SPS Access Safety System

Reliability assessment and Risk Analysis of one safety function

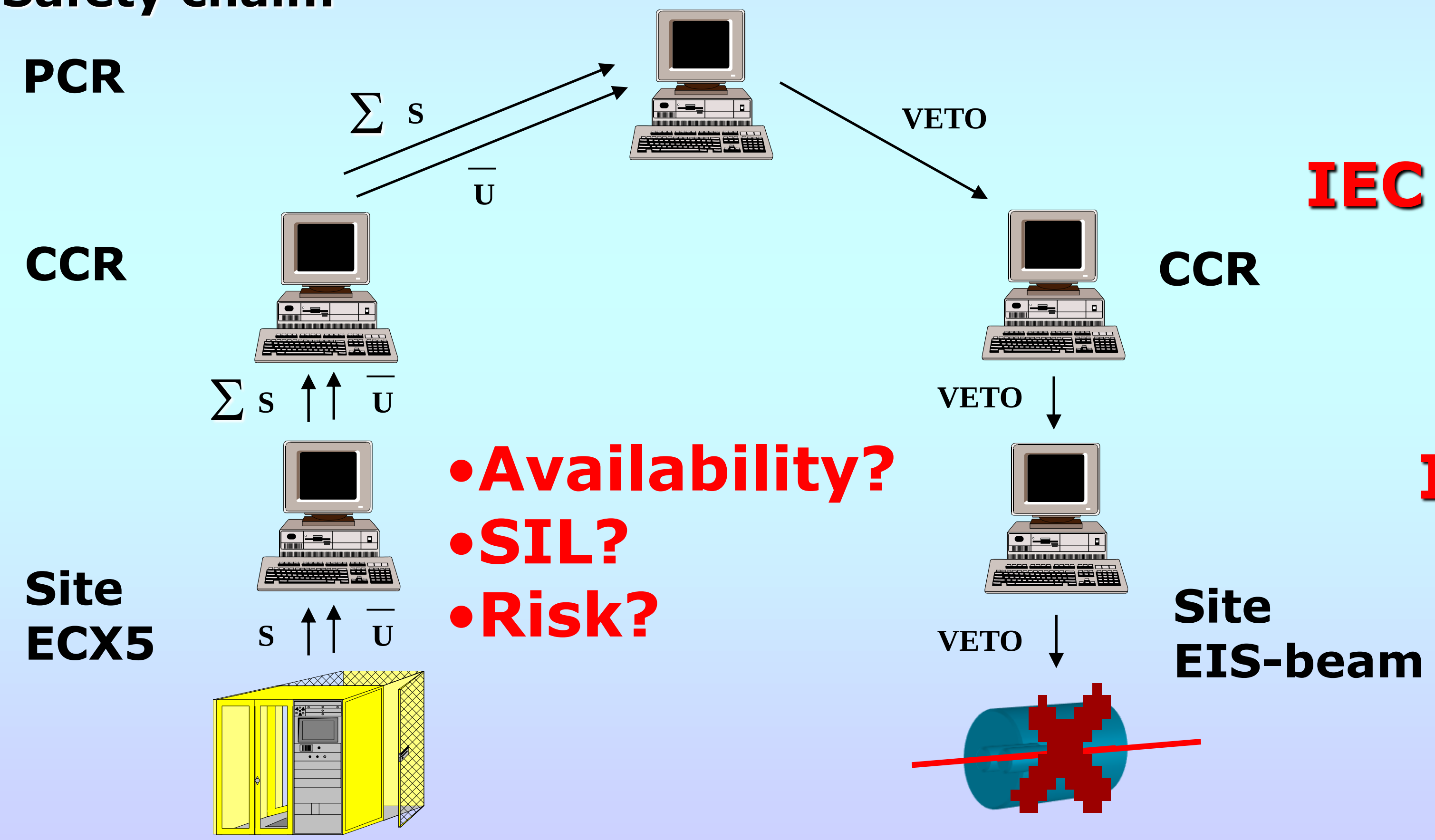
Fabrizio Balda (ST/MA)

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:



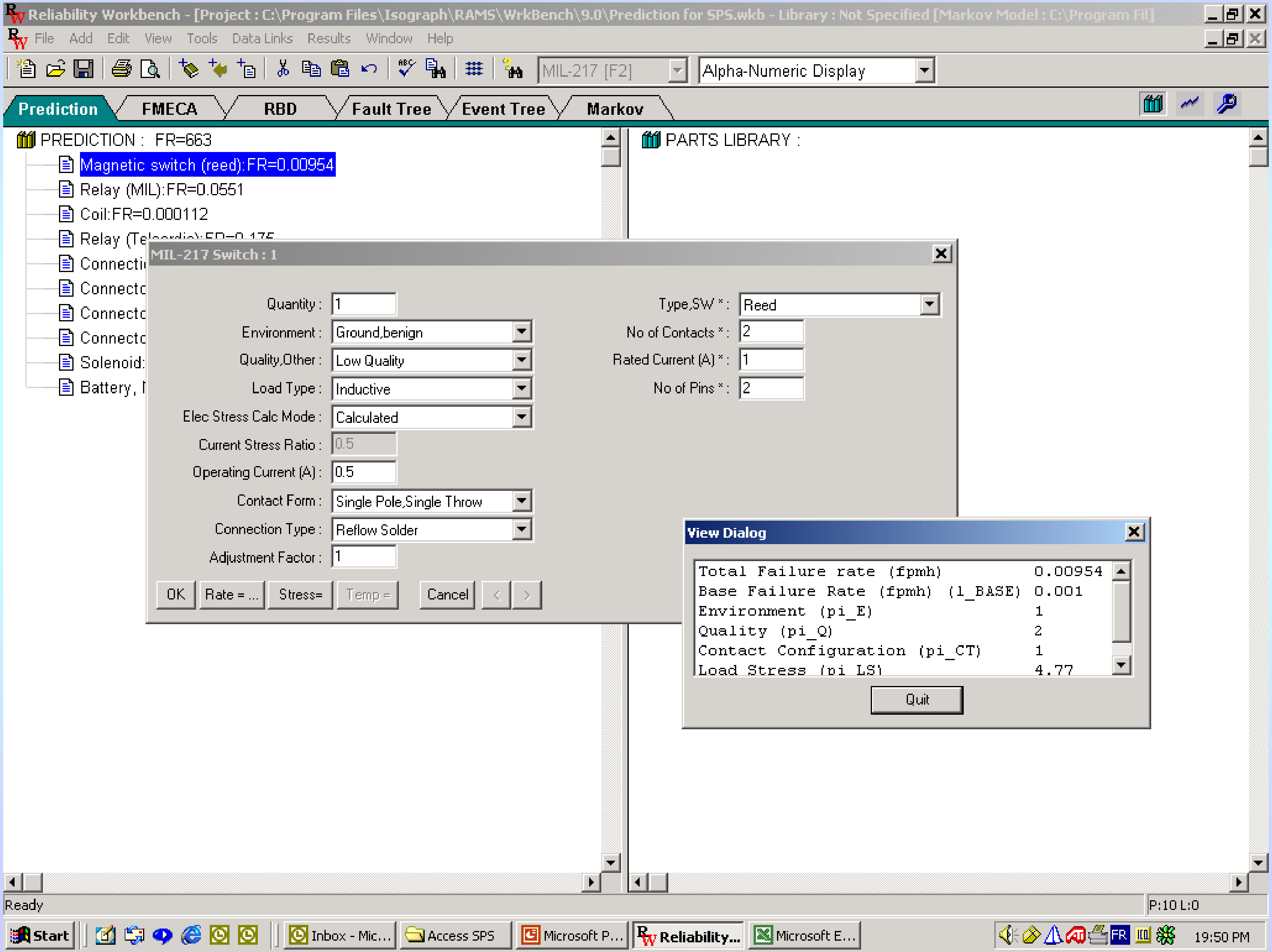
- **Availability?**
- **SIL?**
- **Risk?**

IEC 61508

&

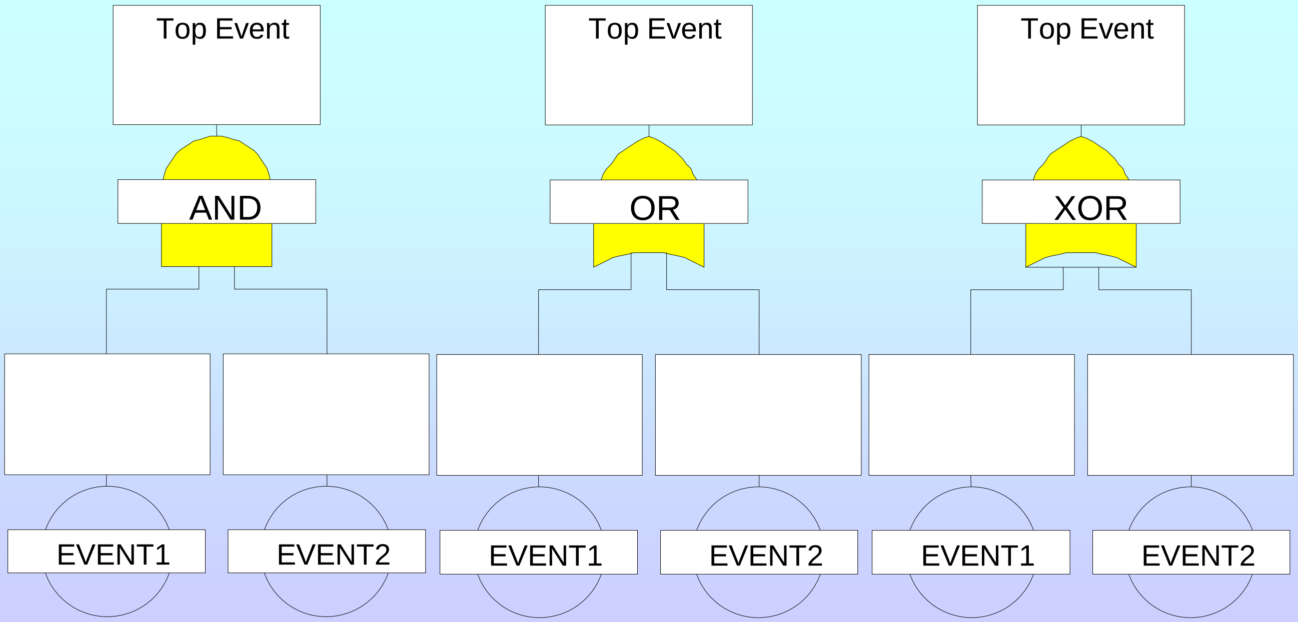
INB

Data collection

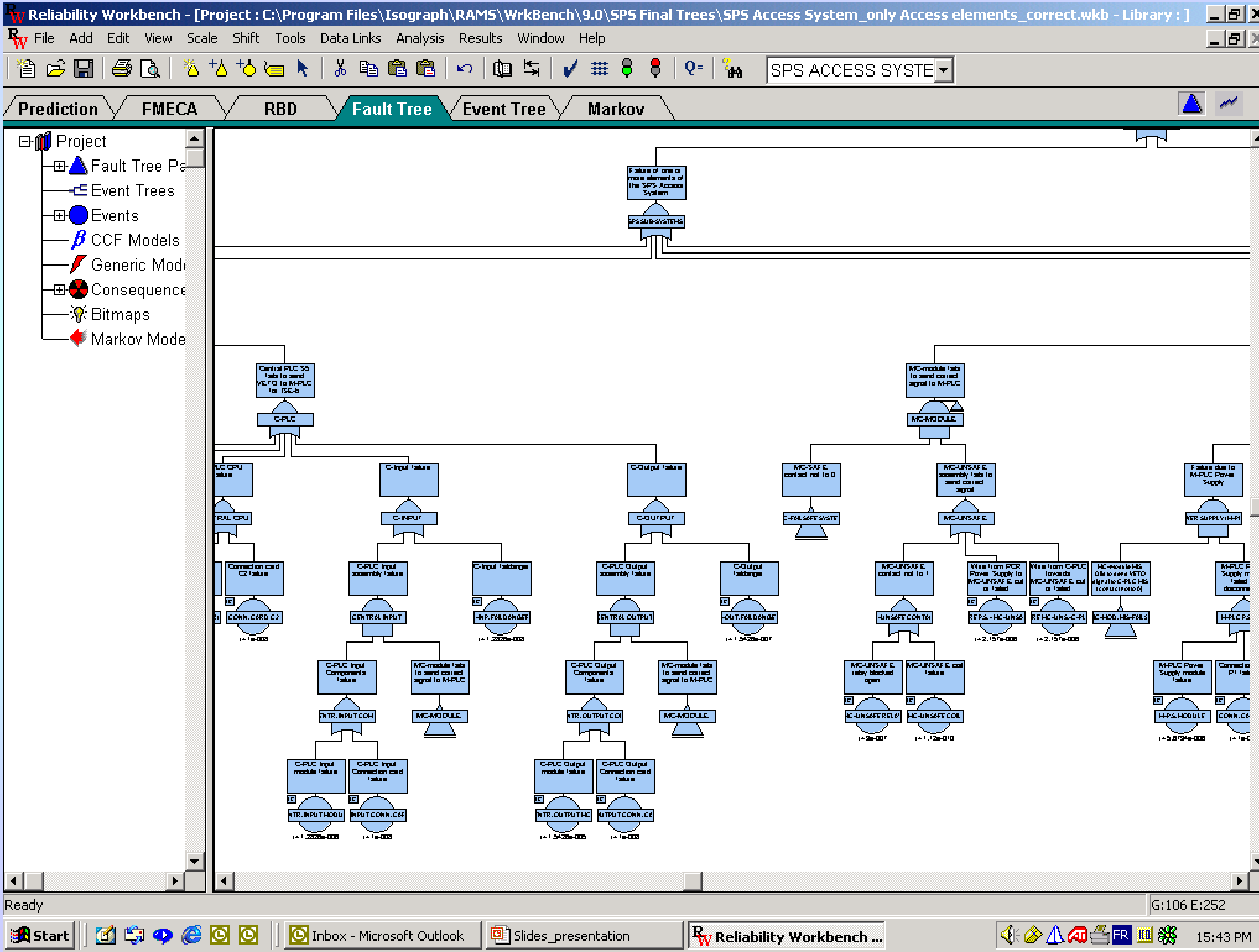


Fault Tree analysis

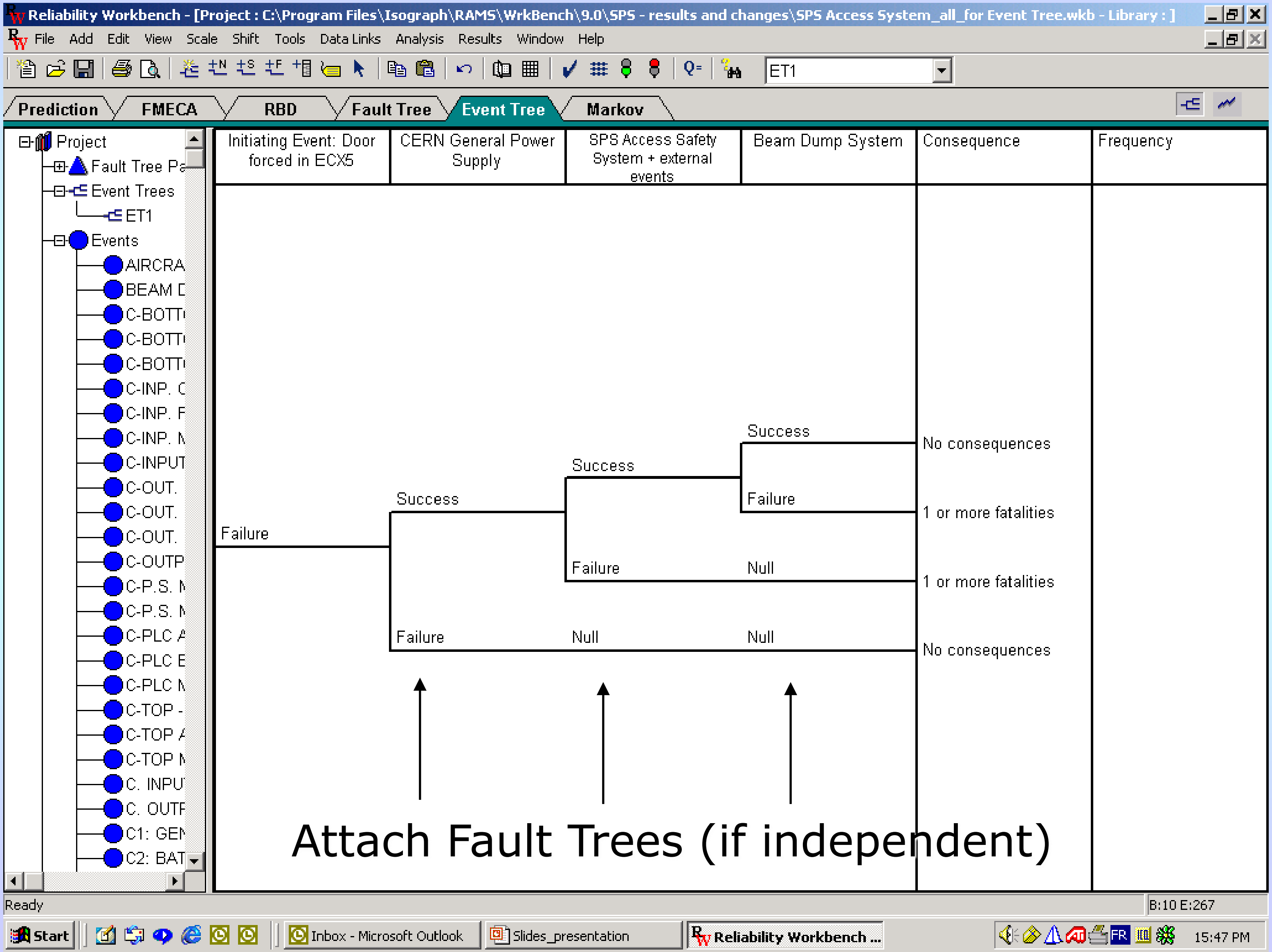
- **Top-down modeling of failure modes of components**
- **Boolean logic scheme (OR, AND, XOR, etc.)**
- **Failure, repair and inspection data**
- **Dependencies between sub-system**



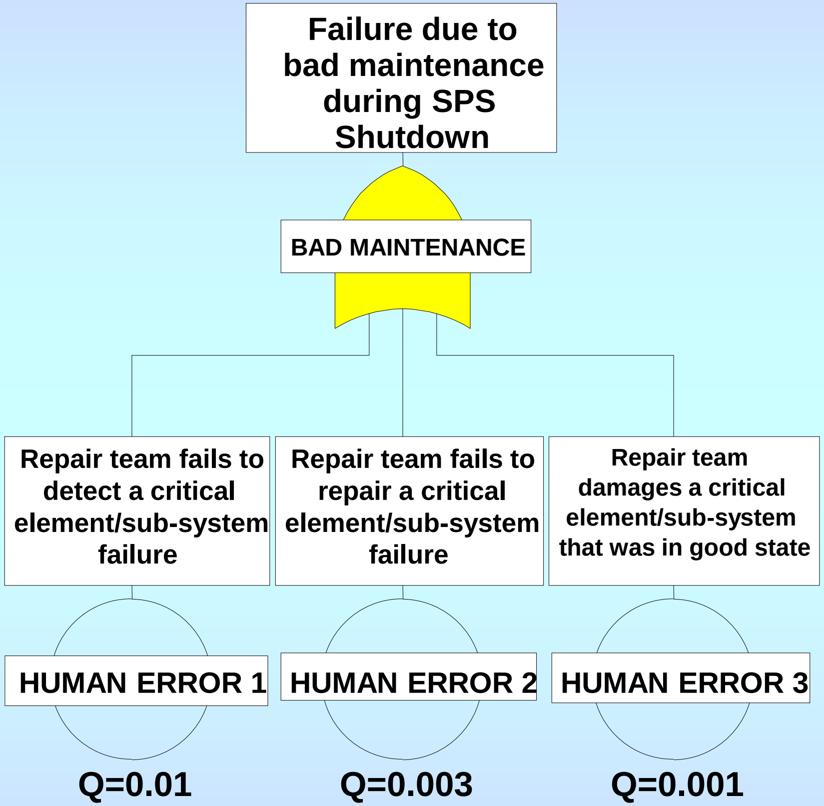
Fault Tree analysis



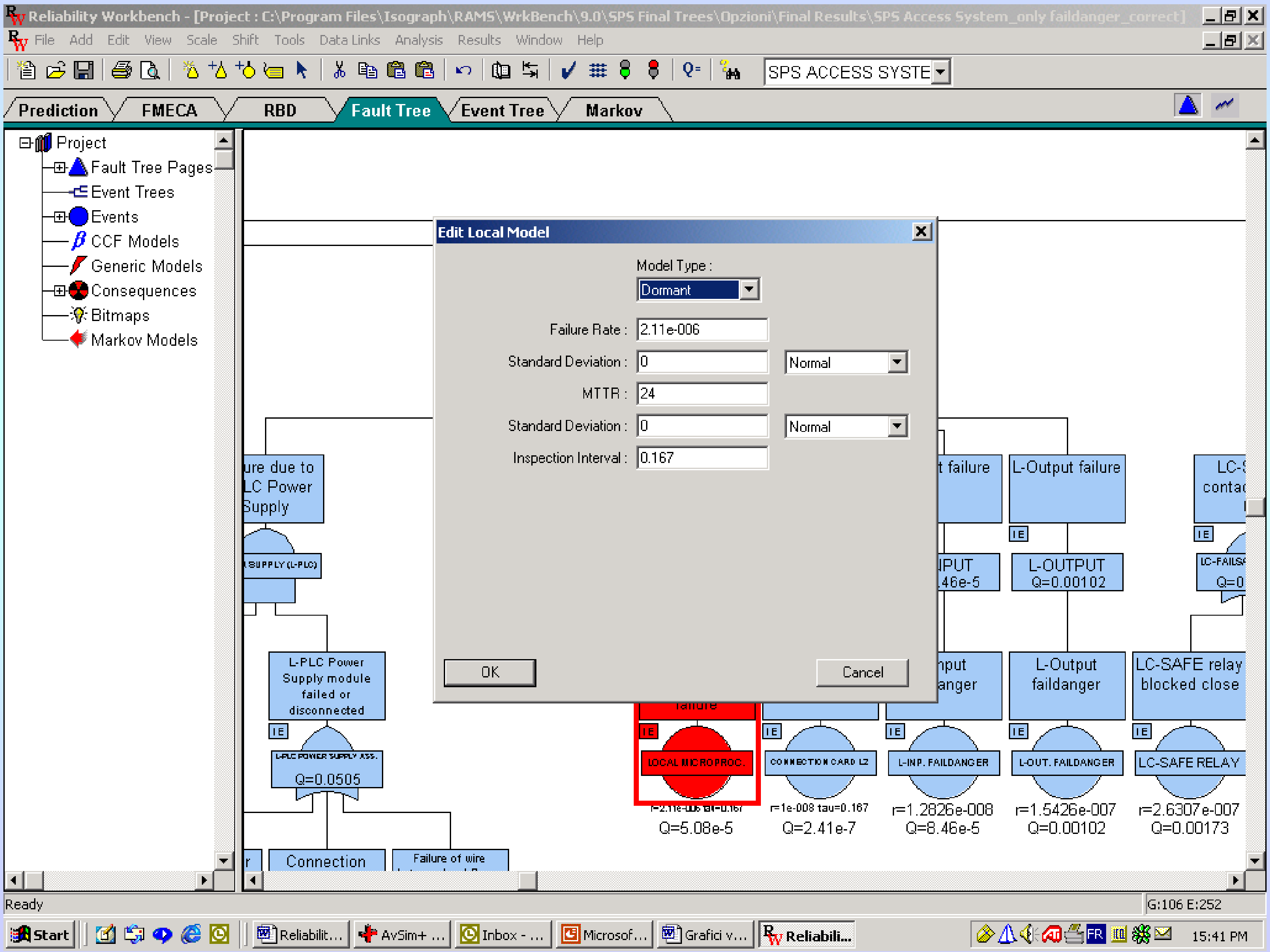
Event Tree analysis – Fault Tree Linking



Human error


Failure due to bad maintenance during SPS Shutdown
BAD MAINTENANCE
Repair team fails to detect a critical element/sub-system failure
Repair team fails to repair a critical element/sub-system failure
Repair team damages a critical element/sub-system that was in good state
HUMAN ERROR 1
HUMAN ERROR 2
HUMAN ERROR 3
Q=0.01
Q=0.003
Q=0.001

Maintenance and repair



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 ~10^8 particles per pulse, typical at ECX5)

- temporary sterility to a man (0.15 Gy) at 1 m distance

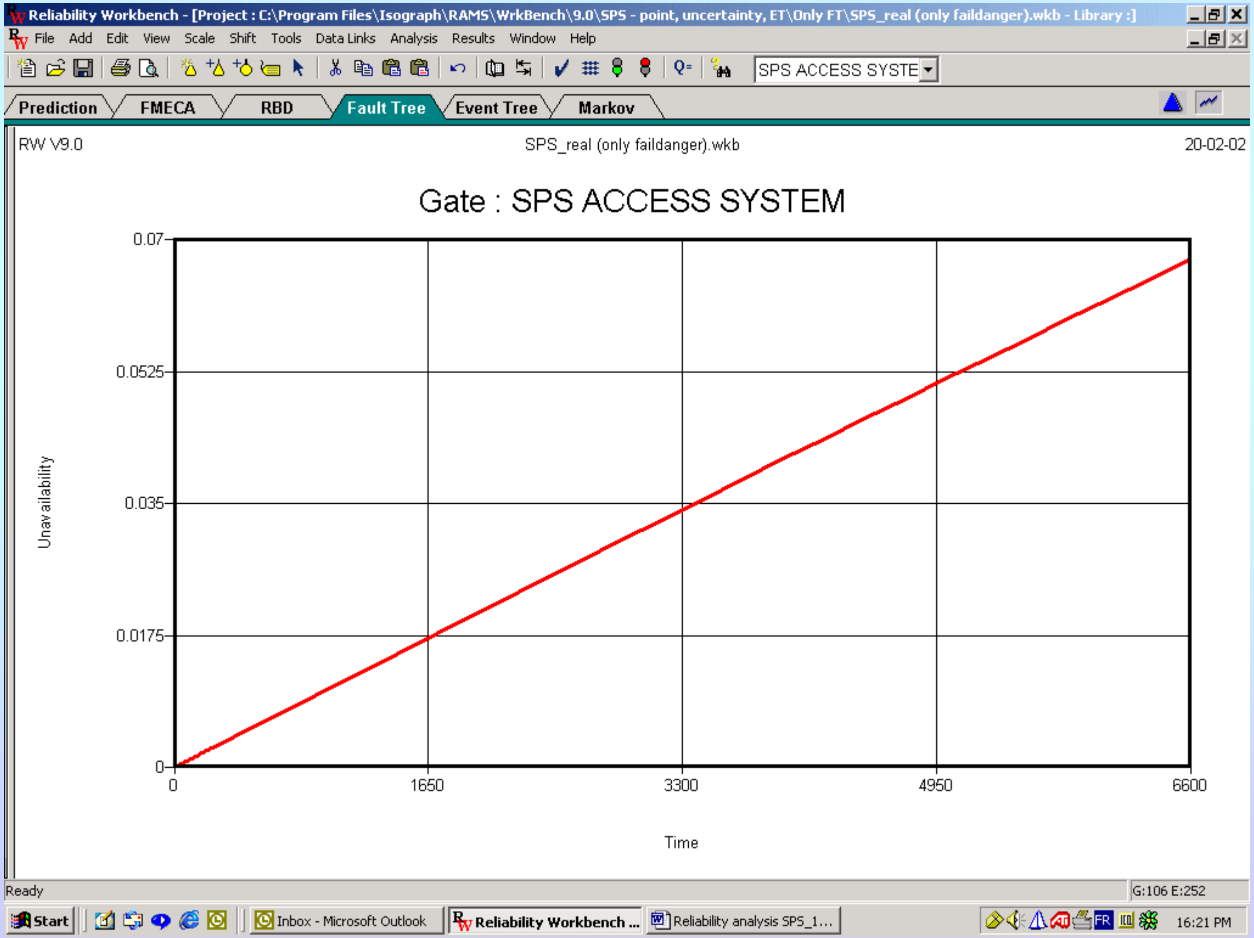
(Loss of ~10^{10} protons, $1.5*10^{-4}$ of a single full beam, typical at SPS ring)

Catastrophic (worst case): death in a few hours or days (≥5 Gy)

(Loss of ~$2*10^{12}$ protons for a man at 1 m, or
loss of a single pulse ($6*10^{13}$ 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 → 3

Current → 1

SIL	Average probability of failure to perform its design function on demand ($FPPD_{ave}$)
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)**

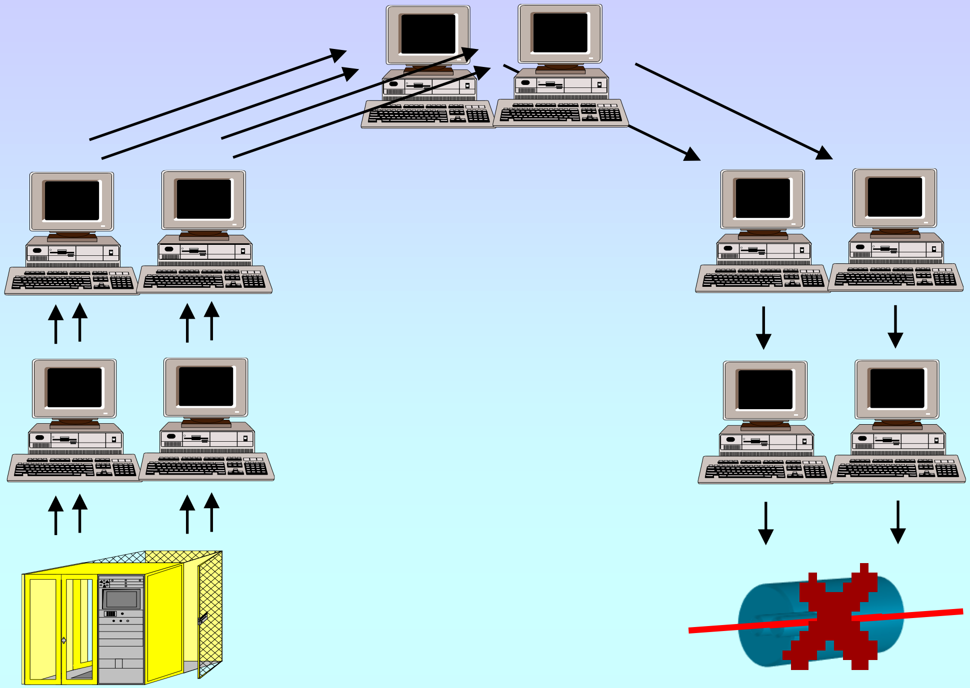
Frequency	**Consequence**			
	Catastrophic	Major	Severe	Minor
Frequent	**I**	**I**	**I**	**II**
Probable	**I**	**I**	**II**	**III**
Occasional	**I**	**II**	**III**	**III**
Remote	**II**	**II**	**III**	**IV**
Improbable	**II**	**III**	**IV**	**IV**
Negligible / Not Credible	**III**	**IV**	**IV**	**IV**

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 ~1% of actual Q to reach a SIL 3 without changing the architecture**
  - **If components' Q is 50% higher, $Q_{tot} > 0.1$ → out of SIL classification**
- **Importance analysis:**
  - **Finds out "critical" components**
  - **Optimizes changes' efficiency with respect to Q**

Improvement option 1: full redundancy



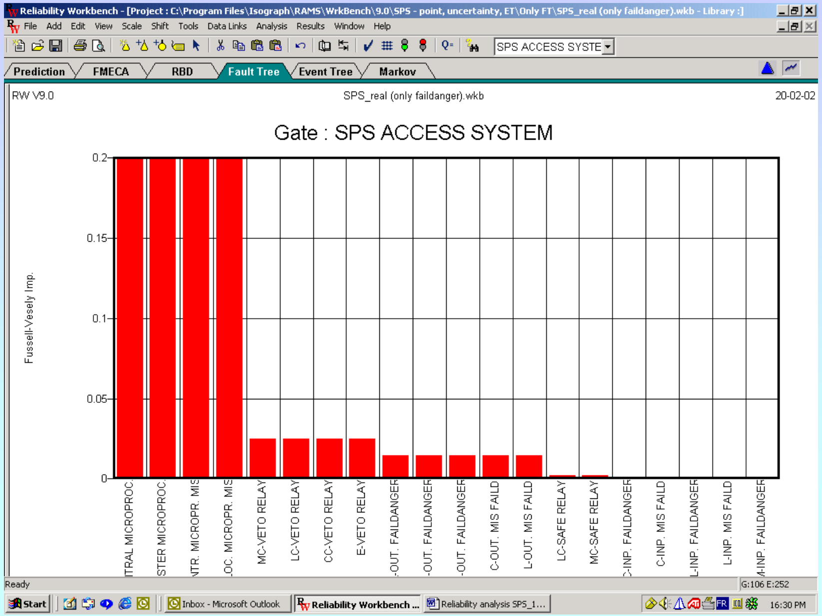
Availability: **99.52 %**

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 %**

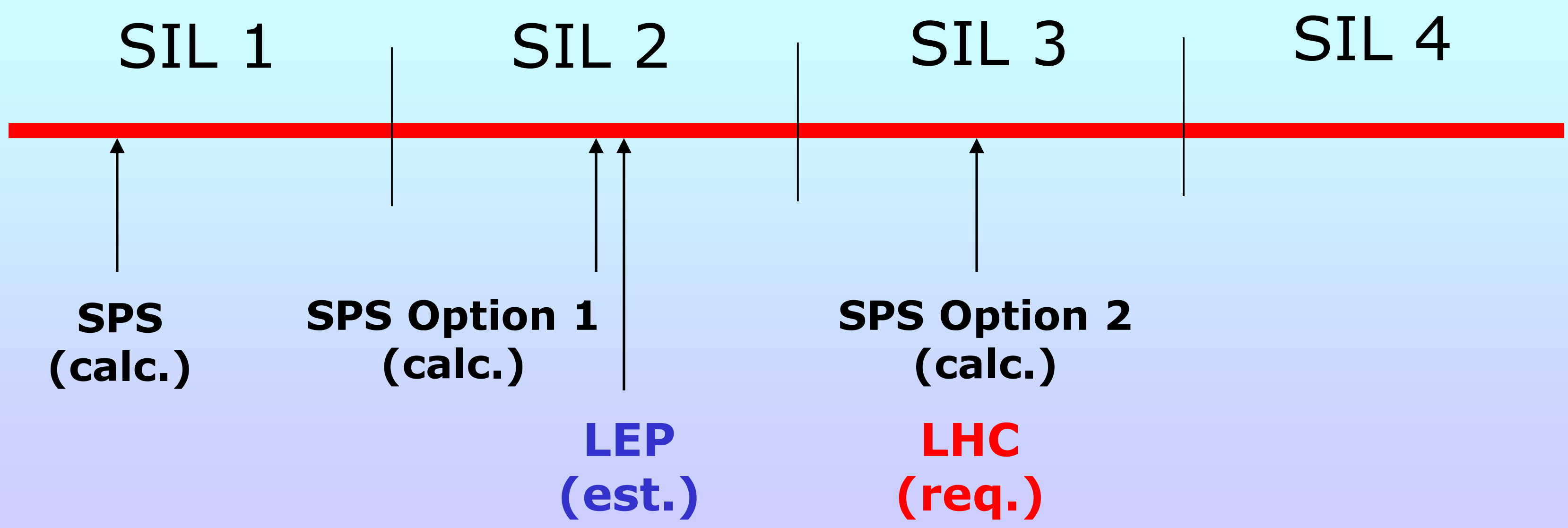
Safety Integrity Level: **SIL 3**

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

Much better and … cheaper !!!

Summary

	Availability	SIL	Risk Class
Today's SPS safety function	93.26 %	**SIL 1**	II (Tolerable)
Option 1 (full redundancy)	99.52 %	**SIL 2**	II (Tolerable)
Option 2 (critical components)	99.93 %	**SIL 3**	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???**