Severe Accidents Lessons Learned

2016 July

Gary Johnson
kg6un@alumni.calpoly.edu

After the Fukushima-Daiichi event I began thinking about severe accidents

- How do they happen, how might they be prevented, role of defense in depth?
- Both IAEA and EPRI have supported this work

IAEA	EPRI
Training material	Lessons learned for I&C and HSI
Long overview of each event	Short overview of each event
Explain basic principles	Role of I&C
What, then why	Role of HFE features of I&C (HSI)
Defense in depth	Possible enhancements
Relevance of IAEA requirements	

This presentation draws from both efforts

There's lots of overlap. I'll highlight the things that are unique to the EPRI report

I found 19 severe accidents

	Estimated INES Level
Chernobyl Unit 4	7
Fukushima Daiichi Units 1,2, & 3	7
Windscale Unit 1	5
TMI-2	5
Heat Transfer Reactor Experiment-3	4
NRX	4
Fermi Unit 1	4
KS 150	4
Sodium Reactor Experiment	4
Saint Laurent Unit A2	4
SL-1	4
Westinghouse Testing Reactor	4
Saint Laurent Unit A1	4
Lucens	4
Experimental Breeder Reactor 1	3
Chapelcross Unit 2	3
105 K-West	3

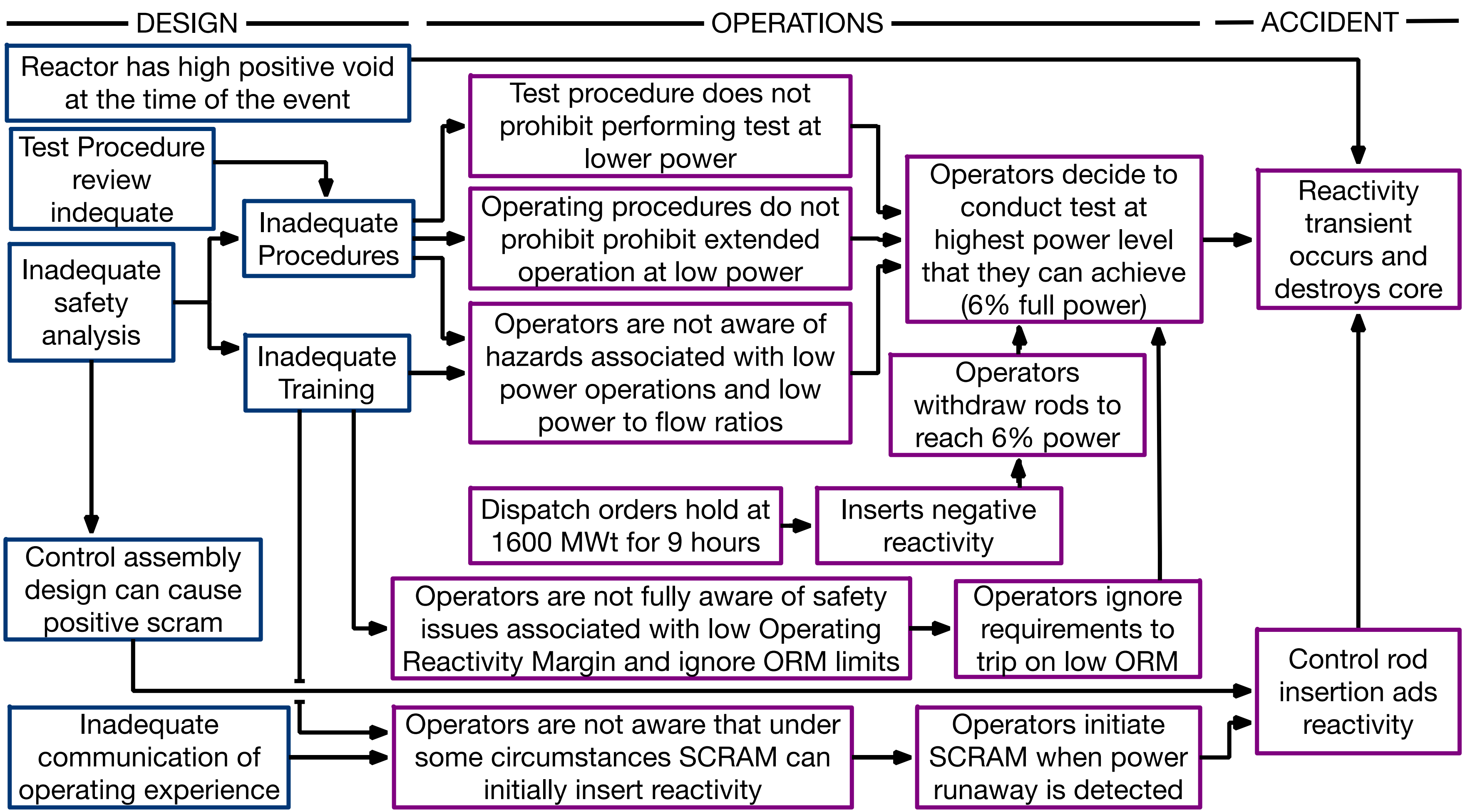
Types of Plants

4 Generation 2 LWR
7 Other power reactor types
2 Isotope Production Reactors
6 Test or research reactors

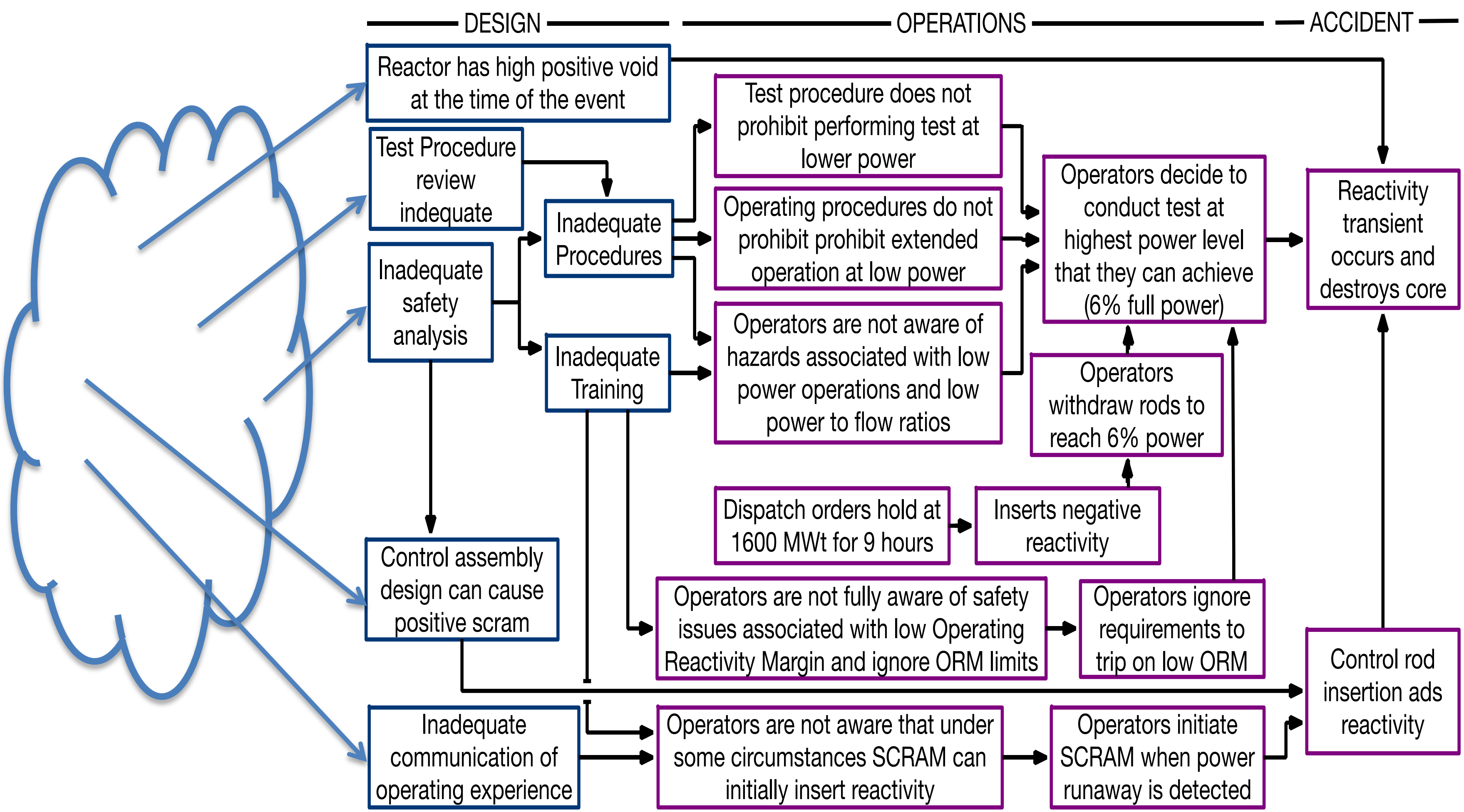
Countries Involved	
Canada	1
Japan	3
Ukraine	1
France	2
US	8
Slovakia	1
Switzerland	1
UK	2

INES = International Nuclear Events Scale
See http://www-ns.iaea.org/tech-areas/emergency/ines.asp

We can (more or less) understand the direct causes of severe accidents (Chernobyl for example)



But I don't understand the more basic causes



Severe accidents are “black swans”

Things
that were unknown or thought not credible

led to

Unexpected events

which

Neither plant systems nor operators* could
bring under control

before

Significant fuel melt occurred

*Because they didn’t have adequate instrumentation, procedures, training, or systems

Consider Fukushima Daiichi

The maximum tsunami at the site was unknown

Tsunamis > 6 m were considered not credible

led to

Failure of plant AC and DC power

Failure to plan for extended loss of AC & DC

which

Deprived operators the information, systems, procedures and training needed to bring the plant under control

before

Significant fuel melt and radiation release occurred

*Because they didn't have adequate instrumentation, procedures, training, or systems

An alternative model

- They were caused by unknown-unknowns
  – For example at Fukushima-Daiichi

Known Known

A Tsunami exceeding the design basis might happen

Not in EPRI scope

Known Unknown

Height of maximum beyond design basis tsunami

Electrical system operability after tsunami

Operators’ ability to respond after failure of all AC & DC power

Unknown Unknown

Plant and operators will not be able to cope with Beyond Design Basis Tsunami

IAEA Report

Yet another model

- There are always tradeoffs between safety and economics
- No one, and no organization can ever fully understand the risks and benefits of these tradeoff
- A history of successful operation tends to support a reduction of safety margins
- Eventually something bad happens

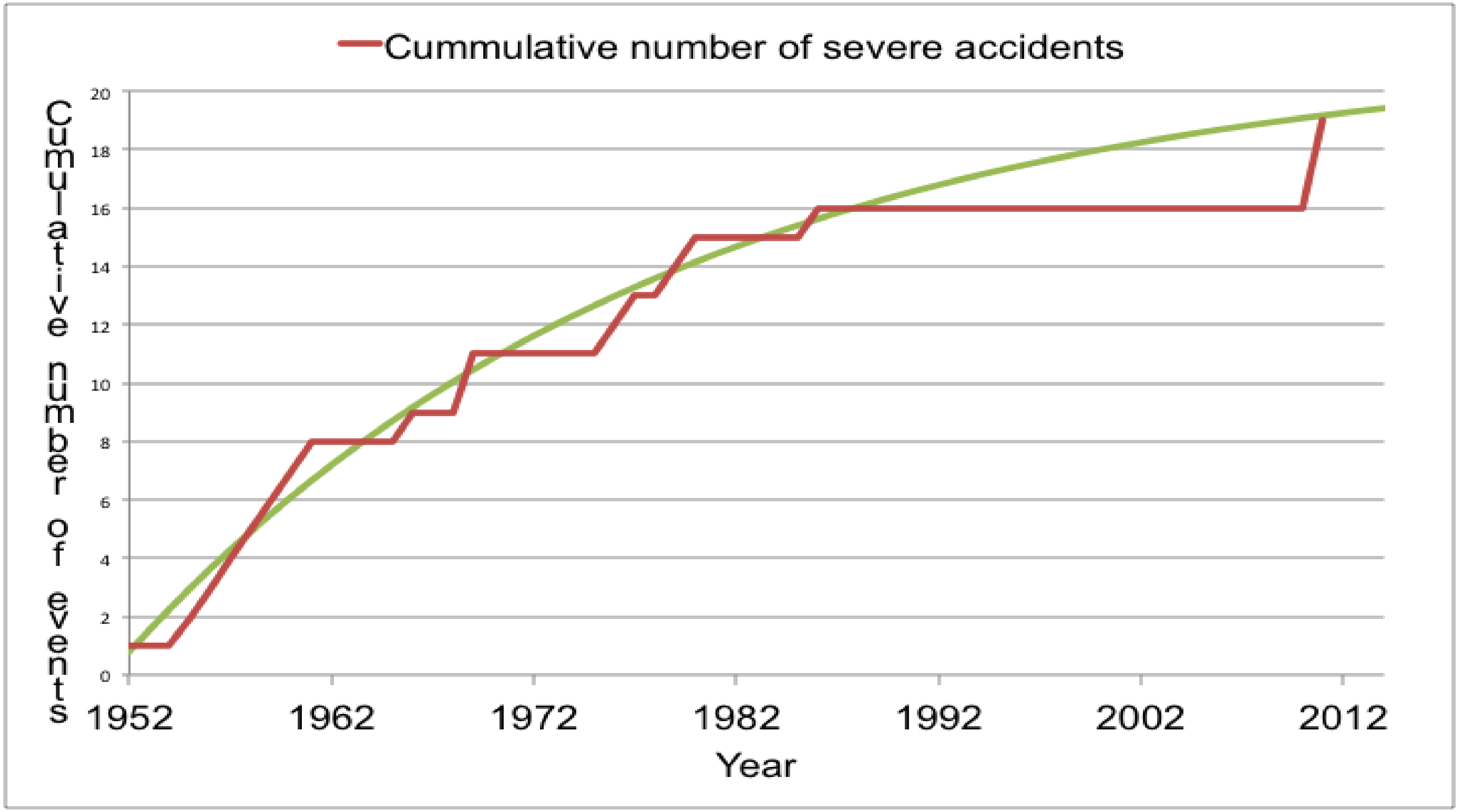
Not in EPRI scope

Following Sidney Dekker's ideas from "Drift into Failure"

We must expect severe accidents

$$\frac{2\ \text{events}^*}{16000\ \text{reactor years}} \approx 10^{-4}/\text{Reactor Year}$$

*In Gen 2 reactors,
counting Fukushima-Daiichi as a single event



All of the accidents involved bypass of defense in depth

INSAG-10 Defense in Depth Levels: Level 1 | Level 2 | Level 3 | Level 4 | Level 5

Events ordered by date	Causes			Termination
Fukushima Daiichi U3	Inadequate design basis for external hazards	Accident management can't deal with effects of extreme external hazards		Operators provide cooling of corium
Fukushima Daiichi U2	Inadequate design basis for external hazards	Accident management can't deal with effects of extreme external hazards		Operators provide cooling of corium
Fukushima Daiichi U1	Inadequate design basis for external hazards	Accident management can't deal with effects of extreme external hazards		Operators provide cooling of corium
Chernobyl U4	Operators unaware of design's hazards. Inadequate, procedures, and operational discipline. Poor accident response			Core disassembly
Saint Laurent A2	In vessel components came loose unexpectedly, No loose parts monitoring. Reactor trip setpoint on fission product release too high to prevent damage			Automatic trip: High Fission Product Activity
TMI-2	Poor training, procedures, operational discipline, MCR design, & I&C design	Operators shut down ECCS and don't recognize symptoms of loss of coolant/flow		Operators restore core cooling
KS 150	Inadequate QA for fuel assemblies. Operation with unreliable fuel temperature channels	Shutdown delayed to check fuel temperature readings		Manual trip: High Fuel Temperature
Lucens	Fuel assembly prone to flow blockage. Effects of water leakage into coolant not considered. Fuel assembly instrumentation not sensitive enough			Automatic trip: High Fission Product Activity
Chapelcross U2	Provisions for detecting fuel damage inadequate Fuel failure not detected before melt due to instrument time delays			Manual trip: High Fission Product Activity
Saint Laurent A1	Training, SW-V&V, HMI, RTS setpoint inadequate	Operator overides interlock		Automatic trip: High Fission Product Activity
Fermi 1	No safety analysis for metal sheets in reactor vessel coolant inlet Hydrodynamic loads caused sheets to come loose and block two fuel assemblies.			Manual trip: High containment radiation
WTR	Inadequate operating procedures, training & fuel QA. No reactor trip on fuel failure. No confinement isolation			Fuel relocation and manual shutdown
SL-1	Single rod withdrawal could cause criticality	Operator withdraws central control rod too far & too fast		Core disassembly & moderator ejection
SRE	Pump shaft coolant properties unknown resulting in flow blockage within core	Operators didn't investigate causes of reactor trips		Manual shutdown to investigate fuel condition
HTRE-3	Inadequate CM. Failure to validate automatic control system design and configuration settings before use. Control/protection interaction.			Beneficial common cause failure of high fuel temperature trip
Windscale U1	Inadequate knowledge about Wigner release. Inadequate core temperature measurement. Inadequate procedures. Confinement only partially effective.			Burning fuel removed from core
EBR-I	Inadequate test procedure. Lack of common operating terminology between test director and operator. RTS set point for high power trip too high for test conditions.			Manual trip: Short period
105 KW	Inadequate control of temporary changes and instrument calibration. 1oo1 reactor trip on low flow in channel			Automatic trip: high flow in channel (rupture)
NRX	Inadequate safety analysis, procedures & I&C.	Operator error	Safety rods fail to fully insert after scram.	Manual trip: diverse shutdown system

Causes

Termination

We’ve done a good job of limiting the public’s radiation exposure

- Five events involved offsite emergency response
- No deterministic effects of radiation exposure to the public
- Only Chernobyl had identifiable stochastic effects
    - ~ 6000 additional thyroid cancers
    - ~15 fatalities
- 14 events had low or no offsite release
- Two events killed operators

At two sites radiation exposure was not the most important consequence

- Chernobyl and Fukushima Daiichi
- At Fukushima Daiichi for example
  - 210,000 people were evacuated
  - A 2013 survey of 1/3 of the evacuees found:
    - 16,000 people were still living in evacuation shelters
    - 8,000 considered themselves socially disabled due to traumatic symptoms, and
    - 17,000 thought that they or their offspring would suffer health effects from radiations exposure.
  - About 60 hospital patients died because of difficulties with evacuation
  - About 300 km^2 of land removed from use for a long time
  - Serious economic consequences
- We must prevent this in the future

I&C or HSI issues contributed to every event (EPRI results)

• Inadequate functionality	6 events
• I&C availability	7 events
• Design issues	14 events
• HSI issues	8 events
• I&C lifecycle issues	5 events
• Lack of data for investigation	5 events

  – Such issues usually result from incomplete or incorrect requirements

- Most events involved more than one issue

Contributions to Severe Accidents	Fukushima Daiichi 1	Fukushima Daiichi 2	Fukushima Daiichi 3	Three Mile Island 2	Chernobyl 4	Saint Laurent A2	KS-150	Chapelcross 2	Saint Laurent A1	Lucens	Fermi 1	SRE	SL-1	WTR	HTRE-3	Windscale 1	EBR-1	105 KW	NRX	FD Spent Fuel Pools	Number of Issues
Appendix	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	#
Functionality issues	x			x				x			x			x	x						6
Indication of possible fuel failure								x			x			x	x						4
Coolant inventory indication	x			x																	2
Loose parts monitoing systems											x										1
Monitoring of I&C operability															x						1
I&C systems availability issues	x	x	x		x								x			x				x	7
Robust instruments for SAMG	x	x	x																	x	4
Power failure sequence	x																				1
Robust control power	x	x	x																		3
Robust instrument air	x	x	x																		3
Release monitoring																x					1
High range portable monitors					x								x								2
I&C design issues	x	x	x	x	x		x	x		x	x	x			x	x	x	x			14
Instrument response time					x			x		x							x				4
Instrument sensitivity										x	x										2
Instrument range				x																	1
System unreliability							x					x									2
Parameter spatial delpendence								x								x					2
Level measurement	x	x	x																		3
Fukushima instrument behaviour	x	x	x																		3
Fukushima thermocouple	x	x	x																		3
Communicaitons	x	x	x																		3
Redundancy - lack of																		x			1
Redundancy - implementation																	x				1
Diversity - lack of															x						1
Control protection interaction															x						1
Indirect measurements				x																	1

Contributions to Severe Accidents	Fukushima Daiichi 1	Fukushima Daiichi 2	Fukushima Daiichi 3	Three Mile Island 2	Chernobyl 4	Saint Laurent A2	KS-150	Chapelcross 2	Saint Laurent A1	Lucens	Fermi 1	SRE	SL-1	WTR	HTRE-3	Windscale 1	EBR-1	105 KW	NRX	FD Spent Fuel Pools	Number of Issues
Human-system interface issues				x	x				x		x	x	x	x					x		8
Display location				x								x		x							3
Operator aids				x	x						x										3
Range				x															x		2
Present reasons for interlocks									x												1
Too many hands needed																			x		1
Inadvertent operation													x						x		2
Data for accident reconstruction	x	x	x										x				x				5
Loss of power	x	x	x																		3
Turned off													x								1
Failed channel																	x				1
I&C lifecycle issues									x						x	x	x	x			5
Sensor location															x	x					2
Setpoint suitability									x												1
Setpoint verification																		x			1
Configration data V&V									x						x						2
Surveillance tests																	x				1
Configuration management															x						1
Validation of modifications															x						1
Number of Issues	10	8	8	6	3	0	1	3	3	2	4	2	3	2	8	3	4	2	3	1	#

Additional issues that I am investigating

- Inadequate knowledge of the plant 13events
- Procedure issues 12 events
- Operational discipline issues 6 events
- Training issues 9 events

This bit is still work in progress

Not in EPRI scope

Very Preliminary!!

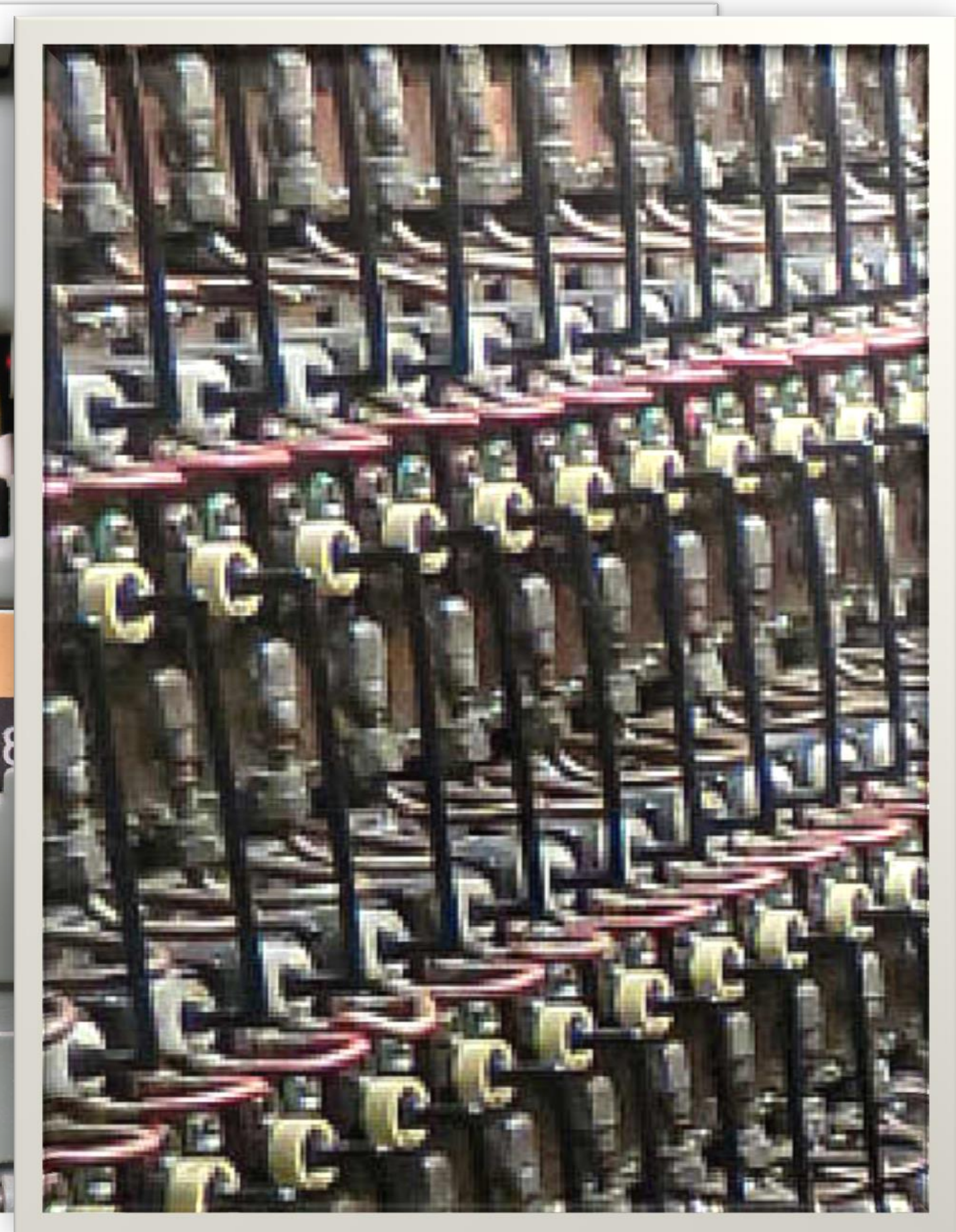
Human Factors Contributions to Severe Accidents	Fukushima Daiichi 1	Fukushima Daiichi 2	Fukushima Daiichi 3	Chernobyl 4	Saint Laurent A2	Three Mile Island 2	KS-150	Chapelcross 2	Saint Laurent A1	Lucens	Fermi 1	SRE	SL-1	WTR	HTRE-3	Windscale	EBR-1	105 KW	NRX	Number of Iss
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
Knowledge issues	x	x	x	x		x	x	x		x		x	x	x		x	x			
Lack of basic knowledge				x			x			x		x				x				
Recognized hazards discounted	x	x	x			x							x							
Failure to communicate safety issues				x										x		x				
Procedure issues	x	x	x	x		x	x	x			x			x		x	x	x		
Failure to adress known issues	x	x	x			x	x													
Not informed by analysis				x				x								x		x		
Lack of shutdown criteria											x			x			x			
Operational dicipline issues				x		x			x			x					x	x	x	
Operational dicipline				x		x			x			x					x		x	
Inadequate oversight of operations				x		x												x		
Failure to disable or lock out manual controls that should not be operated																			x	
Training issues	x	x	x	x		x	x				x			x		x				
Incomplete training	x	x	x	x		x	x				x			x		x				
Lack of system familarity				x												x				
Inadequate communicaiton of lessons learned						x					x									

Not in EPRI scope

Alternative means to provide information or control during severe accidents (EPRI results)

- Inherently robust instruments
  - New technology
  - Old technology
- Robotics
  - To work where operators can't
    - Monitor conditions, robotically actuate equipment
  - To enhance operator abilities
    - E.g., environmental survey
  - Consider providing robots that can assist operators during both normal and abnormal operations

Robust pressure indication at B reactor



Additional conclusions in the EPRI report

- Only one event was caused by CCF of I&C components
- Most I&C contributions to accidents did not result from component failures
  - Caused instead by inadequate design or maintenance
- Most of the I&C that contributed to the accidents was NON-safety
- In a several events the actions of maintenance or field operators strongly contributed to the accident
- Fukushima Daiichi and (perhaps) TMI-2 are the only events where environmental qualification was important

My recommendations to EPRI

- Provide robust instruments to show operators the status of fuel cooling and containment integrity
- Investigate methods for making I&C equipment robust
- Provide alternative means for powering minimum set of devices needed to establish core cooling
- Look again for better alternatives to ΔP level sensing
- Understand instrument performance at Fukushima-Daiichi
- Seek direct means to confirm continued sub-criticality after core melt
- Follow TEPCO's experience with robots to better understand what is needed and what works.

- You can get the EPRI report by going to www.epri.com and searching for 3002005385
- The IAEA work might be available later this year. I’ll let you know.