Quantifying the Qualitative – The Science and Application of Human Factors in Process Safety Modeling and Planning

Ray Huang
Principal Engineer and Office Director
Exponent Inc. – Asia Pacific

Safety Case Symposium 2019
Singapore
Mar 26 - 27, 2019

Introduction

- Exponent is a multi-disciplinary consulting firm that brings together more than 90 different disciplines to solve important engineering, science, and regulatory issues facing our clients

Background

Oklahoma City bombing

Hurricane Katrina

World Trade Center

Main Message

- Rigorous human factor analysis should be employed proactively and early to assess the overall risk with the goal to minimize it
- Human factor analysis ideally should be based on scientific method and testing; decisions need to be based on both qualitative and quantitative data via thorough analysis and testing
- New tools have been developed to help with HF testing, including AR/VR, training regimes and physiological sensing

Operator Error

33 miles west of Los Angeles, the 2008 Chatsworth accident occurred on Metrolink's Ventura Subdivision. Source: NTSB

Bilevel passenger coach of the type involved in the 2008 Chatsworth accident. Though referred to as bilevel, these coaches actually have three separate levels of passenger seating accommodations for 142 to 143 seated passengers or about 360 passengers (standing and sitting). Source: NTSB

The 2005 Glendale accident. A southbound Metrolink commuter train derailed after colliding with a Jeep Cherokee and smashed into the locomotive of a sidelined freight train. As the southbound train jackknifed, it hit a northbound Metrolink commuter train passing on an adjacent track.

Off the rails

Every unique railroad accident produces an abundance of unique data that must be analyzed and interpreted

January 26, 2005: In an alleged attempt to commit suicide, a man parked his gasoline-drenched Jeep Cherokee on train tracks in Glendale, California. Changing his mind at the last minute, he jumped out of the way before a fast-moving southbound Metrolink train struck the Jeep, derailed onto a siding and struck a parked Union Pacific freight locomotive, and jackknifed to collide with another Metrolink train traveling in the opposite direction. 11 people died and nearly 200 were injured.

September 12, 2008: The worst U.S. train crash in 15 years is attributed to the train driver who sent and received text messages seconds before his crowded Metrolink commuter train allegedly skipped a red light. The Metrolink train collided head-on with a Union Pacific freight locomotive in Chatsworth, California, killing 25 and injuring over 100 people.

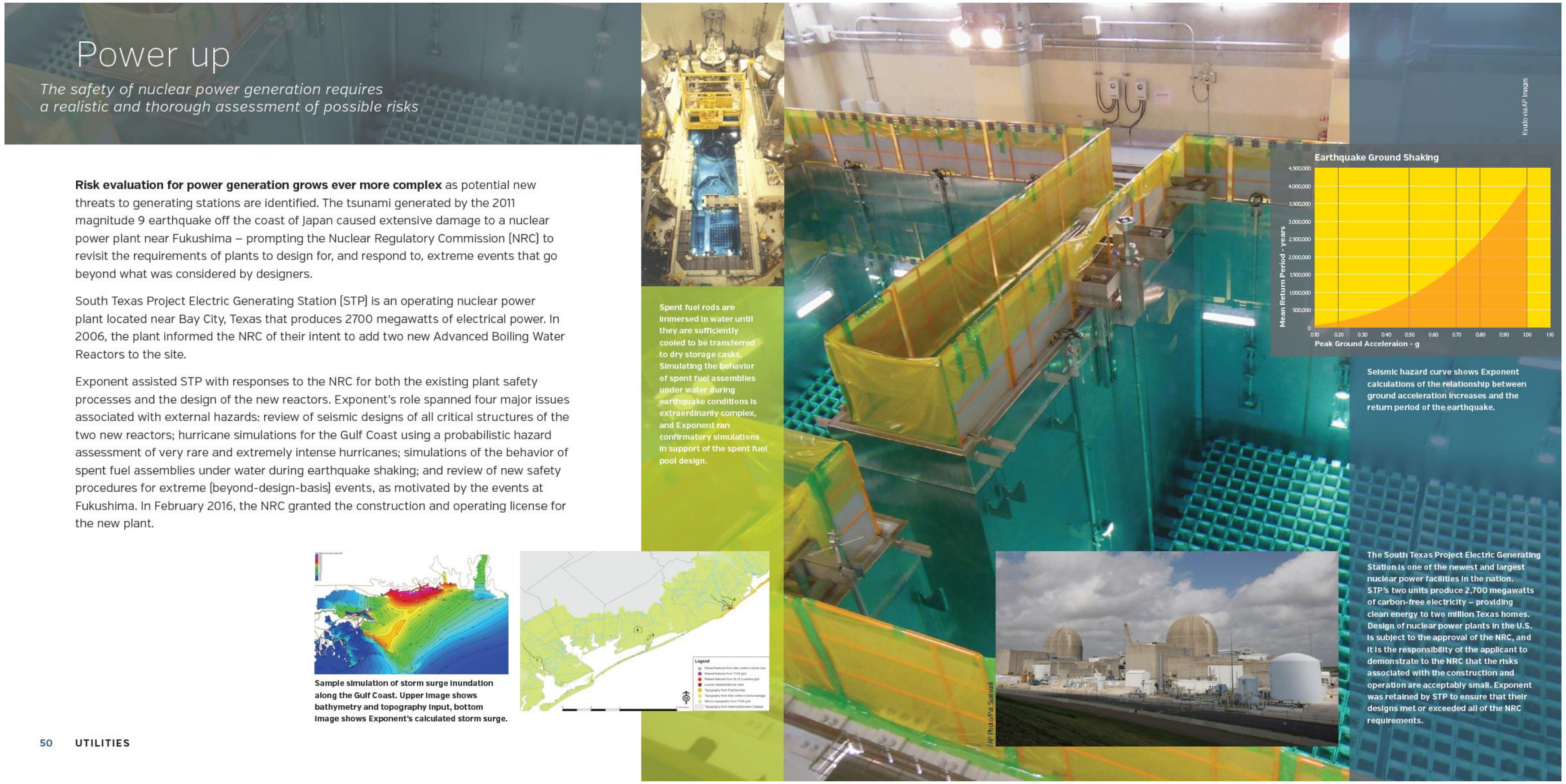
What these cases have in common, beyond the regrettable human tragedy, is the vast amount of data they produce. Passenger and freight rail lines, owners of rights-of-way, individuals, rail car manufacturers, and many other parties have a vested interest in accurately understanding what happened in order to assign culpability, ensure future preventability, and promote public safety.

As in these and other cases, Exponent lends its expertise to those who seek to better understand events where an integrated approach can be advantageous. Exponent provides engineering design, testing, accident reconstruction, and human factors expertise (such as signaling or visibility) to better reach scientific, regulatory, and legal clarity.

The 2008 Chatsworth accident. The Metrolink's locomotive and lead passenger car (out of a total of three passenger cars) derailed. The Union Pacific Railroad freight train derailed its two locomotives and 10 of its 17 cars. Source: NTSB

TRANSPORTATION 23

Ultimate Goal – Process Safety



Power up

The safety of nuclear power generation requires a realistic and thorough assessment of possible risks

Risk evaluation for power generation grows ever more complex as potential new threats to generating stations are identified. The tsunami generated by the 2011 magnitude 9 earthquake off the coast of Japan caused extensive damage to a nuclear power plant near Fukushima – prompting the Nuclear Regulatory Commission (NRC) to revisit the requirements of plants to design for, and respond to, extreme events that go beyond what was considered by designers.

South Texas Project Electric Generating Station (STP) is an operating nuclear power plant located near Bay City, Texas that produces 2700 megawatts of electrical power. In 2006, the plant informed the NRC of their intent to add two new Advanced Boiling Water Reactors to the site.

Exponent assisted STP with responses to the NRC for both the existing plant safety processes and the design of the new reactors. Exponent's role spanned four major issues associated with external hazards: review of seismic designs of all critical structures of the two new reactors; hurricane simulations for the Gulf Coast using a probabilistic hazard assessment of very rare and extremely intense hurricanes; simulations of the behavior of spent fuel assemblies under water during earthquake shaking; and review of new safety procedures for extreme (beyond-design-basis) events, as motivated by the events at Fukushima. In February 2016, the NRC granted the construction and operating license for the new plant.

Sample simulation of storm surge inundation along the Gulf Coast. Upper image shows bathymetry and topography input, bottom image shows Exponent's calculated storm surge.

Spent fuel rods are immersed in water until they are sufficiently cooled to be transferred to dry storage casks. Simulating the behavior of spent fuel assemblies under water during earthquake conditions is extraordinarily complex, and Exponent ran confirmatory simulations in support of the spent fuel pool design.

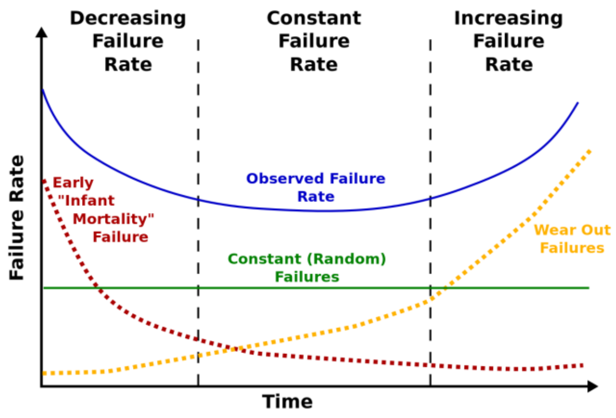
Seismic hazard curve shows Exponent calculations of the relationship between ground acceleration increases and the return period of the earthquake.

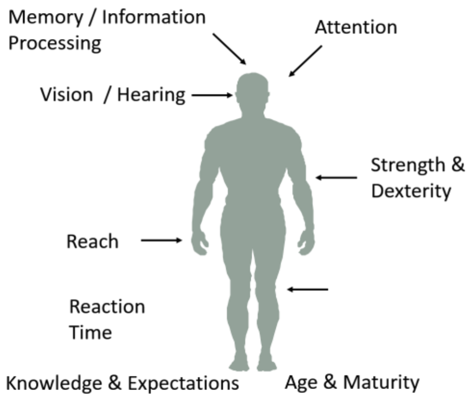
The South Texas Project Electric Generating Station is one of the newest and largest nuclear power facilities in the nation. STP's two units produce 2,700 megawatts of carbon-free electricity – providing clean energy to two million Texas homes. Design of nuclear power plants in the U.S. is subject to the approval of the NRC, and it is the responsibility of the applicant to demonstrate to the NRC that the risks associated with the construction and operation are acceptably small. Exponent was retained by STP to ensure that their designs met or exceeded all of the NRC requirements.

50 UTILITIES

Safety Case Symposium 2019
Singapore
Mar 26 - 27, 2019

Basic Premise





System Safety = Machine Reliability x Human Reliability

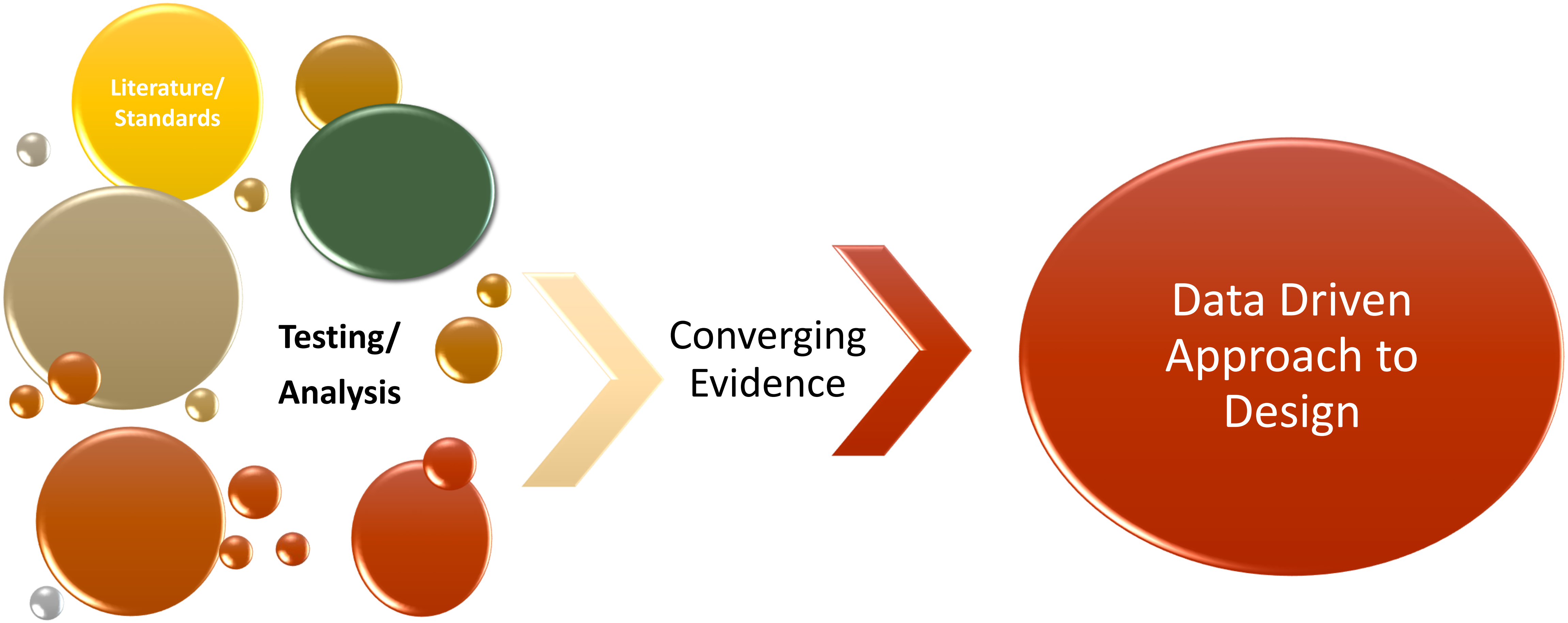
Human Reliability = Probability of Human Error (Human Factor for a Task)

Scientific Approach

- Human Factors is based on well-established scientific knowledge and tools and techniques that enable system optimization
  - "Root Cause Hypotheses"
  - Describes human interactions within a work system and can be applied to different systems – oil platform, chemical process plant, hospital, etc.
  - Applies to all aspect of system lifecycle, including design, operations and decommissioning
  - This includes the tasks people perform, the tools and equipment they use to perform the task, the workspace/work area where the work is undertaken, and the influence

Safety Case Symposium 2019 Singapore Mar 26 - 27, 2019

Toolbox: Methodology



Qualitative Approach

Safety-Critical Task Screening

Screening Tool to Determine Task Vulnerability to Human Failure

	High	Medium	Low	N/A
1. The intrinsic hazards associated with the task (in terms of substances, energies, or conditions)	3	2	1	0
2. The extent to which ignition sources are introduced by the performance of the task	3	2	1	0
3. The requirement to override safety protection systems as part of the task	3	2	1	0
4. The extent to which incorrect performance of the task could lead to damage to the system	3	2	1	0
5. The extent to which the task requires changes to the configuration of the system	3	2	1	0

N/A, not applicable

The results for all five questions are summed, resulting in a possible score between 0 and 15. A series of criticality bands are assigned, linked to the total score, allowing tasks to be defined as High (9–15), Medium (5–8), or Low (1–4) criticality, and prioritized for further analysis.

- In general, qualitative approaches seek to describe the potential error, the consequences and potential error reduction measures

Quantitative Approaches

Existing Standards – Software and Hardware

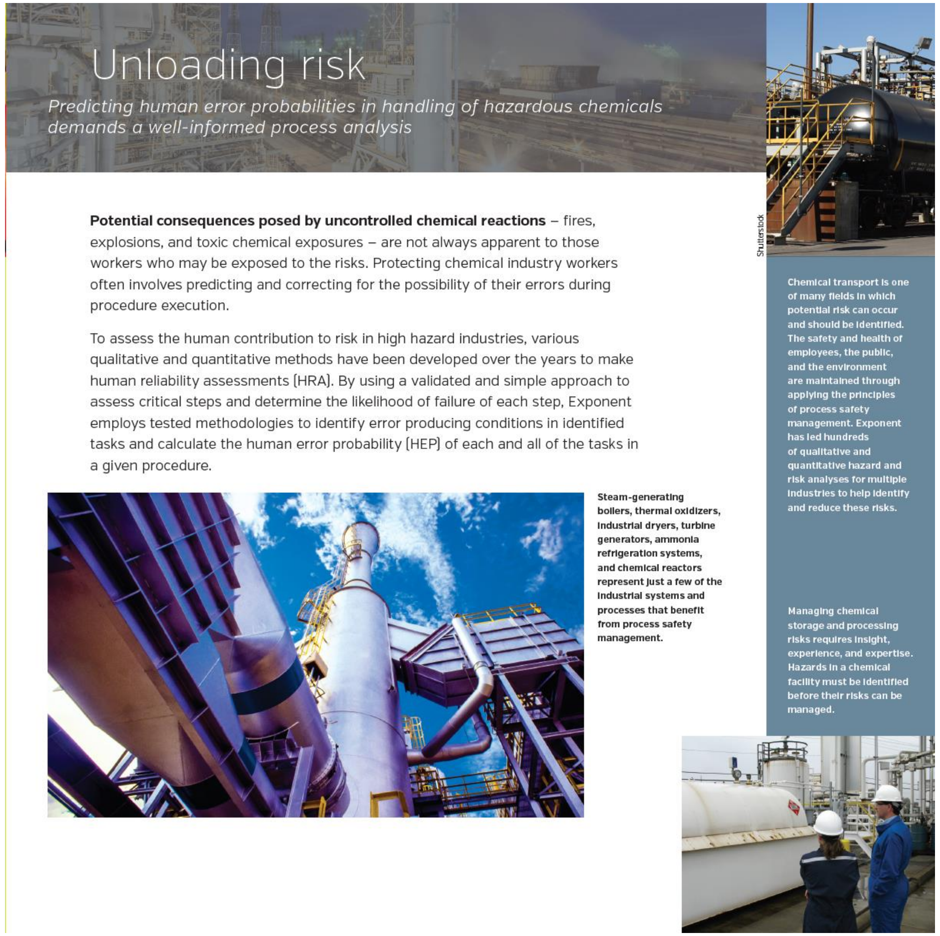
- MIL-STD-882E
- IEC 61508

TABLE A-II. Example probability levels

Probability Levels				
Description	**Level**	**Individual Item**	**Fleet/Inventory***	**Quantitative**
Frequent	**A**	Likely to occur often in the life of an item	Continuously experienced.	Probability of occurrence greater than or equal to 10^{-1}.
Probable	**B**	Will occur several times in the life of an item	Will occur frequently.	Probability of occurrence less than 10^{-1} but greater than or equal to 10^{-2}.
Occasional	**C**	Likely to occur sometime in the life of an item	Will occur several times.	Probability of occurrence less than 10^{-2} but greater than or equal to 10^{-3}.
Remote	**D**	Unlikely, but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur.	Probability of occurrence less than 10^{-3} but greater than or equal to 10^{-6}.
Improbable	**E**	So unlikely, it can be assumed occurrence may not be experienced in the life of an item	Unlikely to occur, but possible.	Probability of occurrence less than 10^{-6}.
Eliminated	**F**	Incapable of occurrence within the life of an item. This category is used when potential hazards are identified and later eliminated.		

What about Human?

- A study in 2010 performed by the NASA suggested that with well-trained flight controllers at Mission Control, the likelihood of errors in sending commands to the International Space Station ranged from approximately <u>0.1 to around 10^{-4}</u>.
  - These errors included selecting the wrong procedures to use, or sending the wrong command to the ISS, and were affected by working conditions such as fatigue, time pressure and cognitive overload.



Unloading risk

Predicting human error probabilities in handling of hazardous chemicals demands a well-informed process analysis

Potential consequences posed by uncontrolled chemical reactions – fires, explosions, and toxic chemical exposures – are not always apparent to those workers who may be exposed to the risks. Protecting chemical industry workers often involves predicting and correcting for the possibility of their errors during procedure execution.

To assess the human contribution to risk in high hazard industries, various qualitative and quantitative methods have been developed over the years to make human reliability assessments (HRA). By using a validated and simple approach to assess critical steps and determine the likelihood of failure of each step, Exponent employs tested methodologies to identify error producing conditions in identified tasks and calculate the human error probability (HEP) of each and all of the tasks in a given procedure.

Steam-generating boilers, thermal oxidizers, industrial dryers, turbine generators, ammonia refrigeration systems, and chemical reactors represent just a few of the industrial systems and processes that benefit from process safety management.

Shutterstock

Chemical transport is one of many fields in which potential risk can occur and should be identified. The safety and health of employees, the public, and the environment are maintained through applying the principles of process safety management. Exponent has led hundreds of qualitative and quantitative hazard and risk analyses for multiple industries to help identify and reduce these risks.

Managing chemical storage and processing risks requires insight, experience, and expertise. Hazards in a chemical facility must be identified before their risks can be managed.

Human Error Probability

$$\text{Ratio} = \frac{\text{Number of times an error is made when performing the task}}{\text{How often the task is completed over a given period of time}}$$

Some can be measured directly, some have to estimated

- Human Error Assessment and Reduction Technique (HEART)
- Nuclear Action Reliability Assessment
- Cognitive Reliability and Error Analysis Method
- And more…

Human Error Assessment and Reduction Technique (HEART)

1. Identify the full range of sub-tasks
2. Construct a nominal human unreliability score for the particular tasks, usually by consulting local experts.
3. Based around this calculated point, a 5th – 95th percentile confidence range is established.
4. The EPCs, which are apparent in the given situation and highly probable to have a negative effect on the outcome, are then considered and the extent to which each EPC applies to the task in question is discussed and agreed, again with local experts.
5. As an EPC should never be considered beneficial to a task, it is calculated using the following formula:

Calculated Effect = ((Max Effect – 1) $\times$ Proportion of Effect) + 1

A final estimate of the HEP is then calculated, in determination of which the identified EPC's play a large part.

Survey Question	EPC(s)	Max. Effect #1	Max. Effect #2	Max. Effect #3	Assessed Proportion of Affect (average)	Assessed Factor – Calc. #1	Assessed Factor – Calc. #2	Assessed Factor – Calc. #3	Generic Task, HEART Nominal Human Error Prob. (HEPs) (Table 20)	Generic Task, HEART Nominal Human Error Prob. Value (HEPs) (Table 20)	HEP %
4	35	1.1			0.556410	1.055641			C	0.16	17%
5	22	1.8			0.495	1.396			C	0.16	22%
6	33	1.15			0.529872	1.079481			C	0.16	17%
7	27	1.4			0.421711	1.168684			C	0.16	19%
8	27	1.4			0.397179	1.158872			C	0.16	19%
9	33	1.15			0.463077	1.069462			C	0.16	17%
10	22, 27	1.8	1.4		0.62561	1.500488	1.250244		E	0.02	4%
11	27	1.4			0.538902	1.2155608			E	0.02	2%
12	5, 22, 38	9			0.597195	5.77756			E	0.02	12%
13	27	1.4			0.603125	1.24125			F	0.003	0%
14	27	1.4			0.529	1.2116			F	0.003	0%
15	5, 22, 38	9	1.8		0.58475	5.678	1.4678		F	0.003	3%
16	5, 22, 27	9	1.8	1.4	0.529146	5.233168	1.423317	1.211658	F	0.003	3%
17	3	10			0.412683	4.714147			F	0.003	1%
18	13, 27, 33	4	1.4	1.15	0.552439	2.657317	1.220976	1.082866	F	0.003	1%
19	22	1.8			0.47622	1.380976			C	0.16	22%
20	22, 27	1.8	1.4		0.448205	1.358564	1.179282		C	0.16	26%
21	35	1.1			0.573415	1.057342			C	0.16	17%

Error-Producing Conditions

	Error-producing condition	*Maximum predicted nominal amount by which unreliability might change going from 'good' conditions to 'bad'*
1.	Unfamiliarity with a situation which is potentially important but which only occurs infrequently or which is novel	× 17
2.	A shortage of time available for error detection and correction	× 11
3.	A low signal-to-noise ratio	× 10
4.	A means of suppressing or overriding information or features which is too easily accessible	× 9
5.	No means of conveying spatial and functional information to operators in a form which they can readily assimilate	× 8
6.	A mismatch between an operator's model of the world and that imagined by the designer	× 8
7.	No obvious means of reversing an unintended action	× 8
8.	A channel capacity overload, particularly one caused by simultaneous presentation of non-redundant information	× 6
9.	A need to unlearn a technique and apply one which requires the application of an opposing philosophy	× 6
10.	The need to transfer specific knowledge from task to task without loss	× 5.5
11.	Ambiguity in the required performance standards	× 5
12.	A mismatch between perceived and real risk	× 4
13.	Poor, ambiguous or ill-matched system feedback	× 4
14.	No clear direct and timely confirmation of an intended action from the portion of the system over which control is to be exerted	× 3
15.	Operator inexperienced (e.g. a newly qualified tradesman, but not an 'expert')	× 3
16.	An impoverished quality of information conveyed by procedures and person–person interaction	× 3
17.	Little or no independent checking or testing of output	× 3
18.	A conflict between immediate and long-term objectives.	× 2.5
19.	No diversity of information input for veracity checks	× 2.5
20.	A mismatch between the educational achievement level of an individual and the requirements of the task	× 2
21.	An incentive to use other more dangerous procedures	× 2
22.	Little opportunity to exercise mind and body outside the immediate confines of the job	× 1.8
23.	Unreliable instrumentation (enough that it is noticed)	× 1.6
24.	A need for absolute judgements which are beyond the capabilities or experience of an operator	× 1.6
25.	Unclear allocation of function and responsibility	× 1.6
26.	No obvious way to keep track of progress during an activity	× 1.4
27.	A danger that finite physical capabilities will be exceeded	× 1.4
28.	Little or no intrinsic meaning in a task	× 1.4
29.	High-level emotional stress	× 1.3
30.	Evidence of ill-health amongst operatives, especially fever	× 1.2
31.	Low workforce morale	× 1.2
32.	Inconsistency of meaning of displays and procedures	× 1.2
33.	A poor or hostile environment (below 75% of health or life-threatening severity)	× 1.15
34.	Prolonged inactivity or highly repetitious cycling of low mental workload tasks	× 1.1 for first half-hour × 1.05 for each hour thereafter
35.	Disruption of normal work-sleep cycles	× 1.1
36.	Task pacing caused by the intervention of others	× 1.06
37.	Additional team members over and above those necessary to perform task normally and satisfactorily	× 1.03 per additional man
38.	Age of personnel performing perceptual tasks	× 1.02

Why?

Toolbox: Testing Methodology

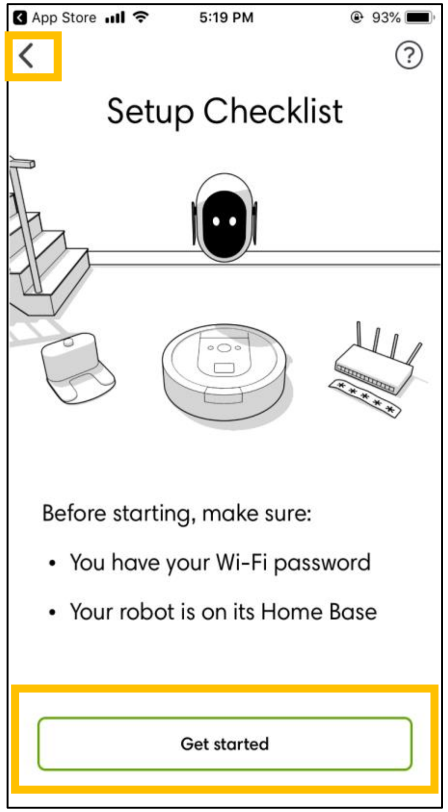
Measured Outcomes

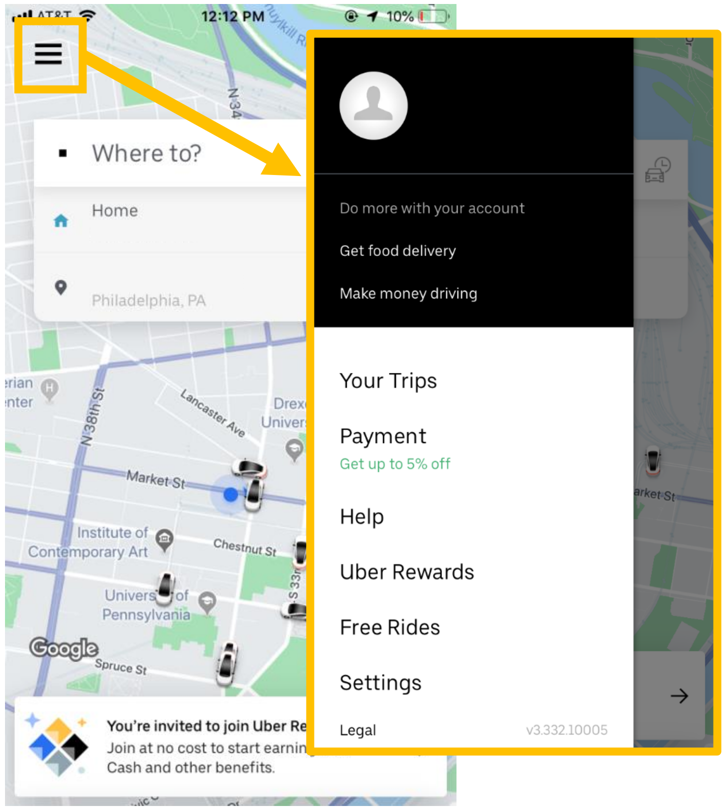
- Response Times
- Time to Completion
- Error Rates

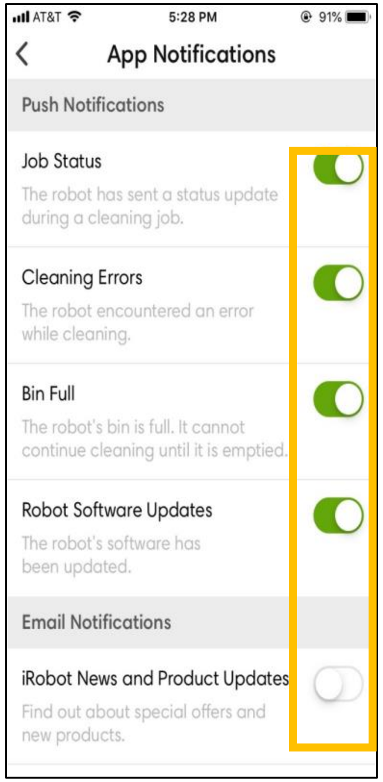
Control Panel

Case Study: User Interface

- **Non-physical affordances that affect user experience**







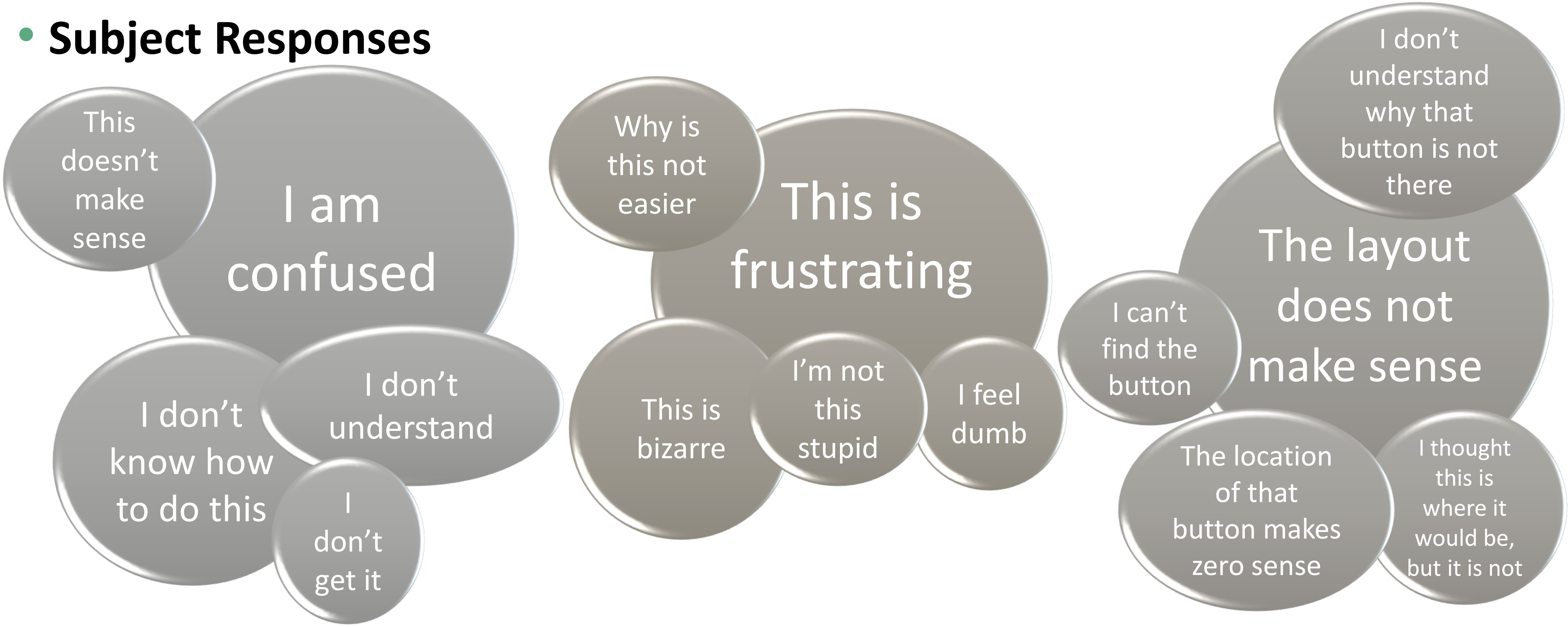
Case Study: User Interface

- Percentage of Success (Errors)

Task	Average Rating (1-7)/Task	Average Number of Prompts
Connect Roomba to app	5.2	2.6
Connect Roomba to Wifi	4.2	1.6
Find home button	3.4	0.6
Setup cleaning schedule	3	0
Rename Roomba	2.2	0

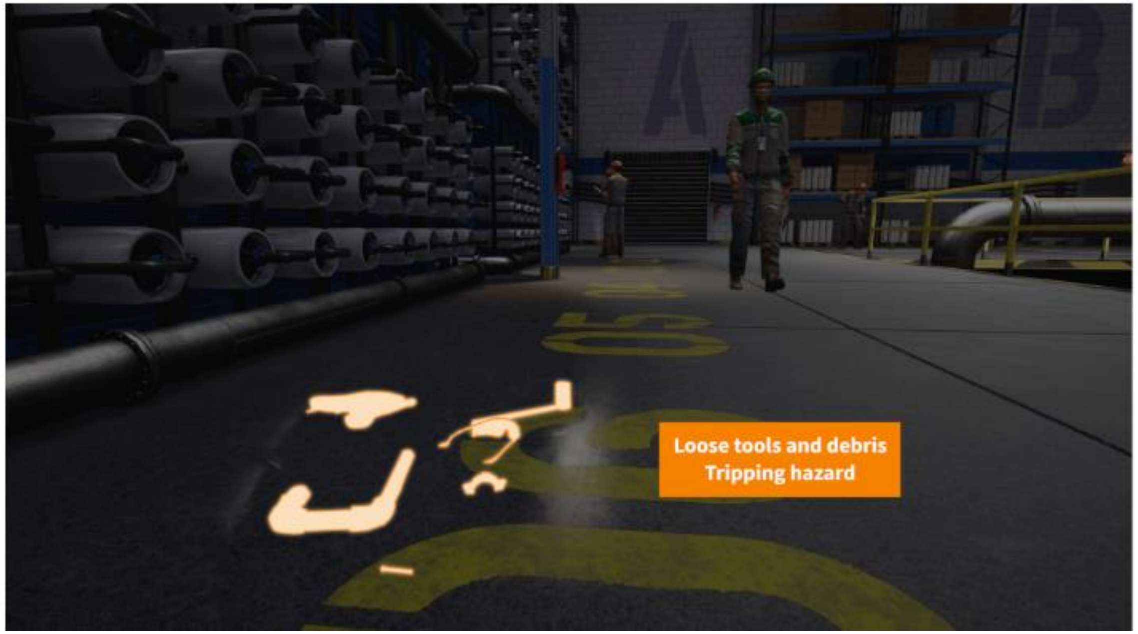
Case Study: User Interface

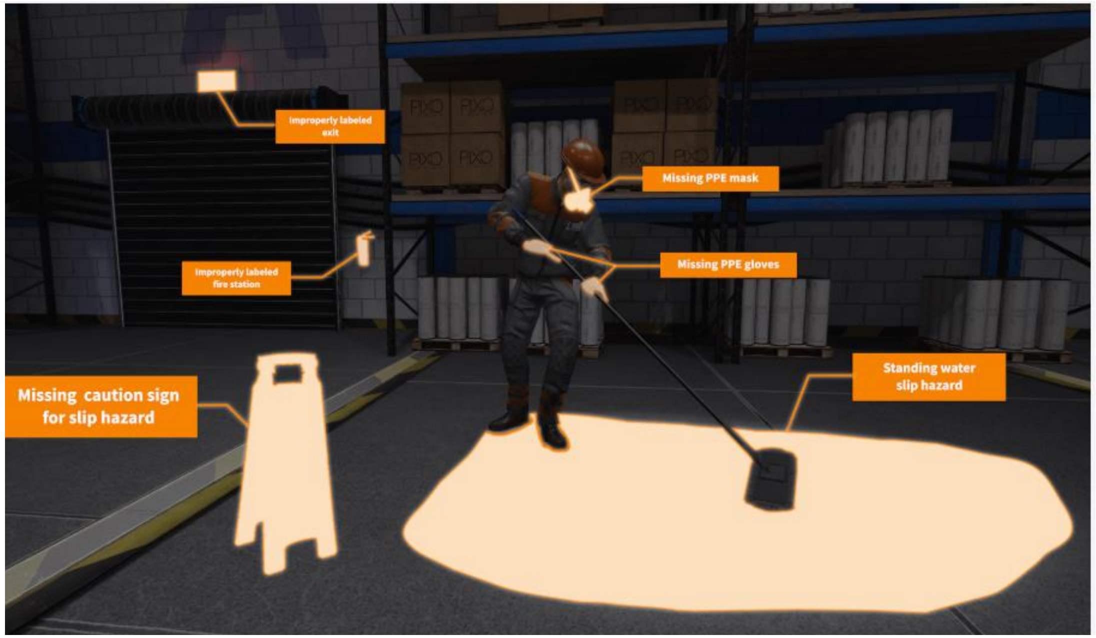
- **Subject Responses**



Additional Toolboxes

New Technology in AR/VR





https://pixogroup.com/osha-safety-sweep/

New Technology in AR/VR

http://www.eyetracking.com/Hardware/Tobii-Pro-Glasses-2

https://www.microsoft.com/en-us/hololens/buy

Physiological Sensing

- Body Condition
- Emotions
  - Electrocardiography, electroencephalography, electromyography, pulse oximetry, blood pressure measurements, respiratory transducer, body temperature measurements, galvanic skin response measurements
- Ergonomics
  - Body pressure transducers
  - Eye tracking

Sometimes it’s inevitable…

Powder keg

The last black powder manufacturer in the United States experiences an explosive mystery

GOEX, the last black powder manufacturing facility in North America, exploded on June 7, 2011, destroying a section of the plant. The accident originated in the corning mill where pressed black powder cakes were fed through an aluminum worm screw into a feed hopper. Cakes were then moved along four sets of rolls and sieve shakers to reduce their size to the desired granular dimensions.

In conjunction with the owners of the plant, Exponent conducted an engineering investigation of the explosion and concluded that friction from a contaminating quartz pebble generated sufficient heat to initiate the explosion. One of the recovered fragments from the hopper exhibited a distinct starburst pattern that is characteristic of a surface initiation of explosives. A quartz pebble was also discovered embedded within this fragment, directly below the starburst pattern. An alternate mechanism that could not be ruled out was frictional heating due to a fragmentation failure of the aluminum worm.

Due to the unique nature of the product, it might not be possible to eliminate such events during the corning operation. However, based on findings from this investigation, the Exponent team developed a series of procedural recommendations that were implemented by the facility to minimize the frequency of such incidents.

The Exponent investigation concluded that a piece of quartz, inadvertently introduced into the chipped black powder from the press bay impacted the sides of the hopper. The friction generated sufficient heat to initiate the explosion.

corning mill

Where product is cracked into a suitable size for use as gunpowder.

The GOEX factory in Minden, Louisiana, produces black powder for a wide range of customers. Black powder is used for loading a variety of antique and other weapons, including such firearms as round ball rifles, muskets, pistols and revolvers.

Embedded quartz piece over starburst pattern on hopper fragment.

Before and after the explosion. The heat of explosion of black powder is about 60% that of TNT. Consistent with the requirements of National Fire Protection Association 495 Explosive Materials Code, all employees evacuated the plant instead of attempting to fight the fire after the explosion. There were no fatalities and only one minor injury to an employee who fell during evacuation.

The explosion fragmented the screw worm and hopper and destroyed the corning mill structure. Subsequent examination of recovered fragments of the screw worm suggested that the incident was likely triggered when a piece of quartz that had contaminated the batch impacted the aluminium worm. Photos (right) depict: (a) fragmented worm; (b) crater under hopper and worm; and (c) destroyed corning mill.

82 CHEMICAL

Main Message

- Rigorous human factor analysis should be employed proactively and early to assess the overall risk with the goal to minimize it

- Human factor analysis ideally should be based on scientific method and testing; decisions need to be based on both qualitative and quantitative data via thorough analysis and testing

- New tools have been developed to help with HF testing, including AR/VR, training regimes and physiological sensing

Contact Information

Ray Huang
rhuang@exponent.com
+852 5596 7869

Exponent Inc. – Asia Pacific

Hong Kong | Shanghai | Singapore

Safety Case Symposium 2019
Singapore
Mar 26 - 27, 2019
www.SafetyCaseSymposium.com