Software Interlocking
&
control room buttons

J. Wenninger AB/OP

- Present SPS Software Interlock System (SSIS)

  Description, limitations

- New Software Interlock System

  Buttons, connections, issues &requirements (no SW design today !!)

What is a SW Interlock System ?

It is the *software analogue* of the HW interlock system:

- The SIS system has clients that generate interlocks/permit signals, the signals are based mostly on SW treatment (although SW is also involved in the HW interlock clients).
- The SIS has a core responsible for interlock transmission that is based on SW. This is the SW equivalent of the PIC/BIC systems.
- The signal transmission relies on standard Ethernet + communication framework.
- The SIS dumps, inhibits… beams.
- The system is not a real-time system. Delays of ~ seconds are typical for such systems.
- The system is not really failsafe – subject to interpretations & design choices.

Why Software Interlocks ?

What is the role of a Software Interlock System (SIS) on top of a reliable and failsafe hardware interlock system ?

- The SIS can anticipate failures and give early alarms:
  - + Reduces remnant radiation (also valid for dumps !).
  - + Accelerator complex or machine efficiency optimization.

    Example : SIS may detect that a PC is off, and prevent *running* the corresponding beam.
- (Very) complex interlock logic may be implemented in the SIS, including ‘situations’ that are not fully covered by the HW system:
  - – Correlation between systems.
  - – Integrity checks (interlock thresholds).
  - – ...
- Software interlocks are very flexible, and new channels may be added ‘rapidly’
- Complement to the HW interlock system.

SIS and Sequencers

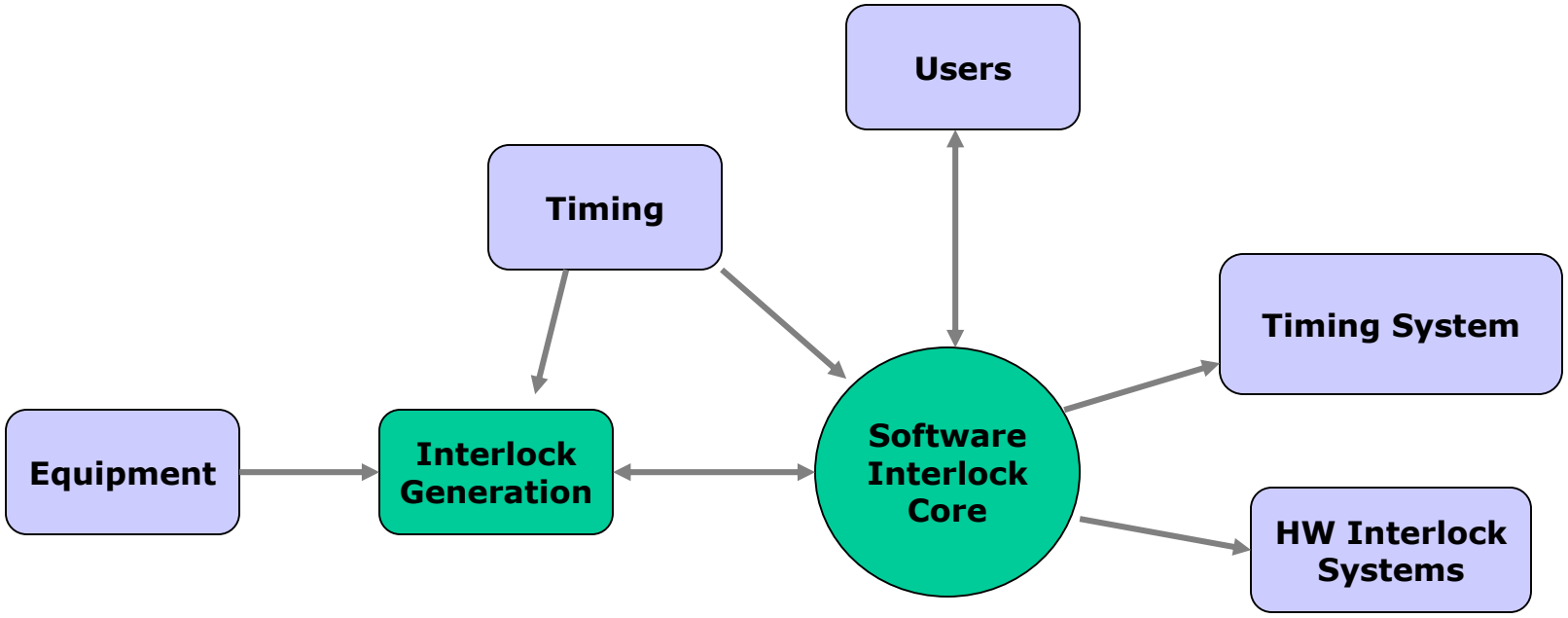
There is a distinct difference between checks performed by the SIS or by the sequencer as it is foreseen for the LHC.

- The SIS is always actively surveying the machine, possibly adapting its strategy to the machine state – in that sense it is really identical to a HW interlock system.

- The sequencer will be driving the LHC through its cycle. Before any major ‘state change’ (injection, ramp, squeeze, collisions…) the sequencer will make appropriate checks of component states to ensure it can proceed. But the sequencer is not continuously monitoring the machine.

Software Interlock System

- The SIS interacts with many players of the accelerator control system.
- At CERN the SIS sends signals to the central timing system & to HW interlock systems.
- Architecture :
  - It is important to separate the system from the individual interlock generation.
  - The core is rather generic – individual interlocks are not !



SPS versus LHC SW Interlocking

I will concentrate today's discussion on the SPS, because the situation at the SPS is much more complex than at the LHC.

- Multiple operational beams.
- Absence of fast HW interlocking between PS and SPS : beams can only be stopped through the timing system → relies on the SW interlocks !
  - **SPS :** an emergency beam dump interlock inhibits the injection kicker, but does not stop the beam that is dumped on the injection stopper → must act on the CPS timing system.
  - **LHC :** an interlock cuts the beam permit, which stops the extraction from the SPS → clean !

    The equivalent of the PS-SPS situation would mean that beam extraction continues and the beam is dumped on the TDI.

A solution that fits the SPS will work for the LHC - if it is carefully designed!

SPS Software Interlock System

- The present SPS SW Interlock System SSIS is used in operation since 1995.
- It was written by an external company according to specifications written by B. Denis (ex-CO). Specifications were produced with input from many people, in particular OP. They were also based on what existed already at that time on the SPS.
- The system uses dedicated hardware (installed in an *old* PC, itsccr) to communicate with the PS control system, the emergency dump system and with 4 ‘console switches’ (switch to stop beam operation).
- SSIS is visible to other players in the control system as a standard device, because it is implemented as an equipment server (based on SL_EQUIP package, the predecessor of CMW). This provides simple access for external cleints.

SSIS Architecture

External clients

Targets

Wobbling

SSIS component

SW link

HW link

SSIS User Interface

itsccr

SSIS KERNEL

SSIS Hardware

MCR (CCC)

CBCM/MTG

CERN Alarm System

Emergency Beam Dump

BA1

PCR (CCC)

SSIS AEM

Console Switches

SPS Timing

SPS Mode

SPS equipment

(for synchronization)

AEM = Accel. Eqp. Monitor

Interlocks

- Interlocks are organized by logical channels (↔ interlock grouping).
  - basic building block is the ‘elementary test’.
- Interlocks are polled every ~ 20 seconds.
- Logical channels are associated to the Hadron beam or to the MD beam.
- Interlock channels may be set by
  - internal surveillance (through the AEM component),
  - external clients (connection via SL_EQUIP).
- Interlocks are conditioned by the mode that describes the current state of the SPS (or at least OP’s current intentions).
  - modes : no beam, beam to TED XX, beam to target T2+T4+T6….
- Every interlock channel can be masked by operators (with the UI).
- Every interlock is also associated to an Alarm.
  - Interlocks that stop a beam → Level3 (red alarm on alarm screen).
  - Some (less critical) interlocks only generate an alarm → Level1/2.

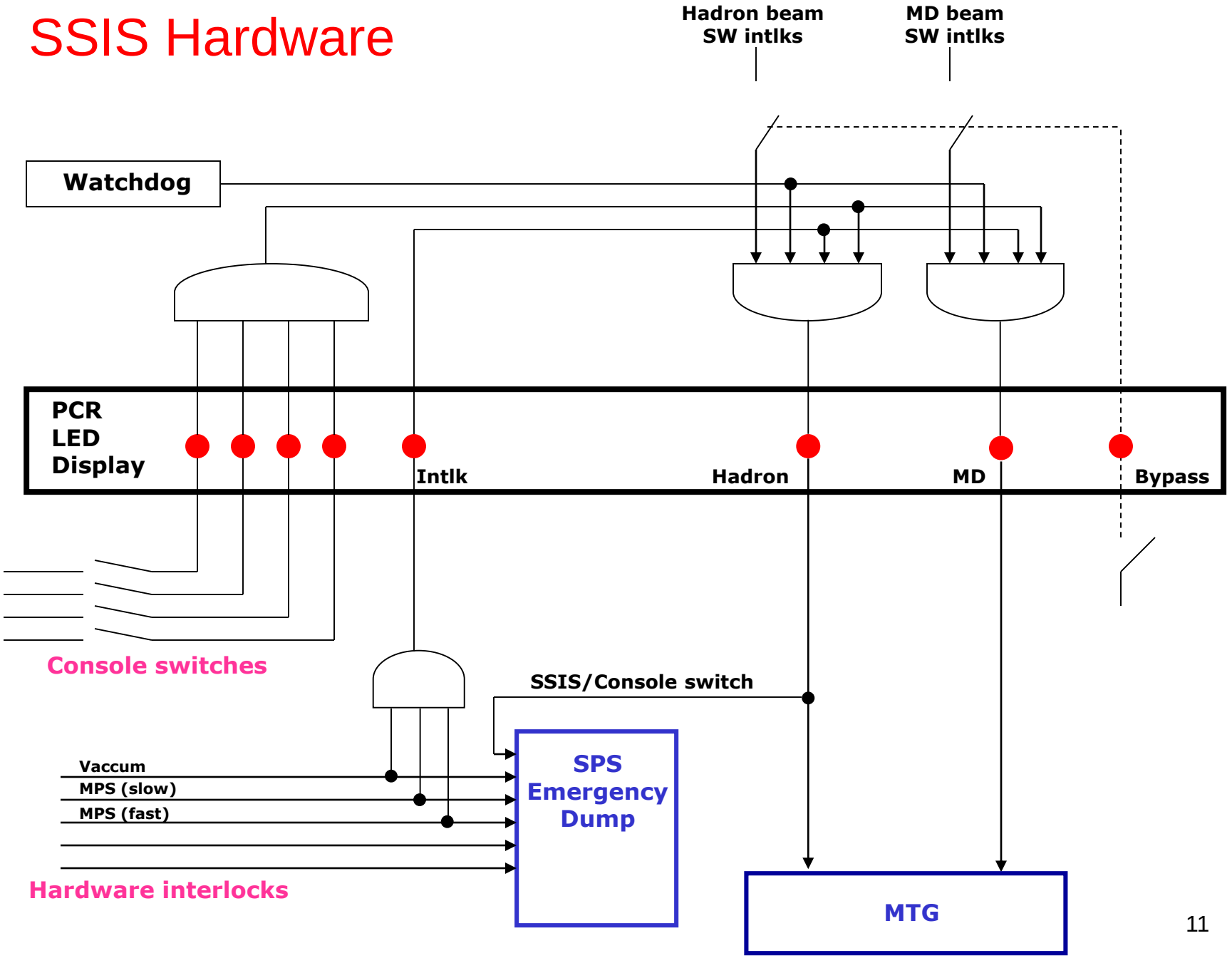
    Example : no access to certain equipment
  - The alarm is present until the interlock disappears.
  - Masked interlocks : Alarm message is modified, but not removed.

Equipment surveyed by SSIS

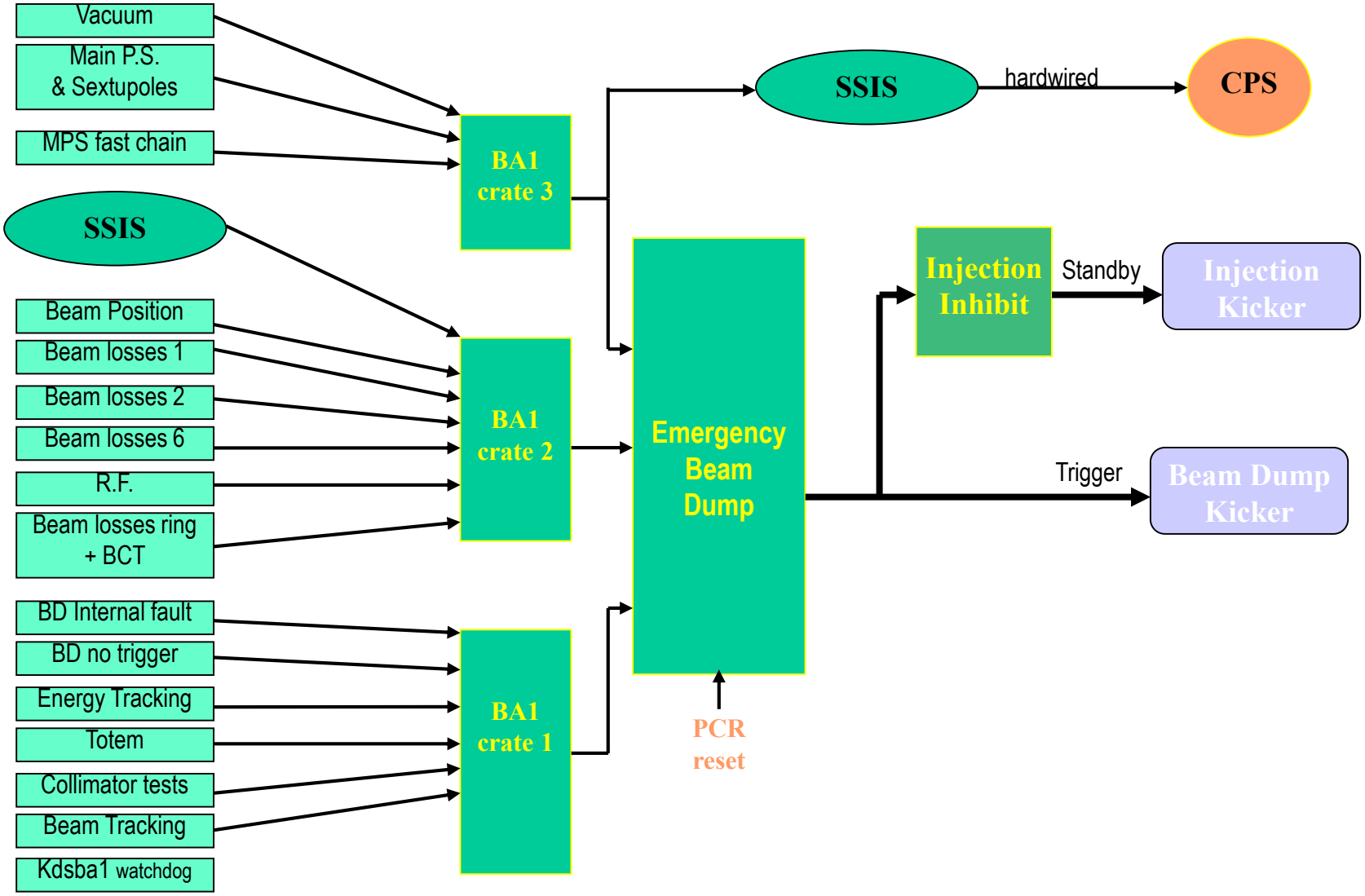
A list of logical interlock channels are :

- Main Power Supplies error
- STOPPER MOVING
- DUMP INTLK DISABLED
- RADIATION BB4/5 or TI8/TT41
- Operator request
- Switching AUXPS / ROCS reload
- MD PODH in 4 should be off
- GEF'S EXT.N RELOAD
- W.Extr. (or N.Extr.) Bumper in bad state
- HIGH ENERGY STORAGE
- HIGH INTENSITY ON NORTH TARGET
- EDF CRITICAL PERIOD
- WOBBLE FAULT NORTH
- Injection Interlock Disabled
- E A UNSAFE
- SETTING UP SEM OFFSET TABLE
- SPS VACUUM INTLK. CHAIN BROKEN
- HIGH INTENSITY/HALO ON WEST TARGET
- W ZS in bad state
- MBBT 6202 OUT OF TOLERANCE
- QBM in 6 ON - should be off
- Beam loss ring
- N ZS in bad state
- TED TT40
- TED TI8
- TBSE TT41
- TBSE 80243 in bad state or position fault
- WOBSU N/alarm system communication problems
- EXTRACTION INHIBIT CHANNEL DISABLED
- BI-BTV RING or BI-BTV TRANSFER could be IN
- Extr. Sextupole OFF
- ZS GIRDERS in beam
- SCHOTTKY PU in beam
- TIDV water fault.
- TED First Turn in beam
- TED TT60 or TED TT20 in bad state
- ACCESS CHAIN broken
- BHZ 377 in bad state
- COLLIMATORS 1 in bad position or COLLIMATORS STEP 4 in beam
- COLLIMAT & SCRAP 5 in bad position
- SCRAPER 5 ENABLED
- TT10 MAGNETS in bad state
- West MST/MSE or North MST/MSE in bad state
- TT60 MAGNET or TT20 MAGNET in bad state
- P0 Line TAX closed or P0 Line BEND error
- EAST BUMPERS in bad state
- COLDEX LSS4
- MDVW in 5 in bad state
- STOPPER TT20 or STOPPER north IN with TED OUT
- East EXT. GIRDER LSS4 in beam
- MBSG 410 OUT OF TOLERANCE
- TT40 MAGNETS or TT41 MAGNETS or TI8 MAGNETS IN BAD STATE
- EAST MSE IN BAD STATE
- TT40 TOO LOW (or TOO HIGH) INTENSITY
- VACUUM PLATES IN 5 IN BEAM
- MDHW / QSE in 5 in bad state
- MKE MAGNETS LSS4 OVER-TEMP
- 1 or 2 TBSE in with TED TT40 out

SSIS Hardware



Present SPS Hw Interlock System



SSIS hardware

- The console switches are used to stop all beams in the SPS.
- The HW watchdog stops all beams if it is not reset by the SW every ~ 100 ms.

  → tests that the SSIS SW (kernel) is alive.

  → NOT a guarantee that external clients are alive !
- A bypass of all SW channels is available.
- The hadron beam channel sets an interlock in the SPS emergency dump system.
- The hadron and MD beam signals are used to stop the beams in the CPS complex → cycle changes in the CPS complex.
  - Without this signal, the CPS continues to send beam to the SPS.
- The logic for the hadron and MD beam channels in terms of beam stops has evolved with time (with the production and MD beams).

Current SSIS problems

- Internal SW issues and compatibility with new LHC controls environment.
  - Our ‘standard’ problem : SL_EQUIP package is no longer supported.
- The number of SW output channels (2 [hadron,MD]) is no longer sufficient.
- Hardware problems:
  - SSIS hardware interface is old, SSIS PC is old and outdated – must be replaced.
  - 2 channels (*bits*) are not sufficient for communication with the PS when we run FT, CNGS, LHC (with 2 destinations)…
- The SPS mode will disappear, use of timing must be changed.
- Adapting the program is probably inefficient and may imply a major effort.

→ We need a more flexible system with more output channels.

→ We must adapt the system to take advantage of SW inputs of the BICs.

→ We must learn from SSIS : the basic architecture can be used as starting point.

New SIS

- The following slides present some issues & ideas for the new SIS.
- They reflect ***MY*** ideas and are a mixture of lessons from the past, estimates on how the SPS will run in the future (controls-wise) and discussions I have started with some people on the subject.
- The major milestone for the new SIS is to have a ‘proto-type’ ready for the CNGS commissioning end of May 2006.
- People that will work over the coming months on this project are :
  - Vito Baggiolini AB-CO – project leader
  - Jakub Wozniak AB-CO – the hard worker
  - Jorg Wenninger AB-OP – mostly consulting & requirements

Beam Inhibit Switches/Buttons in the CCC

- In the CCC ~18 buttons are presently foreseen on each island (CPS, SPS and LHC) to implement simple & direct 'beam stops'.
  - Located at the center of each island.
  - Not within reach of every console as was the case in PCR (to be modified later ?).
- Buttons that are presently foreseen for the SPS:
  - 1 button 'dump/stop all beam', connected DIRECTLY to one SPS ring BIC.
  - 1 button 'inhibit LSS4 extraction', connected DIRECTLY to TT40 BIC.
  - 1 button 'inhibit LSS6 extraction', connected DIRECTLY to TT60 BIC.
  - 1 button / beam, connected to the MTG to stop the corresponding beam in the CPS :

    ALL (?), FT, CNGS, LHC, MD → ≥5 buttons. 'Granularity' to be defined (by experience).
- Buttons that are presently foreseen for the LHC:
  - 1 button 'dump beam1', connected DIRECTLY to one LHC ring BIC.
  - 1 button 'dump beam2', connected DIRECTLY to one LHC ring BIC.
  - 1 button 'inhibit injection beam2', connected DIRECTLY to injection BIC IR8.
  - 1 button 'inhibit injection beam1', connected DIRECTLY to injection BIC IR2.

→ Those buttons do not dependent on the SIS !

SIS output channels : to MTG

After discussion with CO/HT (timing), an output channel scheme emerged that is not based on beams but rather on ‘geographical zones’.

- MTG should receive signals grouped by geographical zones, ~ identical to the scheme used for the HW interlock systems and reflected in the BICs:
  - Signals for TT40, TT41, TI8, TT60, TI2, TT20 & North targets, SPS ring, TT10…
- The logic to stop beams is implemented in the MTG, with the advantage that:
  - MTG knows ahead of anyone else ‘what will be’, in terms of beams but also destinations.
  - MTG will apply appropriate logic taking into account the beam destination.

    Example : SW interlock for TT41 (PC off…)

    If the CNGS beam destination is T41 target → stop beam.

    If the CNGS beam destination is SPS dump → run beam.

    The consequences of inconsistencies between expected (MTG) and actual destination must be analyzed (+ how to catch them).

    A related issue (for OP) : do we maintain the SPS mode (manually set) or do we rely on the destination information provided by the timing system ?

SIS output channels : to BICs

- The same output channels, grouped by zones, that are send to the MTG can be reused to set a SW interlock into the corresponding BICs :
  - TT40, TT41, TI8, TT60, TI2, TT20 & North targets, SPS ring, TT10…
- Issue : what about a SW system bypass ?
  - We may need a ‘concept’ similar to the bypass button of SSIS (but less drastic).
  - To be studied…

SIS – MTG link

Is a hardware connection between the future SIS and the MTG, as it exists now, meaningful in the future ?

- This is a dedicated hardware connection between two pieces of SW, one of which (SIS) is rather huge.
- A SW connection is lighter and easier to change (new output channels).
- Both MTG and the future SIS ‘machine’ will be located in the back of the CCC:
  - If there is a network problem, everything else will be stopped too.
  - A problem with CMW is more likely…
  - The SIS will also stop the beams through the BICs.
- In any case we can cut all beams with the buttons described previously.
- If we choose a hardware link : responsible group must be identified.

→ For the beginning (2006) : use SW link !

Interlock latching

- Latching strategy of the present SPS emergency dump system:
  - By default interlocks are latched (manual reset required).
  - Exception : BLM/BPM interlocks are reset 3 times (internal reset by SW process within emergency dump system) before the interlocks remain latched.
  - This strategy was adopted to reduce the downtime generated by interlocks due to isolated 'bad' cycles with beam loss or large position offset.
- SPS BICs:
  - SPS transfer lines : Interlocks are NOT latched by the BICs (cannot be done !!).
  - SPS ring : Latching, non-latching BICs or *BOTH* (1 latching/non-latching per crate) ?

    Latching BICs → stop ALL beams, even the ones that have no problem.
- The job of latching interlocks may be taken over by the SIS:
  - The SIS has access to the necessary information needed to stop ONLY the beam that is responsible for the interlock without affecting other beams

    → stop beam via timing system – requires outputs by BEAM and not by zones !
  - Individual latching strategies could be defined for various interlock classes.
  - But latching depends then on SW !

→ requires more careful analysis !

SW architecture & issues

- It is too early to define the SW architecture, but I see one concept of SSIS that should be maintained : possibility for external clients to set SW interlocks !
  - More people can participate to the SW effort (can be a plus or a minus !).
  - Issue : we need a mechanism to ensure that external clients are ‘alive’.

    One may use the concept of a permit that must be re-activated by the client at fixed intervals – at least for critical clients.
- What strategy to adopt for masking of SW interlocks?
  - Masking permitted only permitted for certain channels ? For channels that are not ‘covered’ by a HW interlock ? …
- Reliability issue: what strategy to adopt in case of communication errors ?
  - We must provide some margin for data & communication loss over short time periods.
  - …

The LHC case

The SIS designed for the SPS can and should be used for the LHC.

- LHC output channels to MTG & BICs:
  - LHC ring1/2
  - LHC injection1/2
  - By beam (pilot, intermediate…) ?
- Interlock masking :
  - Ad-hoc strategy for the LHC.

Summary & actions

- The main limitations of SSIS for the SPS are known.
- SSIS will be kept alive for the SPS in 2006 – but it will be difficult to survive much longer, as the SW revolution in the SPS condemns SSIS.
- A new SIS must be prepared for the CNGS commissioning in May 2006.
- The core team (VB, JW^2) of the new SIS exists but there is still a lot of work to do.
- I will start to put requirements and design ideas on paper.
- For all: we must start preparing lists of SW interlocks with some level of detail & priorities for both SPS & LHC.