if** the system is failsafe (according to IEC 61508 and ALARP)
- Importance analysis is crucial to optimize changes
- Do it **systematically** for each safety function
- Do it **systematically** for each LHC (sub)-system!
- **...feedback???**