OP view on handling Machine Protection issues

Giulia Papotti

outline

- failure catalogue
  - failures that only experts can detect
  - failures that shift crews can detect
    - after beam dump or with beam still in
  - dumps that could have been avoided

- plenty of examples
  - from 2012 unless otherwise noted
- possible improvements
  - procedures?
  - interlocks?
- some open questions
- some will be addressed later in this workshop

what is an MP issue?

- unpleasant surprise
  - negative connotation!

what is an MP issue?

- unpleasant surprise
  - negative connotation!

- the machine could be in an unsafe state
  - when MP systems do not respond as foreseen
  - often situation that is not covered by interlocks

what is an MP issue?

- unpleasant surprise
  - negative connotation!

- the machine could be in an unsafe state
  - when MP systems do not respond as foreseen
  - often situation that is not covered by interlocks

- next steps might be unclear
  - not thought of, not happened before
  - by definition not covered by procedures
    - exception: "in case dump does not trigger"
  - left to shift crew's experience, feeling, intuition
    - sometimes need to sit and think
    - some other times need to act promptly

system failures

- one failure is generally not an issue
  - e.g. late PIC interlock
    - e.g. IT, LHCb dipole, 60A CODs
  - lose redundancy, but at worst detected by losses
    - BLM/QPS are the last lines of defence
    - BLMs are redundant themselves (3 BLMs per quad)

system failures

- one failure is generally not an issue
  - e.g. late PIC interlock
    - e.g. IT, LHCb dipole, 60A CODs
  - lose redundancy, but at worst detected by losses
    - BLM/QPS are the last lines of defence
    - BLMs are redundant themselves (3 BLMs per quad)

- combined failures are the worry
  - e.g. collimators in wrong position + asynch dump
  - e.g. SIS orbit interlock masked by mistake + orbit excursion (+ asynch dump)

system failures

- one failure is generally not an issue
  - e.g. late PIC interlock
    - e.g. IT, LHCb dipole, 60A CODs
  - lose redundancy, but at worst detected by losses
    - BLM/QPS are the last lines of defence
    - BLMs are redundant themselves (3 BLMs per quad)

- combined failures are the worry
  - e.g. collimators in wrong position + asynch dump
  - e.g. SIS orbit interlock masked by mistake + orbit excursion (+ asynch dump)

- thus: if one system is known to be weak, remove beam and fix it before another one fails
  - minimize the time to try your luck!

system failures

- one failure is generally not an issue
  - e.g. late PIC interlock
    - e.g. IT, LHCb dipole, 60A CODs
  - lose redundancy, but at worst detected by losses
    - BLM/QPS are the last lines of defence
    - BLMs are redundant themselves (3 BLMs per quad)

- combined failures are the worry
  - e.g. collimators in wrong position + asynch dump
  - e.g. SIS orbit interlock masked by mistake + orbit excursion (+ asynch dump)

- thus: if one system is known to be weak, remove beam and fix it before another one fails
  - minimize the time to try your luck!
  - but, in few exceptional cases, better not dump?

failure catalogue

- failures that only experts can detect (1)

- failures that shift crews can detect
  - after beam dump (2)
  - with beam still in (3)

- dumps that could have been avoided (4)

failure catalogue

- failures that only experts can detect (1)

- failures that shift crews can detect
  - after beam dump (2)

  - with beam still in (3)

- dumps that could have been avoided (4)

failure catalogue

- failures that only experts can detect (1)

- failures that shift crews can detect
  - after beam dump (2)

  - with beam still in (3)

- dumps that could have been avoided (4)

failure catalogue

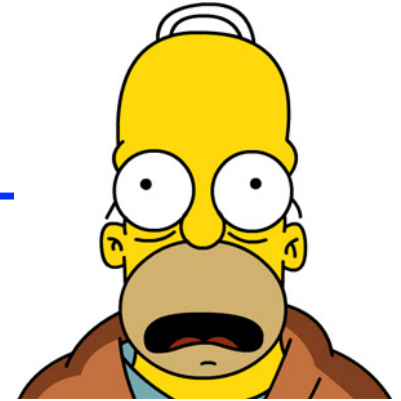- failures that only experts can detect (1)

- failures that shift crews can detect
  - after beam dump (2)
  - with beam still in (3)

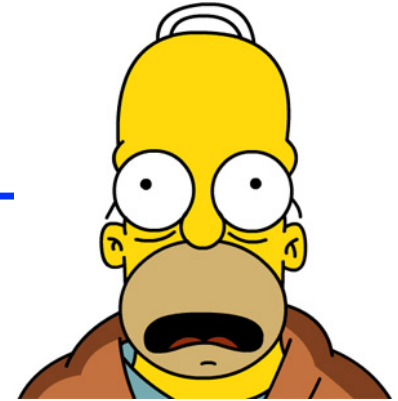- dumps that could have been avoided (4)

category -1-

- failures that only experts can detect
  - major events!
    - e.g. no dump scenario (LBDS 12V supply failure)
    - e.g. wrong transfer line collimator settings (Q20 vs Q26, max offset 1.3σ)
    - e.g. incorrect ring collimators settings
    - e.g. interrupted BLM HV cable (2011)
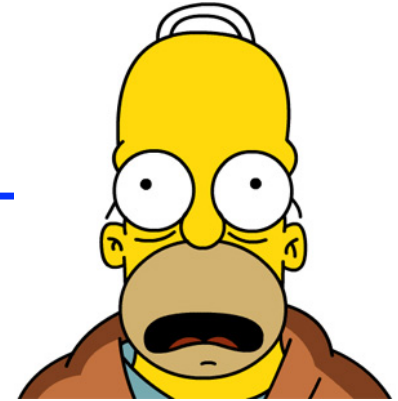
category -1-

- failures that only experts can detect
  - major events!
    - e.g. no dump scenario (LBDS 12V supply failure)
    - e.g. wrong transfer line collimator settings (Q20 vs Q26, max offset 1.3σ)
    - e.g. incorrect ring collimators settings
    - e.g. interrupted BLM HV cable (2011)
  - experts require to stop
  - experts give the ok to restart
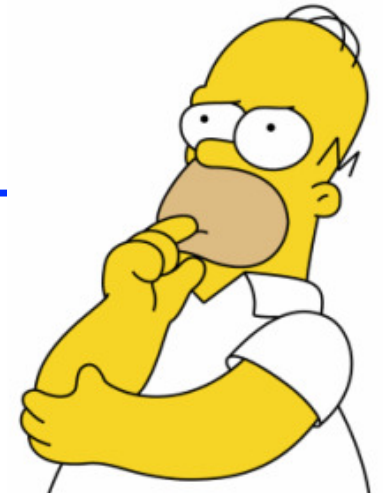
category -1-

- failures that only experts can detect
  - major events!
    - e.g. no dump scenario (LBDS 12V supply failure)
    - e.g. wrong transfer line collimator settings (Q20 vs Q26, max offset 1.3σ)
    - e.g. incorrect ring collimators settings
    - e.g. interrupted BLM HV cable (2011)
  - experts require to stop
  - experts give the ok to restart

  - not much in the hands of OP
    - would not have been detected by shift crews!
  - hopefully this type does not come too often…

category -2-

- failures that shift crews can detect, after dump
  - anomalous situation led to beam dump
    - e.g. RQX trip caught by BLMs and not by PIC
    - e.g. MKI flashover
    - e.g. lack of SPS-LHC synchronization
      - e.g. SPS on local or timing issue (beam in TI2 but MKI8 pulse)
      - M. Zerlauth, Evian 2010: "Beam dumps above injection are rigorously analyzed, we can do better at injection (avoiding repetitive tries without identifying the cause)"
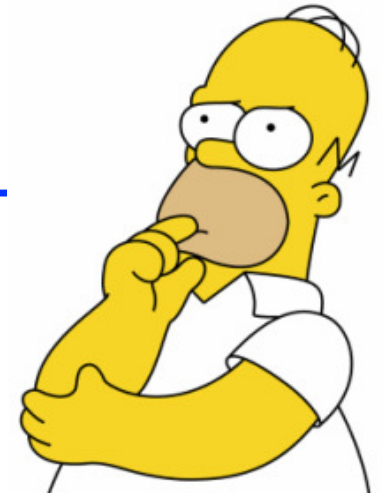
category -2-

- failures that shift crews can detect, after dump
  - anomalous situation led to beam dump
    - e.g. RQX trip caught by BLMs and not by PIC
    - e.g. MKI flashover
    - e.g. lack of SPS-LHC synchronization
      - e.g. SPS on local or timing issue (beam in TI2 but MKI8 pulse)
      - M. Zerlauth, Evian 2010: "Beam dumps above injection are rigorously analyzed, we can do better at injection (avoiding repetitive tries without identifying the cause)"
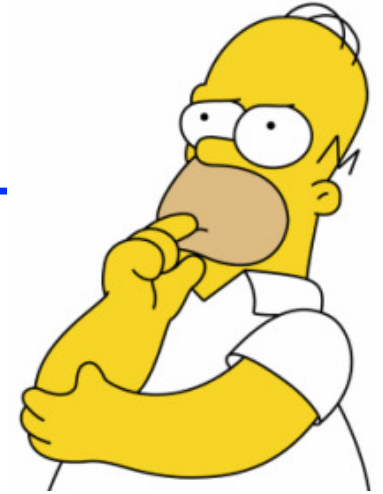 - need shift crews or even system experts to think how to carry on

category -2-

- failures that shift crews can detect, after dump
  - anomalous situation led to beam dump
    - e.g. RQX trip caught by BLMs and not by PIC
    - e.g. MKI flashover
    - e.g. lack of SPS-LHC synchronization
      - e.g. SPS on local or timing issue (beam in TI2 but MKI8 pulse)
      - M. Zerlauth, Evian 2010: "Beam dumps above injection are rigorously analyzed, we can do better at injection (avoiding repetitive tries without identifying the cause)"
  - need shift crews or even system experts to think how to carry on
  - can software tools help catch some?
    - some basic checks in PM expert acknowledge
      - FMCM IPOC, PIC IPOC, BIC IPOC
    - can more checks be added? e.g. to PM analysis?
      - e.g. collimator hierarchy module? redundancy checks? power loss module to recognize losses higher than normal?

category -3-

- failures that shift crews can detect, beam still in
  - could be a case of missing interlock, if first occurrence
  - shift crew to decide whether to dump or not manually

category -3-

- failures that shift crews can detect, beam still in
  - could be a case of missing interlock, if first occurrence
  - shift crew to decide whether to dump or not manually
    - e.g. RF feedback crate down
      - similar interlocks exist to avoid excessive load on collector
        » to be added to RF interlocks?
      - manual dump in agreement with piquet, not time critical

category -3-

- failures that shift crews can detect, beam still in
  - could be a case of missing interlock, if first occurrence
  - shift crew to decide whether to dump or not manually
    - e.g. RF feedback crate down
      - similar interlocks exist to avoid excessive load on collector
        » to be added to RF interlocks?
      - manual dump in agreement with piquet, not time critical
    - e.g. ramp with no BPM data (2011)
      - no control on orbit, no OFB corrections
      - prompt dump by shift crew, time critical
      - now covered in SIS

category -3-

- failures that shift crews can detect, beam still in
  - could be a case of missing interlock, if first occurrence
  - shift crew to decide whether to dump or not manually
    - e.g. RF feedback crate down
      - similar interlocks exist to avoid excessive load on collector
        » to be added to RF interlocks?
      - manual dump in agreement with piquet, not time critical
    - e.g. ramp with no BPM data (2011)
      - no control on orbit, no OFB corrections
      - prompt dump by shift crew, time critical
      - now covered in SIS
    - e.g. collimators not moving during collision beam process
      - did not respond to timing event; gap ok, but wrong centre
      - state machine change to stable beams is prevented, otherwise not protected
      - could be covered by TCTs with BPMs
      - suggested recipe: "if collimators in wrong position and no weird orbit excursion in IR6, dump asap"

the shift crew's choice

- trade-off: Machine Protection vs efficiency
  - be cautious: better to lose 3 hours than 3 months
    - 2011 yearly target as defined by M. Lamont at LMC: "don't break it"
  - define clearer guidelines, at least for after LS1 start-up
    - e.g. just suggested: "if collimators in wrong position, dump"

the shift crew's choice

- trade-off: Machine Protection vs efficiency
  - be cautious: better to lose 3 hours than 3 months
    - 2011 yearly target as defined by M. Lamont at LMC: "don't break it"
  - define clearer guidelines, at least for after LS1 start-up
    - e.g. just suggested: "if collimators in wrong position, dump"

- for the shift crews
  - do we too easily put off dumping manually in case of issues?
    - are we the LHC cowboys?

the shift crew's choice

- trade-off: Machine Protection vs efficiency
  - be cautious: better to lose 3 hours than 3 months
    - 2011 yearly target as defined by M. Lamont at LMC: "don't break it"
  - define clearer guidelines, at least for after LS1 start-up
    - e.g. just suggested: "if collimators in wrong position, dump"
- for the shift crews
  - do we too easily put off dumping manually in case of issues?
    - are we the LHC cowboys?
  - sometimes human checks + manual dump became the short term procedure
    - e.g. TCDQ not moving for ramp (2010)
    - e.g. abort gap monitoring missing due to BSRT mirror failure

the shift crew's choice

- trade-off: Machine Protection vs efficiency
  - be cautious: better to lose 3 hours than 3 months
    - 2011 yearly target as defined by M. Lamont at LMC: "don't break it"
  - define clearer guidelines, at least for after LS1 start-up
    - e.g. just suggested: "if collimators in wrong position, dump"
- for the shift crews
  - do we too easily put off dumping manually in case of issues?
    - are we the LHC cowboys?
  - sometimes human checks + manual dump became the short term procedure
    - e.g. TCDQ not moving for ramp (2010)
    - e.g. abort gap monitoring missing due to BSRT mirror failure
- for the coordinators (MCs, LPCs, …)
  - will you be supportive? or will you regret the "lost efficiency"?

no!
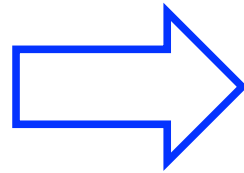
if needed!

build on experience

- many interlocks patched situations that happened before
  - a hole found once, a bug found once, a mistake done once
    - e.g. BLM HV (2011)
    - e.g. zeroed OFB reference during squeeze
    - e.g. incorrect strength settings on mains (2010)

build on experience

- many interlocks patched situations that happened before
  - a hole found once, a bug found once, a mistake done once
    - e.g. BLM HV (2011)
    - e.g. zeroed OFB reference during squeeze
    - e.g. incorrect strength settings on mains (2010)
  - the Software Interlock provides the flexibility
    - now partly based on experience

build on experience

- many interlocks patched situations that happened before
  - a hole found once, a bug found once, a mistake done once
    - e.g. BLM HV (2011)
    - e.g. zeroed OFB reference during squeeze
    - e.g. incorrect strength settings on mains (2010)
  - the Software Interlock provides the flexibility
    - now partly based on experience

- but doubtful we have found all so far!
  - to shift crews: be vigilant!
    - A. MacPherson, Evian 2010, "Vigilance + Experience: Shift crews can react when things don't look right"

build on experience

- many interlocks patched situations that happened before
  - a hole found once, a bug found once, a mistake done once
    - e.g. BLM HV (2011)
    - e.g. zeroed OFB reference during squeeze
    - e.g. incorrect strength settings on mains (2010)
  - the Software Interlock provides the flexibility
    - now partly based on experience

- but doubtful we have found all so far!
  - to shift crews: be vigilant!
    - A. MacPherson, Evian 2010, "Vigilance + Experience: Shift crews can react when things don't look right"

- how to help the crews detect abnormal situations?
  - e.g. BLMs per beam mode, how should they look?
  - e.g. collimators per family and per mode, where should they be?
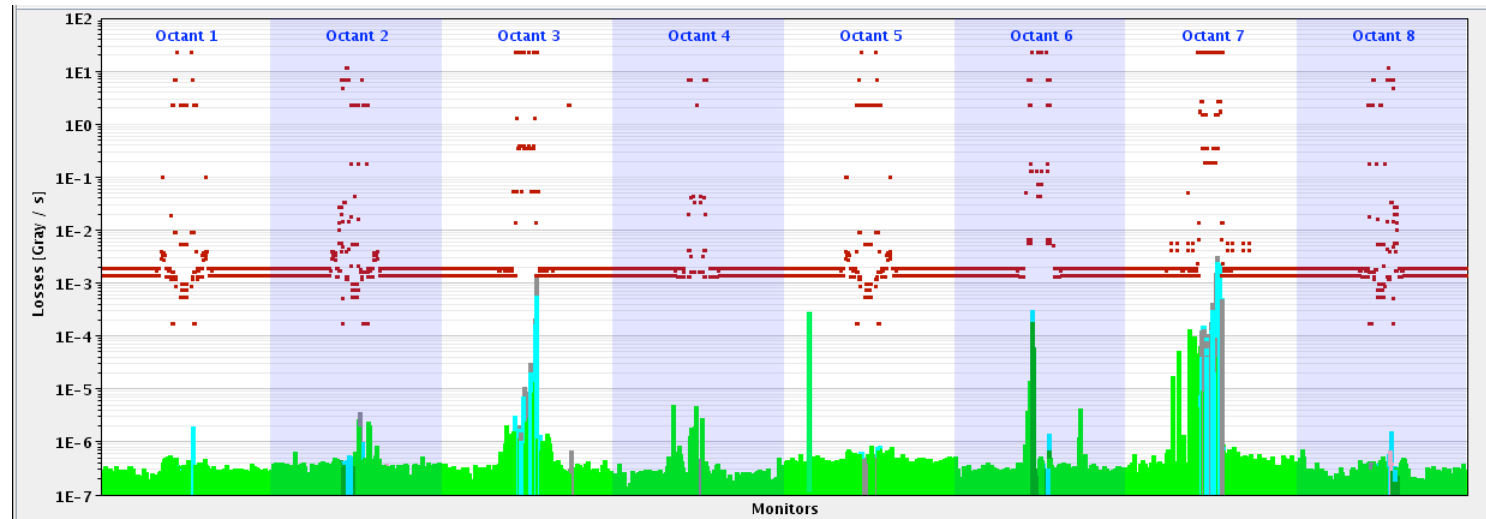
"abnormal"

"abnormal"
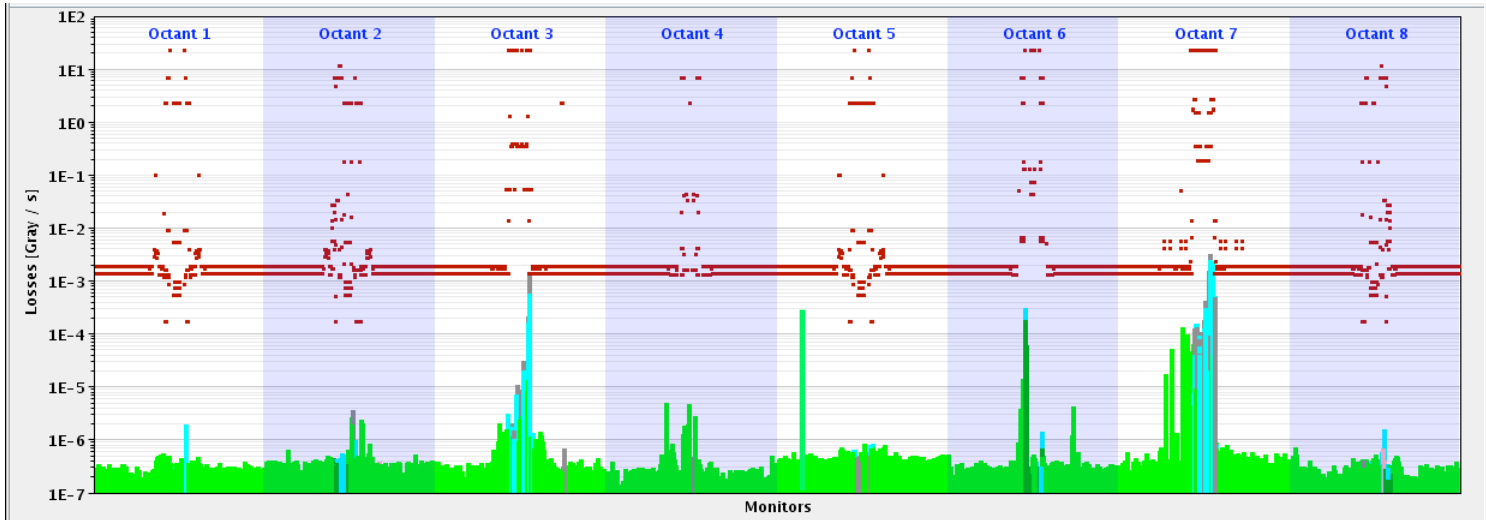
"abnormal"

DO NOT USE THIS BEAM!
- A B N O R M A L -

category -4-

- dumps that could have been avoided
  - machine safety not in danger, but time lost

category -4-

- dumps that could have been avoided
  - machine safety not in danger, but time lost

  - avoid interlocks that kick in for the "wrong" reason
    - e.g. dumps at Setup Beam Flag crossing during MDs as TCTs not setup for collisions at injection
    - e.g. dumps for 6σ VdM scans during 1.38 TeV run
    - e.g. IR6 BPMs on low intensity bunches

category -4-

- dumps that could have been avoided
  - machine safety not in danger, but time lost

  - avoid interlocks that kick in for the "wrong" reason
    - e.g. dumps at Setup Beam Flag crossing during MDs as TCTs not setup for collisions at injection
    - e.g. dumps for 6σ VdM scans during 1.38 TeV run
    - e.g. IR6 BPMs on low intensity bunches

  - improve efficiency by improving procedures
    - for special runs and MDs
    - at transition with nominal operation not to forget masks, different settings, …

settings and masks handling

- BIS masking automatically cleaned up with intensity
  - extra masks impair efficiency more than safety
    - e.g. task that resets all during ramp down?
  - e.g. are AC-dipole keys back in the cupboard?
    - responsibility lies with shift crews (not users), but need to improve procedures for information sharing across shifts

settings and masks handling

- BIS masking automatically cleaned up with intensity
  - extra masks impair efficiency more than safety
    - e.g. task that resets all during ramp down?
  - e.g. are AC-dipole keys back in the cupboard?
    - responsibility lies with shift crews (not users), but need to improve procedures for information sharing across shifts
- SIS masking
  - forgetting to set appropriate masks or interlock settings impaired efficiency for special runs and MDs
    - for nominal operation, mostly cleaned up during commissioning
    - e.g. SIS orbit references for 90 m optics runs
  - forgetting to unmask impacts safety
    - e.g. when going back to nominal operation
  - need to be more thorough, at least with procedures

settings and masks handling

- BIS masking automatically cleaned up with intensity
  - extra masks impair efficiency more than safety
    - e.g. task that resets all during ramp down?
  - e.g. are AC-dipole keys back in the cupboard?
    - responsibility lies with shift crews (not users), but need to improve procedures for information sharing across shifts
- SIS masking
  - forgetting to set appropriate masks or interlock settings impaired efficiency for special runs and MDs
    - for nominal operation, mostly cleaned up during commissioning
    - e.g. SIS orbit references for 90 m optics runs
  - forgetting to unmask impacts safety
    - e.g. when going back to nominal operation
  - need to be more thorough, at least with procedures
- enforce reversion of settings for other systems? how often?
  - e.g. IR6 BPM, BLM MF, collimator settings

procedures procedures procedures

- suggest thorough procedures of special runs and MDs
  - step-by-step plan, settings change list, masks list (if any)
    - helps achieving results, improving efficiency and avoiding misunderstandings
      - minimize surprises and change of plans during machine time
    - helps defining responsibilities and avoids forgetting reversions

procedures procedures procedures

- suggest thorough procedures of special runs and MDs
  - step-by-step plan, settings change list, masks list (if any)
    - helps achieving results, improving efficiency and avoiding misunderstandings
      - minimize surprises and change of plans during machine time
    - helps defining responsibilities and avoids forgetting reversions
  - MP document written for all MD types, A to D
    - need to change our perception: the LHC is not one of our injectors!
      - need procedures, need them well in advance (>2 weeks)
    - e.g. quench tests
      - good: time to discuss as prepared well in advance
      - could still improve: e.g. mask TCSG/TCDQ retraction!

others

- IQC: too many latches
  - D. Jacquet, Evian 2012:
    - "IQC latches almost every injection: are the thresholds correctly set? Can we still afford this with 288 bunches?"
    - "Most of the time we unlatch IQC with no corrective action."

others

- IQC: too many latches
  - D. Jacquet, Evian 2012:
    - "IQC latches almost every injection: are the thresholds correctly set? Can we still afford this with 288 bunches?"
    - "Most of the time we unlatch IQC with no corrective action."
  - if interlock latches or is masked too often, it is useless
    - what is really critical? what is not? risk to be ignored when it should not

others

- IQC: too many latches
    - D. Jacquet, Evian 2012:
        - "IQC latches almost every injection: are the thresholds correctly set? Can we still afford this with 288 bunches?"
        - "Most of the time we unlatch IQC with no corrective action."
    - if interlock latches or is masked too often, it is useless
        - what is really critical? what is not? risk to be ignored when it should not
- LBDS XPOC
    - shift crew can only reset non critical modules
        - e.g. latches from wrong filling pattern, missing fBCT or BLM data … happen very often
    - experts only can reset critical modules (MKD, TSU)

others

- IQC: too many latches
  - D. Jacquet, Evian 2012:
    - "IQC latches almost every injection: are the thresholds correctly set? Can we still afford this with 288 bunches?"
    - "Most of the time we unlatch IQC with no corrective action."
  - if interlock latches or is masked too often, it is useless
    - what is really critical? what is not? risk to be ignored when it should not
- LBDS XPOC
  - shift crew can only reset non critical modules
    - e.g. latches from wrong filling pattern, missing fBCT or BLM data … happen very often
  - experts only can reset critical modules (MKD, TSU)
- MP3 trips
  - "not sure why QPS triggered, but protection worked ok: can carry on, analysis will follow offline"

others

- IQC: too many latches
  - D. Jacquet, Evian 2012:
    - "IQC latches almost every injection: are the thresholds correctly set? Can we still afford this with 288 bunches?"
    - "Most of the time we unlatch IQC with no corrective action."
  - if interlock latches or is masked too often, it is useless
    - what is really critical? what is not? risk to be ignored when it should not
- LBDS XPOC
  - shift crew can only reset non critical modules
    - e.g. latches from wrong filling pattern, missing fBCT or BLM data … happen very often
  - experts only can reset critical modules (MKD, TSU)
- MP3 trips
  - "not sure why QPS triggered, but protection worked ok: can carry on, analysis will follow offline"
  - operation indeed stopped when needed
  - e.g. DFB HTS quench + bad cable connection (2011)
    - lost redundancy: 1 protection left out of 3

open questions

- which other procedures could we devise?
  - better before they are needed on shift!
  - e.g. are there cases in which it is better not to dump?
    - e.g. what if orbit excursion in IR6 is really bad?
    - e.g. what if abort gap population is well above dump thresholds?
      - wait longer? what if it keeps on increasing?
      - scrape or use ADT blow up… but with which settings?

open questions

- which other procedures could we devise?
  - better before they are needed on shift!
  - e.g. are there cases in which it is better not to dump?
    - e.g. what if orbit excursion in IR6 is really bad?
    - e.g. what if abort gap population is well above dump thresholds?
      - wait longer? what if it keeps on increasing?
      - scrape or use ADT blow up… but with which settings?

- are we confident in executing emergency procedures that exist?
  - is it worth training the "in case dump does not trigger" procedure?

open questions

- which other procedures could we devise?
    - better before they are needed on shift!
    - e.g. are there cases in which it is better not to dump?
        - e.g. what if orbit excursion in IR6 is really bad?
        - e.g. what if abort gap population is well above dump thresholds?
            - wait longer? what if it keeps on increasing?
            - scrape or use ADT blow up… but with which settings?

- are we confident in executing emergency procedures that exist?
    - is it worth training the "in case dump does not trigger" procedure?

- can we improve/invent tools to help shift crews notice anomalous situations?
    - e.g. online or in PM analysis

open questions

- which other procedures could we devise?
  - better before they are needed on shift!
  - e.g. are there cases in which it is better not to dump?
    - e.g. what if orbit excursion in IR6 is really bad?
    - e.g. what if abort gap population is well above dump thresholds?
      - wait longer? what if it keeps on increasing?
      - scrape or use ADT blow up… but with which settings?

- are we confident in executing emergency procedures that exist?
  - is it worth training the "in case dump does not trigger" procedure?

- can we improve/invent tools to help shift crews notice anomalous situations?
  - e.g. online or in PM analysis

- should we periodically check that our settings are correct?
  - e.g. IR6 BPMs, BLM MF, collimator settings

conclusions

- MP works remarkably well and is the base for the success of the LHC

- but: catalogue of "MP issues" from 3 years of operation
  - cases of missing interlocks, design faults, weaknesses
  - experience helped strengthening MP systems
    - have we exhausted the information or can we learn more?
  - better procedures and planning can help improve efficiency

- always rely on shift crews to spot abnormal situations and act
  - but try and help them when possible with software and procedures
  - procedures help aligning decisions in stressful situations