Human Risk Factors

Machine Protection Session
Evian 2010
8 December 2010

Based on input from OP

Human Risk factors

- **What is a Human Risk factor, and how can it be mediated?**

  - Other ways to ask this question
    - Can the shift crew damage the machine?
    - What dangerous back doors are open for equipment experts?
    - Should we have strict guidelines for anomalous situations
    - What are the software, database and settings weaknesses.

- What is the goal:
  - **Minimize risks associated with the human component of operation.**

- Our goal - in Risk management speak:
  - **Resilience** – the ability of a system to adjust its functioning to sustain operations during expected conditions and in the face of escalating demands, disturbances, and unforeseen circumstances

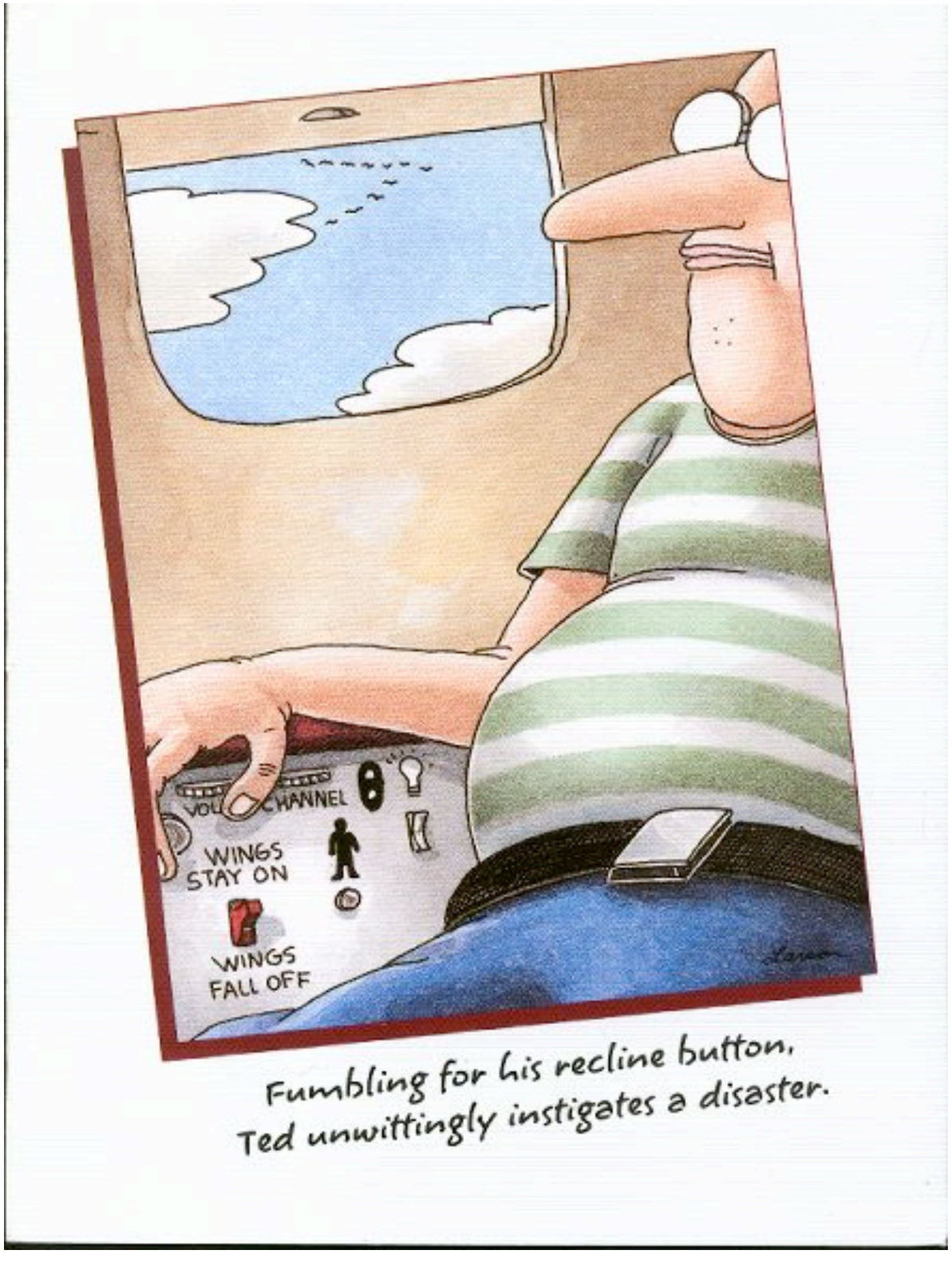
Identifying Human Risk Factors

Human Risk Factors

- Normal Operation
- Non-Standard operation
- Control applications
- Expert interventions
- Alarm storms
- Communication
- Other factors

What can we do to improve

- Understand risk culture
- How to improve - what can we do



Operational Errors: Some examples

- Post Mortems (In last 4 months):
  - ~500 Global Post mortems: 204 were above injection
    - **8 were classified as operational mistakes => 4% level**
      - setting for squeeze had one incorrect point in function ... caused RSF2.A67B2 to trip. Dump was pulled by PIC and was clean
      - SIS latch on TCDQ caused dump of B2 at start of ramp.
      - Active interlocks on masked channels triggering at SBF limit
      - TCDQ was not masked, and then collimators moved
      - Wrong settings on abort gap cleaning during MD
- Others: From the tags in the logbook
  - Switch off S45 by mistake (with machine at injection)
  - Wrong squeeze function played

However ... We know there are more operational errors than this

=> have confidence and support to acknowledge this and then review them

Normal Operation

- Normal Operation: defined in terms of a **Nominal Procedure**
  - **LHC Nominal Sequence** is a **subset** of the **Nominal Procedure**
    - **Automated sequences still require that we think!**

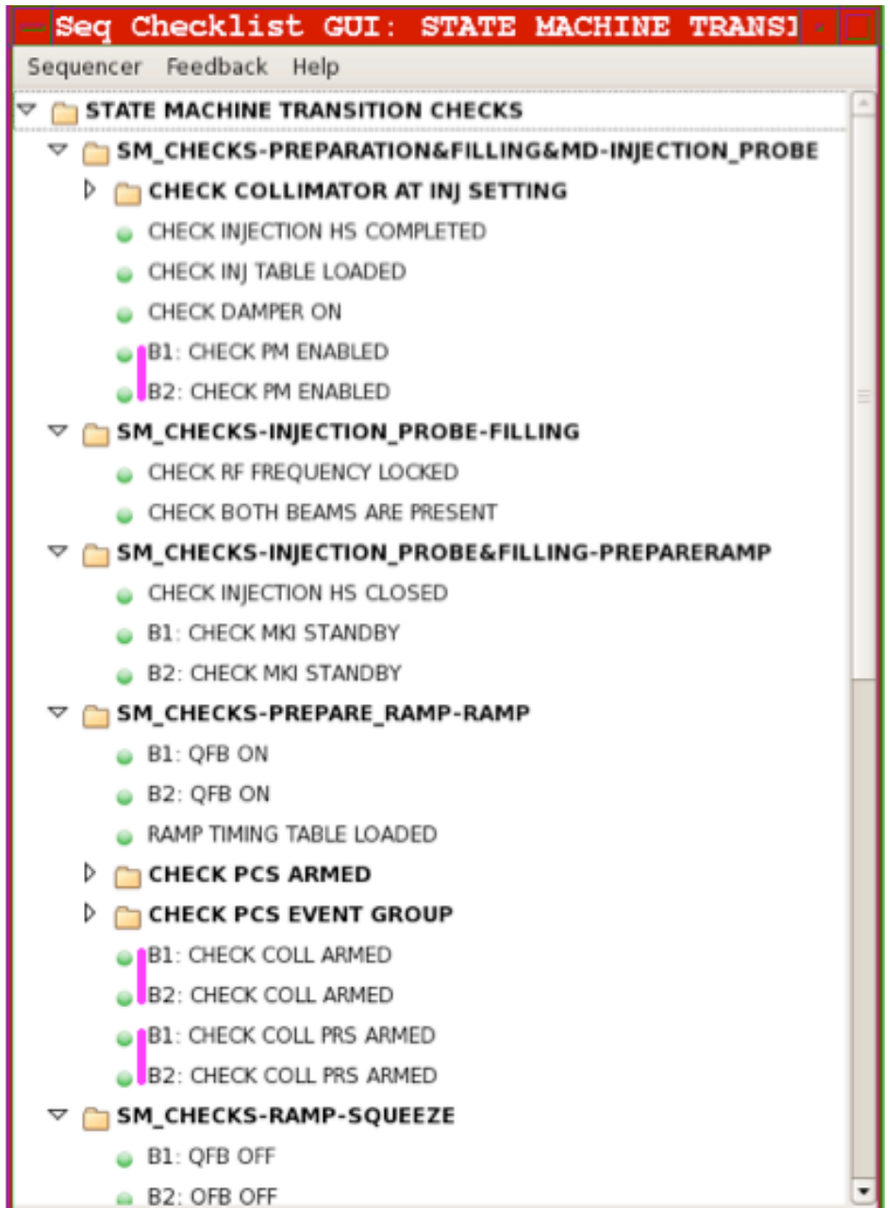
- **Human risk factors with routine operation**
  - **Sequencer**: sequencer can't do everything
    - running through the collision BP with the feedbacks on
  - **Nominal Procedure:** Missing out steps => State Machine + check list
  - **Nominal Procedure:** Not always up-to-date: Responsibility with shift crew
  - **Nominal Sequence**: Always evolving - **big effort to kept it up-to-date**
    - skipped tasks that should be run - this is just confusing
  - **Special Procedures:** Needs clear and persistent documenting

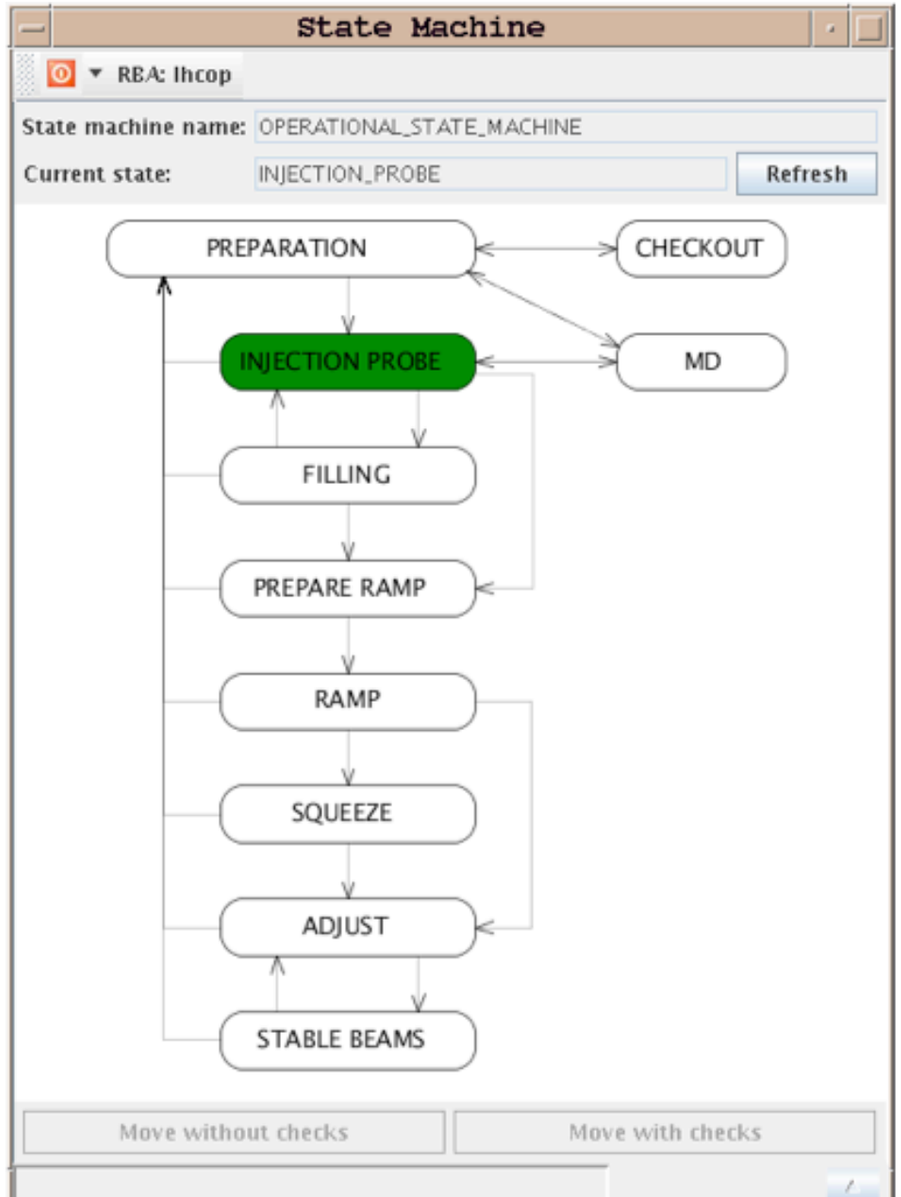
Human Errors - difficult to catch

- **Sending incorrect trim values:** properly define allowed trim envelopes
- **Sending wrong commands:** prompt with confirmation

Normal Operation: State Machine

- New for 2011: Checks all steps in a phase done before transition to next phase
- Based on sequencer check list:
    - Flexibility: tasks can be skipped at discretion of the EiC
- **Concept of allowed tasks:** only runnable when LHC in specific state or mode





Non-standard operation: Where are the risks?

- **Special circumstances:** interim procedures for temporary scenarios
  - **Information needs to be clear, persistent, and available**
    - Bumping around moving RF fingers
    - Loss maps at collision settings
  - **Procedures involving low level actions**
    - Use sensible naming conventions
      - Beam process for Collimator positions

- **Operations: What happens when things are not as expected**
  - **Hardware failures:** Well protected by hardware surveillance => DUMP
  - **Software settings:** Either settings don't load or SIS triggers => DUMP
  - **Operator actions/errors:** Hardest to minimize
    - **Need clear response strategy/decision logic**
      - Operational tools to show implications with 1 orbit corrector missing
    - **Vigilance + Experience:** Shift crews can react when things don't look right
    - **Accountability**: We need to flag errors + review them afterwards

Control applications

Applications and equipment control is an evolving science ... but some problems are of our own making

- Good design and maintenance essential
- No releases/updates in middle of operation

- **Interfaces:**
  - **Distinguish between expert and operations interfaces**
  - **Boy Scout Motto for Experts:** In CCC, **please** leave your apps configured as you found them. If not please explain changes to shift crews

    => avoid operational surprises (Example: Tune viewer, wire scanner)
  - **Ensure "Operator view" is understandable to the operations teams**
    - Make it possible for shift crew to see settings problems from fixed displays
  - **Firmware updates to be advertised and coordinated**
    - no RBAC control over firmware updates during operation
  - GUIs: **Avoid "quick launch button"** type of interfaces for action commands

Experts

- **The LHC depends on its experts**

  ... but we sometimes have to avoid being too clever

  - IT security scan crashed Orbit Feedback Controller with beam in the machine
  - ACCSOFT passwd change blocked RBAC server => no new RBAC connections
  - OASIS to monitor at 50 Hz caused logging outage
    - No logging = breach of machine protection

Some things that would help

- **Monitoring system settings:** Improve Cycling Redundancy Checks (a la PIC)
- **Communicate & Coordinate** any action with the shift crew **prior to starting**

  ... this even applies to 100% “transparent” interventions

  - Un-advertised testing of BGI from SPS Island during a ramp =>beam dump
- **Hard coded parameters under expert control:**
  - **Expert team responsibility**. Cross check implications
    - Changing thresholds on inputs to Beam presence flags

Communication & Coordination

Communication and Coordination = the single most effective way of reducing human risk factors

- **Operations:**
  - EiC and Operators must have a mutual confidence in each others ability
  - Time must be taken for proper shift handovers
  - Decisions from 8:30 meeting must be conveyed to the shift crew

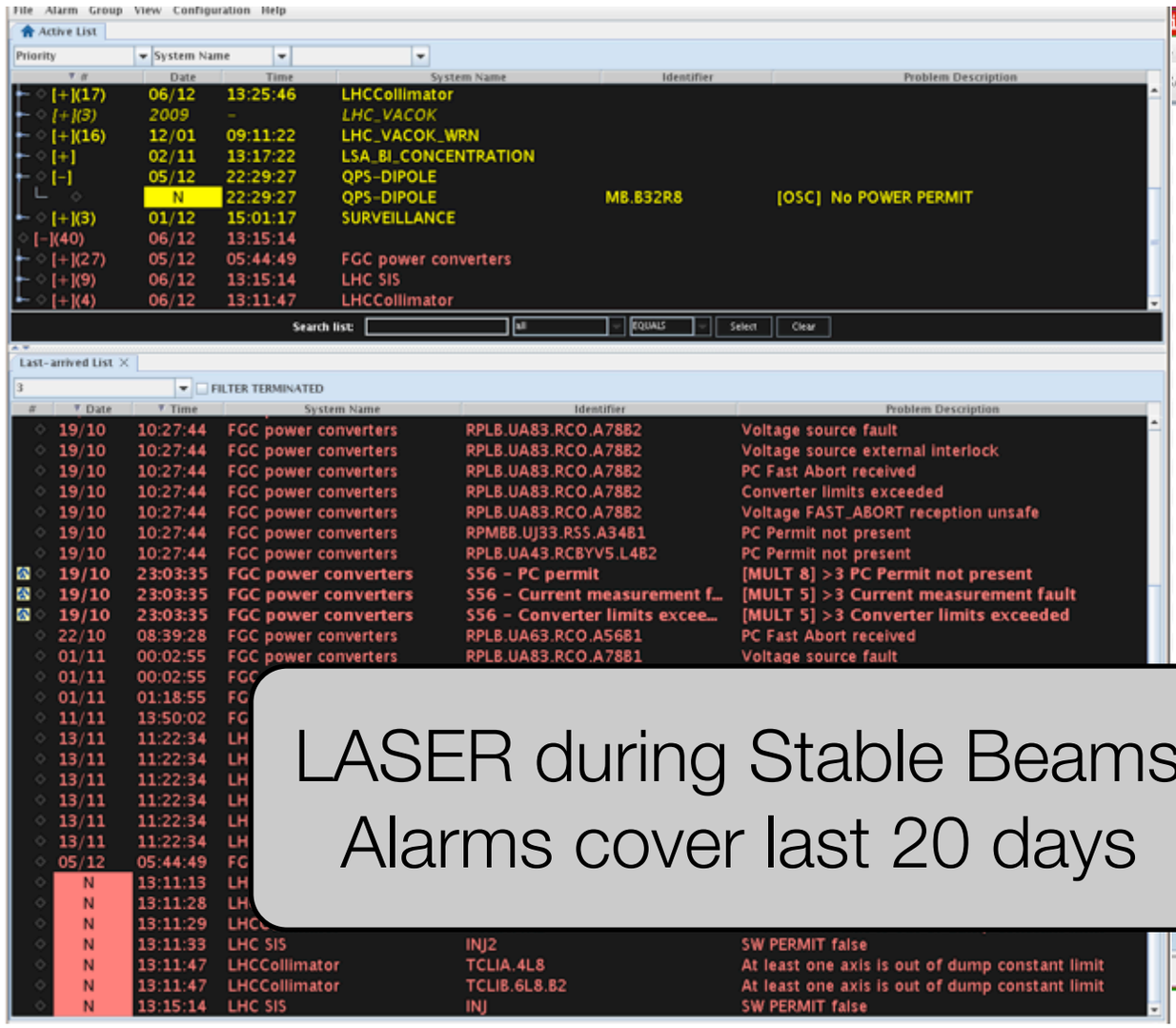
    => responsibility of the coordinator
- Experts:
  - **All actions coordinated with shift crew**
- Across the islands: **Clear lines of communication**
  - Clear requests between islands ...
  - All Islands involved: **LHC SPS CPS TI Cryo**
- **Adhere to defined roles within the CCC.**
  - Give space to team members to do their job

Alarms etc: What is real for the operator?

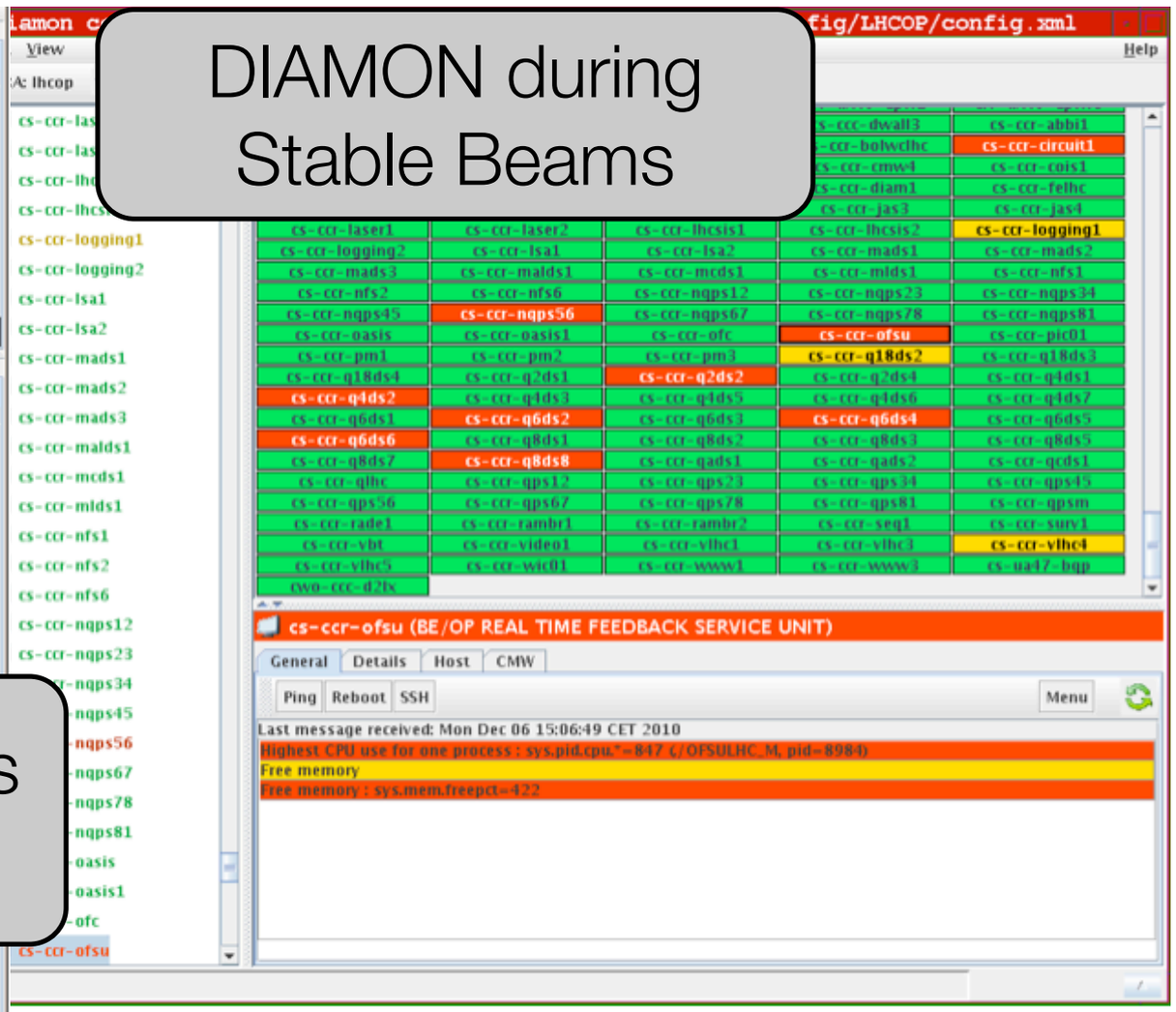
Denial-of-human-service attack: bombarded of alarms, warnings, etc making it impossible to see the significant error states or faults

- LASER: Level 3 alarms not properly defined for operation
- DIAMON: Operational and non-operation front ends not separated

  Alarm indicators not always consistent with actual state



LASER during Stable Beams
Alarms cover last 20 days



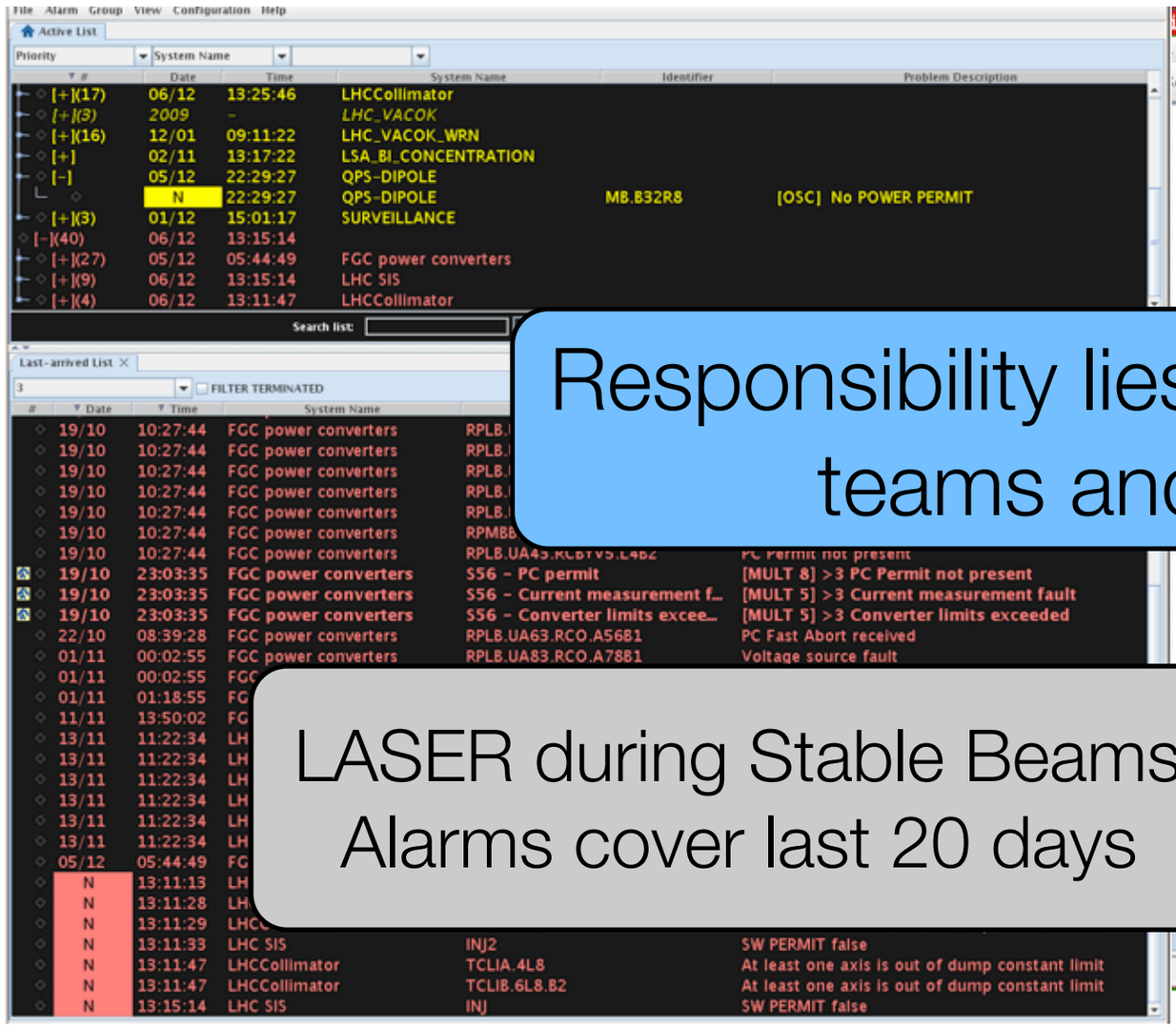
DIAMON during Stable Beams

Alarms etc: What is real for the operator?

Denial-of-human-service attack: bombarded of alarms, warnings, etc making it impossible to see the significant error states or faults

- LASER: Level 3 alarms not properly defined for operation
- DIAMON: Operational and non-operation front ends not separated

  Alarm indicators not always consistent with actual state

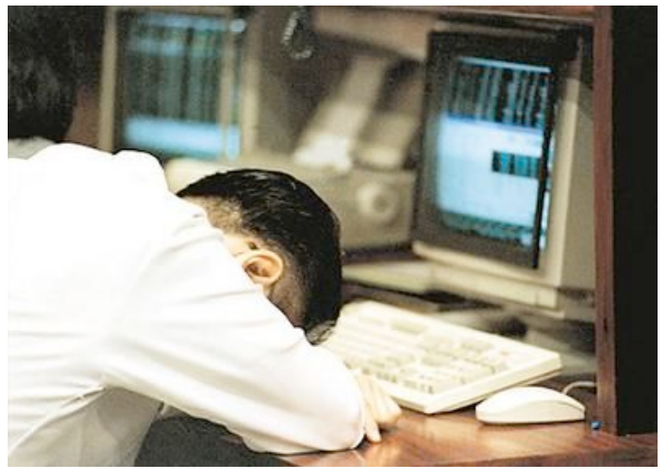


DIAMON during Stable Beams

Responsibility lies with equipment teams and with OP

LASER during Stable Beams
Alarms cover last 20 days

Other Factors



- Environmental factors: **CCC is conductive to operations**
  - **Shift crews must be given space to do their job**
    - Tour groups: CCC is not a zoo
  - Reduce number of keyboards
- **Operations factors**
  - **Tired/overworked people make mistakes**
    - **Ensure balanced load across teams:** shift crews and piquets
      - Need a non-confrontational way of saying people are tired or burnt out
- **Bombardment**: Swamping shift crew with requests is conducive to mistakes
  - Beam commissioning; equip team should define link person to shift crew
- **Unnecessary pressure:**
  - Schedule/turnaround not to compromise operational efficiency or safety:
  - Race for records should not compromise operational procedure
- **Immediate Response Layout:** Essential applications all to have screen space
  - Reassess design of GUI layer of your apps/Fixed displays (eg BCTs)

What Can We Do To Improve

- From the Machine Protection Review:
  - Rigorous discipline associated with the risk level must be reinforced during beam operations, maintenance interventions and component upgrades.
  - Technical and administrative measures to restrict access to accelerator devices and parameters to authorized and qualified personal only.
  - Establish clear procedures to make and approve decisions for implementing or changing thresholds, sequences, firmware, etc.
  - Back-door access or by-passing of established procedures must be banned

- From Industry:
  - Be aware that people routinely make a choice between being efficient (productive / less effort) and being thorough (safe / reliable), since it is rarely possible to be both at the same time.

- From Victor Hugo: “Initiative is doing the right thing at the right time”

  ... this requires both the action and the timing to be correct

=> operate within well defined and understood MPS envelopes

Human Risks: the Cultural Strata

- Adopt a Human Risk assessment culture
  - From the aeronautics industry: Human Risk Factor - cultural Strata

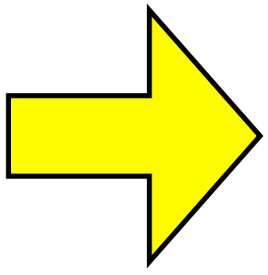
So for the LHC - where are we now?

GENERATIVE	Respects, anticipates and responds to risks. A just, learning, flexible, adaptive, prepared & informed culture. Strives for **resilience**.
PROACTIVE	Aware that ‘latent pathogens’ and ‘error traps’ lurk in system. Seeks to eliminate them beforehand. Listens to ‘sharp enders’.
CALCULATIVE	Systems to manage safety, often in response to external pressures. Data harvested rather than used. ‘By the book’.
REACTIVE	Safety given attention after an event. Concern about adverse publicity. Establishes an incident reporting system.
PATHOLOGICAL	Blame, denial and the blinkered pursuit of excellence (Vulnerable System Syndrome). Financial targets prevail: cheaper/faster.

Human Risks: the Cultural Strata

- Adopt a Human Risk assessment culture
  - From the aeronautics industry: Human Risk Factor - cultural Strata

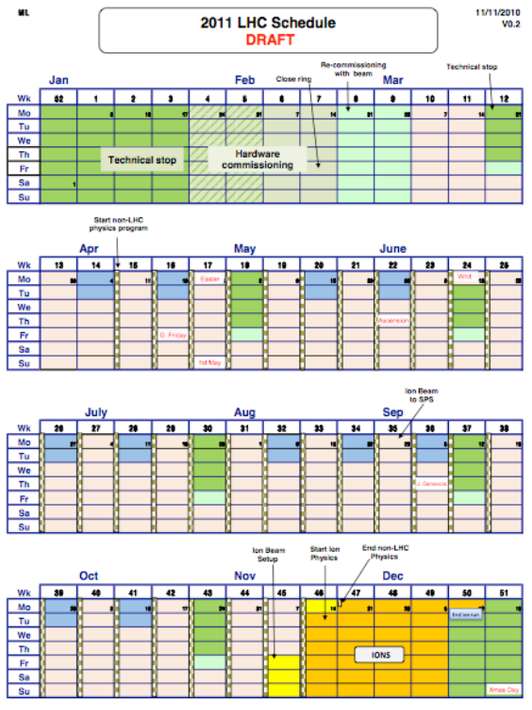
So for the LHC - where are we now?



GENERATIVE	Respects, anticipates and responds to risks. A just, learning, flexible, adaptive, prepared & informed culture. Strives for **resilience**.
PROACTIVE	Aware that ‘latent pathogens’ and ‘error traps’ lurk in system. Seeks to eliminate them beforehand. Listens to ‘sharp enders’.
CALCULATIVE	Systems to manage safety, often in response to external pressures. Data harvested rather than used. ‘By the book’.
REACTIVE	Safety given attention after an event. Concern about adverse publicity. Establishes an incident reporting system.
PATHOLOGICAL	Blame, denial and the blinkered pursuit of excellence (Vulnerable System Syndrome). Financial targets prevail: cheaper/faster.

What can we really do to improve

- Recognize that we are moving to a period of **routine operation**
  - **Problems: Dump, fix, and refill** - move out of commissioning phase
  - **Limit the use of low level applications**
    - Equip State, Generation
    - Standard tasks -> define as modular sequence tasks
  - **Shortcuts: forbidden**
  - **Map out the MPS envelope for routine operation**
    - Establish working regions within operational context
    - Continue to validate and trust MPS



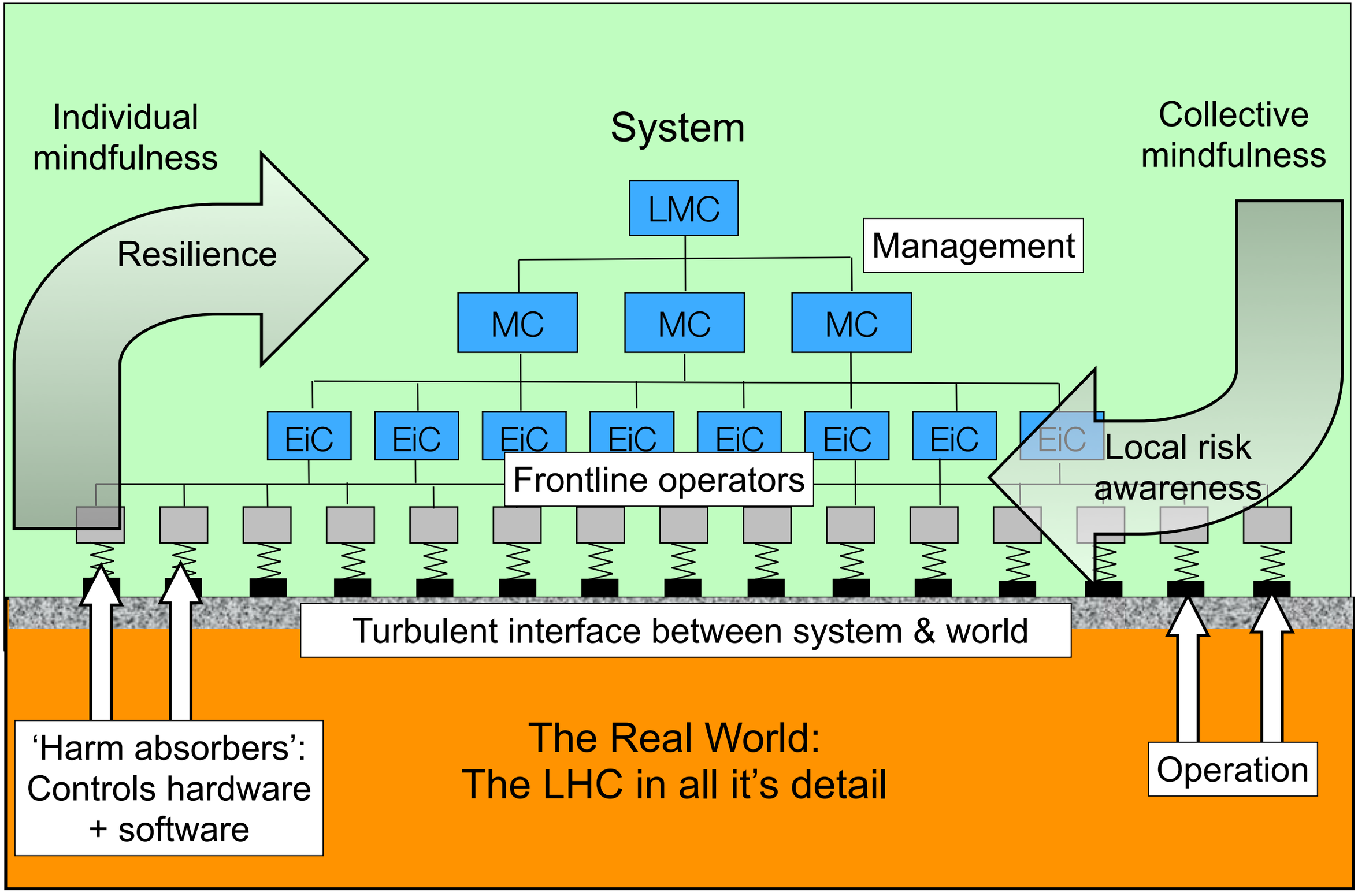
- **Maintain editorial restrictions on critical applications**
  - Machine Coordinators: Hyper cycle management
  - Sequence Editor: LHC_EiC RBAC Role

- Continue to **improve communication & coordination** across all levels/groups

What can we really do to improve - II

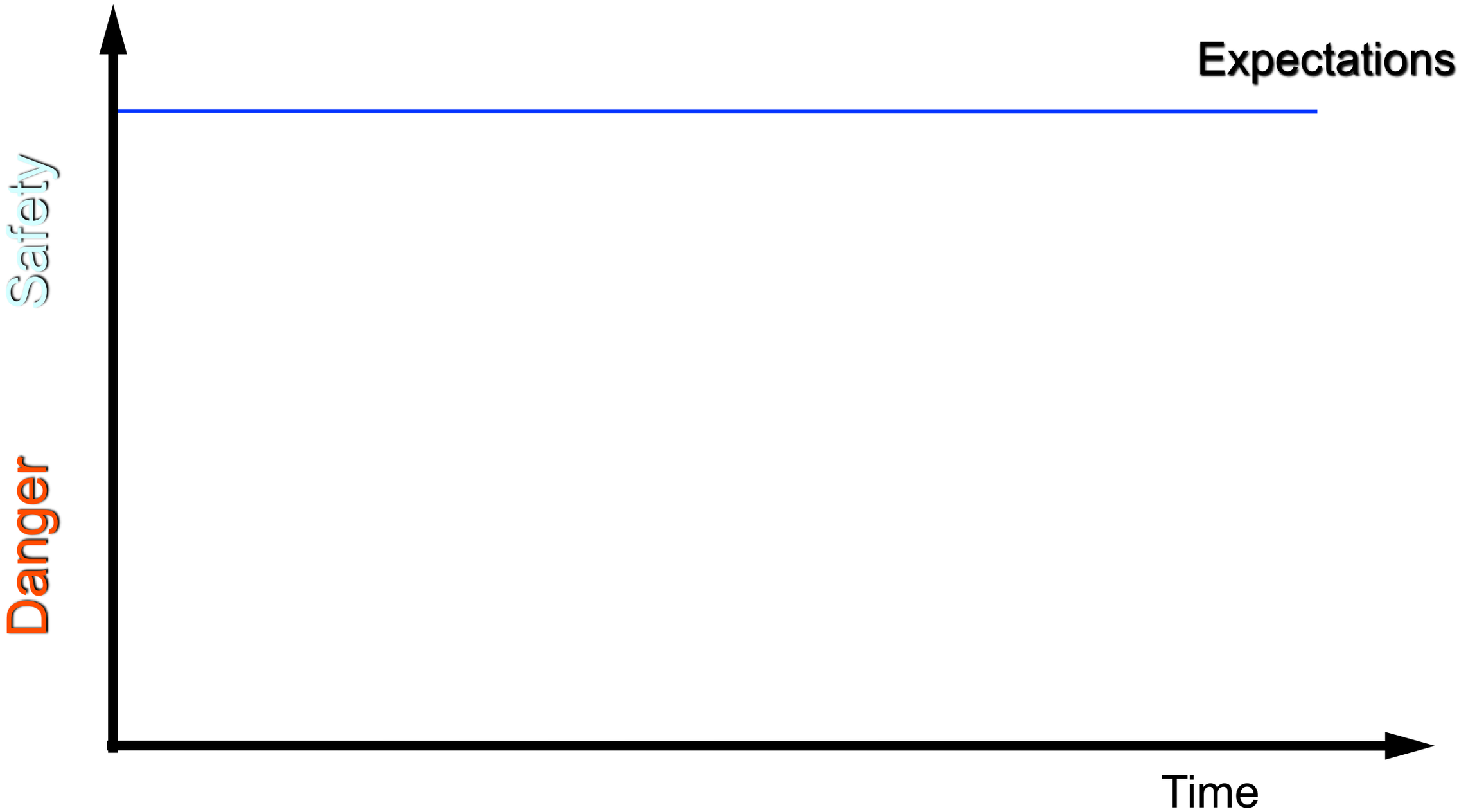
- **Build on experience from 2010**
  - Review the Nominal Procedure + define MPS envelope
- **Self assessment and introspection**
  - OP should set aside time for this throughout the year
  - Conduct observer shifts to assess work flow
- **Manage shift crew work load** - avoid fatigue and burnout
- **Depend** on expertise/professionalism of equipment experts
- **Develop** a fully proactive/generative Human Risk culture
- **Play Together:** Balance LHC needs with programs/constraints in other Islands
  - Target: work as a team to meet the physics programs in all Islands
- Finally: **Have faith in the shift crews.** **We have grown a lot in 2010**

How we achieve Resilience



Human Risk Factors: The Evolution of Risk

Expectations: Desired approach to work (as imagined)

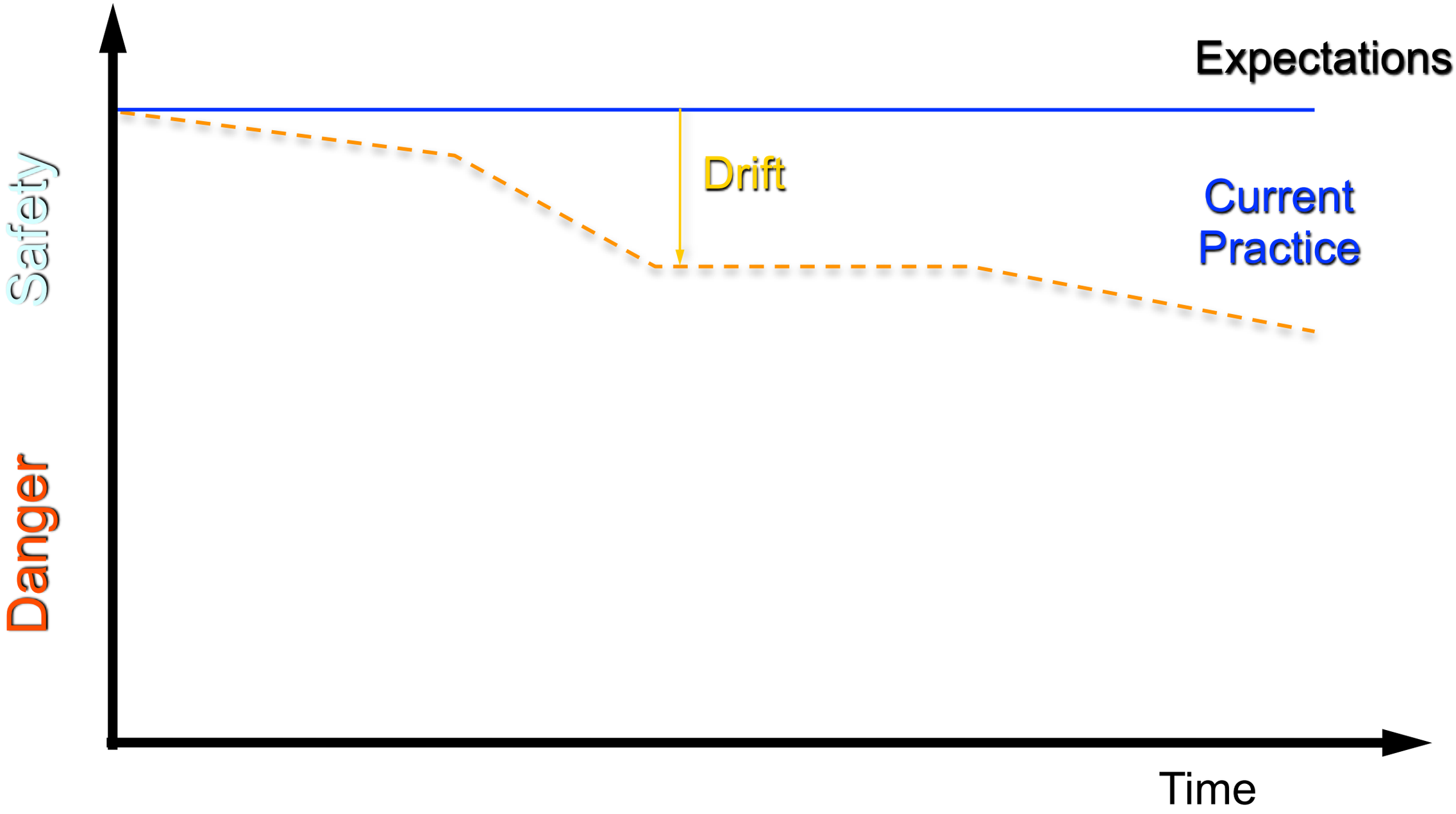


* Adapted from Dekker, S. (2007), *The Field Guide to Understanding Human Error*.

Human Risk Factors: The Evolution of Risk

Expectations: Desired approach to work (as imagined)

Practices: Work as actually performed

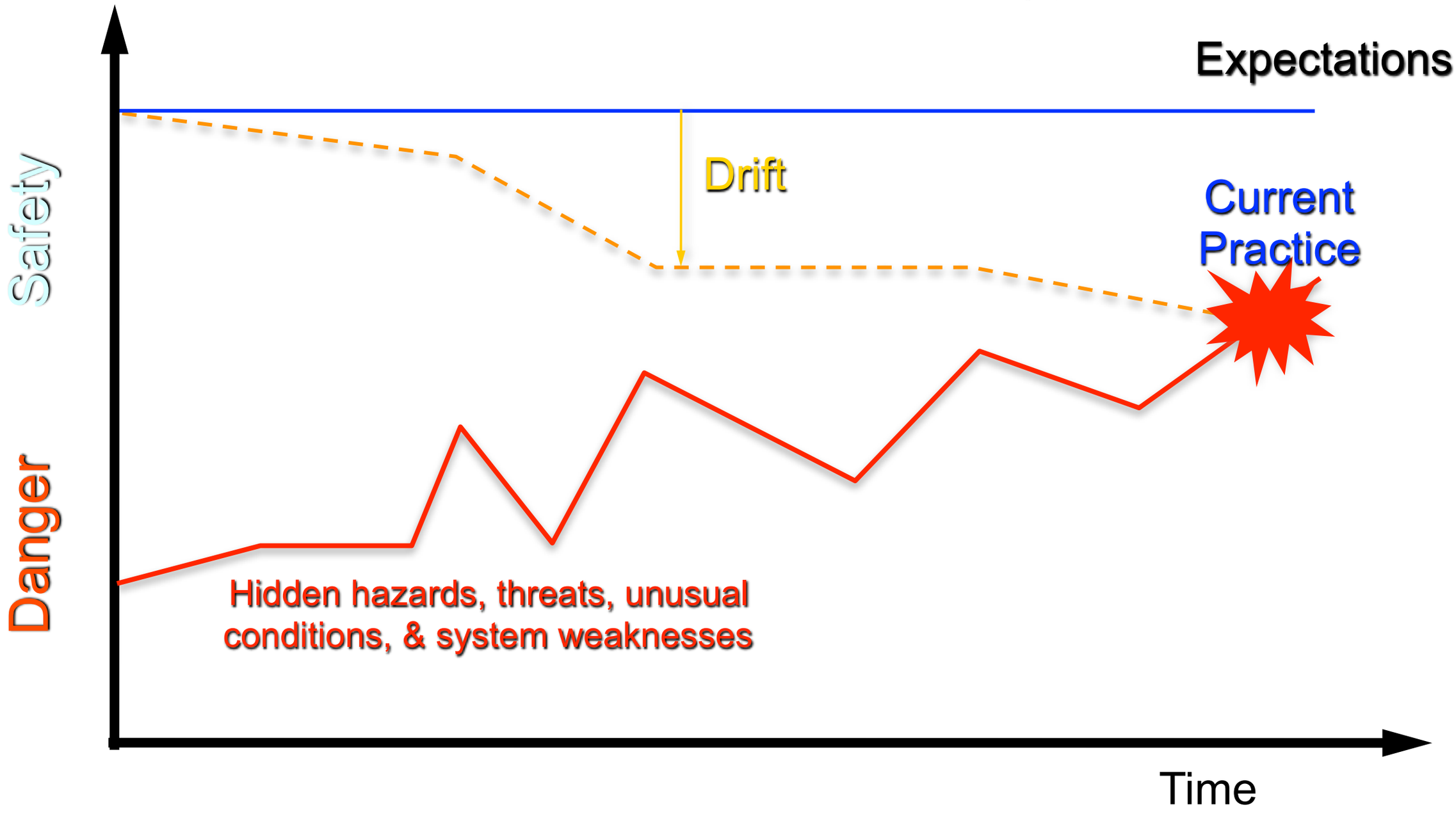


* Adapted from Dekker, S. (2007), *The Field Guide to Understanding Human Error*.

Human Risk Factors: The Evolution of Risk

Expectations: Desired approach to work (as imagined)

Practices: Work as actually performed

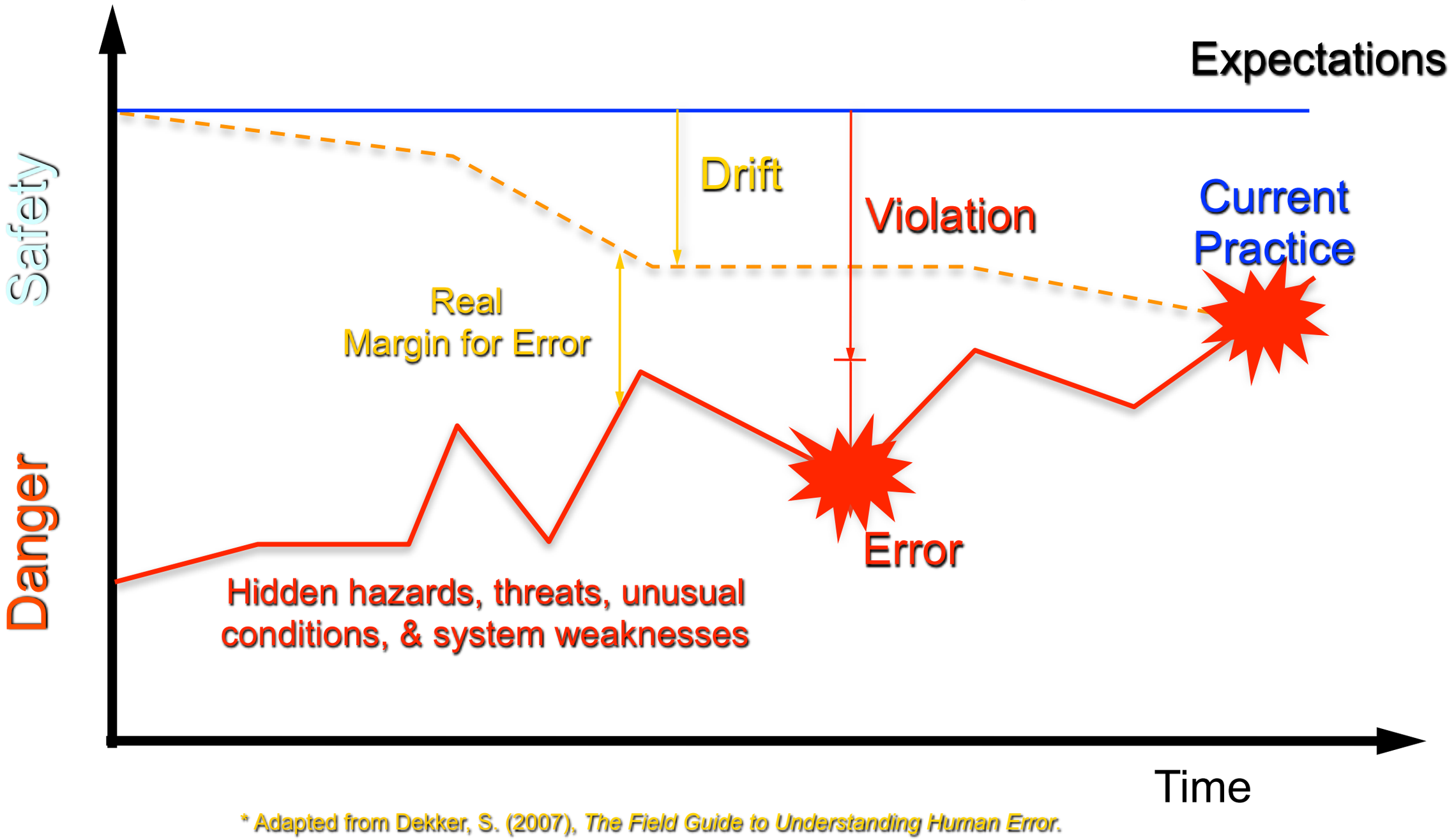


* Adapted from Dekker, S. (2007), *The Field Guide to Understanding Human Error*.

Human Risk Factors: The Evolution of Risk

Expectations: Desired approach to work (as imagined)

Practices: Work as actually performed

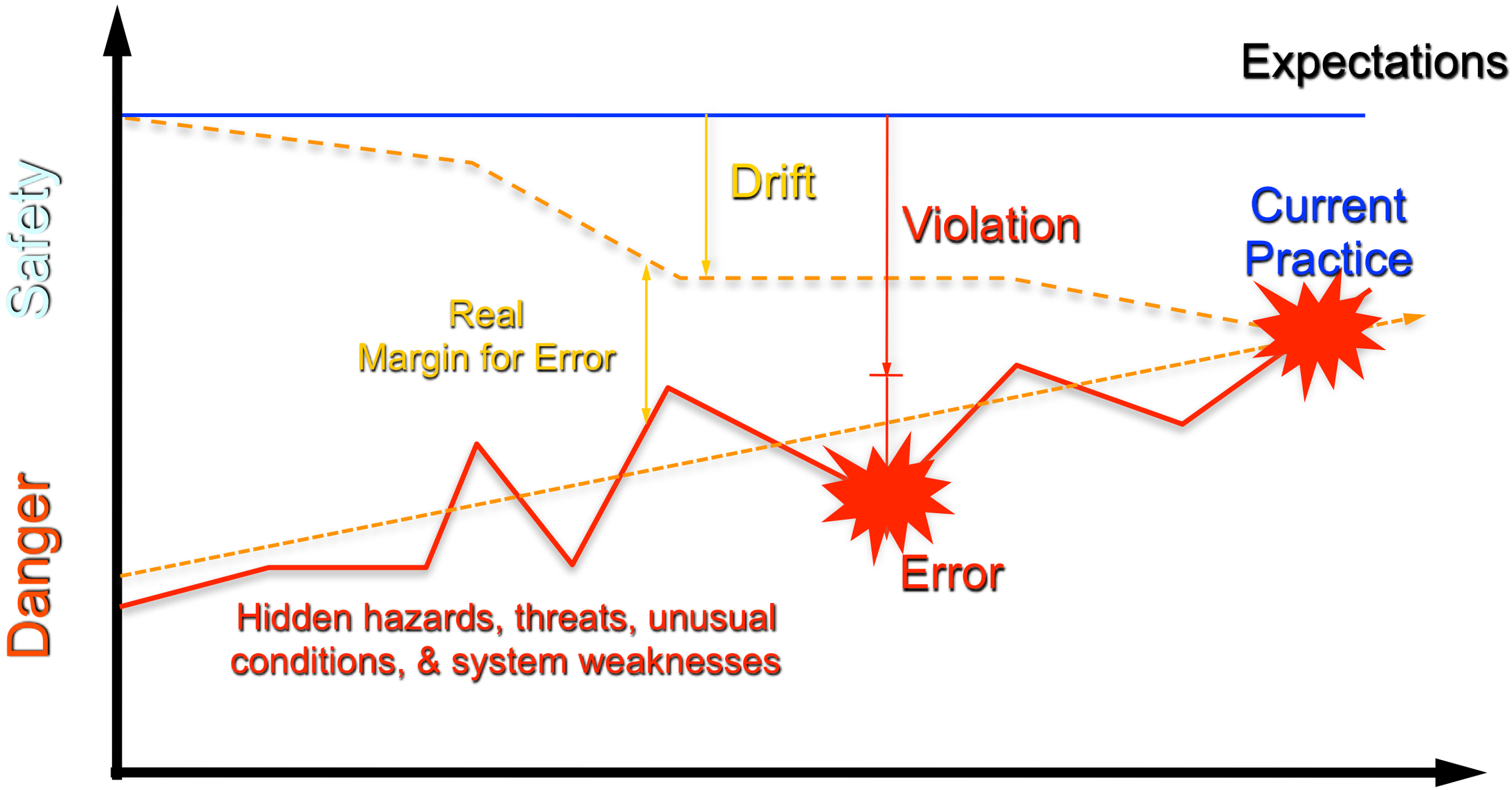


* Adapted from Dekker, S. (2007), *The Field Guide to Understanding Human Error*.

Human Risk Factors: The Evolution of Risk

Expectations: Desired approach to work (as imagined)

Practices: Work as actually performed

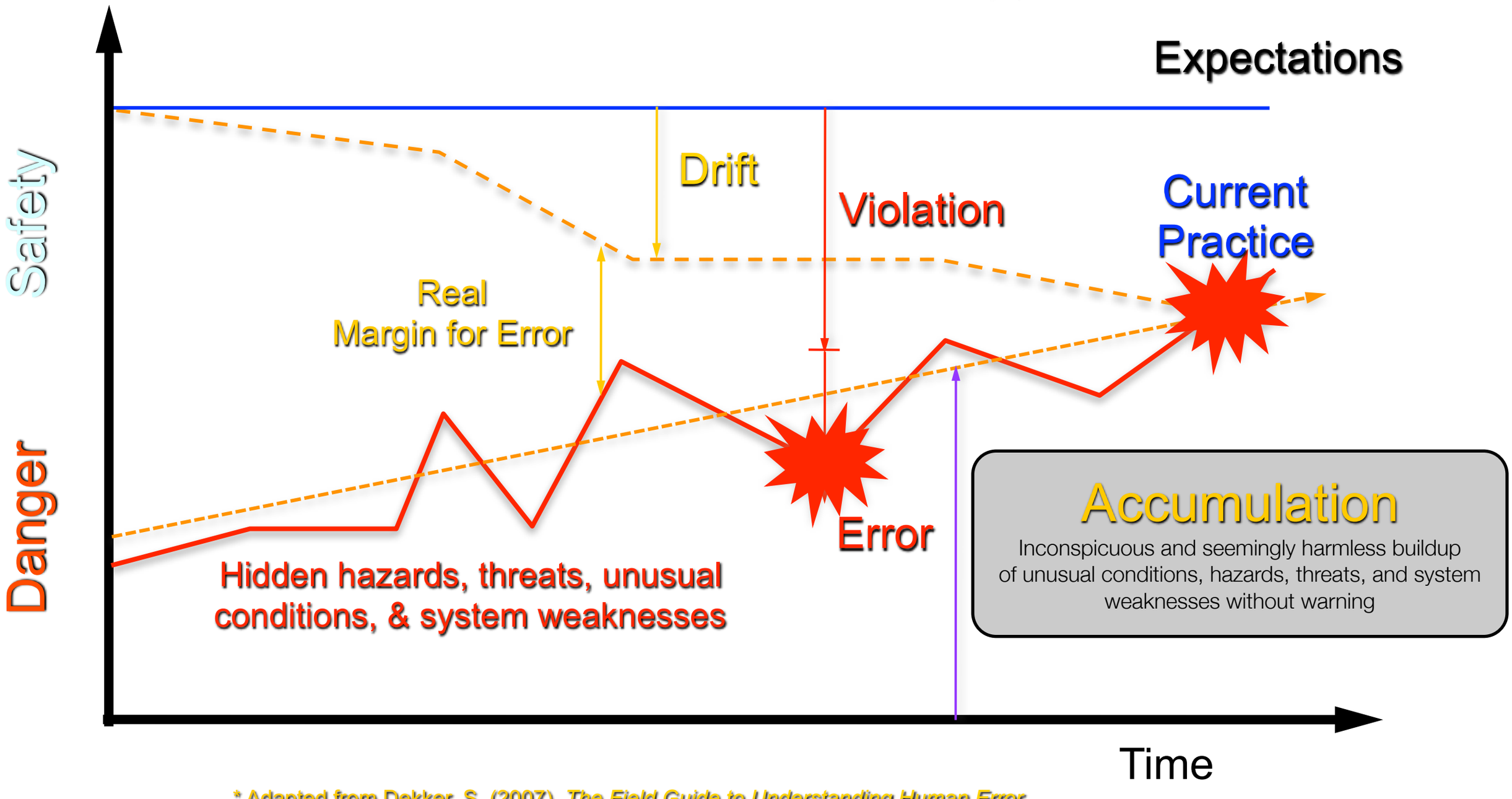


* Adapted from Dekker, S. (2007), *The Field Guide to Understanding Human Error*.

Human Risk Factors: The Evolution of Risk

Expectations: Desired approach to work (as imagined)

Practices: Work as actually performed



* Adapted from Dekker, S. (2007), *The Field Guide to Understanding Human Error*.