A CONCEPT TO IMPROVE THE AVAILABILITY OF PETRA III BY CORRELATION OF ALARMS, TIMESTAMPS AND POST-MORTEM-ANALYSIS

M. Werner, DESY, Hamburg, Germany

Abstract

For current and future accelerators, in particular light sources, high availability is an important topic. Therefore the causes of beam losses must be diagnosed and eliminated as fast as possible. This paper presents a concept using the following signals and data from diagnostic instruments and other sources: i) software alarms transmitted by the control system, ii) hardware alarms received and timestamped by the machine protection system, and iii) Post-Mortem-Analysis. By analysing alarm dependencies and the chronological order of alarms, the cause of the problem can be tracked down. The help of diagnostic instruments is highlighted.

INTRODUCTION

A manual alarm analysis in the case of a beam loss can be a time consuming task. In some cases alarms cause an alarm avalanche, by this hiding the initial alarm. In other cases alarms are mutually dependent and the question arises which alarm occurred first. The following ideas could help to solve some of these problems, and it is intended to use some of them in the context of the Machine Protection System for the new PETRA III light source [1].

SOFTWARE ALARMS

Software alarms are transmitted from the hardware to the server for this hardware via a field bus or via Ethernet or the server generates the alarm by itself. The server sends the alarms to a dedicated alarm server and shows the alarms through the control system interface. The time of an alarm can be determined with a precision in the order of 1 second, and the reaction time is also in the order of 1 second. The alarm description can be very specific, e.g. the name of a magnet circuit (out of hundreds of circuits) can be displayed without big effort. Adding new alarms is just a matter of software.

Non-dangerous events which always cause a beam loss

Alarms from these events can be transmitted by software, and there is no need for a precise timestamp to localize the error, because these events do not depend on other events in a difficult way, so they must be the initial cause of a beam loss. Examples:

- Main dipole or quadrupole power supply breakdown
- RF system breakdown (not triggered by beam loss)
- Mains breakdown

HARDWARE ALARMS

Hardware alarms need dedicated cables, therefore they are limited to critical alarms which need a fast reaction time (order of 1ms) and/or a precise timestamp (order of 1us can be achieved).

Dangerous events which must trigger a fast beam dump

Alarms for these events must dump the beam by the use of the machine protection system (MPS) and they should be timestamped. Together with the timestamps of the other alarms, a statement about the initial alarm can be made in many cases. Examples:

- Cavity sparking
- Vacuum shutter closed
- Temperature too high
- Personal interlock broken (e.g. door opened, emergency button pressed)
- Beam Orbit out of limits or critical BPM not working correctly

Non-dangerous events which need a precise timestamp

These events sometimes cause a beam loss. They should not initiate a beam dump. For alarms from these events the cause of the beam loss cannot be clearly assigned, but if the event occurs shortly before a beam loss, there is a high probability that it is the cause of the beam loss. Examples:

- Main dipole or quadrupole power supply spike
- RF spike
- Mains brownout or spike
- Corrector power supply breakdown

There is an overlap to the software alarms (see above), because, for example, the alarm line for a main dipole power spike will also trigger in the case of a main dipole power failure.

COMBINATION OF SOFTWARE AND HARDWARE ALARMS

A combination of software and hardware alarms can be useful for a group of devices such as corrector magnet supplies: the individual names of the faulty channels can be transmitted by software, while an "OR"-combination of all channels add up to a single hardware alarm to provide a precise timestamp of the first alarm in this group.

ALARM DEPENDENCIES

Studying the way how alarms depend on each other can lead to the initial alarm in some cases even if no timestamps are available. If an interlock door has been opened, the main magnets are switched off and an orbit deviation was observed, it is clear that the opening of the door initially caused the beam loss and all other alarms. See Fig. 1 for typical alarm dependencies.

Independent Alarms

If one of these alarms happens, it is easy to assign the cause of the beam loss. Examples:

- Cavity sparking
- Temperature too high
- Personal interlock broken (e.g. door opened, emergency button pressed)

Dependent Alarms

They can happen as a consequence of another event. Examples:

- Bad Orbit (dependent on magnet currents)
- RF breakdown (sometimes dependent on beam current)

Linear Dependencies

In this case the cause of a problem can be traced back and no timing analysis is necessary. If, for instance, during a beam loss a bad orbit was detected and the main dipole power supply is on error, the problem is the power supply in most cases because the power supply can directly influence the orbit but not vice versa.

Circular or Mutual Dependencies

In this case tracing back the cause of an event can lead to the event itself. An example is a beam loss concurrent with an RF breakdown: an RF breakdown always causes a beam loss, but a beam loss can also lead to RF failure. In this case an analysis of the chronological order of the alarms helps.

CHRONOLOGICAL ORDER OF EVENTS

If the analysis of the dependencies does not show the reason of a beam loss because alarms are circular or mutually dependent, the alarm timestamps can provide more information. The first alarm in an alarm sequence can often point to the initial problem. This first alarm can be a dangerous or a not dangerous alarm. Let us consider the example of a corrector magnet failure (not dangerous) leading to an orbit distortion (detected by a BPM) which is dangerous because then a closed undulator can produce intense light at the wrong place and melt components. Although the BPM triggered the beam dump, the corrector magnet can be identified as source of the beam loss because it happened directly before the beam loss. On the other hand, a corrector magnet fault does not always lead to beam loss if the kick offset of the corrector is small enough.

POST MORTEM ANALYSIS

Post mortem data recording can be triggered by a full or partial beam loss or other events. The recording should cover the interesting time range around the loss, this can be from milliseconds (e.g. for BPM data) until seconds (e.g. for temperature data) with adequate time resolution. All recorders for the different devices (RF, power supplies, BPMs and others) should use the same Post Mortem trigger to allow easy time correlation between the different device groups.

Manual or Automatic Analysis

In many cases automatic analysis of Post Mortem data can help to find the cause of a beam loss or at least support an expert in his manual analysis. For example, a scan of the Post Mortem data of all magnet currents or voltages could reveal anomalies shortly before a beam loss.

Combining Several Data Channels

Useful information can be taken from the BPM Post Mortem data. The evolution of the RMS orbit deviation compared to a reference orbit (taken from the first samples of the Post Mortem data) in both directions can be calculated as well as the evolution of the position sum (trace length) in the horizontal direction. If the sum is constant but the RMS value increases directly before the beam loss, this points to beam instability. If, on the other hand, the sum changes, an RF problem is more likely, because the sum is correlated to the beam energy.

Consistency Checks

Another interesting possibility is the combination of Post Mortem data of BPMs with fast and/or slow orbit corrector magnet currents, using the Orbit Response Matrix (ORM). An inconsistency can directly point to a bad BPM or corrector magnet and help in troubleshooting the orbit feedback system.

AUTOMATICAL ALARM ANALYSIS

Regarding the event dependencies in an accelerator, an automatic analysis of software alarms and the chronological order of hardware alarms can point to the initial cause of a beam loss. For more difficult cases, also Post Mortem data can be automatically analyzed to give concentrated information to the operator. If the source of a beam loss is still unclear, a manual analysis by an expert is necessary, whereas the timestamps and the Post Mortem data are still very helpful.

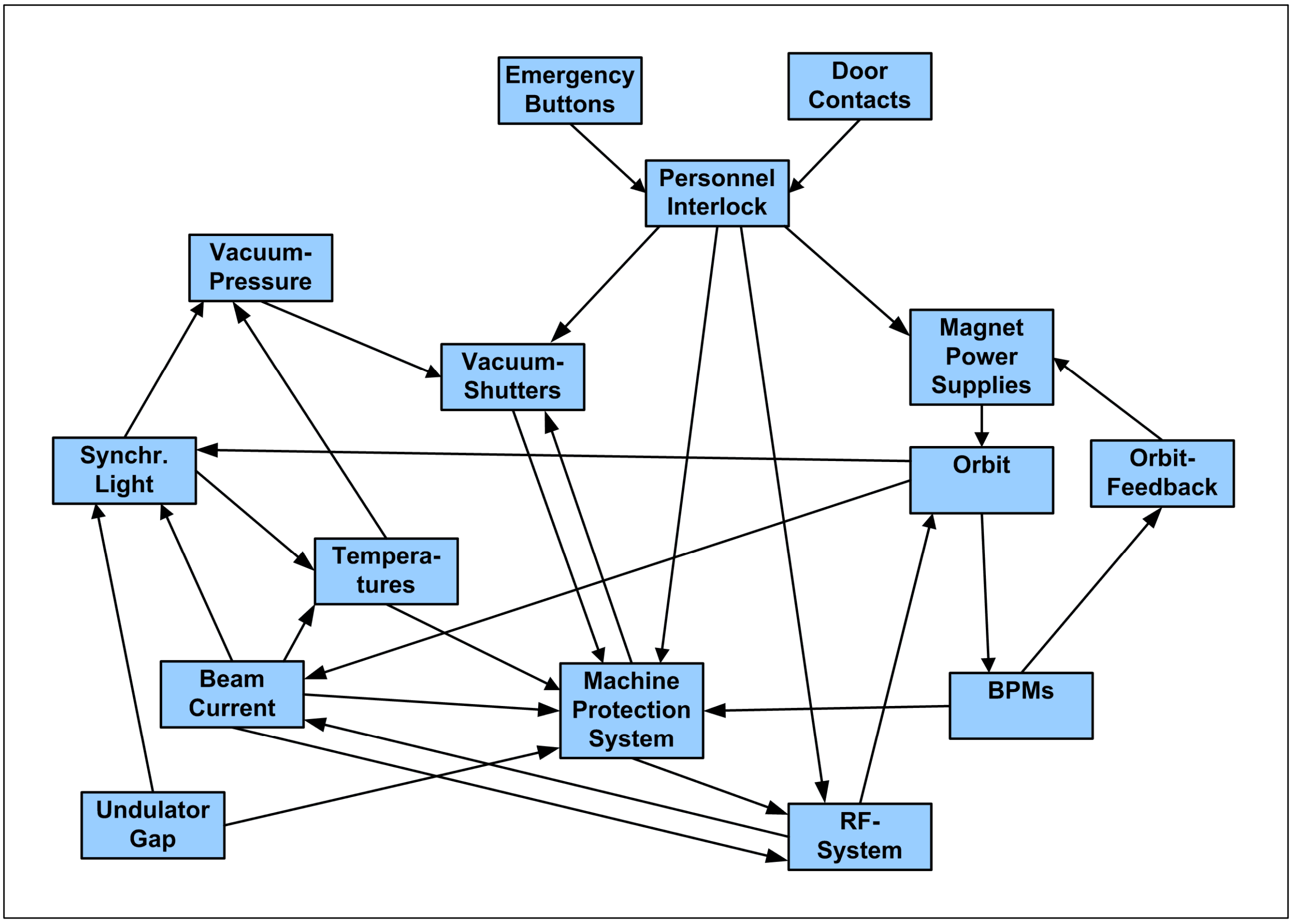

Figure 1: Alarm dependencies. The arrows show in which direction alarms or states influence other alarms and states in the PETRA III light source.

THE BENEFIT OF WARNINGS

Some beam losses can be avoided by observing critical parameters and reacting in time. A software warning system can do this observation automatically and give an acoustical or optical signal to the operator. Examples:

- Beam near position limits (BPM interlock)
- Quadrupole sum of BPM buttons close to limits
- Sum of BPM buttons close to limits (consistency with beam current monitors)
- Vacuum pressure close to limits
- Magnet current close to limit (slow or fast corrector magnets)
- Temperature near limit

CONCLUSION

Ideas and methods were presented to increase the availability of a typical light source by fast automatic or computer-aided manual analysis of beam losses, thereby shortening the downtime. The important role of BPMs in this analysis was shown.

REFERENCES

[1] T. Lensch and M. Werner, "Machine Protection System for PETRA III", these proceedings.