A Survey of the Hazards to Electrical Power Systems

Gary Johnson

Independent Consultant, USA

Abstract

This paper presents the preliminary results of a survey of severe accidents and the lessons learned that are important to the design of electrical power systems. This survey of historical accidents since 1952 identified 19 known incidents in which significant fuel melt occurred within a reactor core. In each of these incidents unexpected events or event sequences played an important role. In all cases the event sequences resulted in bypass of two or more levels of defense in depth.

This study offers clear lessons for electrical power robustness: 1) Robust design must be based upon a clear understanding of what can go wrong, and 2) Robust design will reduce, but cannot eliminate, the potential for failure of electrical power systems.

In order to better understand "what is the worst that can happen" known hazards are reviewed to identify the challenges that they can present to electrical power systems.

Recognizing that unexpected events cannot always be prevented the paper discusses the need for methods to restore plant power sources or provide for alternate power supplies when the plant power sources fail.

1. Lessons learned from historical severe accidents

A literature review identified 19 severe accidents since criticality of the first man-made nuclear reactor on December 2, 1942. These events occurred in very diverse reactor types. A report on these events is expected in early 2015.

Many of the events happened before modern safety regulations and expression of safety culture. All plants included defense in depth features, but most were designed before defense in depth principles[1] were formally expressed. At some plants national security benefits took priority over design safety.

All of these accidents resulted from events that were either unforeseen or discounted as incredible. Consequently provisions to prevent and to mitigate the effects of the events were inadequate, multiple layers of defense failed and operators did not have the knowledge, training or procedures for response.

.[1]. International Nuclear Safety Advisory Group-10, "Defense in Depth in Nuclear Safety," INSAG-10," International Atomic Energy Agency, 1996.

In short, severe accidents result from limits to our knowledge, i.e., "unknown-unknowns" - things that we cannot imagine, and "known-unknowns" - things that we can imagine, but cannot accurately predict their probability or effects. The more formal expression for these limits to knowledge is "epistemic uncertainty." Robust design must account for epistemic uncertainties.

The health and environmental effects of severe accidents have been lower than those resulting from accidents or normal operation of other modes of energy generation[2]. The following discussion considers three types of effects: prompt fatalities, delayed health effects, and interference with the enjoyment of property outside of the plant premises.

Prompt fatalities

Two events, SL-1 in 1961, and Chernobyl in 1986 caused fatalities from the direct effects of radiation exposure or from other causes during the emergency response at the plant site. At both SL-1 and Chernobyl national security benefits took priority over design safety.

Three died in 1961 at SL-1, a US transportable power reactor.

At Chernobyl 28 deaths were attributed to acute radiation exposure. Another 19 highly exposed survivors died in the next few years[3]. Some of these deaths were not due to radiation exposure. There were no cases of acute radiation exposure to members of the public.

Chernobyl seems to bound the worse radiation environment that can result from a reactor accident. It shows that early estimates of the prompt fatalities among the general public were exceedingly conservative. By comparison Wikipedia recognizes 430 prompt worker fatalities and 100,681 prompt public fatalities from other forms of energy production since 1965. The event that created the largest number of fatalities was the 1975 collapse of a hydropower dam in China, which killed 100,000.

Delayed health effects

Three events, Windscale, Chernobyl and Fukushima have caused, or will still cause, delayed health effects or fatalities. Epistemic uncertainties regarding health effects of low levels of radiation exposure, and confounding effects of other possible causes make estimates of these effects controversial.

A 1988 report on the Windscale[4] event estimated an upper bound for public health effects of 100 fatal cancers, 90 non-fatal cancers, and 10 heredity effects. The author went on to state that the actual numbers are likely to be lower and may be zero.

For Chernobyl the main harmful radiation exposure to the public was increased thyroid cancer rates in people who were children or adolescents at the time. Twenty years after the accident 6000 thyroid cancers, 15 of which were fatal, were observed in these groups[3]. A substantial fraction of these cancers probably resulted from the lack of prompt action to prevent ingestion of milk contaminated by ^{131}I.

---

[2]. Caution. The analysis behind the following discussion was not very rigorous, but it is thought that a more rigorous analysis would more fully support the conclusions. A more rigorous analysis would be very interesting.

[3]. "Sources and Effects of Ionizing Radiation, Volume II," United Nations Scientific Committee on the Effects of Atomic Radiation, 2011.

[4]. Clarke, R., "The 1957 Windscale Accident Revisited," paper presented at the REAC/TS International Conference on the Medical Basis for Radiation Accident Preparedness, Oak Ridge, 1988.

It will be many years before such information is available for the Fukushima accident, but based upon the lower level of release and the more aggressive prevention and mitigation of radioactive iodine intake, the Fukushima event will result in substantially fewer thyroid cancers than occurred at Chernobyl.

By comparison recent studies[5] estimate nuclear power has prevented 1.84 million air-pollution related deaths that would have occurred if the nuclear energy had been produced instead using coal or gas.

Interference with the enjoyment of property outside of the plant premises

Two events, Chernobyl and Fukushima resulted in long-term evacuation of a sizeable area. At Chernobyl approximately 130,000 people were relocated and a 2600-km^2 exclusion area was established. For Fukushima the numbers are about 90,000 people and 300-km^2. By comparison the tsunami alone destroyed about 45,000 structures and is responsible for 200,000 people now living in evacuation shelters. Another comparison can be made with the Three Gorges Dam that caused relocation of 1.2 million and it impounds an area of 1045-km^2.

Severe accidents contributes little to energy risks, so it seems reasonable that improving electric power robustness may be an "as low as reasonably achievable" (ALARA) effort.

Severe accidents also have economic consequences. All of the severe accidents have resulted in significant recovery and restoration costs. Plant replacement and cleanup costs at Fukushima may be in the range of 100 to 300 billion US$. To utility CEOs a new nuclear power plant must look like a "you bet your company" proposition. We must give buyers and operators confidence that this is not the case. Consideration of the economic effects may justify more robustness measures than consideration of health and environmental effects alone.

2. Reliability, defense in depth, and diversity in electrical power systems

Electrical power systems in today's nuclear power plants are designed for extremely high reliability and incorporate defense in depth strategies. Most of these systems were produced using management systems that provided for design bases that are informed by plant safety analyses. The designs foster high reliability and tolerance of failure; and provide redundant and diverse power sources and distribution so that nearly every load can be supplied by two or more sources and via several paths.

IAEA DS 430[6] describes these strategies. These design strategies have served the nuclear industry well. Nevertheless, events such as the 25 July 2006 Forsemark incident[7] and the Fukushima Daiichi accident show that we cannot envision all events that may defeat these measures.

The concern is hazards that might cause common cause failure (CCF) of redundant or diverse supplies making critical loads inoperable. Loss of all DC power would be the most severe event as most plants can be brought to a controlled state for some time if DC is available. Also, without DC power many electrical

[5]. Kharecha, P. and Hansen, J., "Prevented Mortality and Greenhouse Gas Emissions from Historical and Projected Nuclear Power," Environmental Science and Technology, 47, p. 4889-4895, 2013.

[6]. DS-430, "Design of Electrical Power Systems for Nuclear Power Plants," International Atomic Energy Commission, in publication.

[7]. NEC/CSNI/R(2009)10, "Defense in Depth of Electrical Systems and Grid Interaction," Nuclear Energy Agency, 2009.

switchgear and standby AC power sources may be inoperable. Normal and emergency supplies should also be robust with the highest attention paid to standby AC supplies and distribution.

Much attention has been given to emergency power sources, but the distribution systems are more important. Batteries or generators might be available or brought in fairly rapidly; distribution systems cannot so easily be replaced. Repair is time consuming and the events that caused failure of distribution may prevent repair or impede the installation of temporary cabling, protective devices, and motor controls.

Further improvement of electrical power systems robustness will come from better understanding of and better means to cope with the epistemic uncertainties concerning the hazards to electrical systems.

3. Hazards to electrical power systems

Hazards to electrical power systems can be categorized as:

- Internal Hazards: hazards that originate within the site boundary;
- External Hazards: hazards that originate outside of the site boundary; and
- Human Hazards: Hazards created by design mistakes, operational mistakes, or malicious acts.

Internal Hazards

IAEA Safety Guides NS-G-1.7[8], and NS-G-1.11[9] describe the recognized internal hazards and discuss means for preventing hazard events and mitigating their consequences. Table 1 summarizes internal hazards and the typical means for preventing CCF. These means are identified as:

- Location: Location of electrical equipment and cable away from hazards,
- Separation: Physical separation and electrical isolation of redundant equipment and cable,
- Barriers: Local barriers that protect equipment and cable from the hazard,
- Coordination: Protective device coordination,
- Qualification: Qualification of equipment and cable for the hazardous environment,
- Fire protection: Provision for suppression of and protection against fire,
- Drains: Provisions to prevent accumulation of water in electrical equipment.

Internal hazards result from design features. Designers try to minimize hazards but cannot eliminate them all. Epistemic uncertainties for internal hazards are low because they are man-made. The greatest uncertainties may concern the efficacy of the existing preventative and mitigative measures.

Following the Browns Ferry fire, existing cable and equipment separation criteria were questioned. Before Browns Ferry separation distances of a few feet were assumed sufficient to prevent CCF in a fire. Afterwards it was assumed that everything within a given fire area could be destroyed unless it was specifically protected. The US industry performed analyses to confirm that plants could be brought to, and maintained in a controlled state, if all equipment and cables in any fire area were destroyed. These analyses were called “safe shutdown analyses.” The robustness of electrical systems in plant fires depends upon such analyses. It also depends upon continued maintenance to ensure that the assumptions of the

[8]. NS-G-1.7, “Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants,” International Atomic Energy Commission, 2004.

[9]. NS-G-1.11, “Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants,” International Atomic Energy Commission, 2004.

analysis remain valid, e.g., that fire barriers including doors, dampers, and penetration seals remain effective. It is incumbent upon plant electrical staff to be aware of the maintenance of such items.

Safe shutdown analysis should be maintained and extended to cover other hazards, such as flooding and structural collapse, that affect large local areas.

Protective device coordination contributes to protection against every internal and external hazard. Coordination studies should be documented and maintained for the life of the plant.

External Hazards

IAEA Safety Guides NS-G-1.5[10], and NS-G-1.6[11] describe the recognized external hazards and discuss means for preventing hazard events and mitigating their consequences. Table 2 summarizes the external hazards and the typical means for preventing CCF. These means are identified as:

- Location: Location of electrical equipment and cable away from hazards;
- Separation: Physical separation and electrical isolation of redundant equipment and cable;
- Barriers: Local barriers (including structures) that protect equipment and cable from the hazard;
- Coordination: Protective device coordination;
- Qualification: Qualification of equipment and cable for the hazardous environment;
- Fire protection: Plans, facilities, and staff for fighting external fires;
- Electrical protection: Protective devices, grounding, surge suppressors, filtering, shielding.

Except for geomagnetic events, the epistemic uncertainty about external hazards is moderate. We have studied these events for decades. Still events that exceed design bases occur nearly every year.

Our knowledge about geomagnetic events is more limited. We have been aware of such events for about 150 years. Our knowledge comes from a relatively short period when we have been able to make measurements and a longer time for which we have anecdotal information about aurora observations or the effects on telegraph communications. Geomagnetic effects have been observed as far south as 8° south latitude. Space weather researchers conclude that we should not be surprised when space weather effects exceed the currently known events[12].

We should understand the epistemic uncertainties in plant external event design bases and the possibilities for more extreme events at each site. Where this identifies undesirable risks, practical means for improving electrical system robustness should be considered, e.g., having both electrical and a driven emergency feedwater pumps, berms around external equipment or improved electromagnetic decoupling.

Some hazards, such as flooding other than tsunami, volcanism, or geomagnetic storms, may give advance warning. In these cases plans for taking protective measures on warning should exist.

The most troublesome consequences for some events will be indirect. For example, during the Mt. St. Helens eruption, diesel air filters, and structural collapse of buildings containing power system equipment

[10]. NS-G-1.5, "External Events Excluding Earthquakes in the Design of Nuclear Power Plants," International Atomic Energy Commission, 2003.

[11]. NS-G-1.6, "Seismic Design and Qualification for Nuclear Power Plants," International Atomic Energy Commission, 2003.

[12]. Cliver, E, Svalgaard, L, "The 1859 Solar-Terrestrial Disturbance and the Current Limits of Extreme Space Weather Activity," Solar Physics, 224, p. 407-422.

were among the concerns. Geomagnetic storms might not directly affect plant power systems but could cause long-term loss of offsite power and hamper resupply of fuel for emergency generators.

Human Hazards

Human hazards include Operational Errors, Design Errors and Malicious Acts. IAEA DS-430[6], DS-431[13], Security Series 4[14], Security Series 8[15], NSS-13[16], and NSS 17[17] deal with these topics. Table 3 summarizes the human hazards and the typical means for preventing CCF. These means are identified as:

- Human Factors Engineering: Design of operational interfaces and maintenance provisions to reduce the potential for human error,
- Training: Education, and qualification of operations, maintenance, design, and manufacturing personnel for the tasks that they must perform,
- Procedures: Established, documented, verified and validated means for performing operations, maintenance, design, and manufacturing activities,
- Design Standards: Corporate, national, and international standards that convey proven methods for achieving technical and reliability characteristics of electrical systems,
- Access Control & Monitoring: Physical, administrative, and technical measures to inhibit unauthorized physical or electronic access to electrical system equipment and to detect such access if it does occur.
- Secure Development Environments: Design, implementation, and maintenance environments having physical, logical, and programmatic controls to ensure that unwanted, unneeded, and undocumented functionality is not maliciously introduced into digital systems,

Humans may be the largest source of epistemic uncertainty. Fourteen of the accidents considered were initiated by human errors, and in some cases clever or heroic human actions terminated accidents.

NEA/CSNI/R/2009(10)[7] identified 23 events involving human errors. Most involved missteps during maintenance. The report recommends task analysis for safety-related operations and maintenance activities. This should also include also maintenance activities that could result in CCF within the preferred power supply. Humans are more reliable if they are prepared in advance, have procedures or guidelines, and realistically practice their tasks. Electrical staff involved in implementing SAMG should have this.

Mechanical and relay-based electrical devices are now being replaced with digital components. This raises the question of how to prevent and mitigate CCF resulting from software errors. The I&C community has settled on the use of rigorous design procedures, design transparency, design standards, defense in depth, and diversity. The electrical community should not uncritically accept the I&C approach. Digital devices for electrical systems are different from I&C. For example, many electrical devices perform

[13]. DS-431, "Design of Instrumentation and Control Systems for Nuclear Power Plants," International Atomic Energy Commission, in final review.

[14]. International Atomic Energy Commission Nuclear Security Series No. 4, "Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage," International Atomic Energy Commission, 2007.

[15]. International Atomic Energy Commission Nuclear Safety Series No. 8, "Preventive and Protective Measures against Insider Threats," International Atomic Energy Commission, 2008.

[16]. International Atomic Energy Commission Nuclear Security Series No. 13, "Nuclear Security Requirements on Physical Protection of Nuclear Material and Nuclear Facilities," International Atomic Energy Commission, 2011.

[17]. International Atomic Energy Commission Nuclear Security Series No. 17, "Computer Security at Nuclear Facilities," International Atomic Energy Commission, 2011.

exactly the same function in both nuclear and commercial applications, perform the same function during normal operation and accident conditions, and are less likely to see untested operational profiles during accident conditions. Such differences may allow the use of a simpler strategy for at least some electrical equipment. The electrical community should work with researchers and regulators to develop a strategy for electrical systems.

Operational errors and design errors are mistakes. Electrical systems must also deal with the possibility of intentional mal-operation of components either directly or through the introduction of malicious code. Digital devices create the risk of cyber attack. That such events can be created has been demonstrated[18,19] and at least one serious attack on nuclear facility electrical controls has occurred[20]. Controlling electronic access to plant equipment, engineering development environments and design tools is critical to controlling the risk. The potential consequences of malicious operation of electrical equipment should be understood. If a cyber attack could result in serious plant consequences, use of non-digital devices to prevent or mitigate these consequences should be considered.

[18]. Video, "Staged Cyber Attack Reveals Vulnerability in Power Grid," http://www.youtube.com/watch?v=fJyWngDco3g, retrieved 2014-02-09, CNN.

[19]. "What You Need to Know (and Don't) About the AURORA Vulnerability," Power Magazine. 2013-09-01

[20]. Langner, R. "To Kill a Centrifuge, A Technical Analysis of What Stuxnet's Creators Tried to Achieve," http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf, retrieved 2014-02-09, Langner Group (2013).

Table 1. Summary of Internal Hazards and Protective Measures

Hazard	Vulnerable Electrical Components	Typical means for preventing common cause failure							Comments
		Location	Separation	Barriers	Coordination	Qualification	Fire Protection	Drains	
Missiles	Cables Local panels	x	x	x	x				Mainly containment and turbine building
Collapse of Structures	Any equipment and cables		x		x				Structural failures have occurred in substations. Structural collapse might result from other events
Falling Objects	Any equipment and cables	x	x		x				In areas where heavy objects are lifted
Pipe Whip	Cables Local panels	x	x	x	x				Mainly containment and turbine building
Jet Effects	Cables Local panels	x	x	x	x				Mainly containment and turbine building
Environmental effects of pipe or vessel breaks	Cables Local panels	x	x		x	x			Mainly containment and turbine building
Floods, leaks, and sprays	Any equipment and cables	x	x	x	x	x		x	Consider also the need for enclosure drains to prevent accumulation of moisture over time
Fires and fire effects	Any equipment and cables	x	x		x		x		
Explosions	Any equipment and cables	x	x		x				

Table 2. Summary of External Hazards and Protective Measures

Hazard	Vulnerable Electrical Components	Typical means for preventing common cause failure							Comments
		Location	Separation	Diversity	Coordination	Qualification	Fire Protection	Electrical Protection	
Earthquake	Any equipment				x	x			Even non-safety equipment is designed for some level of seismic, but qualification may be less rigorous
Aircraft Crash	Any Equipment and Cables	x	x		x				
Fires	Any Equipment and Cables	x			x		x		Applies to out door equipment such as unit transformers and substations.
Explosions	Any Equipment and Cables	x	x		x				
Asphyxiant & Toxic Gases	N/A								A bigger threat to operators than equipment. Could be a maintenance issue
Corrosive Gases & Liquids	Any Equipment and Cables	x	x		x				
Electromagnetic Interference	Any Equipment	x	x			x			Both and internal and an external hazard.
Floods	Any Equipment and Cables	x	x		x				
Extreme Winds	Any Equipment and Cables	x		x				x	Included tornados which could affect indoor equipment if not protected

Hazard	Vulnerable Electrical Components	Typical means for preventing common cause failure							Comments
		Location	Separation	Diversity	Coordination	Qualification	Fire Protection	Electrical Protection	
Extreme Meteorological Conditions	Any Equipment and Cables	x		x				x	Applies to outdoor equipment such as unit transformers and substations.
Biological Phenomena	N/A								Mainly an issue with coolant systems in contact with ultimate heat sink.
Volcanism	Standby Generators			x					Filters may be rapidly consumed. Mudflows may affect UHS. Ash fall could result in structural collapse.
Collisions with Floating Bodies	Standby Generators			x					Affects ultimate heat sink.
Geomagnetic Effects	Any Equipment				x			x	
Grid transients	Any Equipment							x	

Table 3. Summary of Human Hazards and Protective Measures

Hazard	Vulnerable Electrical Components	Typical means for preventing common cause failure						Comments
		Human Factors Engineering	Training	Procedures	Design Standards	Access Control & Monitoring	Secure Development Environment	
Operational Errors	Any equipment	x	x	x				
Design Errors	Any equipment and cables		x	x	x			
Malicious Acts	Any equipment and cables		x	x	x	x	x	Threats to hardware are mainly insider threats needing physical access control only

4. Extremely extreme events

It would be foolhardy to believe that we can completely eliminate the possibility of total loss of plant power such as happened at Fukushima-Daiichi.

Plants must be prepared for the worst-case events. Some necessary functions might be accomplished without electrical power, but where it is needed electrical systems should provide power to implement Severe Accident Management Guidelines (SAMG). These power systems should be independent of the plant electrical systems to the extent possible (including independence from the distribution systems) and must be suitable to supply at least the loads needed to support the "last ditch" efforts of the SAMG, including pumps, valves, air compressors, lighting and instrumentation. These goals might be accomplished with very simple portable supplies and battery backup for designated severe accident monitoring instruments.

5. Conclusions

Severe accidents result from unexpected events that were not considered or were discounted in the plant design or operations and that were not sufficiently mitigated by defense in depth measures.

Electrical power systems can be made more robust to such events by understanding the epistemic uncertainties behind design basis requirements and taking action to deal with more extreme events.

Non-nuclear sources present greater risks to humans and the environment than nuclear power. Thus, it is reasonable that improvements to the robustness of nuclear power plants follow an ALARA approach. That being said, the cost of replacement power, plant replacement and cleanup following an accident might justify more extensive measures.

Epistemic uncertainties are low for internal hazards. The main uncertainties may be the continued effectiveness of the preventative measures. Safe-shutdown analyses should be kept up to date and extended to cover other wide area hazards, such as, structural collapse and floods. Also electrical coordination studies should be reviewed and maintained up to date.

Epistemic uncertainties are moderate for most external hazards. We understand the hazards reasonably well, but hidden evidence is still to be uncovered and predictive models continue to improve. Events that exceed external hazard design bases seem to occur every year. Electrical system engineers should be aware of the epistemic uncertainties behind their external event design bases and consider if practical measures can be taken to make the systems more robust.

Humans represent the greatest hazard to plants, including the electrical power systems. Human error contributed to all nineteen severe accidents. Management systems have served us well, but more effort needs to be given to imagine what failures errors might create and how they might be practically addressed.

Electrical systems are beginning to extensively use digital components. This creates new possibilities for CCF. The I&C community has dealt with this issue. The electrical community should consider if the I&C approach or some other approach is appropriate for electrical systems.

The use of digital components raises the potential for cyber attack. Computer security features should be introduced when digital components are installed in power systems. If potential

consequences of cyber attack are unacceptable, hardware measures should be introduced to prevent or mitigate these consequences. Reference 20 is highly recommended reading.

We can never eliminate the occurrence of unimagined events nor can we afford to build for all worst imaginable cases. Plans and equipment must to be in place to deal with such occasions. This should include plans for complete loss of plant AC and DC power. Electrical supplies that are independent of the plant electrical power system should be available to service SAMG loads for "last ditch" scenarios. Plant electrical staff should also be trained for and realistically practice their role in implementing SAMG.

The next generation plants can tolerate loss of all site AC power for days as opposed to hours. These features will improve safety, but we must consider the possibility of more extreme events such as the loss of plant DC power, the failure of plant distribution systems, or longer-term station blackout.

A Survey of Hazards to Electrical Power Systems

Presented to
CSNI International Workshop on Robustness of Electrical Systems of NPPs in Light of the Fukushima Daiichi Accident
Paris
2014 April 1 to 4

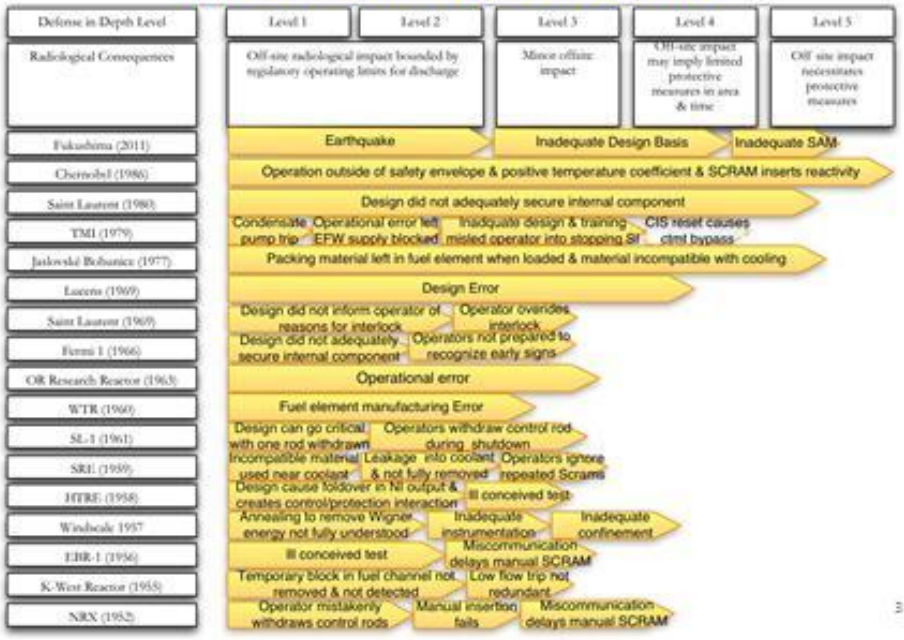
Gary Johnson
Independent Consultant
gljohnson@ieee.org

Agenda

- Historical severe accidents & lessons learned
- Survey of hazards
- Priorities
- Uncovered extreme events
- Conclusions

2

Nineteen severe accidents



Failure of imagination (sometimes) leads to severe accidents

- Severe accidents happen because of limits to our knowledge for which:
  - Plant is not designed to cope,
  - Operators are not prepared to respond, and
  - Multiple levels of defense in depth are often bypassed
- Most were initiated by operational errors, design errors or both
- Design should consider epistemic uncertainties
  - Unexpected events
  - Hazards that may be bigger than design bases
  - Unexpected consequences

Severe accidents are bad, but safety risks don't justify extraordinary measures*

*But economic risks might

5

What's the worst that can happen to electrical systems?

- Failure of all onsite and offsite power sources
- Failure of distribution systems
- Failure of all DC supplies
- Station blackout
- Consideration of CCF should go beyond safety systems
  - Off site supplies
  - Normal supplies

It is not meant that these should be treated as safety systems, but that CCF vulnerabilities should be identified and means for reducing vulnerabilities ALARA should be applied

6

Internal Hazards

Are existing protective measures still effective?
Are further practical improvements possible?

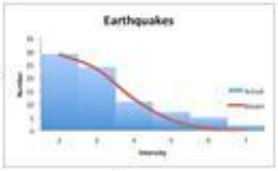
- Epistemic uncertainties about hazards is low
  - Bigger uncertainty: effectiveness of protective measures?
- Potential consequences should be fully studied,
  - E.g., large local events fire, flood, structural collapse
- Safety depends on continued effectiveness of protective & mitigative measures
  - Physical, e.g., fire barriers, dampers, cocoons
  - Analytical, e.g., safe shutdown analyses
  - Electrical, e.g., coordination
- Active maintenance and configuration control is needed

7

External Hazards:

Consider improvements that can deal with fat tails?

- Epistemic uncertainties are mostly moderate
  - Events > design bases are frequent (~1/yr)
- Understand limits and uncertainties
  - Worst consequences, shape of "fat tails"



- Take ALARA measures
  - For slow developing events – plans may be enough
- Uncertainties for geomagnetic events are high
- Keep in mind that effects on electrical power may be indirect
  - E.g., the important threats from volcanoes might be sulfur dioxide concentration in the atmosphere or ashfall

8

9

Human Hazards

Prepare for the unpredictable

- Humans are the least understood hazard
- All severe accidents involved human error
  - For most, human errors were the initiator
  - Humans also took actions to terminate the accidents
    - Humans are more reliable if they are properly prepared
      - Imagine, plan, educate, train, and practice for the worst
- The DIDELSYS report recommends task analysis for safety system maintenance
  - This should include preferred power supply
- Digital devices creates risks of "software CCF"
  - A prevention and mitigation strategy is needed
  - The I&C strategy might not be right for electrical

10

Malicious acts are also a human hazard

Limit the threat and control the consequences

- So far personnel vetting and physical access control have been effective
- Digital devices create new pathways
  - Via plant networks
  - Via development process
- Introduce cyber security measures when digital devices installed
  - Vendors should have secure development environments
- Understand worst consequences
  - Non-digital measures to protect or mitigate high consequence events.

11

Demonstration of cyber attack

Connecting generator to live bus, out of sync

12

Extremely extreme events

- Some hazards can't be predicted
- Some hazards that can be predicted cannot be reasonably prevented or adequately mitigated
- Remedy is severe accident management
  - SAMG need a path for loss of all plant power
    - Electrical staff need to be trained and practiced for their role
  - Power supplies, independent of plant power systems, should be available to support these paths.
  - These might be relatively simple
    - Stand alone battery backup for designated instruments
    - Simple AC supply for "last ditch" pumps and vents
  - Not just more diesels, but sources and connections that support specific loads

13

Conclusions

- Improvement to electrical system robustness can have an ALARA goal
- Epistemic uncertainties and the most extreme consequences should be understood
  - Take practical measures
- It is not possible to be robust to the unimaginable, or even to most worst cases
  - SAMG should include a loss of plant power supplies path
  - Provide supplies and connections that are independent of the plant to implement this path

14