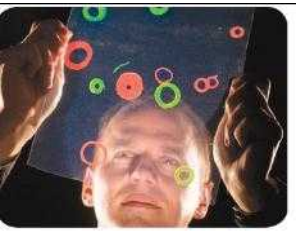
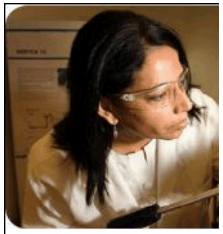
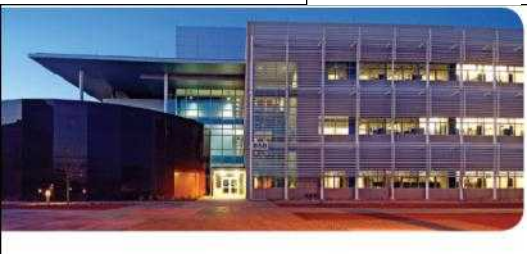
SAND2015-8963C







Engineered Safety

Some key principles and examples

Sandia National Laboratories

Exceptional service in the national interest

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Starting Principles

Sandia National Laboratories

Safety needs to be considered in a “system engineering” context.

Principle-based approach for designing “operational systems” that are inherently safe to the extent possible.

Mature our safety culture.

Management engagement in:

1. Defining “unacceptable consequences” (high consequence risks) for the primary hazards of our activities

2. Ensuring “technical due diligence” is carried out to prevent or mitigate these consequences (engineered controls where feasible, providing defense-in-depth for single points of failure and human performance)

3. Document 1 & 2 in a “Safety Case”

Five Questions that the "Safety Case" should answer

Sandia National Laboratories

1. **Who is the decision maker?**
   - Dependent upon Hazard Level
2. **What are the Unacceptable Consequences?**
   - What are the most significant effects that we do not want to happen?
3. **How can the system fail?**
   - A summary of, or reference to, a sufficiently detailed Hazard Analysis
4. **What are the controls?**
   - Design features, engineered and administrative controls. Justification for not having engineered controls
5. **How do we know it works?**
   - Explain how you maintain and verify the function of the safety controls (positive verification)

Some Lessons Learned So Far….

- Some confusion over definitions of unacceptable consequences (vs. undesired) and engineered controls vs. administrative controls and PPE.
- Effectiveness of administrative controls tended to be overestimated, including “two person checking/inspection”.
- Human limitations on critical thinking about how systems can fail. Especially when encountering off-normal situations, troubleshooting mode and/or multi-org work interfaces.
- Positive verification mindset was less mature than needed. Realization that positive verification of administrative controls is difficult if not impossible.

Unacceptable Consequences

Sandia National Laboratories

What line managers do not want to happen as a result of activity-level work.

- Harmful effects of accidents on people and the environment
- Temporary or permanent loss of mission capability
- Impact to national security
- Serious damage to the reputation of the institution
- The effects of exposure to known health hazards

The unacceptable consequences serve as a reference point for beginning the design of the new system or reviewing the design of an existing system.

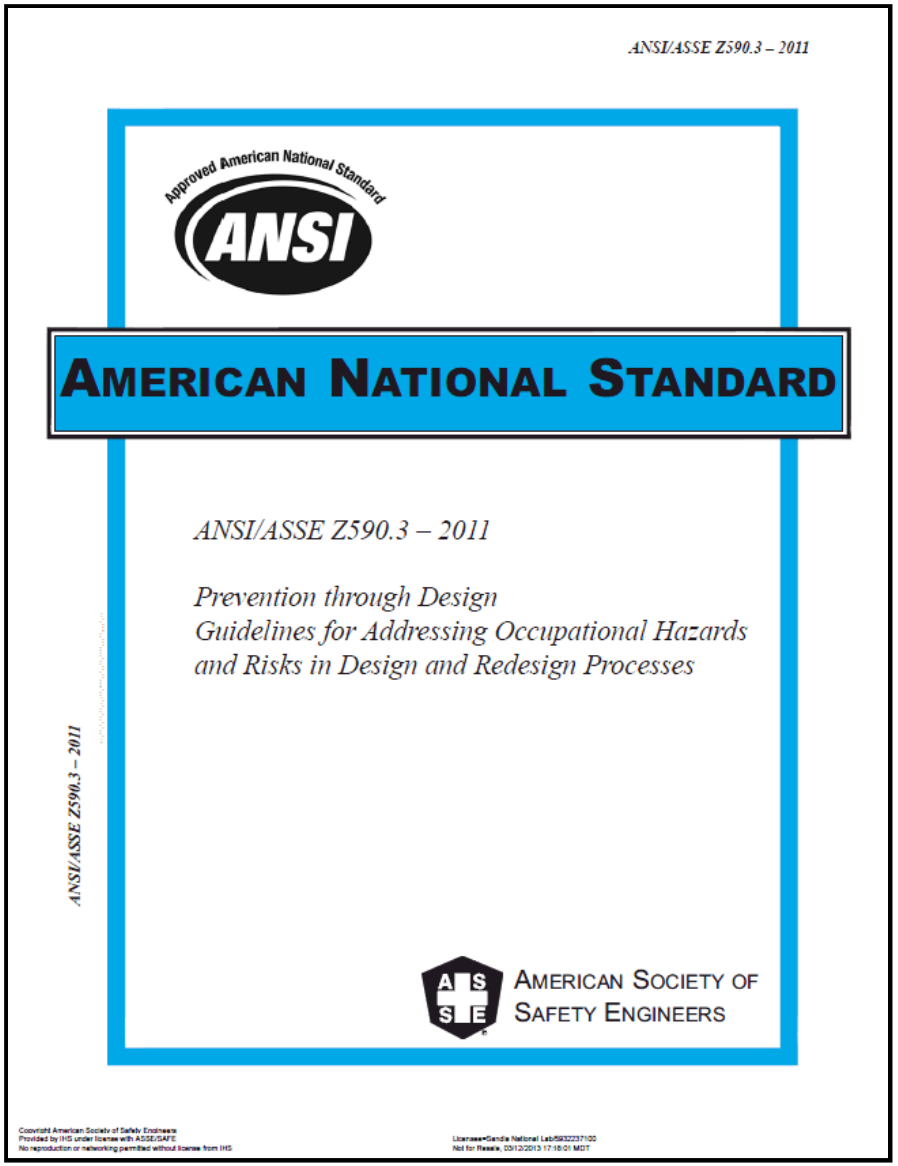
A face-to-face discussion with team members, SMEs, ES&H coordinators and management will facilitate the development of appropriate controls.

Hierarchy of Controls

Most Preferred	
	Risk Avoidance: Prevent entry of hazards into a workplace by selecting and incorporating appropriate technology and work methods criteria during the design processes.
	Eliminate: Eliminate workplace and work methods risks that have been discovered.
	Substitution: Reduce risks by substituting less hazardous methods or materials.
	Engineering Controls: Incorporate engineering controls/safety devices.
	Warning: Provide warning systems.
	Administrative Controls: Apply administrative controls (the organization of work, training, scheduling, supervision, etc.).
Least Preferred	**Personal Protective Equipment:** Provide Personal Protective Equipment (PPE).

This is an area where IH's/ESH Professionals can bring great value and expertise.

Make it a technical challenge that is engaging to the technical leaders and engineers… safer designs are worthy of our best technical efforts



Engineering Controls vs Administrative and PPE

- **Engineered controls are physical or engineered features that prevent accidents by making human error impossible, shutting down if an unsafe condition is about to occur, or providing a clear, unambiguous and compelling alarm signal that drives the human to immediately correct the error before an accident results.** An engineered control does not allow a human error to be made and go undetected long enough for an accident to occur.

- Administrative controls are subject to human error. As a result, **administrative controls always fail eventually – its just a matter of time.** Therefore, an effective safety system cannot be constructed using a string of administrative controls only. At least one (preferably two) engineered control must be included in the string of controls for safety to be assured. As a thought experiment ask yourself, "how long a string of administrative controls (with zero engineered controls included) would be considered acceptable to prevent a nuclear safety accident (unintentional nuclear detonation)"? The answer is, "There is no acceptably long string of administrative controls that can be used to assure nuclear safety". Administrative controls are nice to have but no credit is given for them for nuclear safety. Instead nuclear safety relies heavily on multiple, independent engineered controls.

- Personal Protective Equipment is a control but it is not an engineered control. **PPE does not prevent accidents it mitigates the consequences after an accident has occurred**.

Know this, before you rely on Two Person Checking….

- Adding a second human inspection provides a false sense of security. Joseph Juran demonstrated in the 1920s and 1930s that **adding additional inspectors to improve problem detection performance was not effective.** Intuitively, most people assume that adding a second person to "double check" them provides a large improvement in detecting errors and problems but the research shows that, in general, adding a second person provides a small, almost negligible improvement and adding a third person is actually less effective than if you only had one person checking. As a result **adding a second human inspection step is a weak control and should not be relied on or given much credit when assured safety is desired.**

Effective Engineered Safety relies on Critical Thinking about the Failure Modes

- When determining how the system can fail, general answers such as “human error” or “machine malfunction” are inadequate. Instead identify the parts of the work that might be counter-intuitive, actions that new hires tend to have difficulty with, or actions where human error might result in a specific type of problem that you are most concerned about. Likewise provide more detail about specific machine malfunction types that you are most concerned about or have experienced in the past with similar machines.

Positive Verification

- **Positive verification requires a mindset that something is not safe until otherwise demonstrated**. Without positive verification we can't tell if an accident hasn't happened because our system is effective or because we have just been lucky.
- **Another benefit of engineered controls – they are easier to verify for effectiveness than administrative controls.** An engineered control can be visually inspected or, in some cases, even tested.
- Administrative controls are always suspect due to their susceptibility to human error.

Sandia National Laboratories

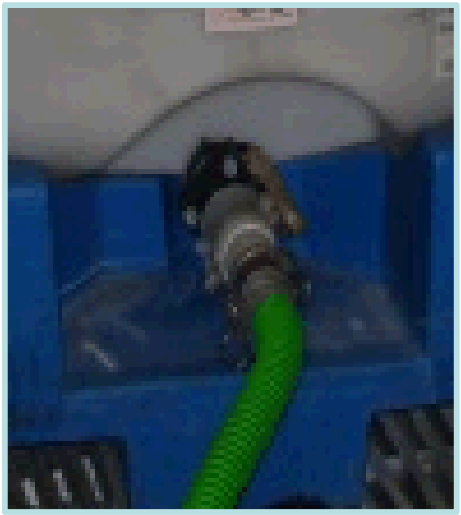
Examples

Chemical Dispense System

Sandia National Laboratories

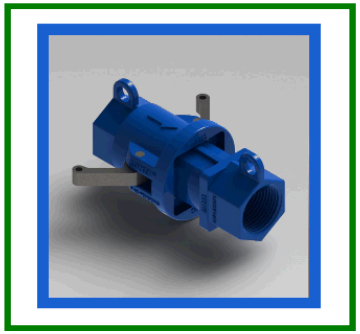
Before

275 gallon tote of Sulfuric Acid (H_2SO_4) was mistakenly hooked up to a Sodium Hydroxide (NaOH) chemical dispense system. The valve from the Sulfuric Acid tote was opened, at which time Sulfuric Acid (93%) was gravity fed into the transfer hose and piping manifold which contained residual Sodium Hydroxide (45%) causing a chemical reaction. The operator noticed the mistake immediately and reacted by closing the tote valve and disconnecting the transfer hose. Approximately 500ml of H_2SO_4 poured from the hose into the secondary containment where it reacted with water generating water vapor that subsequently activated a smoke detector. No injuries occurred but minor equipment damage resulted.



After

In partnership with chemical supplier, Kem-Key mistake-proofed couplers are now used to ensure acid and base interconnects are inherently incompatible.



Base Coupling

Acid Coupling

KEMKEY collaborated with Sandian Juan Romero, on original connector design (2013)

KemKey formed in 2013 - products are relatively new. PNM started using connectors the same month the Sandia accident occurred. MESA is piloting their use at Sandia.

New Base Coupling

http://kemkey.com/

Interim Acid Coupling
(waiting on orange acid coupling)

Sodium Metabisulfite Tank Fill

Removal of Hazard via Engineering Control

Before

The filling of the sodium metabisulfite tank required the use of an air purifying respirator, due to exceeding STEL (short term exposure limit, ACGIH) of .25 ppm of sulphur dioxide. A project was implemented to re-design the tank with LEV (local exhaust ventilation). Design called for 50' of 8" acid duct to tie in with facility acid exhaust system.

After

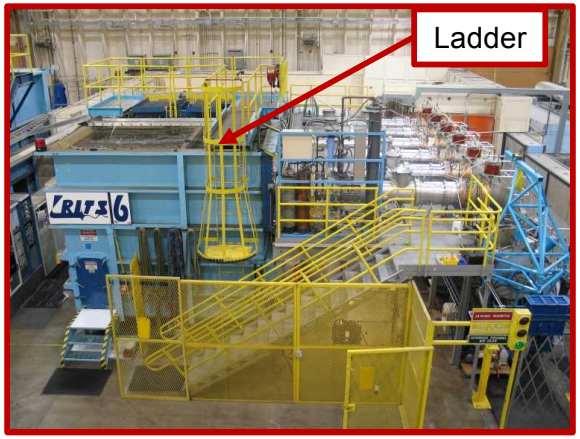
Post project monitoring determined samples were below the lower detectible limit of sulphur dioxide. Due to this, IH has downgraded the PPE needed to perform this task as of 7/30/15. This project has successfully engineered out the use of respiratory protection.

RITS-6 Safety Improvements

Sandia National Laboratories

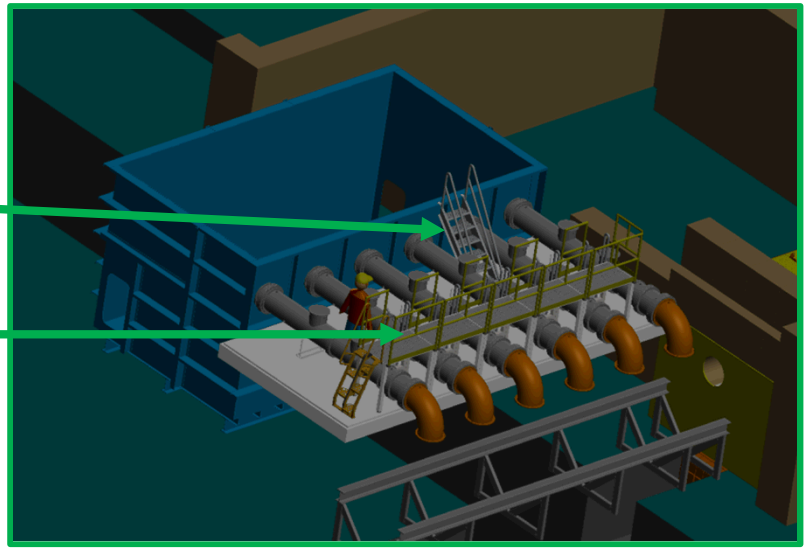
Current

Access to top of the Radiographic Integrated Test Stand (RITS-6) Marx generator tank requires climbing a 14 foot ladder to the platform. This task is conducted at least once per week. Also, access is often needed to the 6 pulse-forming lines (PFLs) for various inspections and maintenance activities. The PFLs are accessed via a narrow walkway and a series of "wobbly" plastic stairs. The RITS-6 team recognizes that these conditions are not ideal and increase the potential for serious fall injuries.



Design Changes being installed in the Near Future (by Sept 2015)

- Stairway with railings for access to work platform on top of the Marx generator tank. Will no longer need to use the ladder.
- Platform with railings and fixed stairs with railings and access steps to the PFLs. Will no longer need to use narrow walkway and wobbly stairs.



RITS-6 Safety Improvements

Sandia National Laboratories

Current

Maintenance on RITS-6 Marx generator banks requires working from ladders to access elevated components. The RITS-6 team recognizes that these conditions are operationally challenging and expose workers to the potential for serious fall injuries.

Design Changes

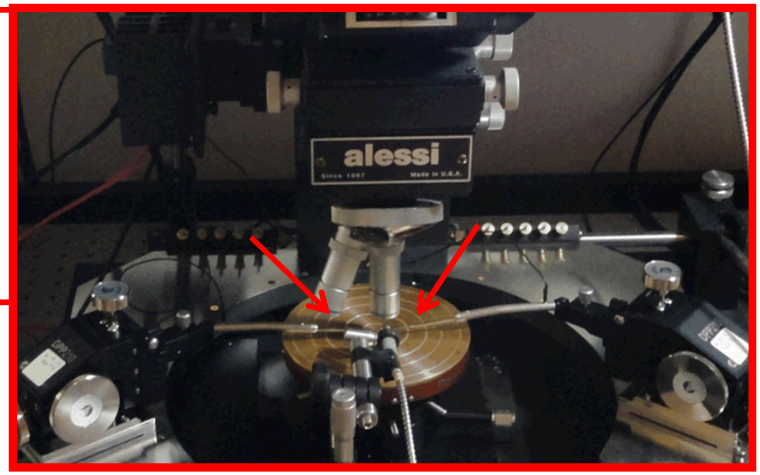
The picture shown below shows how this issue has already been addressed with Ursa Minor. A commercially available, customizable work-platform has been installed to improve access and eliminate much of the need for ladder work. The RITS 6 team is investigating a similar work platform to improve accessibility and safety for maintenance on the RITS-6 Marx generator.

High-Current Pulsed Testing Probe Station

Sandia National Laboratories

Before

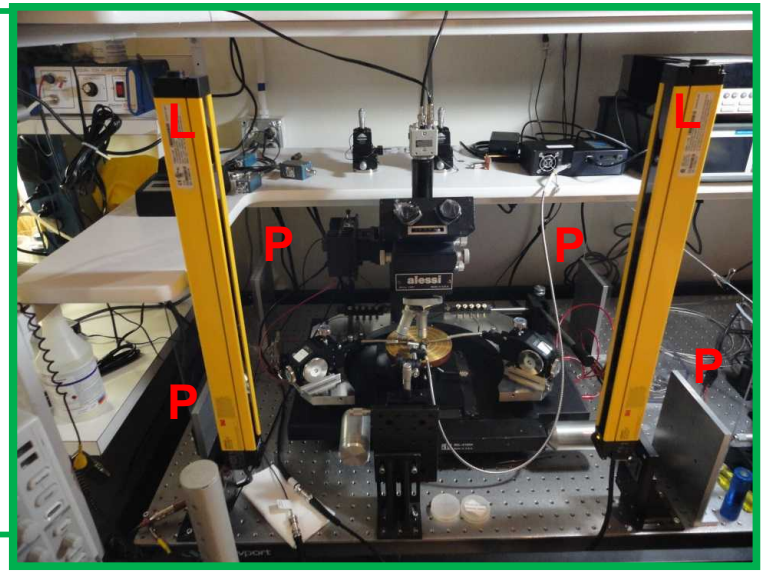
Probe station was used for on-wafer electrical testing (low voltage, <50V) of UV laser diodes. Red arrows show probe manipulators which apply current to device. These probes present a potential exposure point to voltage and current when sample is under test. New project required higher voltages and currents (~ 70V/2A).



After

As a result of the engineered safety process, engineered controls were implemented to control the potential exposure points to hazardous voltages and currents. A "light curtain" and Plexiglas barriers were installed around the probe station.

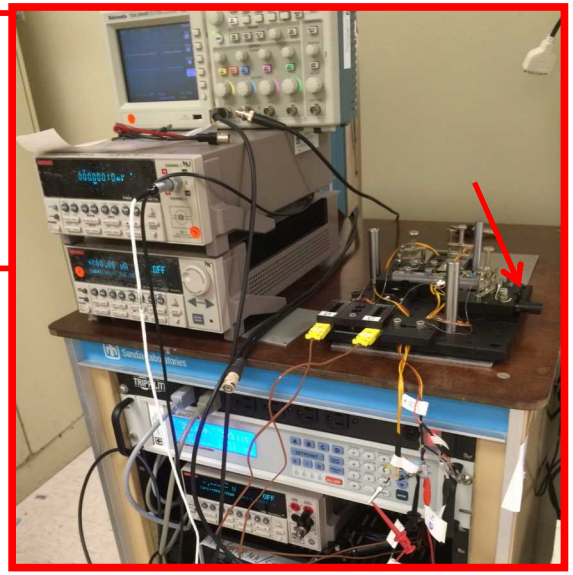
- Light curtain (**L** – in figure) consists of a linear strip of near-IR LEDs on one bar and a matching strip of detectors on the other bar. A switch is added to the circuit that sends current to the probes; it trips if anything intercepts IR beam during testing, shutting off current to the device.
- Plexiglas shielding (**P** – in figure) was added to sides of probe station to prevent reaching around the light curtain.



Probe Station

Before

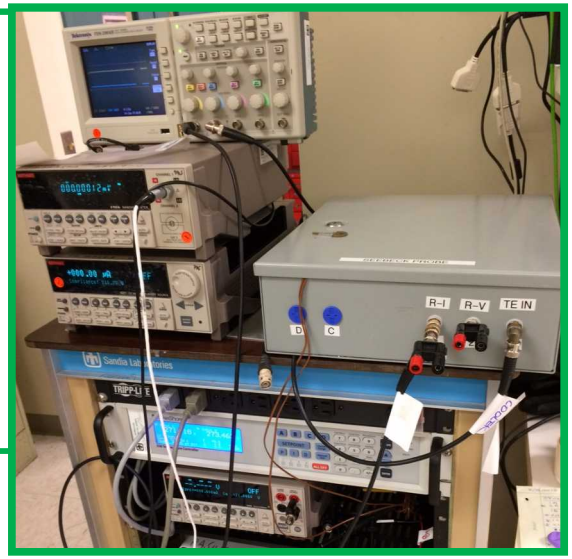
Source meter is used to supply current to a thermoelectric cooler for testing. This experiment requires constant currents of <100mA at a voltage of <1 V. However, the source is capable of up to 200 V output. Red arrow shows probe manipulators which apply current to device.



After

Through the engineered safety process the work planning team identified a potential failure mode. An internal failure in the source meter or human error could result in the maximum 200V to the probes, potentially exposing the user to a shock hazard. An enclosure was made to house the experiment, providing an insulated, physical barrier between electrical probes and the user.

Note: When additional resources are available a source meter with less maximum output potential (<50 V) will be obtained.



RITS-6 Safety Improvements

Sandia National Laboratories

Before

RITS-6 operations involves positioning a 750 pound instrument cart by rolling it over a section of metal grating. This was a strenuous activity that required personnel to pull with significant force, increasing the risk of muscle strain related injury.

After

Creative thinking by the RITS-6 Team resulted in covering the section of metal grating with a solid metal plate. It now requires only 56 lbs. of force to position the cart, making the transition smooth and easy. It also prevents small tools, pens and hardware from falling through the grate to the trench below.

Welded a solid plate over the metal grating.

750 pound shielded camera cart.

Repetitive Motion Injury Moving Gas Cylinders

Sandia National Laboratories

Before

In Sept. 2014, a worker sustained a repetitive motion strain on their right elbow. The strain was felt over several weeks due to the work activity of the Carbon Dioxide (CO_2) cylinder replacement project. The worker loaded and unloaded cylinders and rotated each cylinder onto and off of a 3 inch high grated platform. The grated platforms were originally intended to address the problem of pooled rainwater corroding the bottom of these gas cylinders. Each cylinder is about 5 feet tall and weighs between 100 lbs. (empty) and 300 lbs. (full). The worker rotated approximately 20 gas cylinders in and out of the designated outside storage racks before reporting the injury. (recordable injury, incident # 20140252).

After

The 3 inch high gas cylinder platforms were replaced with a 1 inch high grated platform that covered the entire cart and cylinder storage area.

A low angle ramp was also installed for the 1 inch transition up to the new platform.

This engineered control eliminates the repetitive motion injury threat.

3 inch high grated platforms

1 inch high grated platform

Low angle cart ramp

Acid Waste Tank

Before:
Acid waste tank drain valve stem exposed and single point failure for large volume release of corrosive waste water. Potential risk of damage and leak from carts and equipment in motion and/or foot traffic.

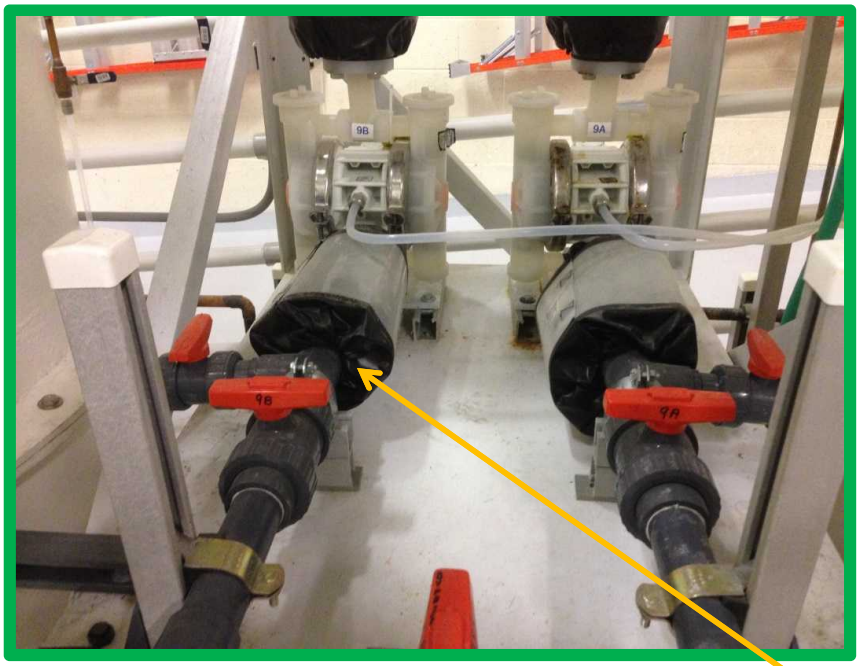
After:
Metal cover installed over acid drain valve stem with high visibility yellow/black striping.

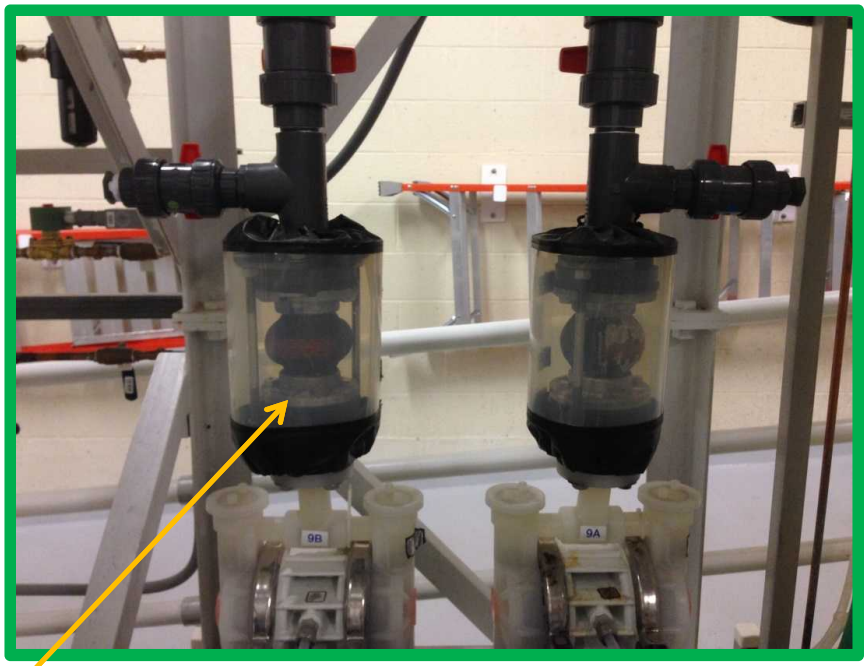
De-ionized Water Tank

Sandia National Laboratories

Overflow drain added to reduce consequences of a flood into DI water room

Acid Waste Neutralization System



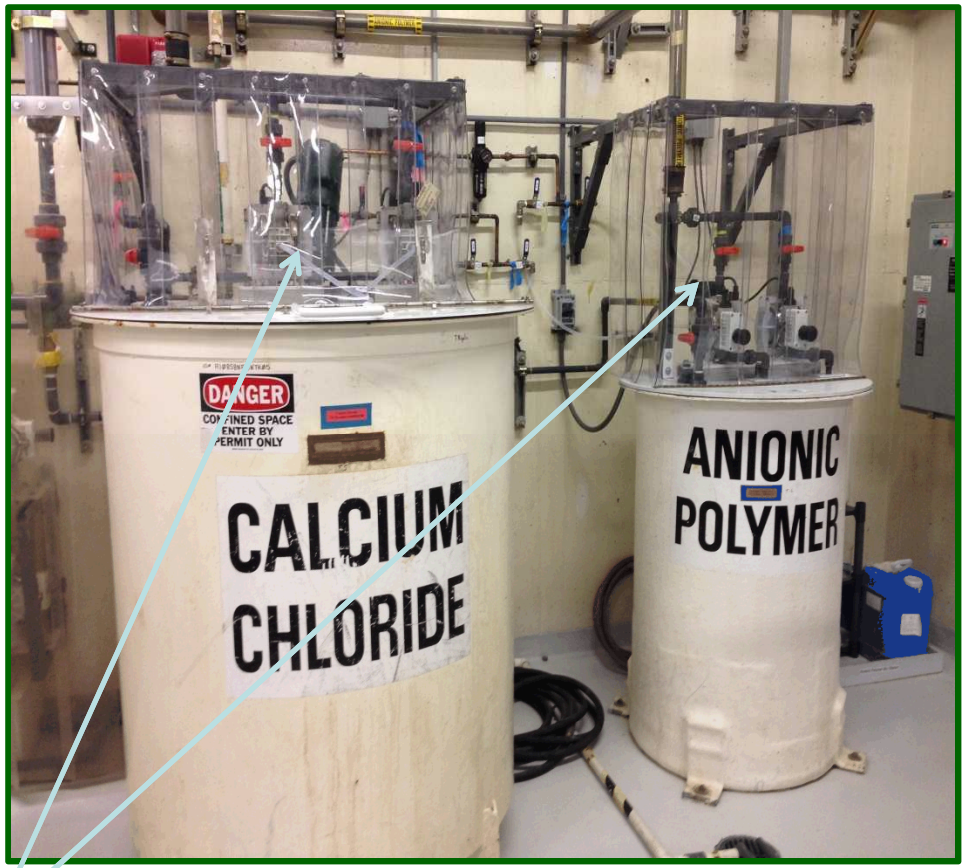


During safety case development walkthroughs, the AWN team identified potential single-point failure on shock absorbers for pressurized fluoride waste distribution systems. Team installed poly guards to contain spraying if leak developed.

Leroy James, SNL
jamesla@sandia.gov

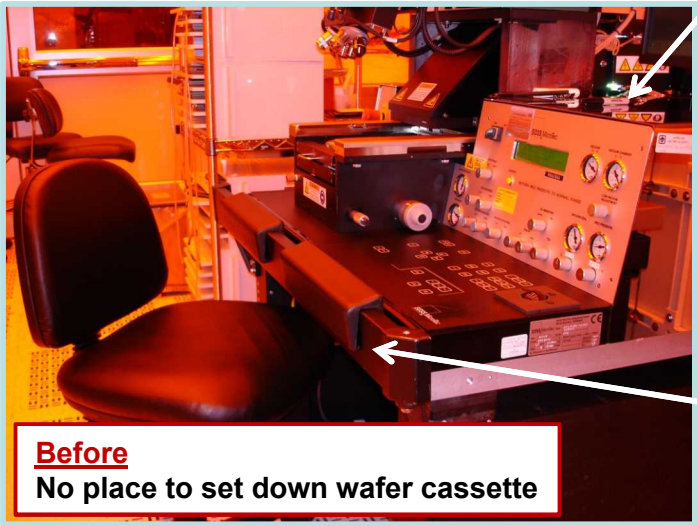
Safety Case on May 21, 2013
858N Acid Waste Neutralization system

Sandia National Laboratories



Poly curtain protection applied to eliminate chemical spraying on workers in the event of pump failure

Improved Wafer Cassette Tables



Before
No place to set down wafer cassette

Fab operator attempted to place a cassette full of wafers on top of an contact aligner.

The cassette slipped in their hands and the operator reflexively moved to catch the cassette.

In the process they seriously jammed their middle finger on the front of the contact aligner.

After
Wafer cassette tables installed by each contact aligner. Supports bolted to floor under aligner. If not needed, table can be folded down by pulling on pull rings. Has large curve radius, ¼" PVC coated clean room bump pad (blue), and 3-sided guard rail w/rounded corners.

Operator Feedback
I like them / Nice to have some extra storage space / They are very helpful / I think they work, needed somewhere to put our stuff / The shape is odd but I like them to hold my traveler and work materials / They are awesome / I was fine with or without them but I use the space now.

Improved Office Safety

Sandia National Laboratories

Before
Computer cable on top of carpet is trip hazard and chair entanglement hazard

After
In-Carpet Wireway with 15” ramps (under existing carpet) eliminates hazard