GMT TIMING MONITORING
Risk analysis

ABSTRACT:

A Central Timing (CT) is a system composed of dedicated hardware (FEC + VME modules) and software. Based on various inputs (human, security, …) the CT calculates information known as General Machine Timing (GMT) Events, defining the accelerator behaviour over time. GMT events are distributed to timing clients via the dedicated GMT network, composed of cables (optical and copper) and a number of various hardware modules such as repeaters, level-adapters and fan-outs. All involved software and hardware components may potentially fail. This document analyses potential sources of failure and proposes solutions to minimize these risks.

We stress the fact that the proposed solutions may under no circumstances be considered sufficient for human safety.

PREPARED BY:	TO BE CHECKED BY:	TO BE APPROVED BY:
Jean-Claude BAU Steen JENSEN	Jan Uythoven Bruno Puccio Verena Kain Etienne Carlier Ivan Romera Ramirez Pieter Van Trappen	

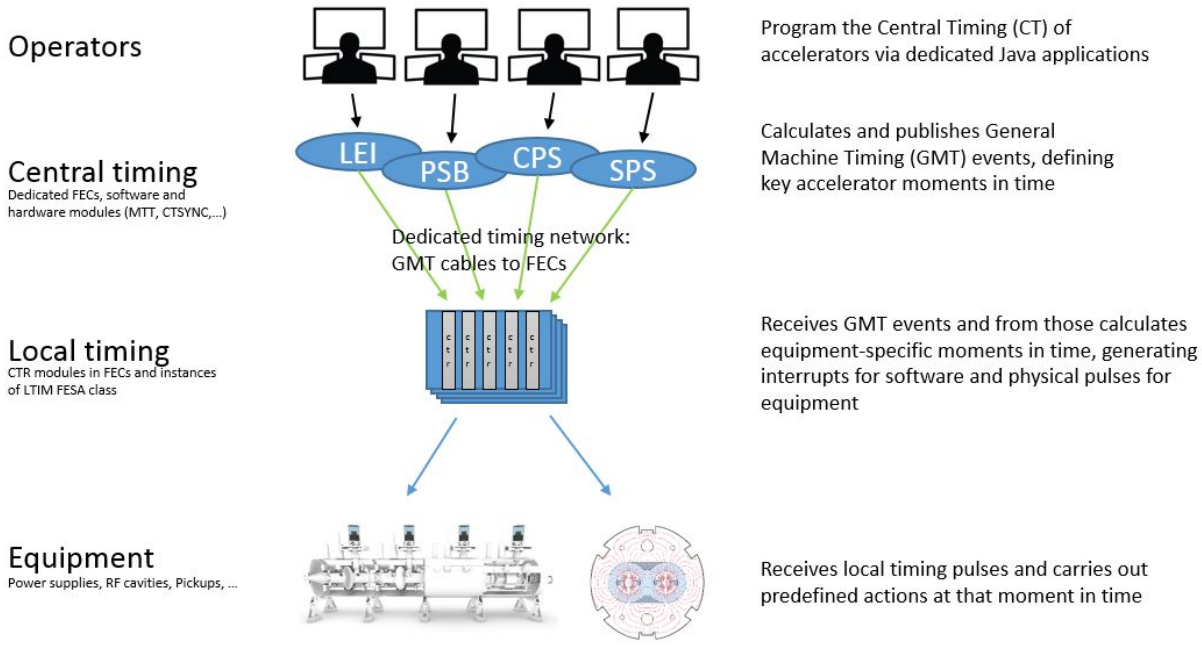
DISTRIBUTION LIST:

HISTORY OF CHANGES

REV. NO.	DATE	PAGES	DESCRIPTIONS OF THE CHANGES
0.1	2017-05-08	all	Draft version

TABLE OF CONTENTS

1.INTRODUCTION



Figure

A Central Timing (CT) is a system composed of dedicated hardware (FEC + VME modules) and software. Based on various inputs (human, security, …) the CT calculates information known as General Machine Timing (GMT) Events, defining the accelerator behaviour over time.

GMT events are distributed to timing clients via the dedicated GMT network, composed of cables (optical and copper) and a number of various hardware modules such as repeaters, level-adapters and fan-outs.

On the client side, GMT events are received in Front End Computers (FECs) by Central Timing Receiver (CTR) hardware modules, connected to the GMT network. The CTR modules are programmed (via the LTIM FESA class) to generate local timing, i.e. VME interrupts and/or physical output pulses derived from the GMT events. These local timings serve to trigger a range of software and hardware actions such as sending a control value, acquire data, pulsing a power supply, etc.

If any component of the CT or the GMT network fails, timing clients will no longer receive GMT events. Depending on the role of the client, such failures can have serious consequences, including accelerator damage.

To minimize the risk of such incidents happening, it is necessary to implement a system by which timing clients will be alerted of failures so they can take proper action in due time.

Of particular concern is currently the SPS accelerator, which is part of the LHC Injector Chain (LIC) which also includes the PSB, LEIR and CPS accelerators and is orchestrated by a single central timing system, the LIC CT, located in the CCR (874-R012).

This document will be a reference document that will be used for the functional specification of such a monitoring/alerting system, the “timingGmtMonitoring”.

2.OBJECTIVES

We present the various possible timing failures and analyze the potential impact for each. Based on this, we propose solutions for detecting the problem and alerting affected timing users.

3.POTENTIAL FAILURES

In this chapter we analyze potential timing failures from the CT through distribution to the final timing client.

3.1.Central Timing

3.1.1.CRATE

The LIC CT is a VME crate with a CPU card, a power-supply and a set of hardware modules. Possible breakdowns are:

3.1.1.1.Crate Power-Supply

When the power-supply fails, the MTT (Multitasking timing generator) card(s) in charge of transmitting GMT events onto the GMT network is not powered. Consequently, there will be no GMT events on the GMT network. This affects all FECs of the accelerator covered by the MTT.

3.1.1.2.MTT (multitasking timing generator) module

It is difficult to predict how an MTT can fail, let alone the consequences. Possible failures include:

1. GMT output: If broken, random and/or meaningless events may be transmitted, or none at all.
2. Software interface: The MTT card is not used in the same way for all accelerators. For LHC and REX, the MTT is used in a static way. It means that the events to produce are pre-loaded in the MTT (Table) and executed on demand. During the execution of such a table, a software failure will have no consequences. Only the programmation and loading of new tables will be affected. For accelerators in the LIC CT, AD and ELENA, MTTs are reprogrammed every 1.2 seconds. A software failure will in this case stop the production and transmission of cycles and events data. However, in both cases, UTC and millisecond frames will continue to be sent.

3.1.1.3.CTR (Central Timing Receiver) module

CTR modules are used in the CT to monitor the produced GMT events but also to inject events called "external events" such as the SPS partial economy, AWAKE triggers for SPS extraction, the 10HZ AWAKE source trigger and the LHC forewarning injection... Also, local timing is used to trigger the FESA task in charge of handling LHC injection requests. If one of these CTRs breaks, the triggers may not be generated, preventing certain real-time tasks from being executed.

3.1.1.4.CTSYN (Synchronous base time generator) module

This card receives the 10MHz and pulse-per-second (PPS) clocks from a GPS receiver or a White Rabbit switch (WRS). From these signals, it generates a PPS and a 40MHz clock for the MTT cards. It also generates real-time interrupts for all the main software components running in the CT crate. In case of failure, an MTT may not receive these clocks and therefore

decide to use internally generated clocks. As these clocks are not synchronized between the MTTs from different CTs, they will start to drift with respect to each other. Consequently, accelerators will be misaligned in time which is critical for the injection/extraction rendezvous.
If interrupts are no longer generated by the CTSYN module, the real-time task will not execute and the MTT will not be reprogrammed every 1.2 seconds as expected.

3.1.1.5. FAN-OUT MODULES

The FAN-OUT modules are used to distribute the PPS, SYNC PULSE, and 40 MHz clock. If one fails, MTTs will start to drift with respect to each other (see: malfunctioning of a CTSYNC)

3.1.1.6. WHITE RABBIT SWITCH

White Rabbit switches (WRS) are used to transport and generate the 10MHz and pulse-per-second (PPS) clocks for a CT. Currently they are used for the AD and ELENA CTs. The WRS receives the clocks from the WRS Timing Master which in turn receives clocks from a GPS receiver. In case of hardware failure, clocks produced by the WRS may be inconsistent or not present. MTTs in this case will start to drift with respect to each other (see: malfunctioning of a CTSYNC)

3.1.1.7. GPS RECEIVER

A GPS receiver generates the 10MHz and PPS clocks that will be used by all CTs.
In case of hardware failure these clocks will be generated locally by the MTT module in each CT and the CTs will start to drift with respect to each other. In this case the injection/extraction of accelerators managed by different CT will be misaligned.
Another case to consider is an issue with the GPS antenna causing the GPS receiver to become unlocked from the satellite signal. In this particular case, GPS clocks with start to drift slowly all together. When the issue disappears (GPS locked to satellites), the clocks will be realigned slowly. This process will not affect the accelerators.

3.2. GMT DISTRIBUTION

GMT signals are generated in the CCR and distributed to other buildings. It implies a lot of cabling (optic fibres, copper cables, patch panels, connectors …) and hardware modules (signal converters like optic-fibre to copper, line drivers for GMT repeaters, etc …). Any component in the distribution can fail, causing disruption or perturbation of the GMT distribution.

3.2.1. DISRUPTION OF THE GMT DISTRIBUTION

Any element in the distribution chain may fail and prevent timing clients from receiving the GMT signal. The CTR is able to detect this anomaly and display it in his hardware status as a GMT error.

3.2.2. PERTURBATION OF THE GMT DISTRIBUTION

In some cases, GMT distribution hardware may malfunction and cause perturbation of the GMT signal. For instance, if too many CTR modules are connected to a repeater, its power supply will be overloaded and its output voltages lowered.
In this case, the CTRs will miss some (not necessarily all) GMT events and its phase-locked loop (PLL) will start to fail staying locked to the GMT signal. The CTR detects missed frames and PLL errors. They appear as internal diagnostic counters. Also the state of the PLL is available in the CTR status.

3.3. TIMING CLIENTS

3.3.1. CTR MODULE

On the client side, failing CTR modules may fail to generate VME interrupts and/or output pulses and they may fail to report status and error counters. The consequences depend on what the role of the client is.

4. EXPERIENCED FAILURES

4.1. CENTRAL TIMING

The LIC CT (VME version) became operational in 1998 and has evolved ever since, including the following changes:

- upgrade of hardware cards,
- evolution of the Operating System
- new software design
- new machine to drive (SPS …)
- extraction to LHC
- moved from MNR (MEYRIN) to CCR (PREVESSIN)
- …

In parallel we developed other CTs for LHC, REX, CTF, AD, LINAC 4 and ELENA.

Despite all these changes over the last 19 years, we find that all the failures we had to face may still occur and have to be taken into consideration. They include:

- Explosion of a capacitor on an ICV196 card: The explosion destroyed several cards in the front-end and made a short-circuit on the power-supply. The incident stopped GMT distribution.
- Apnea of several seconds in a software driver: During the apnea the LIC CT stopped transmitting GMT events at the correct moments. The incident caused an uncontrolled beam loss in the SPS, resulting in a hole being created in a vacuum chamber.
- Desynchronization between the LHC and the LIC CT: The SPS and LHC GMT signals drifted with respect to each other. This misaligned the SPS extraction and LHC injection timing causing in LHC injection issue. This occurred during a technical stop when cables close to the CTs were manipulated. A similar situation occurred when upgrading the GPS receiver.
- Broken hardware module: When turning on the LIC CT crate we have experienced failure of hardware modules several times. In this case, the error is detected at the front-end startup and depending on the failure the software did not start. This is not a critical situation because a reboot is only done when there is no beam in involved accelerators.
- Unexpected reboot: We have seen unintentional reboots made by Operation with beam in the involved accelerator. This caused a disruption of the GMT signal.

Unseen failures:

- Desynchronization between acceleration managed by the LIC (PSB/CPS/LEIR/SPS): We never had an issue on the CTSYN module or on the MTT either.

4.2. GMT DISTRIBUTION

On multiple occasions we have experienced perturbations and disruptions in the GMT distribution chain, for a number of reasons:

- Disruption of the GMT signal: Depending on the source of the failure, this may occur on all front-end computers in a given area (GMT repeater dead, rack accidentally powered off …) , on all CTRs of a given front-end (cable/connector issue) or on only one CTR in a front-end computer (connector issue, GMT signal too weak, CTR broken …)
- Perturbation of the GMT signal: Similar to the disruption case above

5. WHAT DO WE SURVEY IN 2017

5.1. CT SYNCHRONISATION

Since 2014 the phase between CT's has been monitored by an automated system, raising alert signals in case of incorrect synchronization between SPS/LHC, PS/AD and AD/ELENA. The survey system measures the phase between the GMT signal and checks if a drift appears. When an error is detected the survey system generates an inhibit to inform the LIC CT or the Beam Request Server (BRS) for ELENA and AD to prevent beam production. In addition, an error message is displayed in the LASER application for Operation diagnostics.
In the LIC CT, the evaluation is done a few seconds in advance depending on the super-cycle structure. Consequently, when a desynchronization is detected between the SPS and the LHC, we may still extract from SPS two times before stopping the beam production.
The reset of these inhibits is done manually after a reboot of the faulty CT.

5.2. LIC/AD/ELENA/CTF/LINAC 4 CT SOFTWARE

These CTs are based on MTT modules which are reprogrammed every 1.2 seconds by real-time software tasks executing at the same rate. This in turn is guaranteed by a custom-made scheduling process.
If any component of this software breaks, all of them are frozen and the MTT will cease to be reprogrammed, causing all MTTs to play automatically a fail-safe sequence in which the event "MX.WATCHDOG-CT" will be sent repeatedly.
Currently, Timing clients must detect the reception of this event and take the necessary action.

5.3. GMT SIGNAL RECEPTION

The verification of GMT signal reception must be done as close as possible to the client system, for instance by verifying that the millisecond frame arrives every millisecond.
Currently this is only implemented for the SPS extraction kickers.

6. IDEAL MONITORING SYSTEM

In this chapter we will try to see what an ideal monitoring system may look like.

6.1. SURVEY MODULES

6.1.1. SOFTWARE FAILURE DETECTOR

Currently certain CTs (see CT Software) send the "MX.WATCHDOG-CT" event when a software failure occurs.
However, it is not enough to guarantee that the CT is well programmed and that this event will arrive in case of software failure. A better solution would be to produce a heartbeat event "MX.ALIVE-CT" every time the CT software executes. An external system (software error

detector) knowing the repetition rate can easily detect the absence of this event and take decisions. With this new "MX.ALIVE-CT" event, the detector will detect also other failures like GMT disruption and front-end reboot.
The "MX.WATCHDOG-CT" and "MX.ALIVE-CT" events are not exclusive. Both can - and should - be produced.

The following figure represents the software fault detector with its GMT input and an output that will fire when a software error is detected.

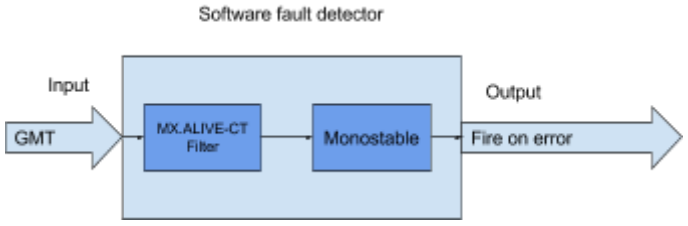


figure 2: Software fault detector (SFT)

For LHC and REX CTs this detector can be also put in place only to detect a reboot of the CT. We can program an MTT task to produce "MX.ALIVE-CT" at a regular rate.

6.1.2. GMT DRIFT DETECTOR

As explained previously, GMT event times can start to drift respect to each other in case of clocks failure (10MHz/PPS). Consequently, accelerators will be misaligned in time which is critical for the injection/extraction rendezvous.
This case must be detected to avoid injection/ejection problems between adjacent accelerators.

The following figure represent the GMT drift detector between two GMT cables.

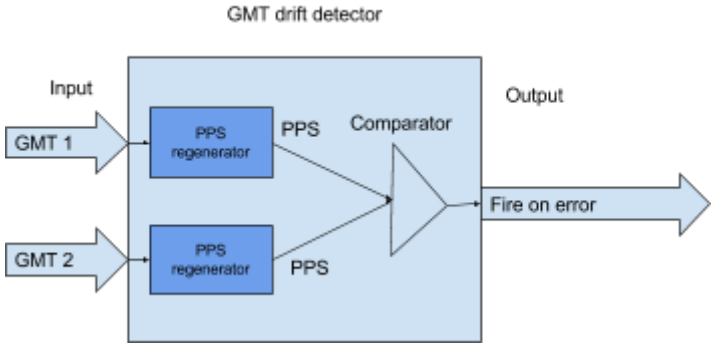


figure 3: GMT drift detector (GDD)

6.1.3. GMT DISTRIBUTION FAILURE

Currently the GMT distribution failure detection is based on the millisecond event being sent every millisecond on each GMT cable. If a millisecond event is missing an error counter will be incremented. It means that the detection time will be greater than one millisecond.
We have experienced occasionally that the GMT distribution is perturbed, causing lost events on a GMT cable. Millisecond events may be present but other critical events may not be present.
A perturbation on the GMT cable can be detected by a CTR using is internal metrics (lost events, PLL unlocked,...).

The following figure represents the GMT distribution fault detector. It is currently represented by a 'black box' since implementation details must first be discussed with the BE-CO-HT team.

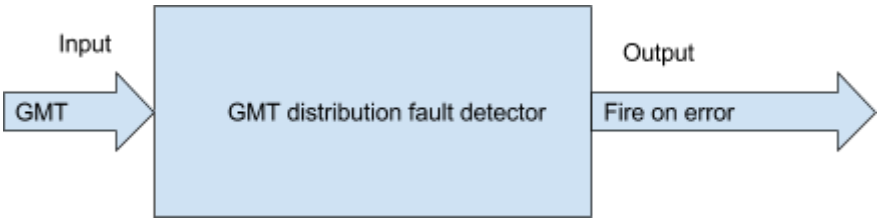


figure 4: GMT distribution fault detector (GDFD)

6.1.4. Interlocks

Interlocks notify clients about failures, allowing clients to protect their devices and the accelerators. Interlocks also serve to stop production of the beam.

We can distinguish two categories of interlocks :

1. Critical interlocks: They must be raised as soon as an error is detected because clients may have to react on the circulating beam to avoid machine damage. The Beam Interlock System (BIS) will be used to propagate these interlocks.
2. Non-critical interlocks: Some systems are not connected to the BIS and do not need to react in real time. It is mainly the CTs which cannot stop a beam which is already circulating, but they can prevent following beams from being produced. The LIC CT and AD/ELENA BRS are the main clients, and the distribution of such interlocks can be done by hardware (not redundant) or software.

6.2. Monitoring of the CTs

All the following monitoring systems must be seen only as a best solution to implement. For a realistic implementation we have to take into account cost versus benefit. We must answer all of these questions :

- Is this system going to generate more benefits than problems (risk of false positive) ?
- Do we really need fast actions like dumping the circulation beam ?
- Do we have equipment able to react in real time (e.g Dumping the beam)
- Who should be connected to the interlocks and how (BIC, software,...) ?
- ...

6.2.1. SPS-LHC MONITORING

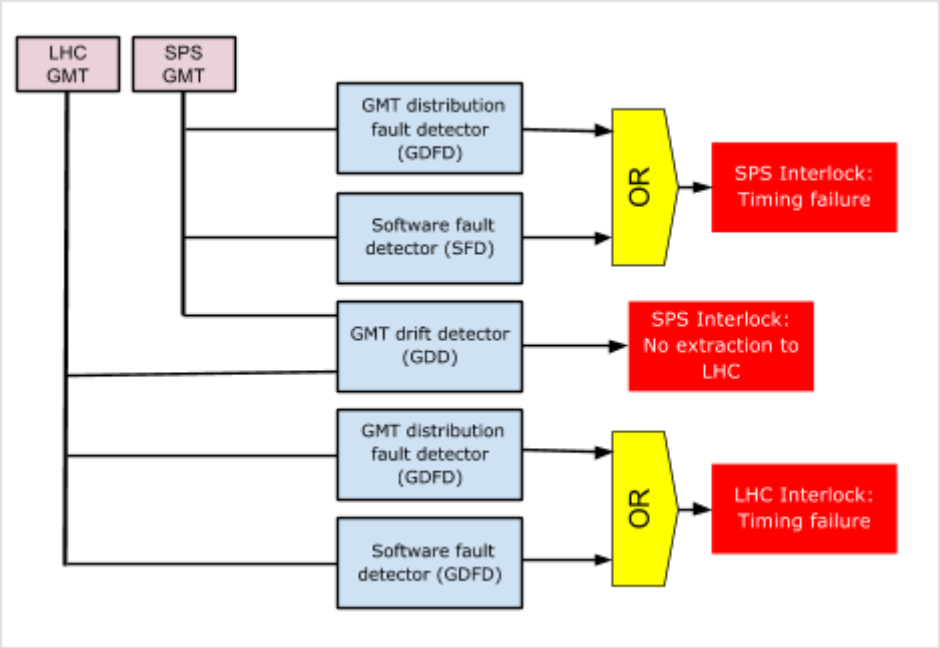


figure 5: SPS-LHC monitoring

The SPS interlock "Timing failure" should be taken into account by critical equipment to dump the SPS beam or doing other critical actions. The LIC CT should also be informed to stop SPS beams. It has a real meaning only when the error come from a SPS GMT distribution fault detected.

The SPS interlock "No extraction to LHC" should be taken into account by critical equipments to dump the SPS beam only when the SPS destination is LHC (TI2 or TI8).

The LHC interlock "Timing failure" should be taken into account by critical equipments to dump the LHC beam or doing other critical actions. Having a software fault detector is questionable but may bring a better level of security. This software detector could monitor all critical processes in the LHC CT to be sure they are alive. These processes allow modification of the LHC telegram and load/unload start of MTT tables which are essential to cycle the LHC.

6.2.2.PS-AD MONITORING

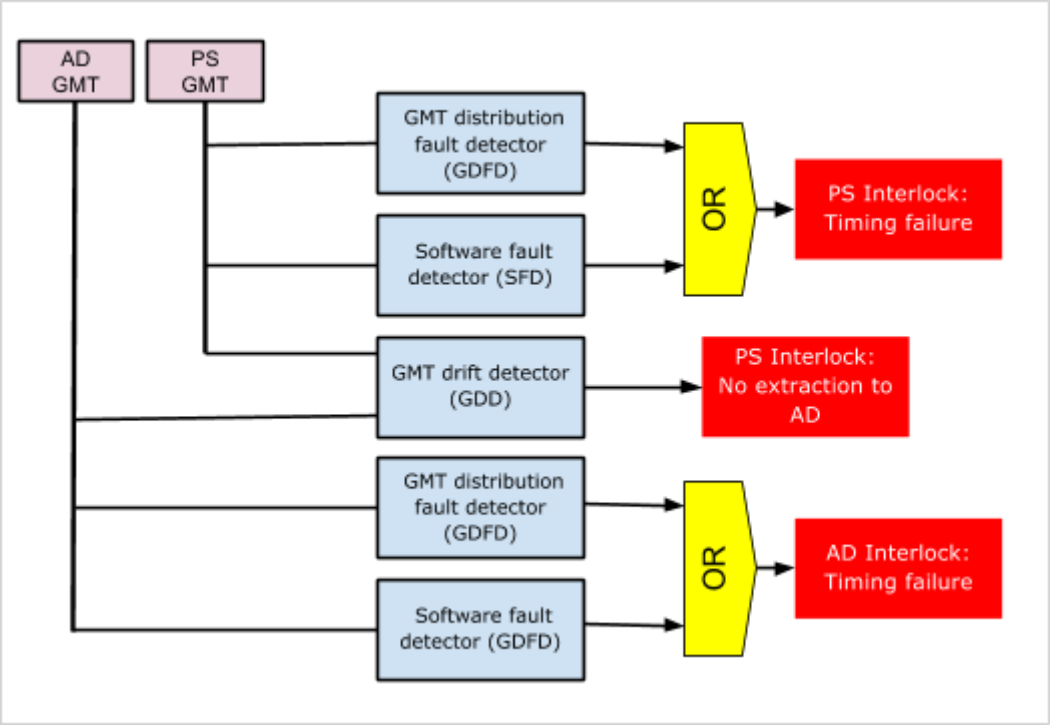


figure 5: PS-AD monitoring

The PS interlock "Timing failure" should be taken into account by critical equipment to dump the PS beam or doing other critical actions. The LIC CT should also be informed to stop the production of PS beams.

The PS interlock "No extraction to AD" should be taken into account by critical equipments to dump the PS beam only when the PS destination is AD (TT2_FTA). This information is already being used by the AD and ELENA Beam Request Servers (BRS) to abort and no longer request beam from PS. Also the LIC CT should be informed to not produce any beam for AD.

The AD interlock "Timing Failure" should be used by critical equipments to dump the AD circulating beam or doing other critical actions. Also the LIC CT should be informed not to produce any beam for AD.

6.2.3.AD-ELENA MONITORING

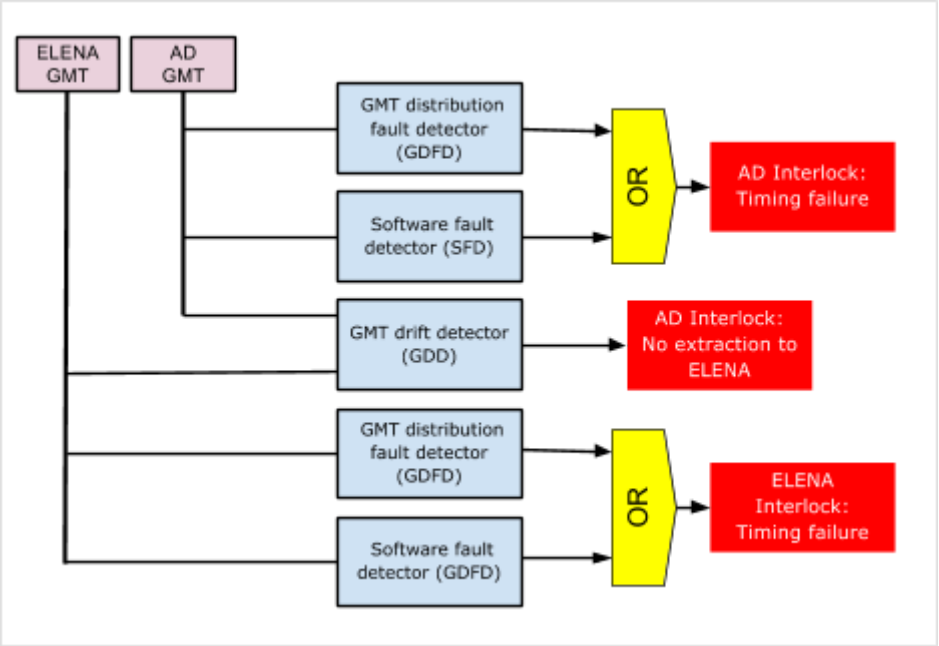


figure 6: AD-ELENA monitoring

The AD interlock "Timing failure" should be taken into account by critical equipment to dump the AD beam or doing other critical actions. The LIC CT should be informed to stop the production of beams for AD. The AD and ELENA BRS should be informed to abort and not request beam in the AD.

The AD interlock "No extraction to ELENA" should be taken into account by critical equipments to dump the AD beam only when the AD destination is ELENA. This information is already being used by the AD and ELENA BRS to abort AD beam and no longer request beam in AD.

The ELENA interlock "Timing Failure" should be used by critical equipments to dump the ELENA circulating beam or doing other critical actions. Also the ELENA BRS should be informed not to request any beam in ELENA.

6.2.4. PSB-PS MONITORING

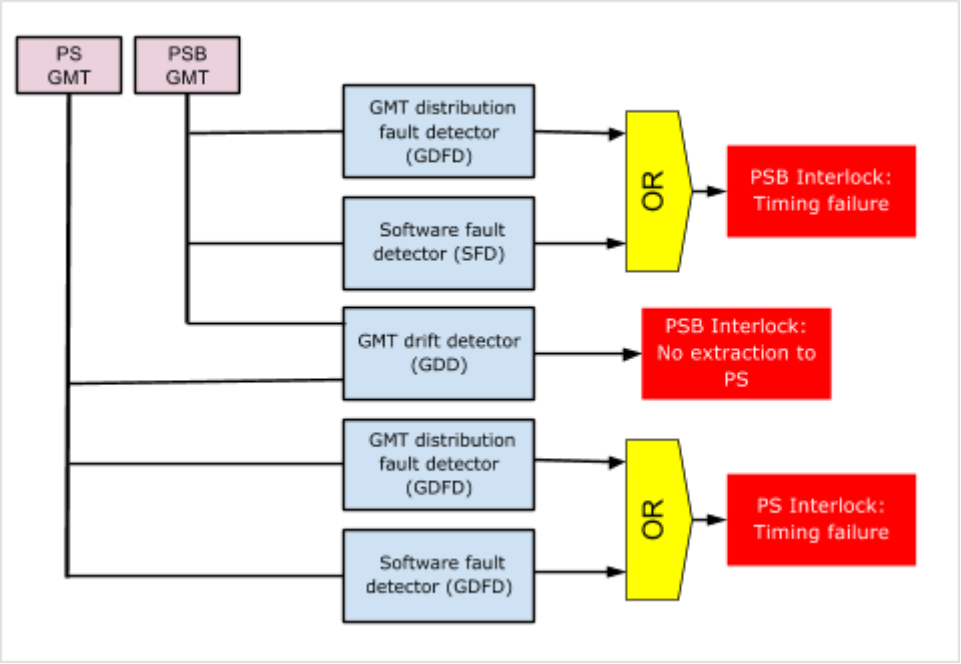


figure 7: PSB-PS monitoring

The PSB interlock "Timing failure" should be taken into account by critical equipment to dump the PSB beam or doing other critical actions. The LIC CT should be informed to stop the production of PSB beams.

The PSB interlock "No extraction to PS" should be taken into account by critical equipments to dump the PSB beam only when the PSB destination is PS (PS_DUMP, EAST_T8, FTARGET, LHC,...). The LIC CT should be informed to stop the production of PSB beams for PS.

The PS interlock "Timing Failure" should be used by critical equipments to dump the PS circulating beam or doing other critical actions. The LIC CT should be informed to stop the production of PS beams.

6.2.5. LEIR-PS MONITORING

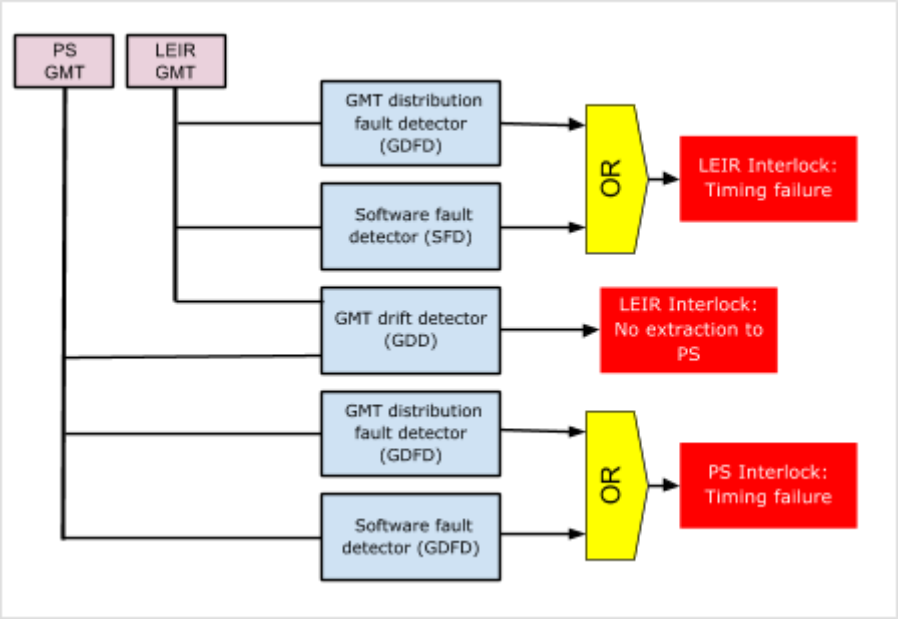


figure 8: LEIR-PS monitoring

The LEIR interlock "Timing failure" should be taken into account by critical equipment to dump the LEIR beam or doing other critical actions. The LIC CT should be informed to stop the production of LEIR beams.

The LEIR interlock "No extraction to PS" should be taken into account by critical equipments to dump the LEIR beam only when the LEIR destination is PS (PS_DUMP, FTARGET, LHC,...). The LIC CT should be informed to stop the production of LEIR beams for PS.

The PS interlock "Timing Failure" is identical to that shown in the PSB-PS Monitoring section.

6.3. MONITORING OF THE GMT DISTRIBUTION

We saw in the previous section that we monitor the GMT distribution as close as possible to the CTs primarily to verify that the GMT output of the MTT boards works properly.

As a lot of hardware is involved between the GMT source and an end user, we should be able to monitor as close as possible to the client GMT receiver in order to verify the GMT signal quality.

The GMT distribution monitoring may be done :

1. close to the last GMT repeater (one per building)
2. close to the FEC
3. on all critical Timing receiver modules in the FEC

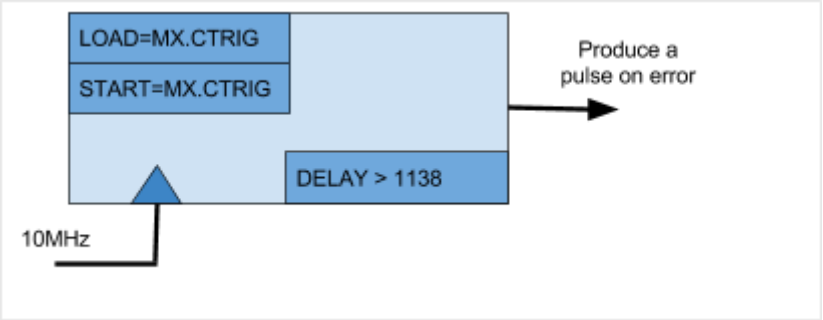
As we saw in the chapter EXPERIENCED FAILURES, section GMT distribution an issue may appear only on one Timing receiver in a given FEC. For this reason we will investigate first the point 3 as a priority.
By critical Timing receiver we mean all cards involved on a critical action that must be

performed by a system. We have to be sure that the Timing receiver will not miss Timing events on the connected GMT cable and will be able to provide Telegram informations, interrupts and output triggers.

6.3.1. GMT ERROR DETECTION USING A TIMING RECEIVER CARD

On each critical Timing receiver card we can program a counter to detect if predictable and recurrent Timing events are missing.
The best candidate is the millisecond event which is sent every millisecond on each GMT cable.

We can program a counter to detect when the millisecond is missing and produce a pulse in this case.



This solution is not expensive as it does not need specific hardware developments. However it does not guarantee detection of sporadically lost events for instance when the quality of the GMT signal is bad but still present.
Furthermore this system will occupy one counter per Timing receiver and the detection will take a little bit more than 1 millisecond.
An alternative - and safer - approach could be to establish a monostable counter. To be investigated.

6.3.2. GMT ERROR DETECTION IMPLYING HARDWARE DEVELOPMENT

A better, but more costly, solution in terms of development would be to embed the detection mechanism in the Timing receiver (VHDL). Like this it could check all Timing frames received including the PLL errors which can indicate a bad GMT reception. The detection will take a little bit more than 125 microseconds in this case.