A so-called Eight Disciplines (8D) process has been implemented by MXL to specifically address accelerator trip events leading to **unscheduled down time of 4 hours or more**. An accelerator fault where recovery exceeds 4 hours will now trigger the 8D process. The process should ideally begin **within seven days** of the event.

- **D1**: Cross functional Team is mandatory to increase efficiency of problem solving
- **D2**: Document the fault **description and event chronology** from the trip to recovery of user operations, including the **repair and recovery** steps that were made
- **D3**: Interim containment actions reduces the effects of the fault to the accelerator
- **D4**: Identify the **Root Cause of the failure**, and if necessary the root causes of any **Excessive Recovery Time**.
- **D5**: Define specific **Action Items** to mitigate the identified failure mode.
- **D6**: Prepare an **Implementation Plan**, including milestones and clear deliverables.
- **D7**: Develop a formal mechanism for **Closing Out** the identified actions and possibly preparing for future preventive measures.
- **D8**: Close out is to clean up. Update documentation, report to management, withdraw Interim containment actions.

Notes:
For smaller events or simple failure pattern you can also use the 8D template in a reduced form, as an 4D-process. To do so just skip D1, D6, D7 and D8. However, a precise 4D-process can always upgrated to a fully 8D, if there any need.

Terms and definitions

Trip, Fault or Event	A failure at some recorded point in time (time stamped) of some sub-system which puts the accelerator into a **down state**.
Time to System Repair (TTSRep)	The length of time needed to identify the problem (operationally) and repair the faulted sub-system.
Time to System Recovery (TTSRec)	Time to recovery the faulted sub-system after its repair.

Issued: Nicholas Walker | 2019-04-03	Revised | Checked: Siegfried Köpke | 2019-12-12	Version: 2.0 | 07.01.2020

1 / 7

Time to Beam Recovery (TTBR)	Time needed to recovery user operations after the faulted sub-system(s) is (are) designated recovered and fully operational.
Excessive Recovery Time (ERT)	Recovery time (any of above) which in this case was considered excessive or unusually long.
Operations Package (OP)	The operations package(s) involved or interfaced to the event.
OP Representative (OPR)	Team Member representing a specific OP. Usually considered as a "Systems Expert" for that domain.
Run Coordinator (RC)	XFEL Run coordinator; specifically, one (or possibly both) of the RCs that were on duty during the Event.
Knowledgeable or Key Systems Expert (KSE)	A Team Member who is considered a key expert in one or more of the sub-systems involved in the Event.
Interim Containment Action	A interim measure or workaround that was taken in order to recover the machine during the Event.
Permanent Correction Action (PCA)	A repair or other action that is considered a permanent (or at least longer term) solution to an identified root cause for the Event.
Event Template Report or Template Report	Used to refer to the formal XFEL 8D Report template, which is the primary documentation for the process.

Process notes and guidelines

- Physical **team meetings** are a mandatory part of this 8D process. However, the number and frequency of the meetings is at the discretion of the Team Leader and should be agreed via consensus with the Team.
- The only constraint is that there should be **at least one meeting** and that this first meeting should happen **within 7 days of the Event**.
- The **Template Report** is the primary document recording the outcome of the process, until it is formally closed. However more detailed documents, presentations, analyses etc. can be appended to the document as needed, although the core results of these additional documents should be summarized in the relevant D sections of the Template Report.

Issued: Nicholas Walker | 2019-04-03	Revised | Checked: Siegfried Köpke | 2019-12-12	Version: 2.0 | 07.01.2020

Preparation for 8D and overview

- Identification of Team Lead, who should then do the following:
- Generate a new Report Number and add event to XFEL 8D Event Register.
- Prepare new Report Template.
- Become familiar with scope of the Event (early discussions with key individuals)
- Prepare the scope of Event Report, e. g.:
    - o Is the scope just the technical systems failure?
    - o Should ERT be considered and included?
    - o Are there procedural/policy issues that should be included?
- Prepare list of experts (OPs, KSE, …) that should be included in the Team

D1: Form the Team (responsibility: Team Leader)

- Formally identify and invite Team Members to first meeting.
- Identify Roles and Responsibility of each Team Member.
- Clearly define (to Team) the scope of the Event Report.
- Distribute prepared 8D template report to the Team to prepare the meeting.

Notes:
The size of the Team depends on the scope of the event and is a judgment call of the Team Leader. However, a good guideline is only one representative for each identified OP acting as a KSE for that domain. At least **one of the acting RC***s should be a mandatory member of the Team.*

D2: Fault description, Event chronology

I. e. What happened in the control room (as seen from the operations perspective):

- Key event steps (with time stamps) from Fault to Beam Recovery.
- Capture key escalation points as well as 'time stamps' for TTSRep, TTSRec, TTBR.
- Identify by name people involved (and their role).

Issued: Nicholas Walker | 2019-04-03	Revised | Checked: Siegfried Köpke | 2019-12-12	Version: 2.0 | 07.01.2020

- Record initial (operator) fault diagnosis, even though this may ultimately not be the true root cause.
- Has this fault occurred before? If so provide references / links.
- Attempt to be comprehensive but avoid too much detail.
- Should set the scope for the remaining discussions.

Notes:
Do not include details of the repairs or other technical measures (that's the next D).
If the scope of the report includes ERT, then it is important to document here as best as possible where the time was lost.

D3: Interim Containment Action(s)

- List actions that were taken during the event to enable recovery.
- Information should include:
  - o Short description of the technical activity, including rationale.
  - o Responsible group/person
  - o Is this action a TCA? And if so what are the consequences and possible risks?

Notes:
Where D2 gives history of the events, D3 provides the specific technical solutions that were made at the time in order to recover the machine. If decisions were needed between alternative approaches that should also be captured here. If the repair or action was considered a workaround (TCA) then this probably needs more explanation, including justifying arguments, whether or not the action left the machine operation compromised in some fashion, and some qualitative assessment of remaining risk.

D4: Root Cause Analysis

- Perform an RCA and document the identified root cause failure in this section.
- Include how the fault manifested itself and what the results were (chain of events).
- If considering ERT, then the additional 'root causes' of failures may be required to be documented in separate sections, and their impact on the recovery time described.

Notes:

In principle the RCA should be part of the Team's mandate but often one or more KSE will come with an existing RCA made within their respective group. These can be reviewed in the meeting and summarized in the template report. An important part of 8D is to establish a consensus across all team members (generally representing the stakeholders) so these results should still be presented and discussed within the Team.

When considering ERT, it can be that recovery was strongly hindered by other possibly unrelated sub-system faults. If this is the case, then these should be captured in this section.

In general, ERT has a strong element of policy failure (procedural, escalation etc.) which is often independent of the identified technical root cause. Such issues should be captured under a clearly-marked sub-heading.

D5: Developing Permanent Corrective Actions (PCA)

- Discuss actions that can lead to more robust solutions to the identified root causes.
- In particular, clearly identify 'final fixes' to any TCA that were applied during the Event recovery.
  Options should be tabled, and their efficacy, scope and risk should be evaluated.
- Final outcome should be approval of preferred PCA and an associated action plan.

Notes:
Where D4 identified the root causes of the Event, D5 attempts to identify the relatively near-term concrete measures that can be done to mitigate the risks. Where there is more than one possible approach, Pros and Cons should be considered. If there is no clear or obvious mitigation measure, then studies should be identified to gain more data on the fault.

One important aspect here is to clearly identify actionable items – i. e. clearly defined actions that can be accomplished and have an unambiguous deliverable and measure of success.

Issued: Nicholas Walker | 2019-04-03	Revised | Checked: Siegfried Köpke | 2019-12-12	Version: 2.0 | 07.01.2020

5 / 7

As with the RCA in D4, the activities in D5 should in principle be a Team effort but often technical group representatives will come with proposals. Again, these should be presented and reviewed, and finally (if accepted) summarized in the Report Template.

If procedural/policy aspects are considered (e. g. ERT), then these should be documented separately under a sub-heading.

D6: Implementation plan for the PCA

Where D5 describes the scope and rationale behind the choice of PCA, D6 provides the plan for implementing them. This is nothing more than project management good practice, but this section is important as it provides the formal mechanism for follow-up to make sure all action items and deliverables have been successfully achieved (or not). For each identified action (work) required to implement a PCA, the following should be captured:

- Description of the work
- Who is responsible (Team member)?
- When will it get done (follow-up date)?
- What resources does it require?
- What additional support from other groups is required?
- What other interfaces should be considered (risk management)?
- What are the validation steps and control measures?

Notes:
*In the case of more open-ended item, such as an ongoing study or the possible development of a procedure, then a **review date** should be set.*

Again procedural/policy (documentation) items should be clearly separated from the more technical works using a sub-heading.

D7: Preventive measures (or other future directions)

This section may not always be needed given the scope of the corrective measures agreed upon in D4-6. However, it is important to consider the following:

Issued: Nicholas Walker | 2019-04-03	Revised | Checked: Siegfried Köpke | 2019-12-12	Version: 2.0 | 07.01.2020

6 / 7

- Has the process emphasized or brought to light other risks which are not entirely mitigated by the PCA?
- What might be a course of action to possibly lower risk solutions in the future?
- Are there procedural / administrative aspects that we should put in place to specifically monitor the remaining risk items?
- Are other sub-systems at risk from similar failure modes?
- Are there general "lessons learned" from this process which could benefit some further consideration to generally improve the situation?

Notes:
This is a general 'catch all' for ideas and concepts that have arisen from the process that potentially do not (yet) lend themselves to concrete actions which will be implemented. Some of these ideas may get taken up and pursued in parallel to the more mainstream (and mandatory) actions.

D8: Close out

- The Team leader should close-out this Event Report when all the agreed quantifiable measures outlined in D6 are complete.
- The Final Report should be filed and disseminated to all stakeholders by the MXL Coordinator, who then formally thanks the Team members for their service and formally disbands the Team.

Notes:
Exactly when a report is considered finally closed is the discretion of the Team Leader. How easy it is to do this will reflect on how well the milestones and deliverables have been specified by the Team in D6.
Less concrete actions (such as longer-duration studies and policy and procedural issue requiring more time), should in general not keep the report (and the Team!) open.

Issued: Nicholas Walker | 2019-04-03	Revised | Checked: Siegfried Köpke | 2019-12-12	Version: 2.0 | 07.01.2020

7 / 7