Machine Protection and Controls

Mike Lamont
AB-OP

12th April 2005

© KURT JONES 2003

Controls

- Control system performs some or all of the following functions:
  - Monitoring, recording and logging of accelerator status and process parameters;
  - Provision of operator information regarding the accelerator status and parameters;
  - Provision of operator controls to affect changes to the accelerator;
  - Automatic process control and sequence control during start-up, normal operation, shutdown, and disturbance. i.e. control within normal operating limits;
  - Prevention of automatic or manual control actions which might initiate a hazard.

  - Detection of onset of hazard and automatic hazard termination (i.e. dump the beam), or mitigation (i.e. control within safe operating limits)

It should be noted that control systems for equipment under control which are not safety related as defined above may also contribute to safety and should be properly designed, operated and maintained.

Where their failure can raise the demand rate on the safety related system, and hence increase the overall probability of failure of the safety related system to perform its safety function, then the failure rates and failure modes of the non-safety systems should have been considered in the design, and they should be independent and separate from the safety related system.

Thus

- **We don't rely on the control system for machine protection**
  - **networks, front-ends, software, databases, timing system etc.**

- **Deterministic PLC, or custom made component, based safety system separated from accelerator control**

However…

A lightning strike on 24 July 1994 contributed to causing a gigantic explosion that rocked the Texaco oil refinery in Milford Haven. The explosion was followed by a fierce blaze, with flames soaring 100 ft into the air.

However the direct cause of the explosion that occurred some five hours later was a combination of failures in management, equipment and control systems during the plant upset

The Explosion and Fires at the Texaco Refinery, Milford Haven. 24th July 1994

Failures in Technical Measures

- A control valve being shut when the control system indicated it was open. Inadequate maintenance of plant and instrumentation.
  - Control Systems: actuator/valve, sensors
  - Maintenance Procedures: maintenance systems
- Modification of the plant which had been carried out without an assessment of the potential consequences.
  - Plant Modification / Change Procedures: HAZOP
- Control panel graphics did not provide necessary process overviews. Excessive number of alarms in emergency situation reduced effectiveness of operator response.
  - Control Room Design: plant layout, human factors/ergonomic issues
- Attempts to keep the unit running when it should have been shut down.
  - Emergency Response / Spill Control: emergency operating procedures/training

CS in general - help

- Reduce the load on machine protection
  - catch errors, enforce procedures
  - catch problems – surveillance, software interlocks
  - impose limits, secure settings
- Diagnostics
  - Post-mortem, logging, alarms
- Monitoring
  - Status of MPS, critical components
- Ensure reliability
  - XPOC
  - Checks: test sequences
  - Standards
- Simulations
  - Tests of acquisition system, system response etc.

CS in general - hinder

- Availability
- Reliability
  - Loss of diagnostics
- Failures
  - gateways, networks (band width, response), servers, databases, timing
- Source of false manipulations
  - bugs
  - poor ergonomics
  - mis-conceived sequencing
  - run away feedback loops
- Personality clashes

Injection Kickers

- The injection kicker control system is fully integrated in the LHC controls infrastructure following the standard controls framework. Integration of the different control entities described above is based on dedicated equipment servers implementing the required functionalities through standard communication, contracts and low-level threads.

- Operational settings management like kick delay, kick length and kick strength is performed at the application layer through accelerator wide standard application programs.

- Equipment settings management, such as fine timing delay or interlock thresholds are managed by the equipment experts.

- The injection kickers are linked to the machine post-mortem system for correlation of injection related data with other accelerator processes in case of faults. Typical signals acquired are the magnet current pulse shape, the currents of the injected and circulating beams, and the beam permit and beam abort gap signals.

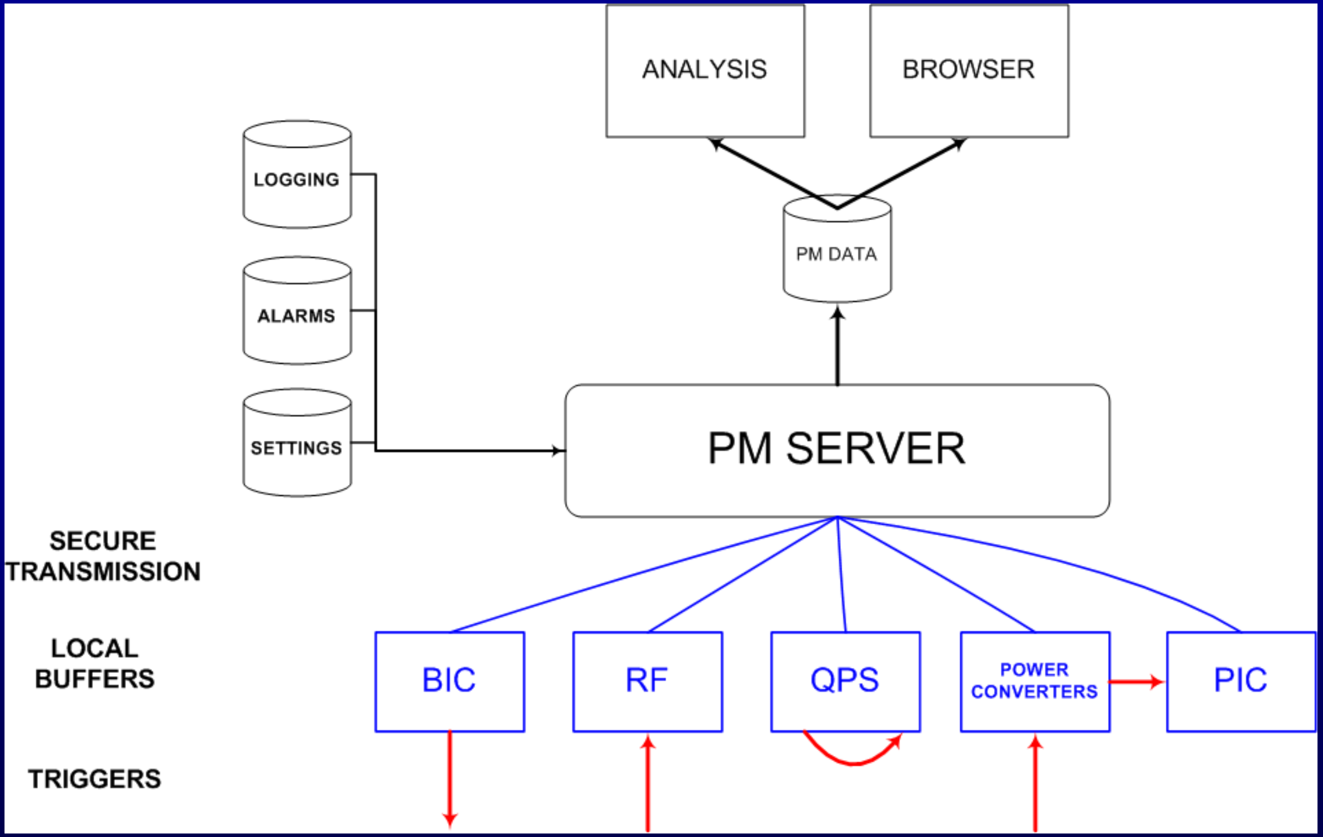
- Triggering of the post-mortem system will be based on the opening of the beam permit loop. The same signals are also acquired and analysed on a shot-by-shot basis at each injection to continuously monitor the injection kickers with the objective to detect any degradation of their performance.

Post Mortem

- Vital to establish:
  - cause of failure
  - proper functioning of system specific response
    - E.g. QPS
  - proper functioning of machine protection response
- Whole swath of requirements but what must be guaranteed from a protection standpoint is the generation and capture of the data:
  - triggers:
    - slow timing event, generation & transmission
    - fast timing
    - self-triggering
  - capture
    - front-ends, networks, servers
  - timing
  - get it out of the front-ends
    - some reasonably secure transfer protocol
    - exception handling
    - back-up plan

Post Mortem

- Standard, global system foreseen for the LHC
- Stability, reliability, error recovery, clearly required
  - Controls failures & the ability to capture PM data…
  - Utility failure & the ability to capture PM data…



Needed for HWC, prototyping in progress

Post Operation Checks

- Mandatory Beam Dump XPOC
  - Checks that LBDS is OK, to enable beam permit (CO responsibility)
  - Impact position and shape of the beam on the absorber block
  - Check of the synchronization with the particle free gap
  - Losses in extraction channel
  - Dumped intensity
  - All LBDS system status
  - Controls system readiness
  - Origin of the dump request
    - Operation, beam loss monitor, quench, …

Performed after every beam dump

Logging

- Established system foresees logging of all relevant parameters
  - Oracle database
  - Web based browsing, data extraction etc.
  - Frequency of order 1 Hz
  - Input into post-mortem analysis
  - OPERATIONAL (TI8, Vacuum…)

timber
The LHC Logging System

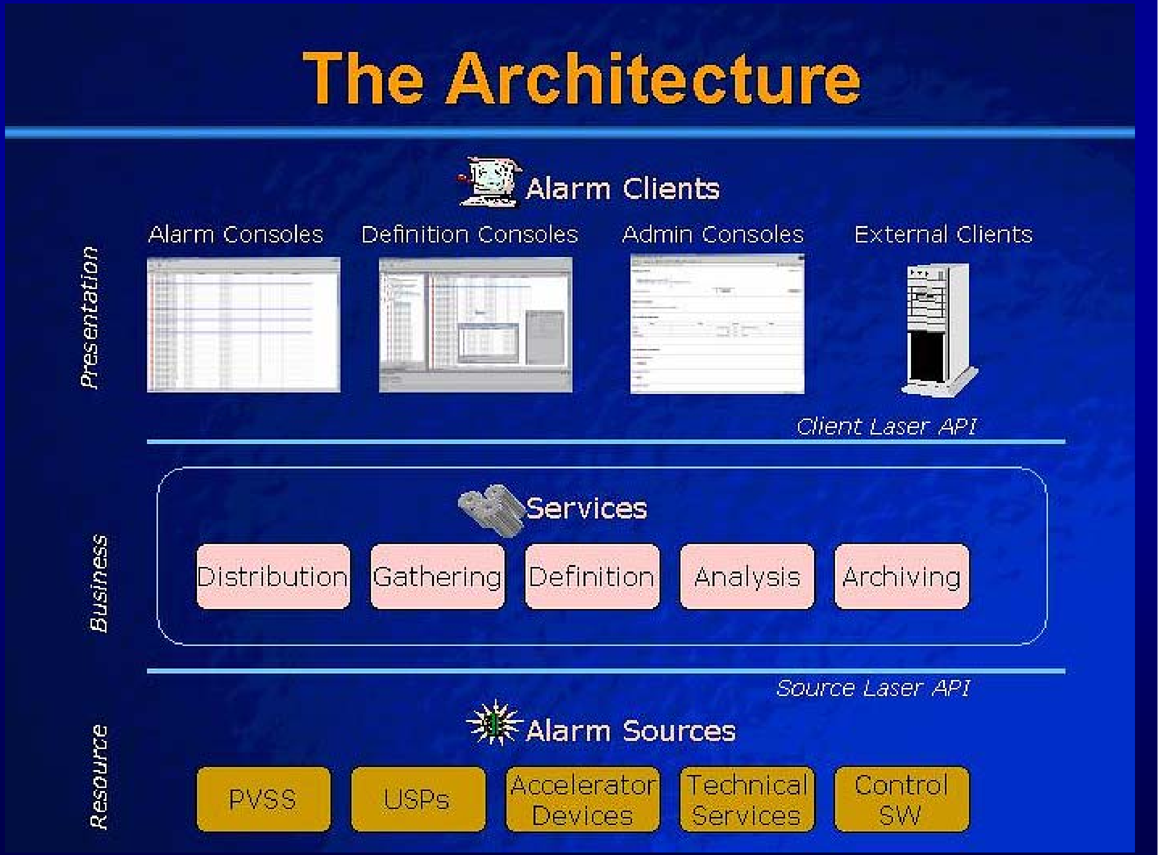
- Complemented by logging of (real-time) feed of fast signals:
  - 10 – 50 Hz
  - Beam Loss Monitors, Orbit, Power Converters, Beam Current etc.

Alarms

Alarm systems are not normally safety related, but do have a role in enabling operators to reduce the demand on the safety related systems, thus improving overall accelerator safety.

CERN wide alarm system (LASER)

- **Deals with level 3 alarms**
- **Standard solution**
- **Good reduction**
- **Logs everything**



Timing System

- Slow timing
  - Optical long distance, RS485 short hauls.
  - UTC timestamps (1/25ns resolution),
  - Timing Events:
    - Post Mortem Freeze, Start ramp etc. etc.
  - Telegrams (specific message information e.g. energy, intensity, GPS)
  - 1KHz events

- TTC/BST
  - 40MHz bunch clock & 11kHz F_{rev} distribution
  - BI hardware triggers [including post mortem]
  - Telegrams

Secure Settings

- **BLMs**
  - **Thresholds & masking tables**
  - **External Non-volatile RAM – read in at system power-on**
  - **Changeable during commissioning, authorised user thereafter**

- **TDI**
  - **Position has to be locked in place during the injection of high intensity batches**
    - **Safe Beam Flag,**
    - **Mode (or energy) mode dependent lock out (need to pull these things out after injection has finished)**
  - **intended intensity dependent settings ranges**
    - **(not only do settings have to be locked, they have to be right)**
    - **front-end lockin**

Secure Settings

- Collimators
  - intensity, β* (at IR 1 and/or 5), [mode] dependent
  - position ranges will have to be locked into front-ends,
  - reject requests for movement outside these range,
  - fire beam abort if surveillance sees collimators outside range, plus demanded not equal to read +/- tolerance.
  - imagine beam finding at β* = 0.55 m

- TCDQ & TCS
  - Has to track collimators
  - Again intensity, β* dependent settings lock-in

  - Position with respect to closed orbit
    - orbit drifts, orbit monitoring

Secure Settings

- Injection kickers,
  - All operational parameters, like timing settings, interlock thresholds, etc., are remotely controllable.
  - Control of critical parameters is password protected.
- Injection septa
  - Slowly pulsed, surveillance of current, adjustment of reference, timing
- Dump kickers
  - Etienne to point 6, cross-checks against reference
- Dump septa
  - I(t) lock in FGC [?]

Software Interlocks

- **Essential principle:**
  - High level surveillance in software
  - Control system dependent

- **Equipment Settings**
- **Equipment State**
- **Orbit**
  - slow orbit drifts w.r.t. reference
- **Interlock monitoring**
- **Movable objects:**
  - Wire Scanners

Requirement capture in progress

Safe beam conditions

Monitoring and control

- **Orbit**
  - Monitor Excursions
  - Monitor Local orbit bumps
  - Feedback – Network, Servers etc.
    - Local orbit at collimators, TCDQ, TDI
    - Global orbit
- **Tune & Chromaticity**
  - Acceptable ranges with intensity, acceptable trims
- **Beta beating**
  - relative beam sizes,
  - settings, reproducibility
- **Emittance variations**
- **Beam Lifetime**

False Manipulations

Protect the machine from deliberate but undesirable actions

Protect machine from inadvertent actions

- **Operations (SIL -99)**
  - **Validation**
    - **Limits,**
    - **State changes**
    - **Orbit, local orbit bumps, limit corrector ramp rates**
  - **Reproducibility, settings management**
  - **Settings modification lock-out**
  - **State change lock out**
  - **Secure settings for critical components**
- **Feedback systems**
  - **tight, configurable, parameter adjustment ranges**
  - **intelligent strategy in case of**
    - **lost lock etc.**
    - **bad pick-up rejection**

Machine State Change

Defining and handling machine modes (inject, inject & dump, ramp, squeezed, ...) and transitions between them.

- **Pre-OP checks**
  - **BLMs: Automatic test procedure of analog signal chain between 2 fills**
  - **QPS/PIC tests**
  - **As good as new checks – beam dump etc.**
- **Rigorous enforcement of operational procedures**
  - **nothing forgotten, nothing in error.**
  - **magnet hysteresis**
  - **staging injection intensities**
  - **conditions for measurements (wire scanners, screens…)**
- **Checks before Machine State changes**
  - **PIC, BIC, WIC, power converters, RF, position of movable objects**
  - **Anticipate Safe beam Flag changes in ramp**

Security

- Sabotage – protect the machine from malicious actions
  - How would you do it?
  - Network security,
  - Restrict low level access,
  - Remote access (Piquets (bad manipulations by experts))
- Secure consoles
  - lockouts, timeout of privileges
- Override management
  - authorisation, security, recording, monitoring and review of overrides, reset requirements

To be addressed…

Conclusions

All elements of the system which are required to perform the safety function are safety related, and should be considered part of the safety related system.

Teetering on the brink here

- **Control system is clearly implicated:**
  - **Post-mortem**
    - **trigger & transfer**
  - **Pre and Post operation checks**
  - **Software interlocks**
  - **(Secure settings)**
  - **Error trapping**
  - **Beam State**
  - **Machine State: procedure, procedure**
  - **Security**