Incident Investigations at SLAC

(Causal analysis and the emerging role of HPI)

Rich Poliak,
SLAC QA Manager & WPC Program Manager

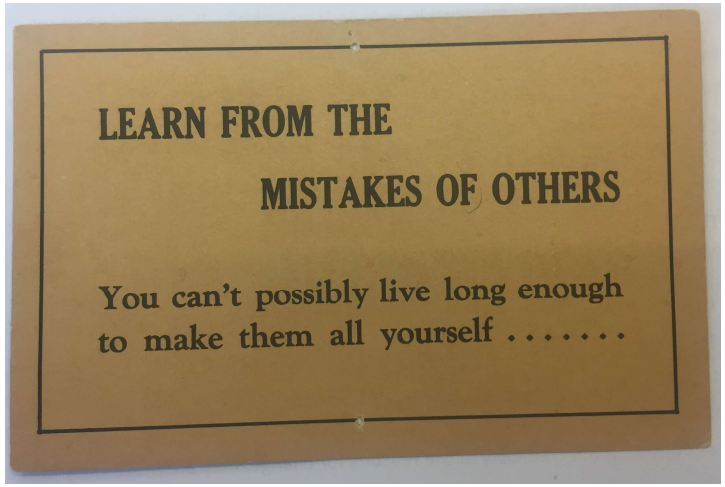
Fall 2020 EFCOG ISM/QA Joint Virtual Meeting – 11/10/2020

Agenda

- Some introductory thoughts
- Quick overview of the SLAC Incident Management process
- Anatomy of an Event – a biased perspective
- Alternate perspective to understanding deviation from expectations
- Incidents that drove a different approach to QA, WPC and HPI
- The integration of QA, WPC and HPI
- Questions

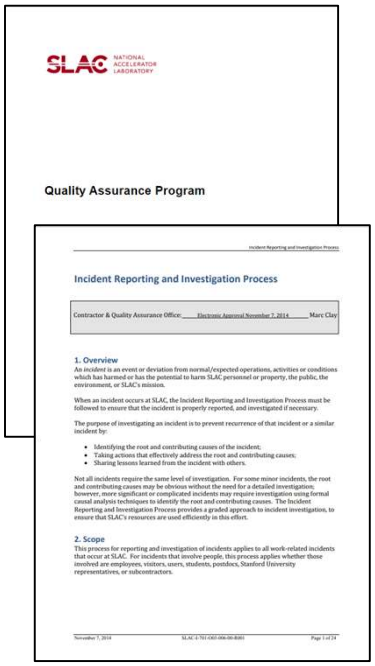
Some Introductory Thoughts

"Skill of the Craft"
Is necessary but not sufficient



"You don't have time to do it right, but you have time to do it over?"

The SLAC Incident reporting and investigation process



Initial reporting and response

Determination of investigation requirements

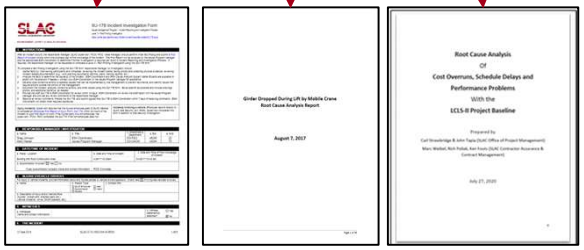
Investigation

Development of actions and lessons learned

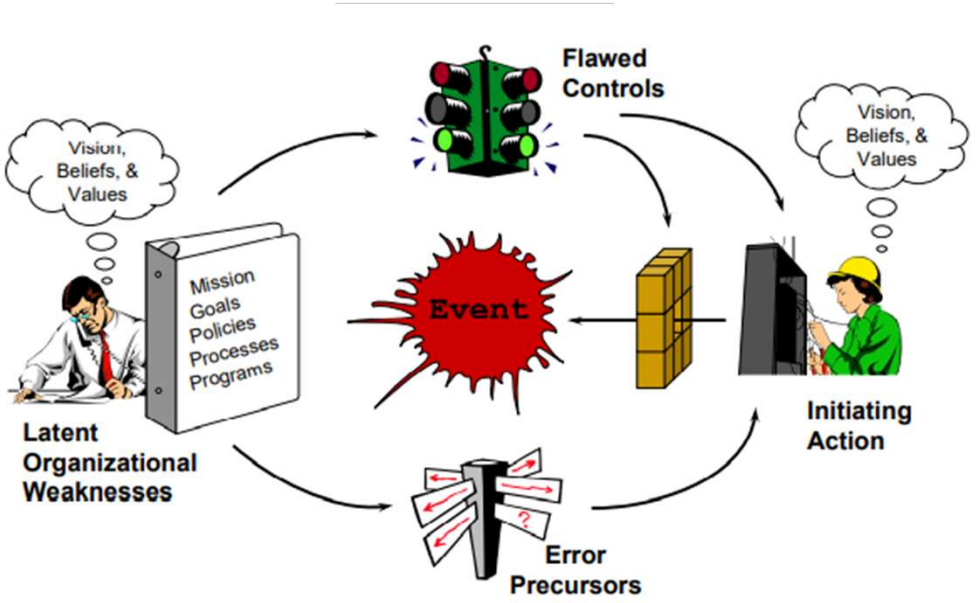
Who gets notified
- x5555 (site security)
  - SLAC Duty Officer
- Line Management
  - Issues Program Manager
  - Chief Safety Officer
  - Division Director
  - Associate Lab Director
- Occupational Health
- DOE Site Office
- etc.

Incident Types
- Injury/First Aid
- ORPS Occurrences
- Operational incidents
- Security
- etc.

Investigation Types
- Fact finding
- Causal analysis
- Independent RCA



There is a latent bias in ‘our’ approach



Anatomy of an Event

Our approach to incidents, understanding causation and the mitigations we apply have an inherent bias.

Our best and most rigorous efforts tend to be applied to individual events…..

In other words we ‘wait’ until the deviation is severe enough to draw our attention.

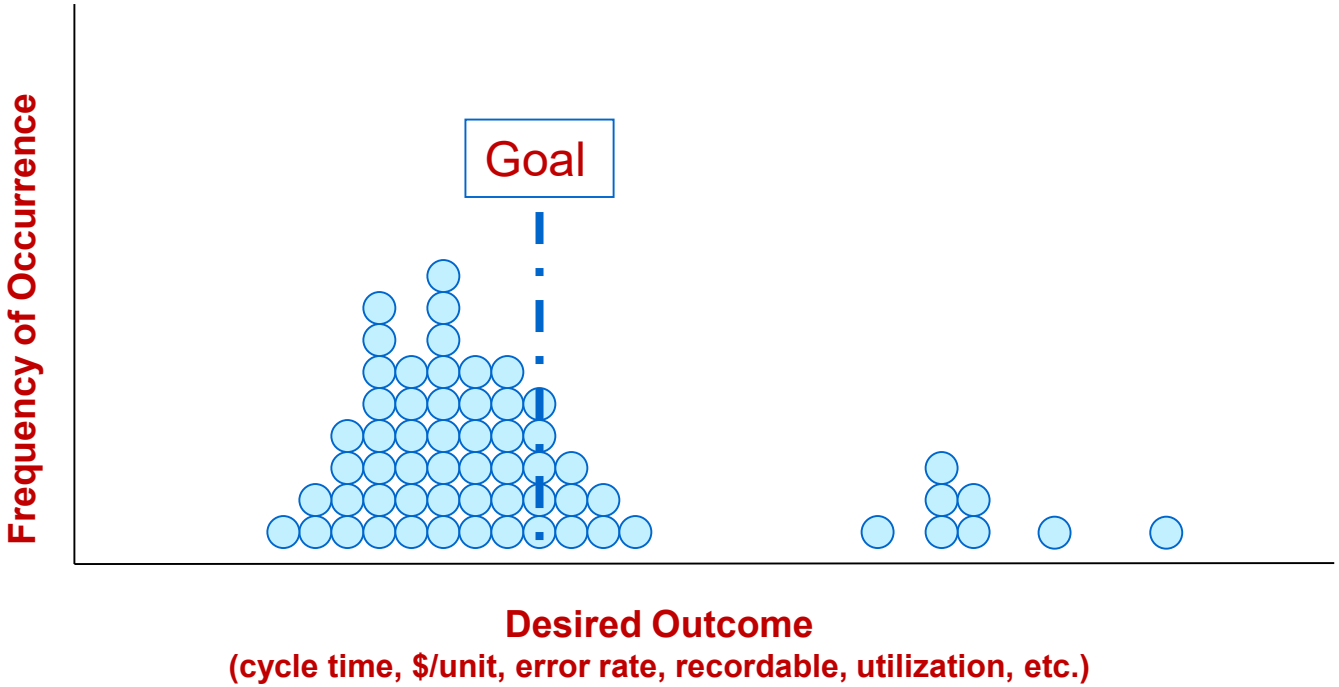
A different context to consider

Current Condition ≠ Desired Performance

What is ≠ **What must be, should be, or could be**

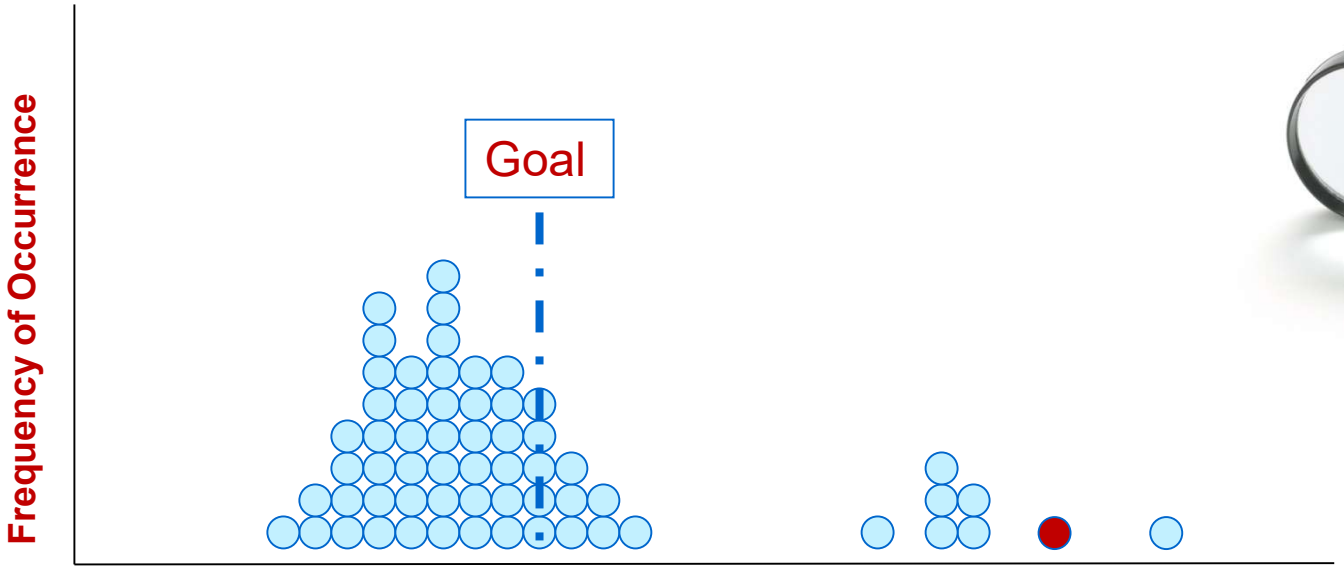
Understanding why & how to reduce or eliminate is the goal of an investigation

Let’s consider a the following



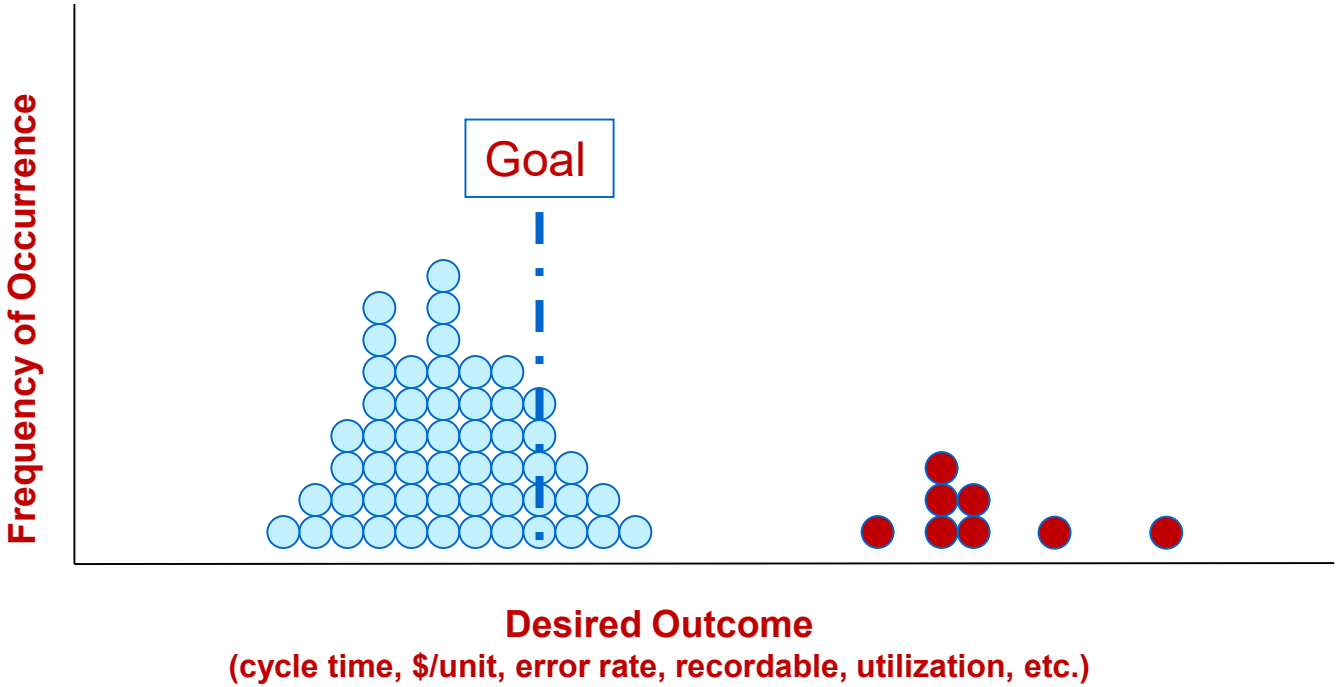
Here we have many instances of results that are failing to meet the goal.

Is it a single event we need to understand?



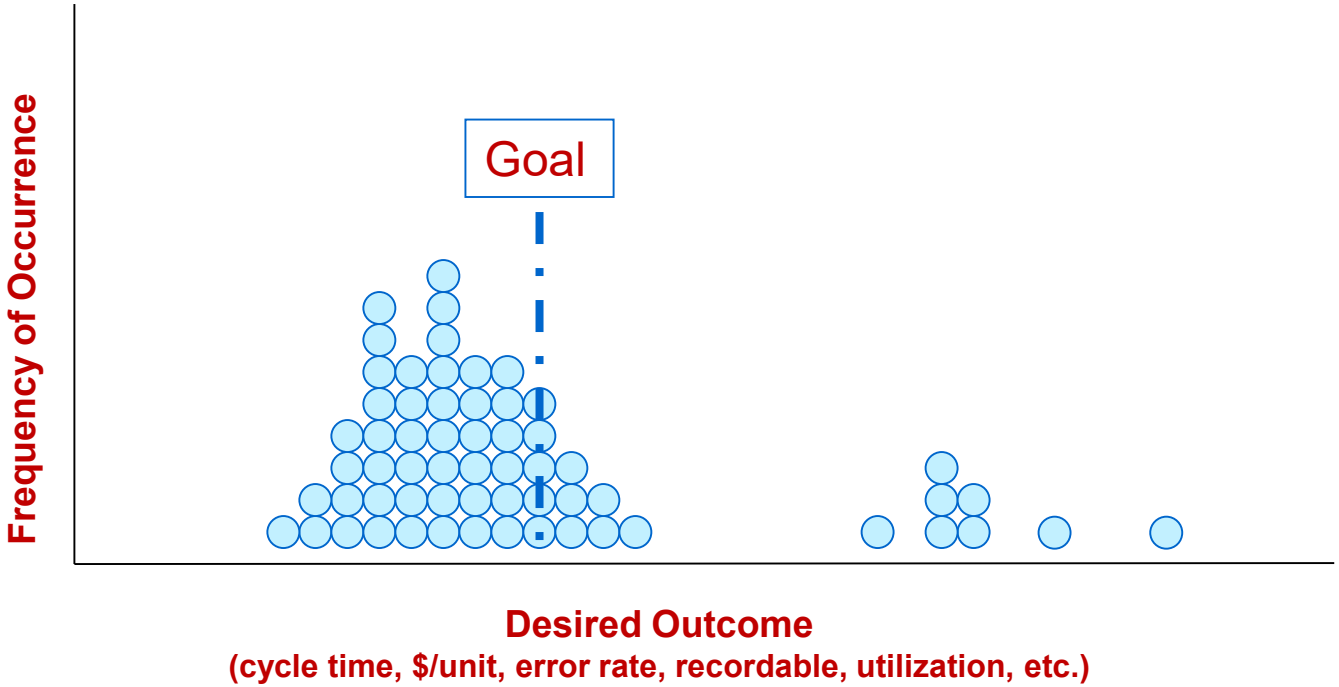
Does understanding the individual deviation tell us about the others?

Do we need to eliminate the outliers?



Eliminating the outliers is improvement but what about those outside the goal?

Do we need to move the distribution?

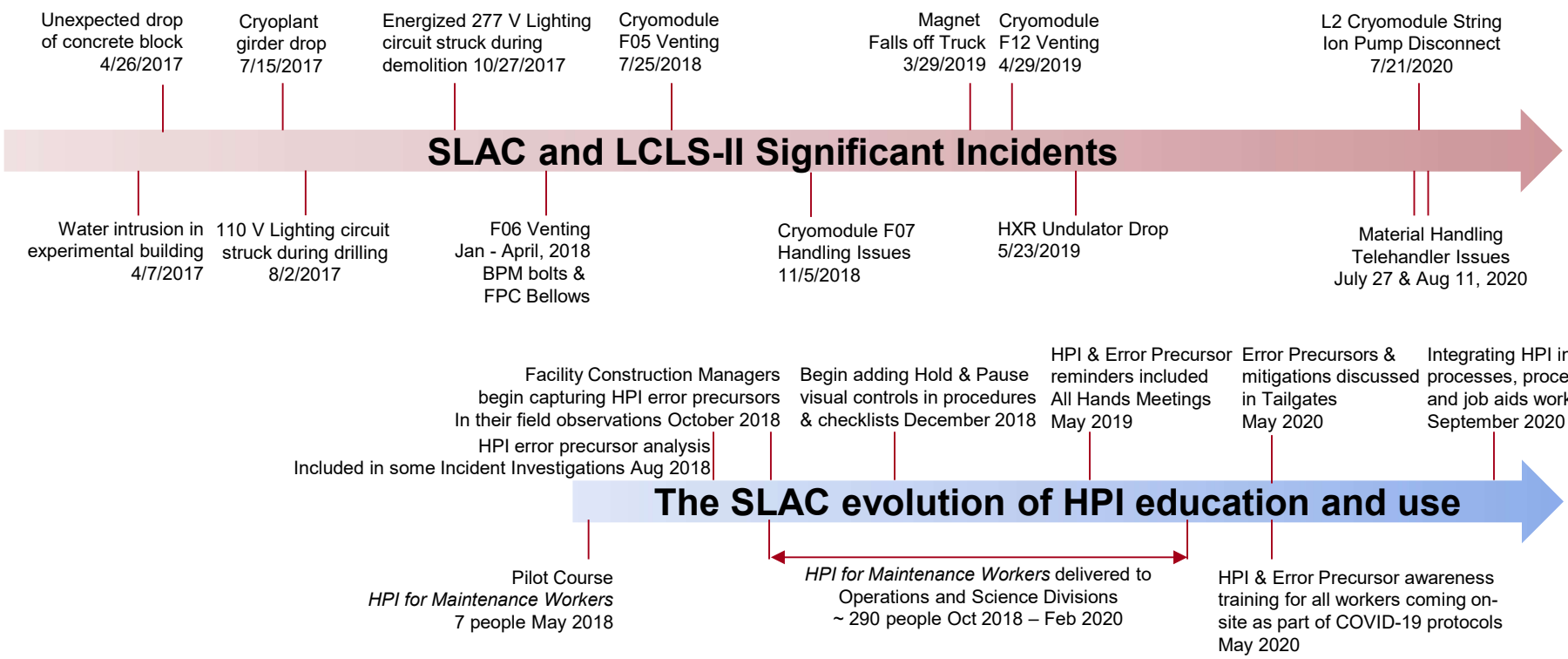


Changing the process may require the greatest level of effort to achieve

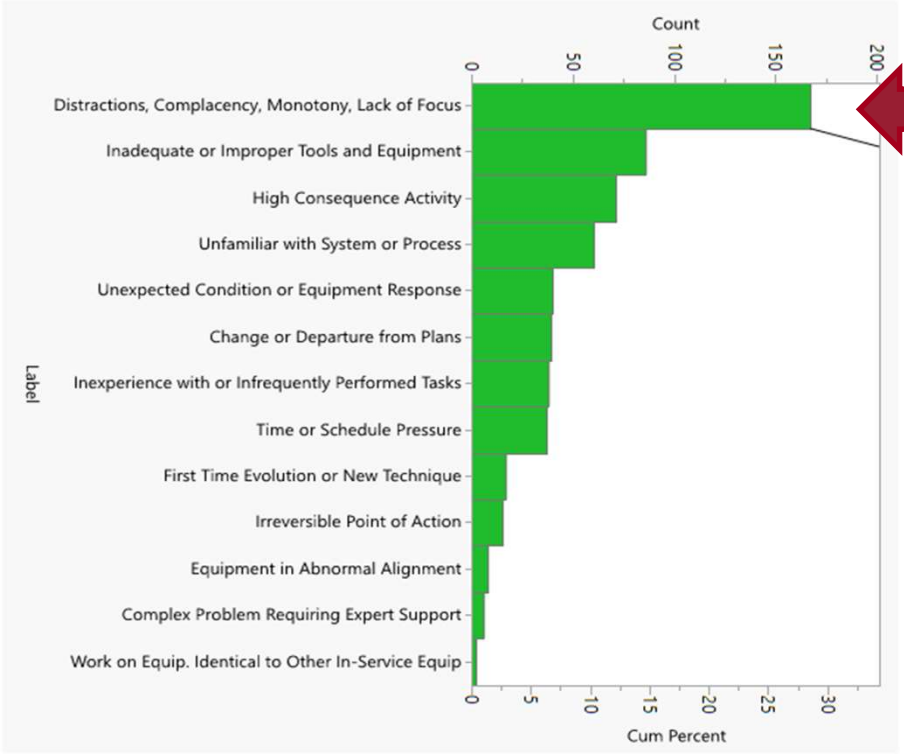
That's interesting but 'so what?'

- Fortunately the tools and methods to that can be used to address each scenario are largely the same.
- Let's look at the ASQ definition of Root Cause Analysis:
  - A root cause is defined as a factor that caused a nonconformance and should be permanently eliminated through process improvement.
    - The root cause is the core issue—the highest-level cause—that sets in motion the entire cause-and-effect reaction that ultimately leads to the problem(s).
  - Root cause analysis (RCA) is defined as *a collective term that describes a wide range of approaches, tools, and techniques* used to uncover causes of problems.
    - Some RCA approaches are geared more toward identifying true root causes than others, some are more general problem-solving techniques, and others simply offer support for the core activity of root cause analysis.

SLAC & LCLS II incidents that drove increased QA, WPC rigor & HPI



Field Construction Manager Observations of Error Precursors



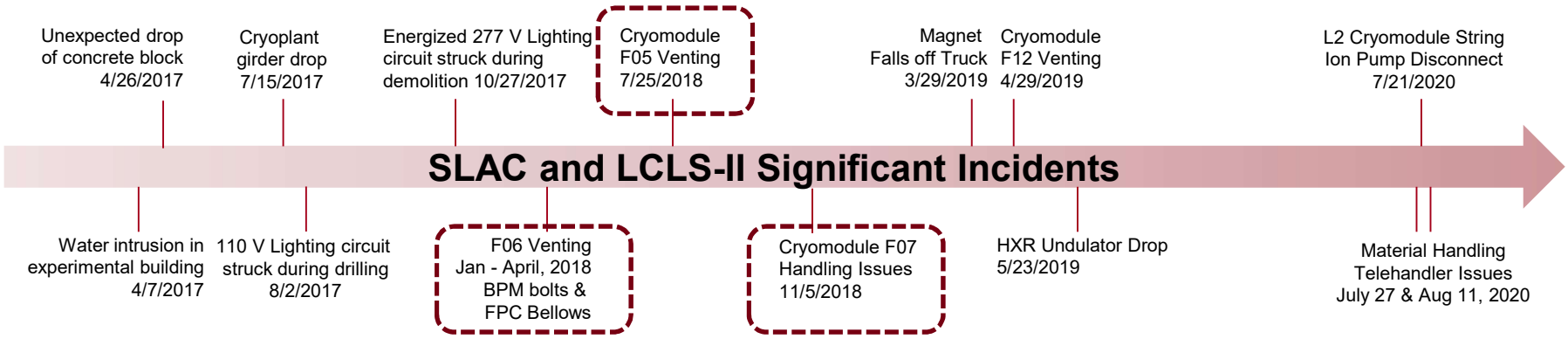
~ 30% of the observations

Tools to help mitigate:

- STAR
  - Stop
  - Think
  - Act
  - Review
- Reinforce communication
- Peer-checking
- Pause & 2 Minute Rule

Lack of events and work becoming routine create opportunities for complacency

Incidents that precipitated increased WPC rigor



Responses and Mitigations:

- Increased levels of engineering, characterization & testing new processes
- Creation of Enhanced Rigor Work Planning and Control
- Adding emphasis on Human Performance Improvement (HPI) in procedures

Key message to the LCLS-II team in November 2018 All Hands

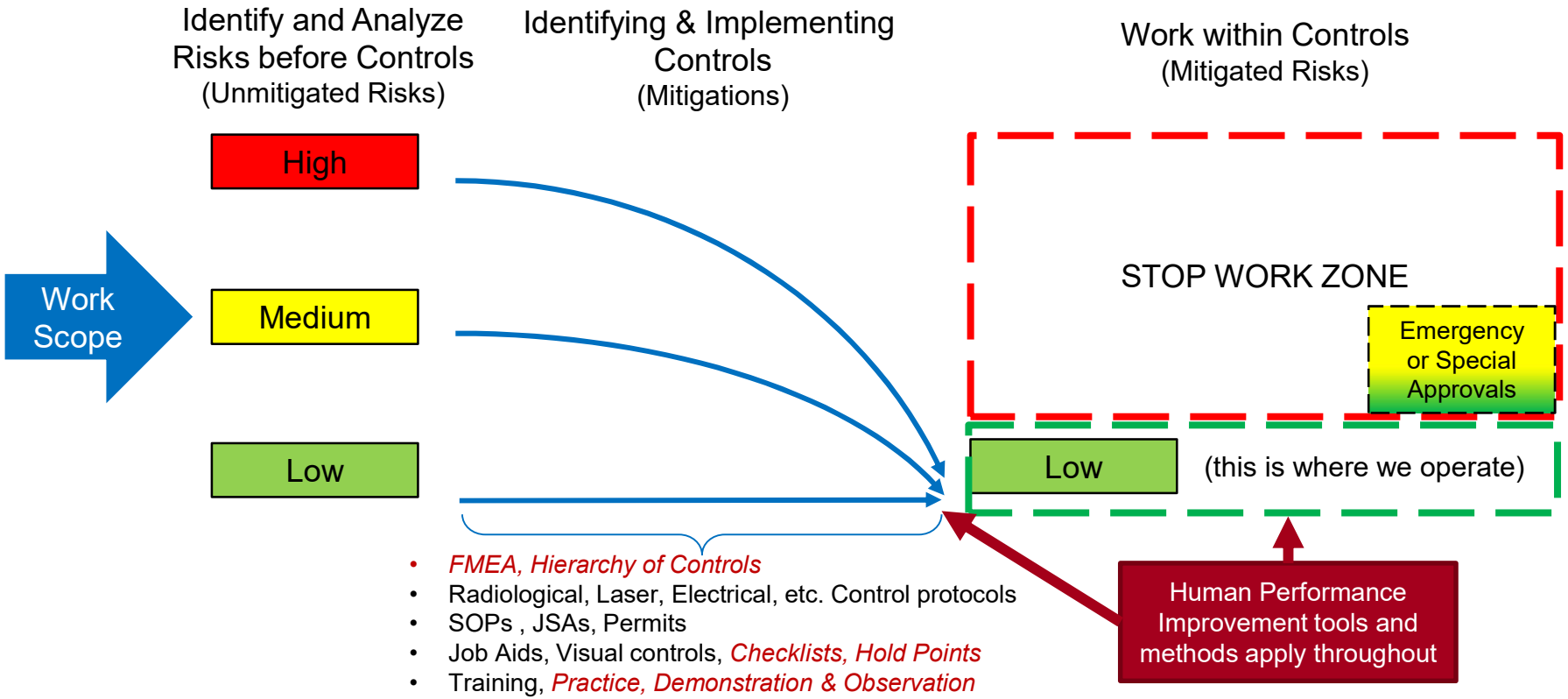
Superconducting linac requires a different, *much more controlled* approach to handling, installation, maintenance and repair

- *You **never** want to introduce a speck of dust in the linac*
- *Warm or cold, you **never** want to "vent" the linac to air*
  - *Air is **dirty** and **freezes** if it enters the cold linac*
- There is *almost nothing you can do in the way of maintenance to the linac when it's cold (2 degrees K)*
- *You want the linac to stay cold 2-3 or more years at a clip*

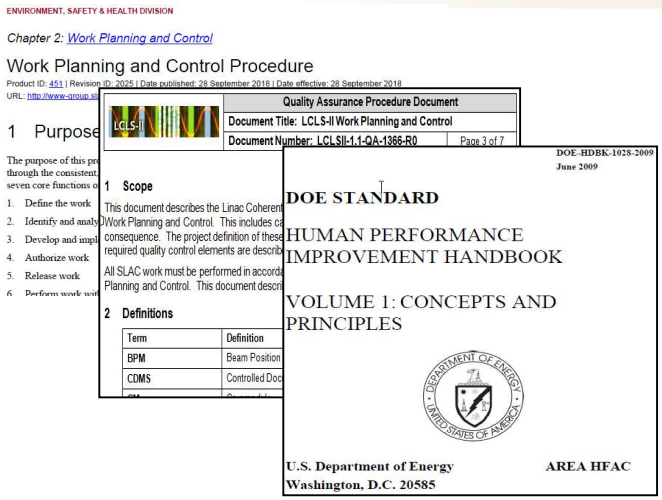
Greater rigor required

- Require we can do it successfully without having to do over
- Risk based approach
- Changing the base culture built over 50 years of warm linac experience

A simple but important model for WPC



SLAC Enhanced Rigor Work Planning and Control


ENVIRONMENT, SAFETY & HEALTH DIVISION

Chapter 2: Work Planning and Control

Work Planning and Control Procedure

Quality Assurance Procedure Document

Document Title: LCLS-II Work Planning and Control

Document Number: LCLSII-1.1-QA-1366-R0

DOE-HDBK-1028-2009
June 2009

DOE STANDARD

HUMAN PERFORMANCE IMPROVEMENT HANDBOOK

VOLUME 1: CONCEPTS AND PRINCIPLES

U.S. Department of Energy
Washington, D.C. 20585

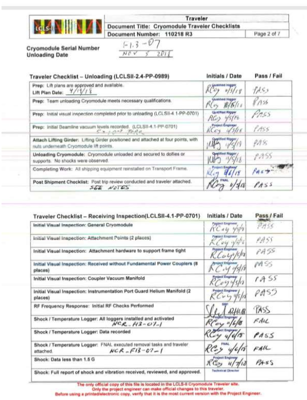
AREA HFAC

- LCLS-II Lessons Learned drove changes to WPC by applying greater levels of rigor to the design and execution of work plans.
- This approach has proven critical to the current progress and SLAC continues to learn and extend this elsewhere at the lab.

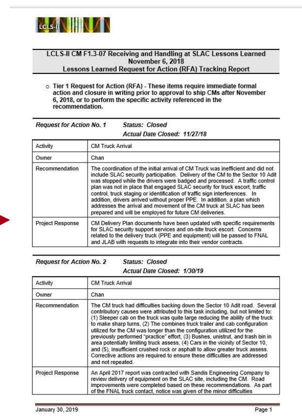
WPC Core Functions	Additional rigor and enhancements
Define the Scope of Work	• High consequence work activities • Detailed review of requirements
Identify hazard and error potential	• High consequence risk categorization • FMEA • Human Performance Error Precursors
Develop and Implement Controls	• Hierarchy of Controls (defense in depth) • Procedures, Checklists, Readiness reviews • Specialized Training/Authorization
Perform work within controls	• Procedures, Checklists, Travelers, 5S • Hold Points (pause & check), Observation • Integrated Tailgates and Release Work
Feedback & improvement is captured and acted upon	• Lessons Learned • Demonstration, Practice & Improvement • Post action reviews

Rapid deployment of Enhanced Rigor WPC to CM Handling

Receiving/Handling Incident
November 6, 2018



Lessons Learned Followup
November14, 2018



Multi-tiered Improvements
Nov 2018 – Jan 2019

- Enhanced Rigor WPC
  Refined procedures & travelers
- Site improvements & preparation
- Multiple practice sessions w/F05
- Readiness reviews to restart

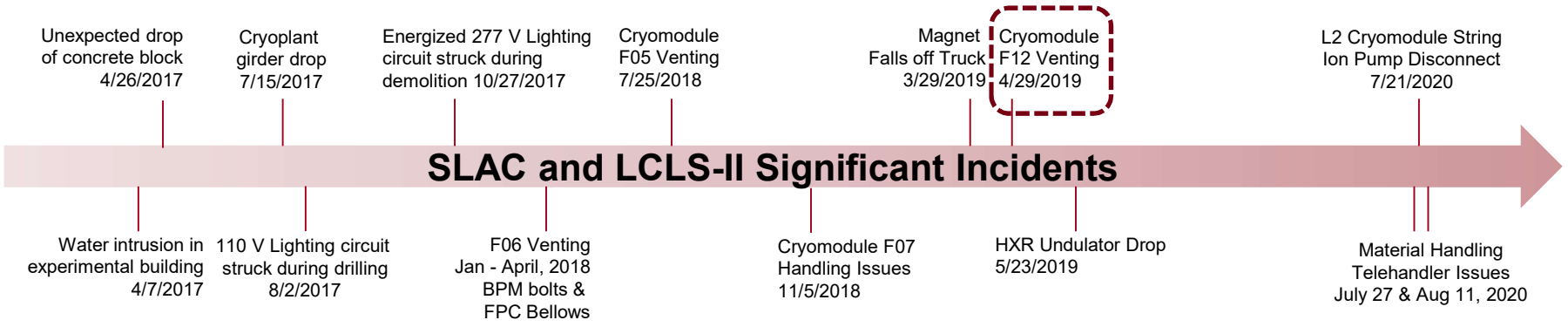
Procedures and Checklists have been iterated and improved

Handling has evolved from being a stressful event to a routine activity

Cryomodule handling improved from challenging to efficient and routine

We do have a Cultural challenge to consider

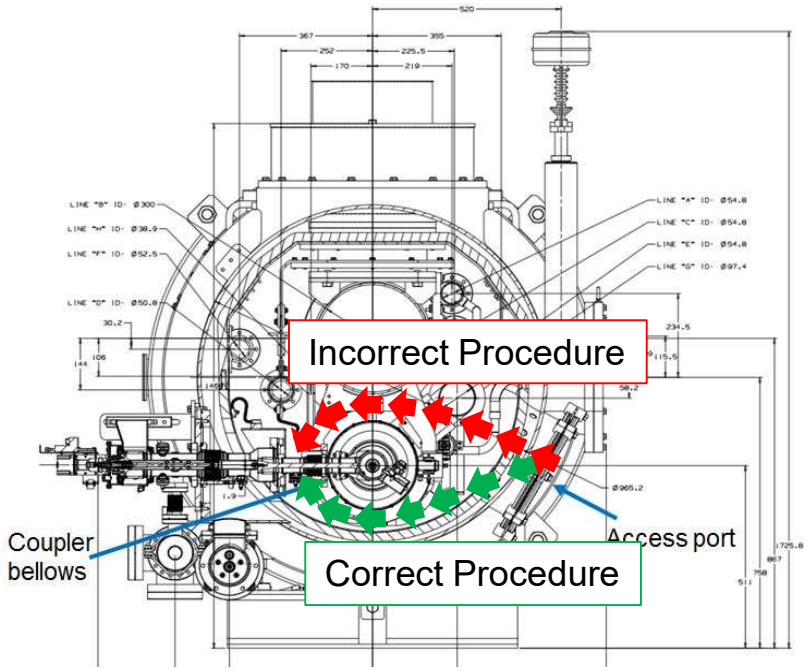
Then we vented another Cryomodule

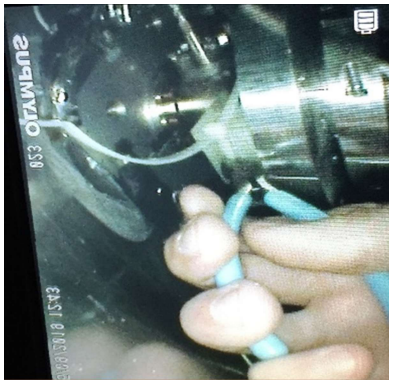


Responses and Mitigations:

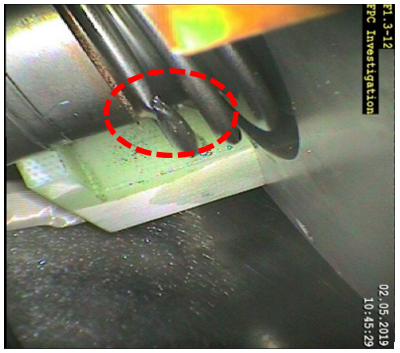
- Increased levels of engineering, characterization & testing new processes
- Creation of Enhanced Rigor Work Planning and Control
- Adding emphasis on Human Performance Improvement (HPI) to our toolset

Details matter – F12 Venting Incident



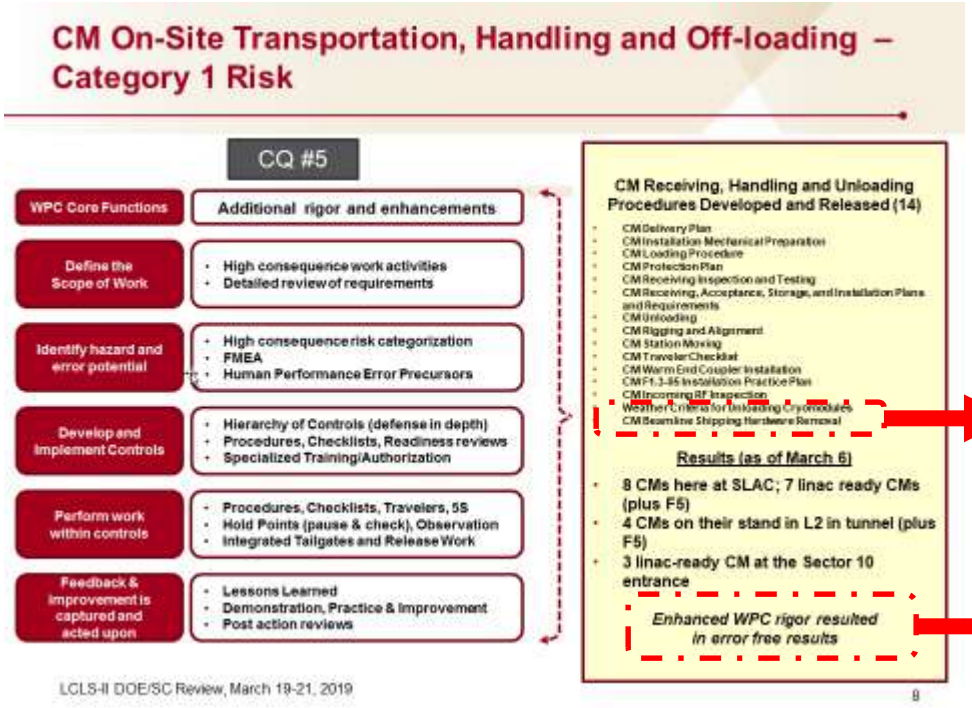


VS



We thought we had it covered – Enhanced Rigor WPC

From the March, 2019 DOE/SC Review



CM Beamline Shipping Hardware Removal

We claimed we had the right approach

Obviously we were mistaken

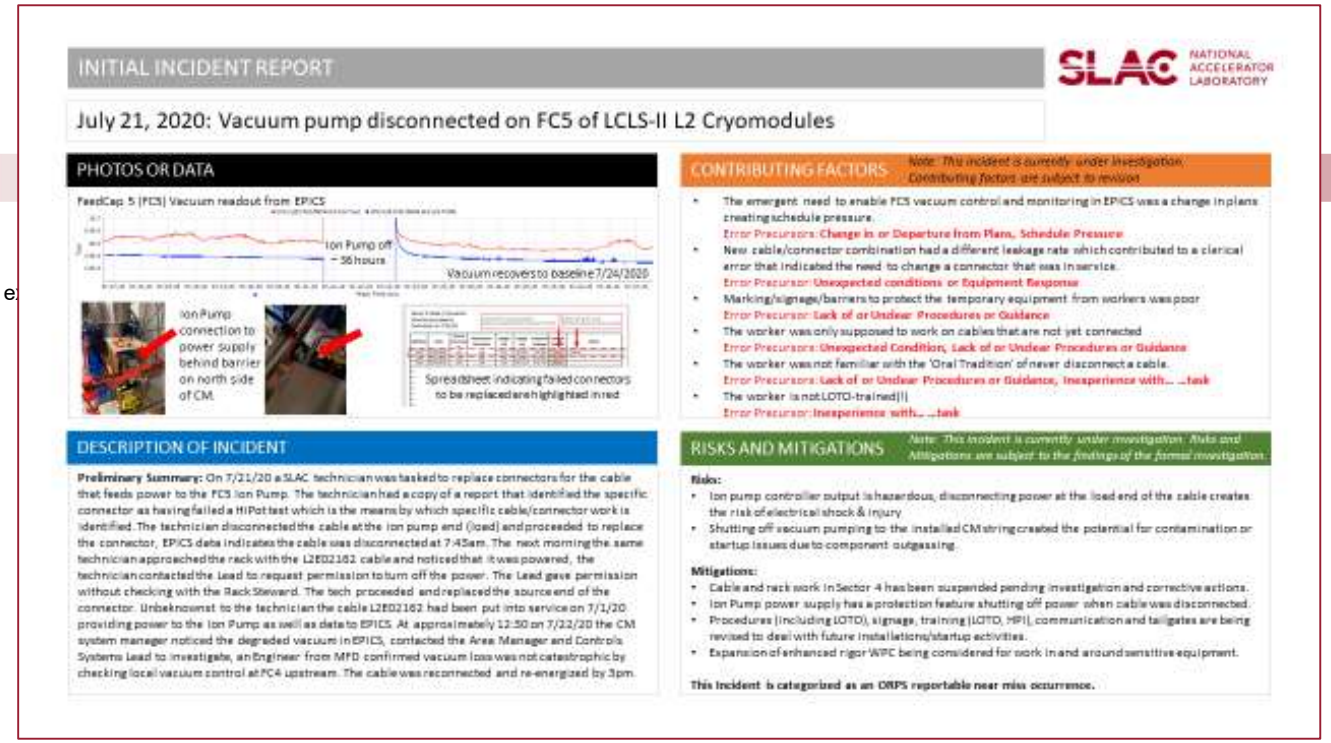
Our path forward

We have recognized that must rethink exactly how we apply the appropriate levels of rigor in our definition, practice and validation of our work by being able to answer ‘yes’ to the following questions:

1) Are our processes and procedures able to be executed successfully and provide adequate risk mitigation?
2) Are we following our processes and procedures?

How do you know?

Recently we disconnected an active Ion Pump



INITIAL INCIDENT REPORT

SLAC NATIONAL ACCELERATOR LABORATORY

July 21, 2020: Vacuum pump disconnected on FC5 of LCLS-II L2 Cryomodules

PHOTOS OR DATA

FeedCap 5 (FC5) Vacuum readout from EPICS

Ion Pump connection to power supply behind barrier on north side of CM

Spreadsheet indicating failed connectors to be replaced are highlighted in red

CONTRIBUTING FACTORS *Note: This incident is currently under investigation. Contributing factors are subject to revision*

- The emergent need to enable FC5 vacuum control and monitoring in EPICS was a change in plans creating schedule pressure.
  Error Precursors: Change in or Departure from Plans, Schedule Pressure
- New cable/connector combination had a different leakage rate which contributed to a clerical error that indicated the need to change a connector that was in service.
  Error Precursor: Unexpected conditions or Equipment Response
- Marking/signage/barriers to protect the temporary equipment from workers was poor
  Error Precursor: Lack of or Unclear Procedures or Guidance
- The worker was only supposed to work on cables that are not yet connected
  Error Precursors: Unexpected Condition, Lack of or Unclear Procedures or Guidance
- The worker was not familiar with the 'Oral Tradition' of never disconnect a cable.
  Error Precursors: Lack of or Unclear Procedures or Guidance, Inexperience with... ...task
- The worker is not LOTO-trained(!)
  Error Precursor: Inexperience with... ...task

DESCRIPTION OF INCIDENT

Preliminary Summary: On 7/21/20 a SLAC technician was tasked to replace connectors for the cable that feeds power to the FC5 Ion Pump. The technician had a copy of a report that identified the specific connector as having failed a HiPot test which is the means by which specific cable/connector work is identified. The technician disconnected the cable at the ion pump end (load) and proceeded to replace the connector. EPICS data indicates the cable was disconnected at 7:45am. The next morning the same technician approached the rack with the L2E02162 cable and noticed that it was powered, the technician contacted the Lead to request permission to turn off the power. The Lead gave permission without checking with the Rack Steward. The tech proceeded and replaced the source end of the connector. Unbeknownst to the technician the cable L2E02162 had been put into service on 7/1/20 providing power to the Ion Pump as well as data to EPICS. At approximately 12:50 on 7/22/20 the CM system manager noticed the degraded vacuum in EPICS, contacted the Area Manager and Controls Systems Lead to investigate, an Engineer from MFD confirmed vacuum loss was not catastrophic by checking local vacuum control at FC4 upstream. The cable was reconnected and re-energized by 3pm.

RISKS AND MITIGATIONS *Note: This incident is currently under investigation. Risks and Mitigations are subject to the findings of the formal investigation.*

Risks:

- Ion pump controller output is hazardous, disconnecting power at the load end of the cable creates the risk of electrical shock & injury
- Shutting off vacuum pumping to the installed CM string created the potential for contamination or startup issues due to component outgassing

Mitigations:

- Cable and rack work in Sector 4 has been suspended pending investigation and corrective actions.
- Ion Pump power supply has a protection feature shutting off power when cable was disconnected.
- Procedures (including LOTO), signage, training (LOTO, HPI), communication and tailgates are being revised to deal with future installations/startup activities.
- Expansion of enhanced rigor WPC being considered for work in and around sensitive equipment.

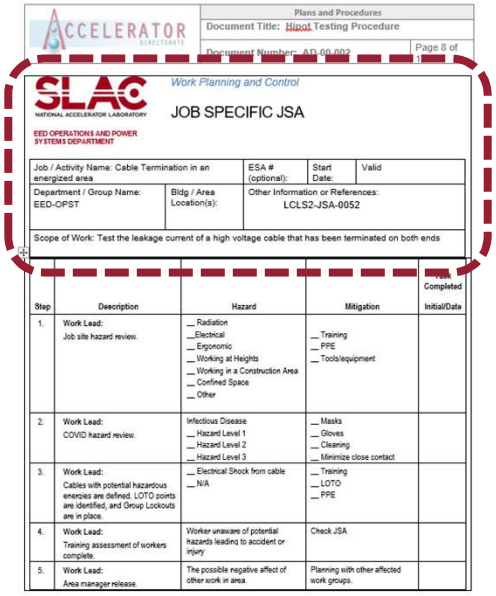
This incident is categorized as an ORPS reportable near miss occurrence.

L2 Cryomodule String Ion Pump Disconnect 7/21/2020

Material Handling Telehandler Issues July 27 & Aug 11, 2020

This incident highlighted a gap in WPC Rigor and recognition of HPI Error Precursors

We identified the need to drive the level of rigor more broadly



ACCELERATOR DIRECTORATE | Plans and Procedures | Document Title: Hipot Testing Procedure | Document Number: AD-00-002 | Page 8 of 12

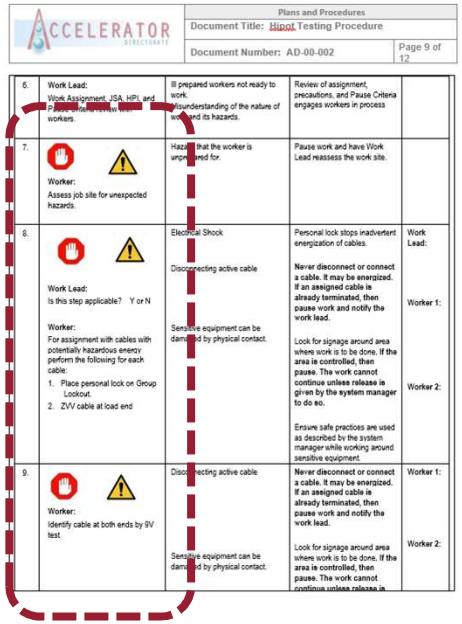
SLAC NATIONAL ACCELERATOR LABORATORY — EED OPERATIONS AND POWER SYSTEMS DEPARTMENT

Work Planning and Control

JOB SPECIFIC JSA

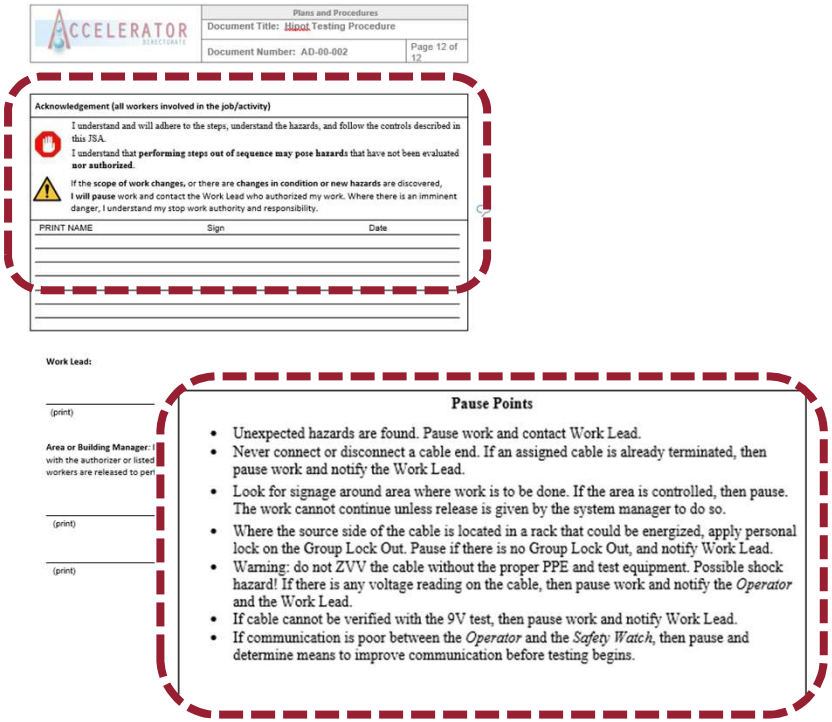
Job / Activity Name: Cable Termination in an energized area		ESA # (optional):	Start Date:	Valid
Department / Group Name: EED-OPST	Bldg / Area Location(s):	Other Information or References: LCLS2-JSA-0052		
Scope of Work: Test the leakage current of a high voltage cable that has been terminated on both ends				

Step	Description	Hazard	Mitigation	Task Completed Initial/Date
1.	Work Lead: Job site hazard review.	__ Radiation __ Electrical __ Ergonomic __ Working at Heights __ Working in a Construction Area __ Confined Space __ Other	__ Training __ PPE __ Tools/equipment	
2.	Work Lead: COVID hazard review.	Infectious Disease __ Hazard Level 1 __ Hazard Level 2 __ Hazard Level 3	__ Masks __ Gloves __ Cleaning __ Minimize close contact	
3.	Work Lead: Cables with potential hazardous energies are defined, LOTO points are identified, and Group Lockouts are in place.	__ Electrical Shock from cable __ N/A	__ Training __ LOTO __ PPE	
4.	Work Lead: Training assessment of workers complete.	Worker unaware of potential hazards leading to accident or injury	Check JSA	
5.	Work Lead: Area manager release.	The possible negative affect of other work in area.	Planning with other affected work groups.	



ACCELERATOR DIRECTORATE | Plans and Procedures | Document Title: Hipot Testing Procedure | Document Number: AD-00-002 | Page 9 of 12

6.	Work Lead: Work Assignment, JSA, HPI, and Pause Criteria review with workers.	Ill prepared workers not ready to work. Misunderstanding of the nature of work and its hazards.	Review of assignment, precautions, and Pause Criteria engages workers in process	
7.	Worker: Assess job site for unexpected hazards.	Hazard that the worker is unprepared for.	Pause work and have Work Lead reassess the work site.	
8.	Work Lead: Is this step applicable? Y or N Worker: For assignment with cables with potentially hazardous energy perform the following for each cable: 1. Place personal lock on Group Lockout. 2. ZVV cable at load end	Electrical Shock Disconnecting active cable Sensitive equipment can be damaged by physical contact.	Personal lock stops inadvertent energization of cables. **Never disconnect or connect a cable. It may be energized. If an assigned cable is already terminated, then pause work and notify the work lead.** Look for signage around area where work is to be done. **If the area is controlled, then pause. The work cannot continue unless release is given by the system manager to do so.** Ensure safe practices are used as described by the system manager while working around sensitive equipment.	Work Lead: Worker 1: Worker 2:
9.	Worker: Identify cable at both ends by 9V test.	Disconnecting active cable Sensitive equipment can be damaged by physical contact.	**Never disconnect or connect a cable. It may be energized. If an assigned cable is already terminated, then pause work and notify the work lead.** Look for signage around area where work is to be done. If the area is controlled, then pause. The work cannot continue unless release is	Worker 1: Worker 2:



ACCELERATOR DIRECTORATE | Plans and Procedures | Document Title: Hipot Testing Procedure | Document Number: AD-00-002 | Page 12 of 12

Acknowledgement (all workers involved in the job/activity)

I understand and will adhere to the steps, understand the hazards, and follow the controls described in this JSA.

I understand that **performing steps out of sequence may pose hazards** that have not been evaluated **nor authorized.**

If the **scope of work changes,** or there are **changes in condition or new hazards** are discovered, **I will pause** work and contact the Work Lead who authorized my work. Where there is an imminent danger, I understand my stop work authority and responsibility.

PRINT NAME | Sign | Date

Work Lead:

(print)

Area or Building Manager: I with the authorizer or listed workers are released to per

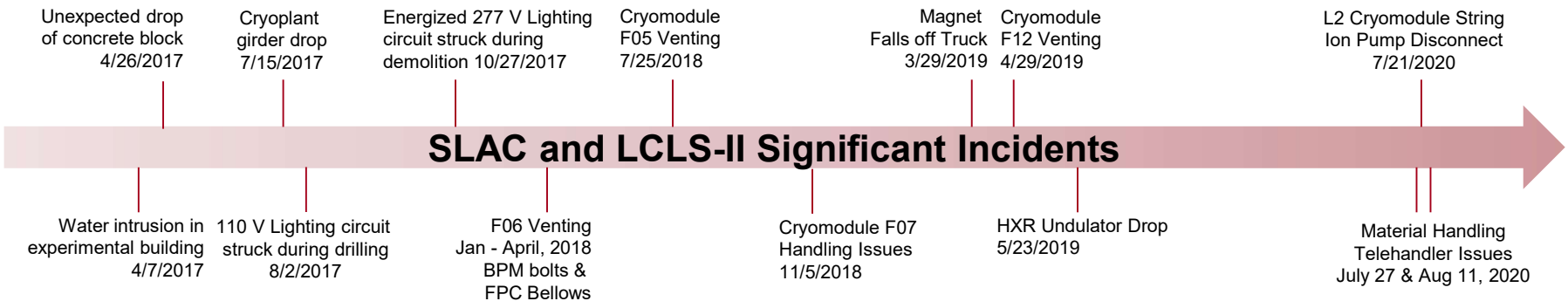
(print)

(print)

Pause Points

- Unexpected hazards are found. Pause work and contact Work Lead.
- Never connect or disconnect a cable end. If an assigned cable is already terminated, then pause work and notify the Work Lead.
- Look for signage around area where work is to be done. If the area is controlled, then pause. The work cannot continue unless release is given by the system manager to do so.
- Where the source side of the cable is located in a rack that could be energized, apply personal lock on the Group Lock Out. Pause if there is no Group Lock Out, and notify Work Lead.
- Warning: do not ZVV the cable without the proper PPE and test equipment. Possible shock hazard! If there is any voltage reading on the cable, then pause work and notify the *Operator* and the Work Lead.
- If cable cannot be verified with the 9V test, then pause work and notify Work Lead.
- If communication is poor between the *Operator* and the *Safety Watch*, then pause and determine means to improve communication before testing begins.

The key lessons learned

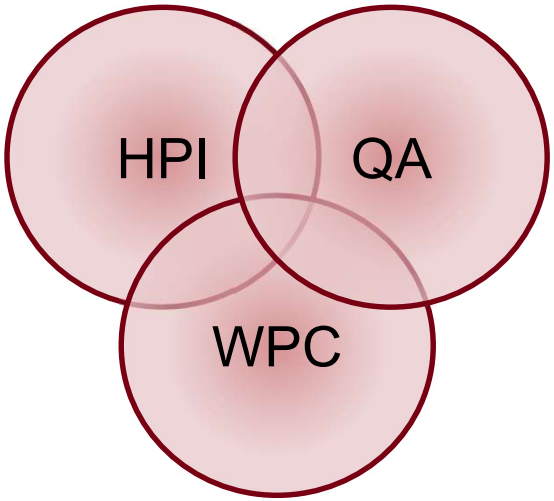


While investigating individual incidents is both useful and required the findings and actions have been less effective than expected.

Taking a broader examination of all deviations from expected, i.e. Incidents to Non-Conformance will in the long term drive greater improvement.

How Human Performance Improvement, Quality Assurance and Work Planning & Control exist together

- Why & how human errors occur
- Identify mitigations
- Design controls to reduce/stop errors



- Ensure all the pieces are in place and working together as required.
- Answer the question, How do you know?

- Scope & Requirements
- Risks & Mitigations & Controls
- Perform work within controls
- Learn and Improve

Questions?