INSTRUMENTATION, CONTROL, AND HUMAN SYSTEM INTERFACE CONTRIBUTIONS TO HISTORICAL SEVERE ACCIDENTS

Gary L. Johnson*
Independent Consultant
1255 Higuera Ct., Livermore CA
kg6un@alumni.calpoly.edu

ABSTRACT

In 2015 EPRI completed a study of historical severe accidents. This study was intended to identify the lessons that these events had for instrumentation and control (I&C), and human systems interfaces (HSI) for nuclear power plants. The project studied 19 severe accidents that were identified by a parallel study that was underway for the International Atomic Energy Agency. I&C or HSI issues made significant contributions to 18 of the 19 events studied. This paper will summarize the I&C and HSI deficiencies that contributed to the propagation of the accidents, discuss the likely causes of these deficiencies and describe the role of I&C and HSI in finally terminating the events.

Key Words: Instrumentation, Control, Human Machine Interface, Reactor Safety, Reactor Accidents

1 INTRODUCTION

Actions that seem prudent in foresight can look irresponsibly negligent in hindsight.
Daniel Kahneman, "Thinking Fast and Slow"

The March 2011 severe accident (SA) at Fukushima Daiichi resulted in the plant losing normal monitoring and control capabilities for an extended period of time. Severe accidents are beyond design basis events (BDBE) that involve significant core degradation. Beyond design basis events present a potential challenge to existing plant-specific coping capabilities.

When operators lack adequate plant data they will not understand the plant state during BDBEs or SAs. This will hinder proper responses to minimize: 1) public and plant personnel radiological exposure, 2) plant and environmental damage and 3) public and plant costs.

These facts led EPRI to identify the need for instrumentation and control (I&C) and human factors (HF) communities to examine the lessons learned from the severe accidents at Fukushima Daiichi and other severe accidents. In particular EPRI was interested to know if experience from previous severe accidents reveals needs or gaps in I&C or human system interfaces (HSI) that represent opportunities for better preventing the progression of beyond design basis events to severe accidents and to control the consequences of severe accidents. The results of this study are given in reference [1].

Concurrent with the EPRI request, the International Atomic Energy Agency (IAEA) was sponsoring work to identify and analyze previous severe accidents. The EPRI study was able to use the knowledge gained in the IAEA project to give a head start to the identification and analysis of I&C and HSI issues.

2 METHODOLOGY

The IAEA project made an extensive search for information about previous severe accidents. Events were identified mainly from ORNL/NSIC-1672 [2] and from internet sources. The ORNL report, which was developed as background information for members of the Presidential Committee on the Three Mile

Island 2 Accident, proved to be fairly complete up to 1980. Internet claims were carefully vetted. No claim that a severe accident had occurred at a site was accepted unless a credible authority acknowledged that significant fuel damage had occurred. Table I describes the 19 severe accident events identified.

Detailed information describing the causes and progress of each event was gathered as far as possible. This information was used to develop short summaries of each event and these summaries were reviewed to identify I&C and HSI issues involved. The issues were grouped into six topic areas. Five of which are discussed in this paper[1]:

- I&C Functionality Issues – I&C functions that could have prevented the accident or given the operators information needed to prevent or better mitigate the accident were not included in the plant design;
- I&C Availability issues: I&C functions that could have prevented the accident or given the operators information needed to prevent or better mitigate the accident were not operable when needed;
- I&C Design Issues: I&C functions that were intended to prevent or mitigate accidents did not have the characteristics needed for response to the accident;
- Human System Interface Issues: HSI design characteristics did not adequately support the operators' understanding of the plant state or deter them from taking inappropriate control action, and
- I&C Lifecycle issues: deficiencies in documentation, analysis, or quality assurance activities that led directly to conditions that enabled the accident.

These issues were then described and examined to identify lessons learned.

This paper doesn't discuss the accidents in detail. Readers are directed to the EPRI report's appendices for those details. This paper discusses instrumentation, control, and human-machine interface issues contributions to the severe accidents.

3 IDENTIFIED ISSUES

The contributions related to each of the five topics were further subdivided as will be shown in the next five sections. The subdivisions given here are not the only way that the issues could be grouped, but this grouping was useful for analysis of the contributions to the accidents[2]. Short descriptions of how I&C or HSI issues contributed to the accidents are given for each event.

3.1 I&C Functionality Issues

In six of the nineteen events the plant design did not include I&C functions that could have helped to prevent the accident or better mitigate its consequences as shown in Table II.

Chapelcross 2, Fermi 1, WTR, and HTRE-3 had no reactor trips on a rapid drop of reactor power. Fuel melt or relocation usually causes an unexpected decrease in power. At all but Chapelcross Unit 2 such trips may have terminated the event without significant fuel damage. At Chapelcross Unit 2 they would have reduced the damage.

[1] The sixth topic, Information Needed to Reconstruct the Accident, is omitted here. It is less related to the subject of the paper.

[2] In the EPRI report some of the issues were viewed from more that one perspective. Some of the alternative views are excluded from this paper for brevity.

Table I Severe Accident Events Considered[3]			
Plant, Event date	**Type of accident**	**Termination mechanism**	**Consequences**
Commercial light-water cooled and moderated (LWR) power reactors			
Fukushima Daiichi Unit 1 Fukushima Prefecture Japan 2011.03. Boiling Water Reactor (BWR/3)	Loss of forced coolant flow and loss of coolant inventory	Cooling restored after partial core melt	Extensive core melt 630 PBq release[4][5] Evacuation of population
Fukushima Daiichi Unit 2 Fukushima Prefecture Japan 2011.03. Boiling Water Reactor (BWR/4)			
Fukushima Daiichi Unit 3 Fukushima Prefecture Japan 2011.03. Boiling Water Reactor (BWR/4)			
Three Mile Island Unit 2 Pennsylvania, USA 1979.03. Pressurized Water Reactor (B&W)	Loss of forced coolant flow and loss of coolant inventory	Cooling restored after partial core melt	Most of core destroyed 0.001 PBq noble gas release Plant not operated again
Commercial power reactors other than LWR type			
Chernobyl Unit 4 Prypiat, Ukraine 1986.04. Boiling-water cooled, Graphite-moderated (RBMK)	Reactivity accident	Core disassembly	Core and reactor building destroyed 1470 PBq release Evacuation of population
Saint Laurent Unit A2 Loir-et-Cher, Center, France 1980.03. Gas-cooled, Graphite-Moderated	Partial coolant flow blockage in core	Automatic SCRAM	Two melted fuel assemblies No significant release Plant shut down for four years
KS-150 Bohunice, Slovakia 1977.02. Gas cooled, D_2O-moderated	Partial coolant flow blockage in core	Manual shutdown	One or more melted fuel assemblies Minimal offsite release Plant not operated again
Chapelcross Unit 2 Scotland, UK 1976.03. Gas-cooled, Graphite-Moderated (Magnox)	Partial coolant flow blockage in core	Manual shutdown	Six melted fuel assemblies Minimal offsite release Plant shut down for two years
Saint Laurent Unit A1 Loir-et-Cher, Center, France 1969.10. Gas-cooled, Graphite-Moderated	Partial coolant flow blockage in core	Automatic SCRAM	Five melted or burned fuel assemblies Minimal offsite release Plant shut down for one year

[3] See Reference 1 for the references supporting Table I and detailed information on I&C and HSI issues discussed in this paper.

[4] A Bq is one decay per second and is approximately equal to 2.7×10^{-11} Ci.

[5] Release values are given in Iodine-131 equivalent activity calculated as specified in reference [3]. Often the quantity of radiation release is dominated by the noble gas release, which poses little radiation risk to the public. Converting all releases to ^{131}I allows for more meaningful comparison of effects between events.

Table I Severe Accident Events Considered[3]			
Plant, Event date	**Type of accident**	**Termination mechanism**	**Consequences**
Prototype and demonstration plants			
Lucens Lucens, Switzerland 1969.1. Gas cooled, D_2O-moderated	Partial coolant flow blockage in core	Automatic SCRAM	Two melted fuel elements Minimal offsite release Plant not operated again
Fermi Unit 1 Michigan, USA 1966.10. Sodium-cooled, Fast breeder	Partial coolant flow blockage in core	Manual SCRAM	Two melted fuel assemblies Minimal offsite release Plant shut down for four years
Stationary Low Power Reactor 1 (SL-1) Idaho, USA 1961.01. Boiling-water cooled, Water-moderated	Reactivity accident	Core disassembly and ejection of moderator	Core destroyed About 20 % of fuel melted Minimal offsite release Three operators died
Sodium Reactor Experiment (SRE) California, USA 1959.07. Sodium-cooled, Graphite Moderated	Partial coolant flow blockage in core	Manual shutdown	About 16% of fuel melted Minimal offsite release Plant shut down for about 15 months
Non-power reactors			
Westinghouse Testing Reactor (WTR) Pennsylvania, USA 1960.04. Low-pressure water cooled, water moderated	Fuel failure or inadequate core cooling during planned operations	Manual scram	One fuel assembly melted Small noble gas release Plant shut down for six months
Heat Transfer Reactor Experiment (HTRE-3) Idaho, USA 1958.11. Air-cooled, Metal-hydride-moderated	Reactivity accident	Automatic SCRAM Manual SCRAM Core disassembly	Most of core destroyed Minimal offsite release Plant shut down for 8 months
Windscale Pile 1 Sellafield, UK 1957.10. Air-cooled, Graphite-moderated	Inadequate core cooling during planned operations	Manual shutdown	Fuel in about 150 channels burned 67.6 PBq release Plant and second similar unit not operated again
Experimental Breeder Reactor 1 (EBR-1) Idaho, USA 1956.01. Sodium-potassium-cooled, Fast breeder	Reactivity accident	Manual shutdown	About 50% of core melted Minimal offsite release Plant shut down for 18 months
105 KW Reactor Washington, USA 1955.01. Air-cooled, Graphite Moderated	Partial coolant flow blockage in core	Automatic SCRAM	About 5 kg of fuel melted Minimal offsite release Plant shut down for 6 weeks
National Research Experimental Pile (NRX) Ontario, Canada 1952.12. Water- and air cooled, D_2O-moderated	Reactivity accident	Manual shutdown, diverse system	Severe damage to core and calandria Minimal offsite release Plant down for 16 months

Table II. Events where needed I&C functions were not included in the design

Missing functions	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
Indication of possible fuel failure								x			x			x	x				
Coolant inventory indication				x															
Loose parts monitoing systems						x					x								
Monitoring of I&C operability															x				

At TMI 2 reactor vessel water level indication was not provided. In fact, at the time no US commercial pressurized water reactors had such instruments. It was believed that pressurizer water level indication was sufficient to confirm that water covered the core. At TMI 2, however, an unrecognized loss of coolant through the pressurizer relief valve caused steam in the pressurizer to move into the reactor vessel while filling the pressurizer full of water. This blinded operators to the loss of core cooling. That they were unaware of the need to provide high makeup water flow led directly to fuel melt.

The Fermi 1 event was initiated when metal liners in the bottom of the reactor vessel came loose. Eventually these liners blocked flow in three fuel channels. For some time before that operators were aware that there was some kind of problem but were unable to diagnose the situation. Similarly at Saint Laurent A2 the accident was caused when an aerodynamic fairing for and in-vessel thermocouple broke lose and eventually blocked a fuel channel. It was later found that numerous fairings had suffered damage due to turbulent flow of reactor coolant in their area. At both units loose parts monitoring may have allowed operators to avoid the accident.

During HTRE-3 start-up testing an unexpected reduction of high voltage to ion chambers caused reactor power readings to decrease as power increased. These readings were used by both the automatic power control and the reactor trip systems. The incorrect readings caused continual control rod withdrawal and disabled the reactor protection system high power trip. Reactor power increased to about 400% of the planned maximum power for the cooling conditions existent at the time. An alarm on low voltage to the ion chambers would have alerted the operators that the reactor should be manually shutdown.

3.2 I&C Availability Issues

Failure of I&C functions contributed to four of the 19 events as shown in Table III below.

In the three events at Fukushima-Daiichi, instrumentation needed for severe accident management (SAM) failed, initially due to loss of electrical power. After power was restored level channels failed due to environmental conditions, and pressure and temperature instruments became unreliable for reasons not yet known. The worst issues involved RPV level instruments. These continued to function whenever power was available, but evaporation of water in the level instrument sense lines eventually resulted in readings that were higher than the actual water level. This led the operators to be overly confident that their actions to keep the cores covered were effective. Instrument drift or failure of other instruments such as RPV pressure and surface temperature measurements caused confusion. Tokyo Electric Power Company has not yet determined the reasons for the problems with measurements other than RPV level.

Also at Fukushima-Daiichi robust alternative power sources were not available to operate instruments and controls. Both electrical power and instrument air were involved. Temporary electrical

power was provided from car batteries taken from on-site vehicles and later from off site. Hours to days were needed to restore power to key instrument channels.

Table III. Events where needed I&C functions were not available

I&C Failures	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
Robust instruments for SAM	x	x	x																
Robust power for SAM	x	x	x																
Robust instrument air for SAM	x	x	x																
Release monitoring																	x		

Restoration of control power sources was not as successful. Operators used construction air compressors to operate containment vent valves but they had trouble maintaining both instrument air and electric power to solenoid valves for containment venting. The temporary installations failed frequently. Without reliable containment venting, drywell pressures sometimes were high enough to reduce, or stop, low pressure coolant flow to the Unit 2 and 3 RPVs. The vent valves had dedicated nitrogen tanks, but the gas in these tanks was exhausted sooner than expected. The reasons for this are still unknown.

At Fukushima-Daiichi Unit 2 operators knew that the turbine driven high pressure cooling system, RCIC, would fail at some point and that when it did they would have to switch to low pressure injection. They constructed a makeshift 120 VDC power supply so that when RCIC failed they could open a safety relief valve to depressurize the reactor. Unfortunately this supply failed when needed. The supply had been miss-wired. Considerable core damage occurred before the problem was corrected.

At Windscale Pile 1, two systems for monitoring fission product release from the core were unavailable. Radiation monitors in the plant stack did not detect fuel failure because the operation in progress required that the reactor's air coolant be exhausted at ground level, not up the stack. A system for detecting fission products in the reactor exhaust plenum, worked by moving detectors behind each fuel channel. The structure that moved the detectors could not operate in the high plenum temperature caused by plant conditions. Operators were unaware of fuel failure until some fuel elements were on fire.

3.3 I&C Design Errors

I&C design errors contributed to ten of the 19 events as shown in Table IV. The I&C equipment worked as designed, but their characteristics were not suitable for detecting or controlling the event.

At Chernobyl Unit 4 the system that displayed the amount of negative reactivity in the core ran about 15 minutes behind real-time. Because of these delays the operators initiated the fatal test without realizing that the negative reactivity in the core was well below a safe condition.

At Chapelcross Unit 2 and Lucens high fission product concentration in the core was a reactor trip parameter. At both sites the time required to transport fission products from the core to the radiation monitors together with detector response times were on the order of minutes. At Chapelcross this delayed plant shutdown and resulted in more fuel damage. At Lucens the reactor trip came about three minutes after fuel melting began and seconds after a fuel rod ignited.

At EBR-1 a reactivity feedback test was to be manually terminated on high temperature in a fuel channel. Three thermocouples were provided for this purpose, but only one read out on a high-speed display. Before the test, the thermocouple connected to the high-speed display failed and the failure was not detected. During the test the slower responding channels were not fast enough to trigger operator response before positive reactivity feedback effects launched a rapid power increase.

Table IV. Events where I&C characteristics were not fully appropriate

Inadequate I&C characteristics	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
Instrument response time					x			x		x							x		
Instrument sensitivity										x	x								
Instrument range				x															
System unreliability							x					x							
Parameter spatial dependence								x								x			
Redundancy - lack of																	x	x	
Control protection interaction															x				
Fail safe design	x																		
Indirect measurements				x															

Core exit thermocouples at Fermi-1 and fuel channel flow meters and thermocouples at Lucens were not sensitive enough to detect blockages in the associated fuel assemblies. Thus operators did not have information that would have clued them to shutdown the plant before the accidents began.

Core exit temperature readouts at TMI-2 were programmed to show question marks when temperatures exceeded about 370 °C even though they could work in much higher temperatures. This deprived operators of one clear indication that fuel damage was in progress.

At KS-150 and SRE a history of unreliable instrument channels led operators to ignore valid signals. When high fuel temperature was indicated at KS-150 the operators did not act until instrument technicians confirmed the readings. The delay resulted in significant fuel damage. At SRE operators repeatedly reset what they believed to be spurious negative period trips. The reactor ran with significant fuel damage for about two weeks.

At Chapelcross Unit 2 several fuel channels did not have temperature monitoring, including one fuel channel that, unbeknownst to the operators, had a partial flow blockage. Had this channel's temperature been monitored the blockage would have been corrected years before the accident occurred.

In the Windscale Pile 1 accident high fuel temperature was the main criteria for plant shutdown during an infrequent operation. Fuel thermocouples were not, however, placed where the hottest fuel temperatures were expected. With the sensors about 2 meters away from the hot spots, operators were unaware of the high temperatures until several fuel slugs began to burn.

The reactor protection system at 105 KW had a single pressure sensor in each fuel process tube. These sensors were used to trip the reactor on either high or low flow through a tube. During initial startup one process channel had a flow blockage and that channel's flow sensor was miss-calibrated such that it indicated normal flow when there was no flow in the channel. Fuel in the blocked channel melted.

In the HTRE-3 event ,already mentioned, failures to account for a previous modification of the ion chamber power supplies and ill-considered placement of neutron detectors enabled the event.

At Fukushima-Daiichi the containment isolation system logic for Unit 1's Isolation Condenser and for Units 2 and 3's Reactor Core Isolation Cooling system (RCIC) were similar. Four power supplies were involved: DC supplies for ex-containment isolation valves, AC supplies for in-containment isolation valves, and two DC supplies for the two trains of Containment Isolation System (CIS) Logic. At Units 1 and 2 all four supplies failed during the tsunami, but not in the same sequence. As long as both CIS Logic signals remained energized neither set of isolation valves would close, but if the valves had power when CIS Logic power failed they would close. At Unit 1 three of the valves were normally open and the IC

was put in to service by opening one ex-containment valve. Here the CIS Logic lost power first and apparently in-containment and ex-containment valves closed. With the in-containment valves closed the division A IC could not be restarted when DC power for the ex-containment valves became available. The situation in Unit 2 was reversed and the containment isolation valves, fortuitously, stayed open.

A primary cause of the TMI-2 accident was that the operators were unaware that the Pressurizer Power Operated Relief Valve (PORV) was stuck open. The valve's control room displays showed if power had been applied to open the valve or not, but they did not indicate actual valve position. At the start of the event the PORV automatically opened but soon was commanded to close. It didn't close but the control room display showed that it had, leading the operators to reduce makeup flow in accordance with Loss of Feedwater procedures when indeed they should have followed Small Break Loss of Coolant procedures, which required a high rate of makeup flow. Coolant in the core boiled off for several hours.

3.4 Human-System Interface Issues

Human-system interface issues contributed to seven of the 19 events as shown in Table V below.

Table V. Events where Human-System Interface Issues Contributed

Human-system interface issues	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
Appendix	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Display location				x								x		x					
Operator aids				x	x						x								
Present reasons for interlocks									x										
Inadvertent operation																			x
Ergonomics																			x
Range																			x

Displays that the control room operators could not easily see contributed to three accidents. At TMI 2 the status of the reactor coolant drain tank (RCDT) was displayed behind the main control boards. Had the operators known early on that the RCDT was overflowing it may have alerted them to the stuck open PORV. Also, the operators seem to have focused on average RCS temperature (Tavg). The Tavg displays were driven by narrow range RCS temperature channels. When temperatures exceeded the range of these instruments Tavg readings became misleading. Wide range temperature channels were available but only on multipoint strip charts located on the tall control boards behind the main operating horseshoe.[6] At SRE core outlet temperature, and at WTR coolant boiling indication were only displayed outside of the control room. At WTR this delayed the manual shutdown. At SRE the excessive fuel temperatures were seen only when the strip-charts were recovered after the accident.

TMI-2, Chernobyl Unit 4, and Fermi 1 operators had difficulty forming an accurate view of plant conditions from multiple sources of information. At all three sites the operators needed synthesized information: for example, display of sub-cooling margin at TMI-2, display of coolant channel void fraction at Chernobyl Unit 4, and reactivity balance and rapid scan of core exit temperatures at Fermi-1. Fermi-1 was restarted in 1970. Before restart a digital computer based system was installed to detect severe accident conditions such as unexplained reactivity distribution in the core. This system anticipated the need for Safety Parameter Display Systems that were required after the TMI-2 accident.

[6] These are only two examples of indications of trouble that the operators could not readily access or readily understand.

At Saint Laurent A1 the refueling machine HSI gave the operator unclear and ambiguous information about why interlocks prevented the machine from loading the selected components into the core. Not understanding why the interlocks stopped him, he overrode them. The assemblies in the fueling machine location he was using contained flow restrictors not fuel. Loading these caused the fuel already in the channel to melt.

While setting up a low power and low flow test at NRX field operators inadvertently opened valves that withdrew control rods, creating a potential for an unintended criticality. These valves were not tagged or locked to prevent inadvertent operation. The incorrect alignment was noted and the plant supervisor went into the field to correct the situation. After diagnosing the problem he called the control room and gave instructions meant to insert all control rods. From the control room control rods were operated by four switches labeled only as 1, 2, 3, and 4. Switches 1 and 2 withdrew banks of rods. Switch 3 inserted rods, and switch 4 had to be pushed simultaneously with any other switch to hold the rods in position. Over the phone the supervisor inadvertently told the control operator to actuate switches 1 and 4, which withdrew a bank of safety rods. He immediately recognized his mistake, but could not correct it because the operator had left the phone to operate the two switches. Withdrawing the rods brought the reactor critical and started power increase. The operator recognized this and initiated manual scram within 20 seconds, but some of the rods did not fully insert. Rod position indicators showed only if the rods were full in or full out so the operator was not immediately aware that some rods were stuck. It was not uncommon for the control rods to move slowly. It took the operators about 90 seconds to realize that the reactor was not shutting down. At that point the operator manually initiated a diverse shutdown mechanism, but by that time reactor power was substantially above the point where the core could be cooled and considerable core damage occurred.

3.5 I&C Lifecycle Issues

I&C lifecycle issues, i.e., deficiencies in documentation, analysis, or quality assurance activities, contributed directly to four of the 19 events as shown in Table V.

Table VI. Events where Lifecycle Issues Contributed

I&C lifecycle issues	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
Sensor location																x			
Setpoint suitability									x										
Setpoint verification																		x	
Configuration management															x				
Validation of modifications								x							x				

It has already been mentioned that fuel temperature thermocouples were incorrectly located for the Windscale Pile 1 operation at the time of the accident. Loss of information during staff turnover contributed to this situation. The accident investigation revealed that it had once been common practice to locate fuel thermocouples near the expected hot spots during the type of operation in progress, but for unknown reasons this practice was discontinued. At the time rapid expansion of the United Kingdom's nuclear programs caused rapid turnover of the Windscale staff. The reasons for thermocouple placement were not conveyed to new personnel. When investigators asked if the operator is not getting the information he needed when the sensors are several feet away from the hot spot, the General Manager of the Windscale Works said "I know that now." [4]

Saint Laurent A1 had a reactor trip on high fission product concentration in the core coolant. At the time of the event the setpoint for this trip assumed high-burnup fuel, but the accident occurred early in the plant life. Hence when the accident happened the trip was delayed, increasing core damage.

At 105 KW instrument setpoints were not independently verified before startup. This set up conditions for the reactor protection system failure as previously discussed.

HTRE-3 was the third of three reactors that used basically the same instrumentation, control, and protection instruments. During the startup of the HTRE-1 the neutron monitoring channels suffered from 60 Hz hum. An L filter with a 1 MΩ series resistor was added to correct this but the change was not recorded on the drawings. For HTRE-3 an automatic power control system using these neutron sensors was installed. The additional load that this put on the power supply was considered acceptable. A startup was conducted using automatic power control. The power supply saturated before full power was reached causing the ion chambers to leave the ionization region. In addition to the drawing error, the new automatic power control system was not validated before it was put into service.

3.6 Role of I&C and HSI in terminating the accidents

Two events, Chernobyl Unit 4 and SL-1, were reactivity accidents that led directly to core disassembly and termination of the accident. I&C and HSI functions had no role in the shutdown.

At Windscale Pile 1 some of the reactor fuel ignited. Reactor shutdown did not stop the fire. The event was terminated by operators manually pushing as many burning fuel assemblies possible out of the back of the core followed by water injection into the fuel channels. Injecting water was a “last ditch” measure because it was feared that it might cause re-criticality.

Four events, three at Fukushima-Daiichi and the event at TMI-2, the initiating events immediately shutdown the reactors, but restoration of cooling was necessary to bring the plants to a controlled state.

At TMI-2 all systems needed to restore cooling were available, but because of I&C and HSI design issues it took the operators several hours to recognize that there was insufficient coolant in the reactor vessel. By that time conditions were such that operation of plant systems couldn’t immediately correct the situation. Eventually the operators brought RPV level above the core remains.

At Fukushima-Daiichi a tsunami took out all normal sources of coolant makeup, and in Unit 1 the passive core cooling system as well. Several days were needed to establish makeshift water supplies that could reliably bring RPV and drywell water levels above the fuel in the reactor vessels and the drywells.

Five events, Saint Laurent A1, Saint Laurent A2, Lucens, HTRE-3, and 105 KW, were automatically terminated by the reactor trip systems. In each of these events the reactor trip came too late to prevent significant fuel damage.

At HTRE-3 and 105 KW the reactor was automatically tripped by a diverse backup function after damage had already occurred. The HTRE-3 backup was a 13 out of 13 in-core high fuel exit temperature trip. Post event analysis concluded that core axial power distribution would have prevented some of the thermocouples from reaching the trip setpoint. Upon disassembly of the reactor it was found that all thirteen sets of thermocouple leads exited the reactor vessel at the same point near a hot spot. At this location all thermocouple lead wires melted and caused the trip. It is ironic that this event, the only one resulting from common cause failure of I&C, was terminated by another I&C common cause failure.

At 105 KW the low ΔP trip failed, but when the fuel channel failed the reactor tripped on high ΔP measured by the same instrument.

Seven events, KS-150, Chapelcross Unit 2, Fermi 1, SRE, WTR, EBR-1, and NRX were terminated by manual scram or manual shutdown. For six of these events the manual scrams were too late to prevent the accident because the operators did not have the information that they needed to act in time. At SRE

the reactor protection system repeatedly shutdown the plant, and was repeatedly reset. Plant shutdown came only after operators withdrew a fuel assembly and found that they had retrieved only the top half.

In the NRX accident control rods didn't fully insert on reactor trip. The reactor was shutdown by draining the D_2O moderator from the calandria.

4 CONCLUSIONS

In 18 of the 19 events I&C or HSI issues either enabled the accident or degraded the ability of operators or plant systems to mitigate accident consequences. The one event not included was SL-1 where the event resulted from an operator physically lifting a high worth control rod.

Of the 50 I&C and HSI contributions to severe accidents discussed here, only one was caused by a single random failure of I&C or HSI equipment. This was the failure of the fuel temperature thermocouple connected to the high-speed readout at EBR-1 combined with the failure to provide fast displays for two redundant instruments. Procedure and training issues[7] were also involved.

In only one case was a single I&C issue sufficient to enable an accident. This was at Saint Laurent A2 where the lack of means to detect vibration of in-core components and loose parts in the reactor led directly to the accident.

Only at HTRE-3 did I&C issues directly cause an accident. Several related errors were involved: 1) the failure to record a design change, 2) the use of the same I&C circuits for both protection and control, and 3) the failure to validate the power control system before placing it in service. This was also the only event where common cause failure internal to the I&C system contributed a severe accident.

Nearly one third of the events were terminated by manual SCRAM. This highlights the importance of manual trips. In modern plants manual reactor trip is usually not directly credited in accident analyses, but clearly such trips provide an important diverse actuation method.

For a quarter of the events restoration of core cooling was needed to bring the plant to a controlled state. It is critical that operators have robust instrumentation to inform them of the plant condition and controls that will allow them to respond to BDBE.

Three of the events were terminated by diverse functions after the primary trip function failed. This experience reinforces the need for diverse trip functions, particularly for reactor shutdown.

For 17 of the 19 events multiple I&C or HSI issues were needed to enable the accident. In 16 of the events the multiple issues would have been considered independent of each other before the accident. Furthermore, the causes were not I&C or HSI equipment failures but the lack of needed I&C functions or inadequate characteristics of the I&C or HSI functions.

That multiple independent I&C and HSI issues were involved points to the existence of common causes at a higher level than what we normally consider. Many events were caused by design errors that probably can be attributed to inadequate design bases or a misunderstanding of design basis requirements. The events point out the need for I&C and HSI design to be informed by a thorough understanding of the possible plant accidents and the needs of plant operators.

Some of the design errors may be attributed to poor design or poor accident analysis, but more often it seems that they should be attributed to unknown unknowns that were not imagined in the design process. In popular culture such events are often called "Black Swans."

[7] Procedure, training, and mechanical system design issues also contributed to most of the events but study of these issues was not in the scope of the EPRI study. A discussion of these contributions may be the topic of future papers.

While we can expect future severe accidents to be less likely, note that the Fukushima-Daiichi incident happened after the nuclear industry had experienced about 16000 reactor years of operation. That four generation-two LWR experienced severe accidents during this time indicates that it is unreasonable to expect that severe accidents can be practically eliminated in the near future.

Nevertheless, history gives us good reason to be optimistic about our ability to protect the public from such events. Looking at Table 1 we can see:

- Severe accidents don't necessarily result in significant offsite radiological release, only Chernobyl Unit 4, Fukushima-Daiichi, and Windscale Pile 1 had hazardous releases;
- No event resulted in any member of the general public suffering from deterministic effects of radiation exposure;
- Stochastic radiation effects among the public can be demonstrated only for the Chernobyl Unit 4 accident; and
- The frequency of severe accidents has constantly decreased with time.

Furthermore, the operators at Fukushima-Daiichi came quite close to preventing significant radiological release from Units 2 and 3 even though they lacked: effective accident management guidelines for severe external events, training and practice for the event that occurred, and pre-placed equipment for dealing with the accident that they faced. This accident clearly established the importance of comprehensive severe accident management guidelines together with the training and support equipment needed to effectively implement the SAMGs.

As I&C and HSI engineers, our next challenge is to make certain that the operators will have the information, control functions, and user interfaces necessary to implement SAMG's.

5 REFERENCES

1. G. Johnson, *Severe Nuclear Accidents: Lessons Learned for Instrumentation*, *Control, and Human Factors*, EPRI, Palo Alto, CA (2015). available for free at http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000003002005385
2. ORNL/NSIC-1672, H. W. Bertini, et. al, *Descriptions of Selected Accidents that have Occurred at Nuclear Reactor Facilities*, Oak Ridge National Laboratory (1980).
3. *INES, the International Nuclear and Radiological Event Scale, User's Manual*, International Atomic Energy Agency (2013).
4. *A Revised Transcript of the Proceedings of Enquiry into the Fire at Windscale Pile No. 1, October 1957*, United Kingdom Atomic Energy Authority (1989).