# Report of the Reliability Sub-Working Group


Roberto Filippini on behalf of the RSWG

*AB-BT*


*Machine Protection Working Group Meeting*

*CERN, 28 October 2005*

# Topics of the Presentation

- **The mandate**
- **The studies**
- **The results**
- **The conclusions**
- **Future**

***RSWG MEMBERS LIST***

- *Jan Uythoven - AB/BT (joint Chair)*
- *Roberto Filippini - AB/BT (joint Chair)*
- *Brennan Goddard - AB/BT*
- *Bernd Dehning - AB/BDI*
- *Gianluca Guaglio - AB/BDI*
- *Ruediger Schmidt - AB/CO*
- *Bruno Puccio - AB/CO*
- *Markus Zerlauth - AB/CO*
- *Benjamin Todd - AB/CO (Scientific Secretary)*
- *Silvia Grau - TS/CSE*
- *Felix Rodriguez Mateos - TS/HDO*
- *Antonio Vergara Fernandez - TS/IC*
- *Angela Czizsek - SC/IE*

# The Mandate

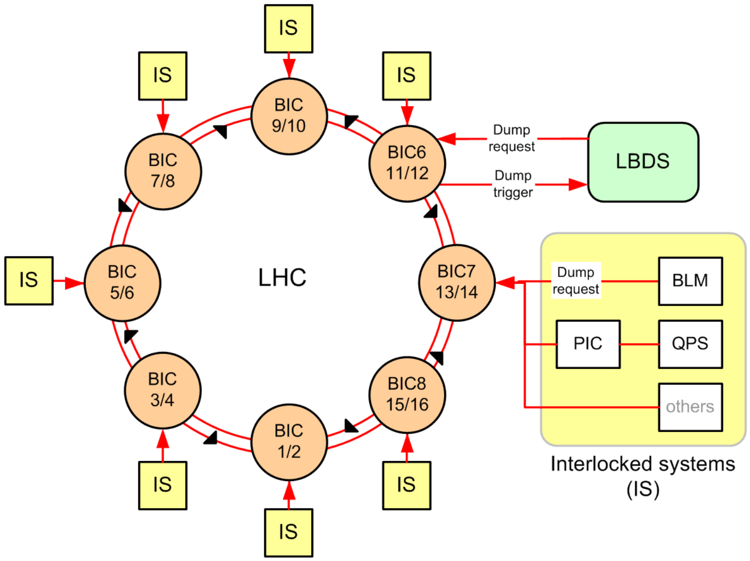
## $2^{nd}$ RSWG meeting, 22/3/2004

- The group mandate is resumed in four points:
  - Analyze the **dependability** (safety, availability) of the LHC Machine Protection System.
  - Identify possible "**weakest links**".
  - Validate the **SIL3 level** required for safety of the present MPS architecture.
  - Study the **impact on dependability** of continuous surveillance, diagnostics, post-mortem activities and maintenance.

- Actions followed:
  - Agree on a **simplified core-architecture** of the MPS.
  - Agree on a **methodology** to be used for comprehensive reliability prediction, failure modes analysis and dependability modeling.

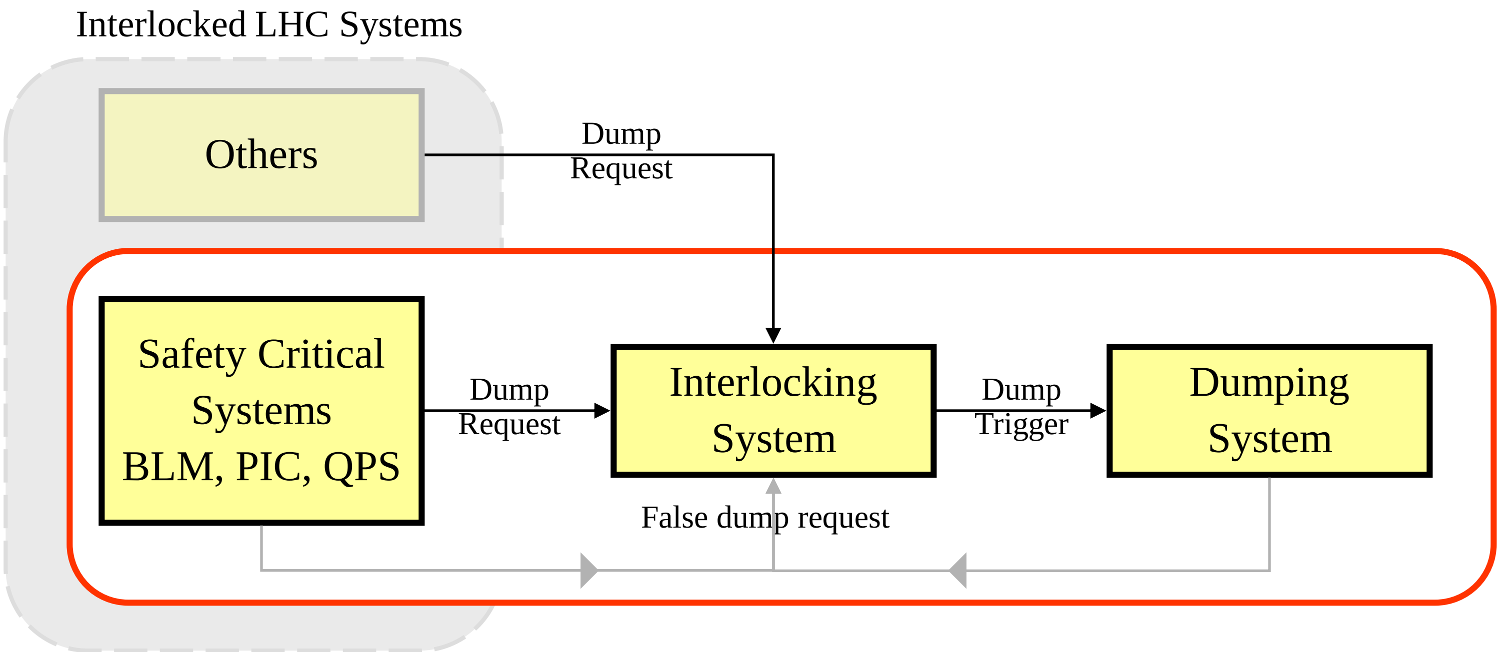
# The MPS Core Architecture

- The **core architecture** includes those systems that are at the basis of the machine protection.
  - Beam Loss Monitors System (3500),
  - Quench Protection System (4000),
  - Power Interlocking Controller (36),
  - Beam Interlocking Controller (16) and the
  - Beam Dumping System (2)




- **Internal status surveillance** is also included. It detects failures in each system and issues failsafe operation aborts, called **false dumps**.

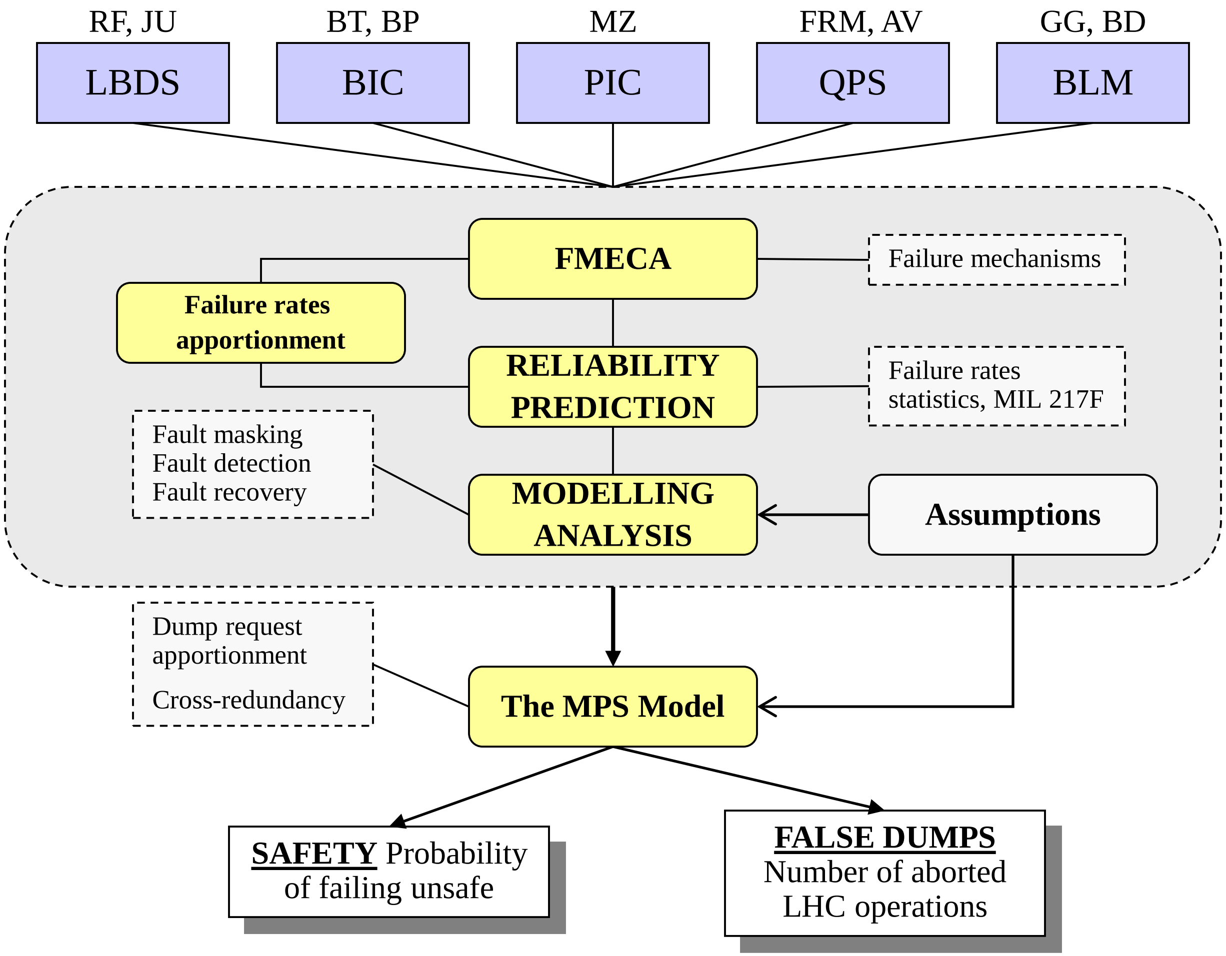
# The MPS Core Architecture




- The MPS includes the **safety critical systems** of the LHC
- Also other systems send their interlock to the interlocking system
- Internal **surveillance** also sends signals to the interlocking system (false dumps)

# The Studies Framework

## Overview



# Modeling Aspects

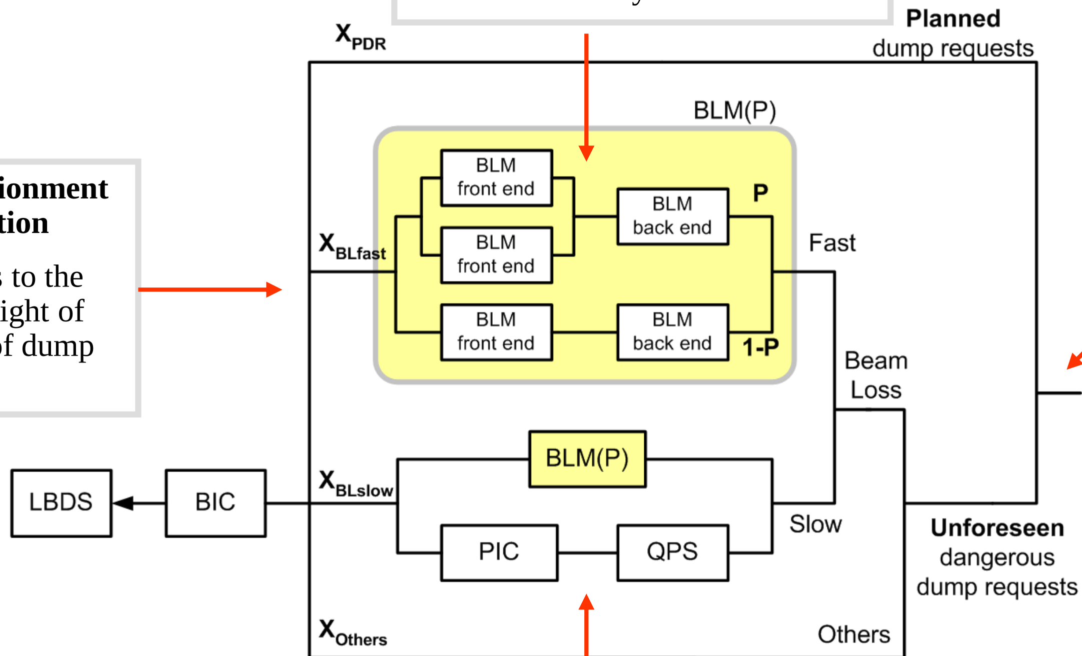
## The MPS Model

**BLM cross-redundancy**

P [0,1] is the probability the beam loss is detected by both monitors

**Dump request apportionment for safety calculation**

Each branch contributes to the total unsafety by the weight of the respective fraction of dump request **X**




| **SOURCES** |
|---|
| User/operator |
| PC failures |
| Magnet failures |
| Collimators failures |
| RF failures |
| Obstacles |
| Vacuum |
| … |

**BLM-QPS cross-redundancy**

For slow beam losses, BLM and QPS detect the same event

# The Results

## Summary Table For a Default Case Study

- **Operational scenario**
  - 200 days/year of operations, 400 beam operations (10h each) followed by checks (2h each)
- **Diagnostics effectiveness**
  - LBDS and BIC "as good as new" after checks (BLM, partially)
  - QPS and PIC "as good as new" after periodic inspection or power abort
- **Example of DR apportionment**
  - 60% planned dumps
  - 15% fast beam losses
  - 15% slow beam losses
  - 10% others
- **Cross-Redundancy**
  - No cross-redundancy within the Beam Loss Monitors (P = 0, worst-case)
  - Yes cross-redundancy between BLM, QPS and PIC

| **System** | **Unsafety per year** | **False dumps/y Average** | **Std.D.** |
|---|---|---|---|
| LBDS[RF](1) | $1.8\times10^{-7}$(2x) | 3.8(2x) | +/-1.9 |
| BIC [BT](2) | $1.4\times10^{-8}$ | 0.5 | +/-0.5 |
| BLM [GG] | $1.44\times10^{-3}$ (Front-end)<br>$0.06\times10^{-3}$ (Back-end VME) | 17 | +/-4.0 |
| PIC [MZ] | $0.5\times10^{-3}$ | 1.5 | +/-1.2 |
| QPS[AV] | $0.4\times10^{-3}$ | 15.8 | +/-3.9 |
| **MPS** | **$2.3\times10^{-4}$**<br>**$5.75\times10^{-8}$/h is SIL3** | **41**(3) | **+/-6.0** |

**(1)** The **LBDS false dumps are updated** to 7.6 per year in total for the contribution of the Beam Energy Tracking system, calculated in 0.8/year (D.Huw Jones, summer student).

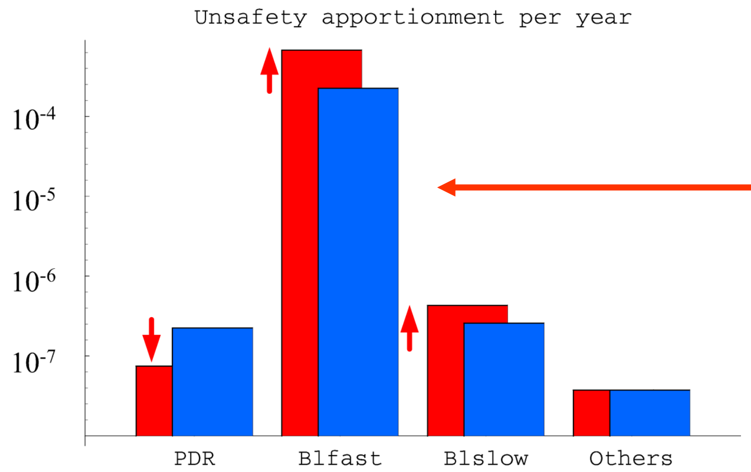
**(2)** A **simplified BIC** was studied, further analysis is needed.

**(3)** False dumps do not exactly sum up as they are concurrent events.

# The Results

## Sensitivity to Dump Request Apportionment

| X | (blue) | (red) |
|---|---|---|
| **PDR** | **60%** | **20%** |
| **BL fast** | **15%** | **45%** |
| **BL slow** | **15%** | **25%** |
| **Others** | **10%** | **10%** |
| | | |
| **UNSAFETY per year** | **$2.3\times10^{-4}$** **$5.8\times10^{-8}$/h** | **$6.8\times10^{-4}$** **$1.7\times10^{-7}$/h** |




**Protection to fast beam losses** takes the largest contribution to Unsafety

For certain dump requests apportionment and no cross redundancy within BL monitors, the MPS might not be SIL3

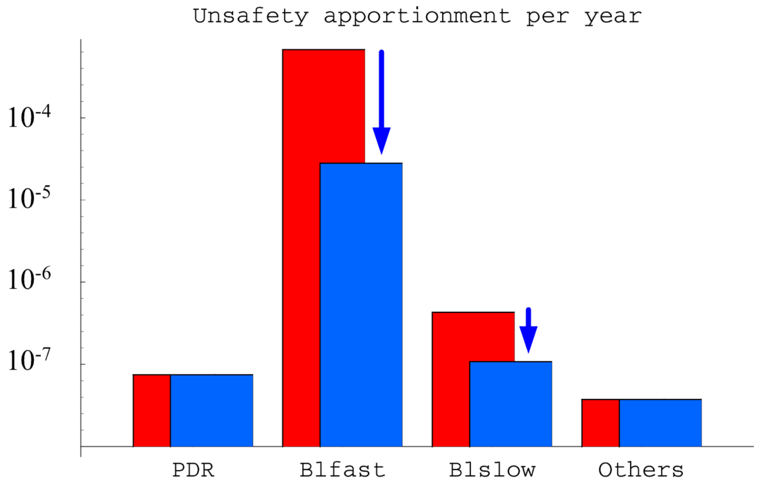
In this case, the system is **SIL2**!

Dump requests apportionment affects unsafety, not the false dumps

# The Results

## Sensitivity to BLM Cross-redundancy

- **The parameter P** stands for the probability a beam loss is detected with two monitors (connected to the same VME electronics). If we vary P then unsafety will change. Nothing happens for the false dumps.




**Unsafety = $6.8\times10^{-4}$ /y**

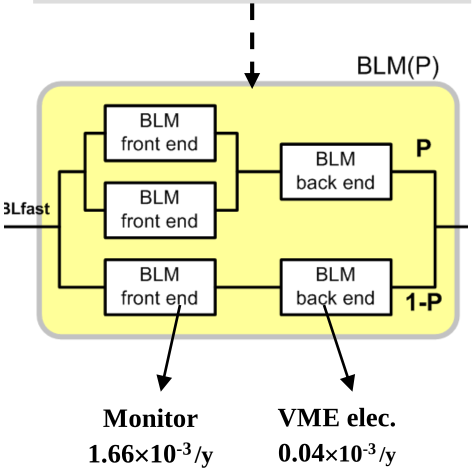
**$1.7\times10^{-7}$/h** is **SIL2**

**Unsafety = $2.8\times10^{-5}$ /y**

**$7.0\times10^{-9}$/h** is **SIL4**

**BLM cross-redundancy**

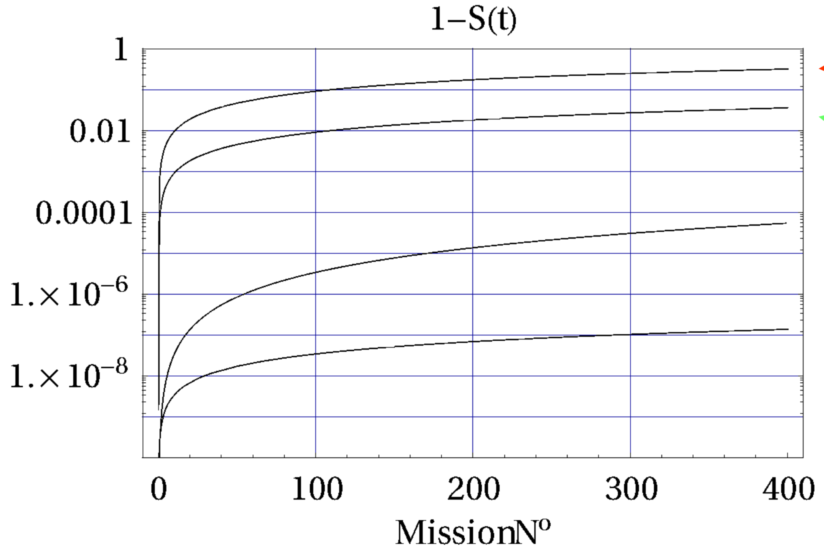
P [0,1] is the probability the beam loss affected both monitors




**NOTE**: The **BLUE** bar is for **P = 1**, while the **RED** bar is for **P = 0**
The dump request apportionment is (20,45,25,10)%

# The Results

## Sensitivity to Surveillance and Diagnostics for the LBDS MKD system

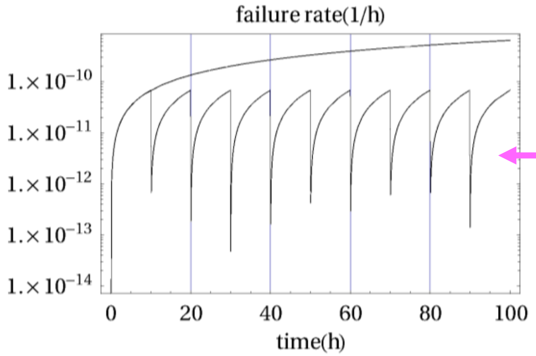



**No erratic trigger surveillance**
Unsafety is 0.32/y

**No beam energy tracking surveillance**
Unsafety is 0.031/y

**No post mortem diagnostics**
Unsafety is 5 $10^{-5}$/y

**Default case study**
Unsafety is 1.4 $10^{-7}$/y,
That is 3.5 $10^{-11}$/h.




Thanks to post mortem diagnostics, the system is always recovered to **full redundancy.**
This implies that the system failure rate turns to be the same at every new machine fill.

# Conclusions

## MPS Safety and Availability

- **SAFETY**
  - **Calculations were based on** a simplified MPS.
  - The results depend on the apportionment of dump requests, cross redundancy and the effectiveness of surveillance and post mortem diagnostics.
  - Those parameters are unknown before the start-up of the LHC. Depending on these parameters, **safety can vary between SIL2 and SIL4**.

- **FALSE DUMPS**
  - **Calculations were based on** 3500 BLMs, 4000 channels for QPS, 36 PIC, 16 BIC and 2 LBDS.
  - **The number of expected false dumps per year is 41 [+/-6] (on average), which is about 10%** of all fills.
  - Results are independent from dump requests apportionment and cross-redundancy.

  - The different systems within the MPS seem to be well balanced from a dependability point of view.

# Conclusions
## Some Remarks

- **Unsafety and unavailability are probably overestimated** due to the conservative nature of the reliability prediction methods.
  - Unavailability is more sensitive to reliability prediction accuracy than unsafety. If failure rates are taken one order magnitude smaller, the false dumps would pass from 40 to only 4 per year.
- **Fast beam losses are the main concern for safety**.
  - Only beam loss monitors can cover them.
- **The rearming procedure,** presently assumed never failing**, might affect safety.**
- **Other systems**, presently not included, **add coverage for many dump requests**, with an expected safety improvement.
  - They are the Beam Current Decay Monitors, the Beam Position Monitors, the Fast Magnet Current Change Monitors of the magnet PC, etc…
- **Power supplies in the electronics (VME crates, etc.)** cause the largest fraction of false dumps.
- **False dumps are also generated by systems outside the MPS** like the magnet PC.
- **Downtime due to repairs and lack of spares** can further reduce the system availability.

# Future

## What to Do Next?

- The **group's mandate has been accomplished** for a simplified though realistic MPS architecture.

- **To fruitfully continue with the group it is necessary to:**
  - Redefine the direction of further studies and the coordination (new mandate).
  - Find the people to carry out these studies (end of contract RF).

- A list of some **possible topics to be investigated** …
  - Build a more complete model for the MPS especially for the BIC system.
  - Look at reliability of arming and post mortem procedures.
  - Split the mission into phases (filling, ramping, etc.) and ranking the failure of the MPS with respect to the phase criticality.
  - ?…

# The Results

## Formulas for Safety and False Dumps

- **SAFETY**: The system is safe if **the demanded systems are safe.**
  - **One mission**

$$S = S_{LBDS} S_{BIC} \{ X_{PDR} + X_{Others} + X_{BLfast} S_{BLM}(P) + X_{BLslow} [1 - (1 - S_{BLM}(P))(1 - S_{PIC} S_{QPS})] \}$$

$$S_{BLM}(P) = [ P S_{BLM2} (2 S_{BLM1} - S_{BLM1}^2) + (1-P) S_{BLM1} S_{BLM2} ]$$

  - **N mission**

$$S(N) = S^N$$

- **FALSE DUMPS**: The system has generated a false dump if **at least one system has generated an internal dump request**
  - **One mission**

$$P_{FD} \cong 2 \times P_{LBDS} + 16 \times P_{BIC} + 36 \times P_{PIC} + 3500 P_{BLM} + 4000 P_{QPS}$$

  - **Distribution**

$$\binom{N}{n} P_{FD}^{n} (1 - P_{FD})^{N-n}; \begin{cases} Average = N \times P_{FD} \\ Std.dev. = \sqrt{N P_{FD} (1 - P_{FD})} \end{cases}$$