Lessons Learned from Severe Accidents in Nuclear Reactors

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

Presented to
Fall 2018 Colloquium Series
UC Berkeley Department of Nuclear Engineering's
2018 08 27

Gary Johnson
kg6un@mac.com

What are severe accidents?

- The International Atomic Energy Agency (IAEA) defines severe accidents as:

  "Accidents more severe than a design basis accident and involving significant fuel degradation"

- It is one of five plant conditions that they define

Operational States		Accident Conditions		
Normal Operation	Anticipated Operational Occurrences	Design Basis Accidents	Design Extension Conditions	
			Without Significant Fuel Degradation	With Significant Fuel Degradation

After Fukushima-Daiichi I began thinking about severe accidents

I produced two studies*

International Atomic Energy Agency

Training material

Long overview of each event

What and why

Intended for university students

Videos for six events

Three Mile Island, Chernobyl,
Fukushima Daiichi X 3, and HTRE-3

Electric Power Research Institute

Lessons for instrumentation & control and human machine interaction

Short overview of each event

Role of instrumentation control and human system interfaces

Intended for industry personnel

Published 2015

*With a lot of help from Dan Welbourne from the UK

There have been 19 severe accidents

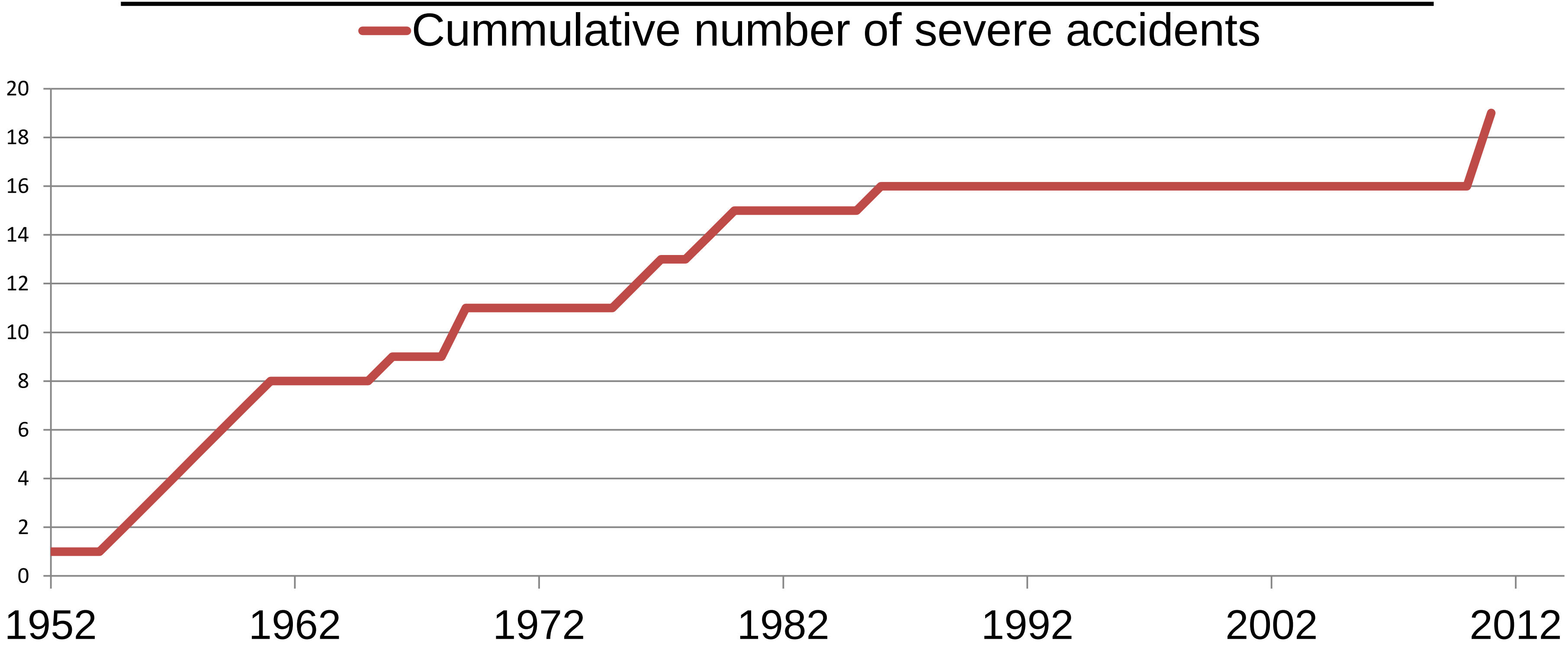
Types of Plants

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

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

Fukushima Daiichi Units 1, 2, & 3	Japan
Three Mile Island 2	US
Chernobyl Unit 4	Ukraine
Fermi Unit 1	US
KS 150	Slovakia
Sodium Reactor Experiment	US
Saint Laurent Unit A2	France
Saint Laurent Unit A1	France
Chapelcross Unit 2	UK
Windscale Unit 1	UK
105 K-West	US
Heat Transfer Reactor Experiment-3	US
NRX	
Canada	
SL-1	
US	
Westinghouse Testing Reactor	US

Severe accidents are more common than we think



$$\frac{2\ \text{events}}{17000\ \text{reactor years}} \approx 10^{-4}/\text{reactor year}$$

In US designed gen 2 reactors, counting Fukushima-Daiichi as a one event

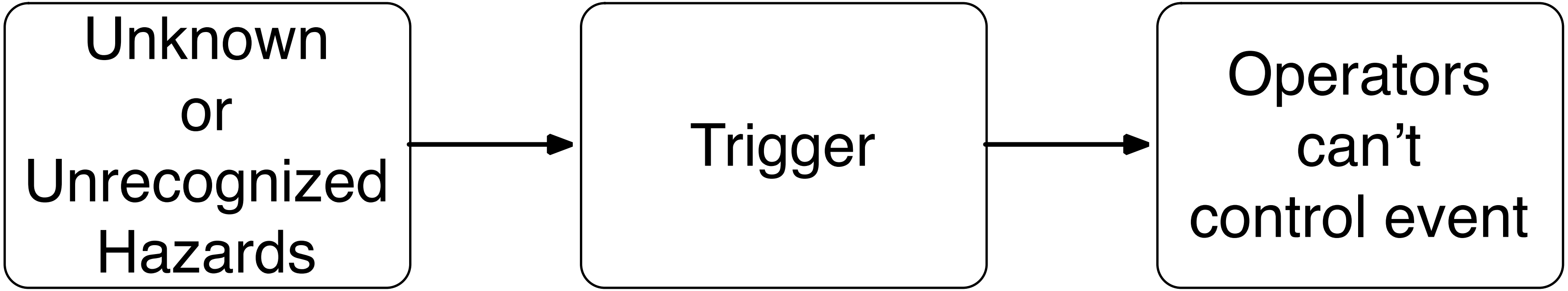
Severe accidents resemble black swans

Characteristics of a Black Swan:

Hard to predict

Serious consequences

Obvious in retrospect . . . Nassim Nicholas Taleb



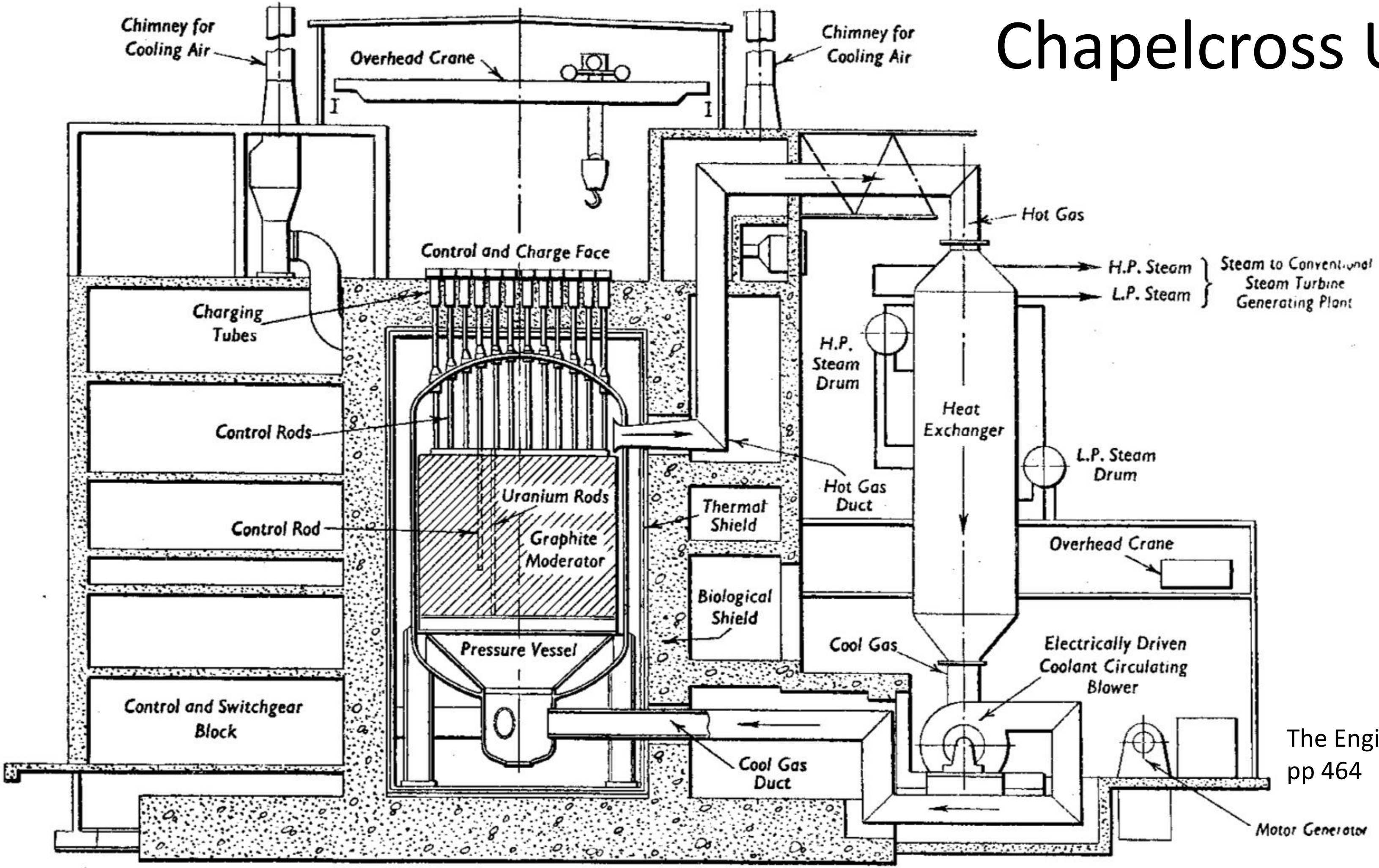
Sometimes just unknowns

Routine operation Abnormal operation

About half the time there was no opportunity

Taleb gives a 4 minute summary of black swans at https://www.youtube.com/watch?v=BDbuJtAiABA

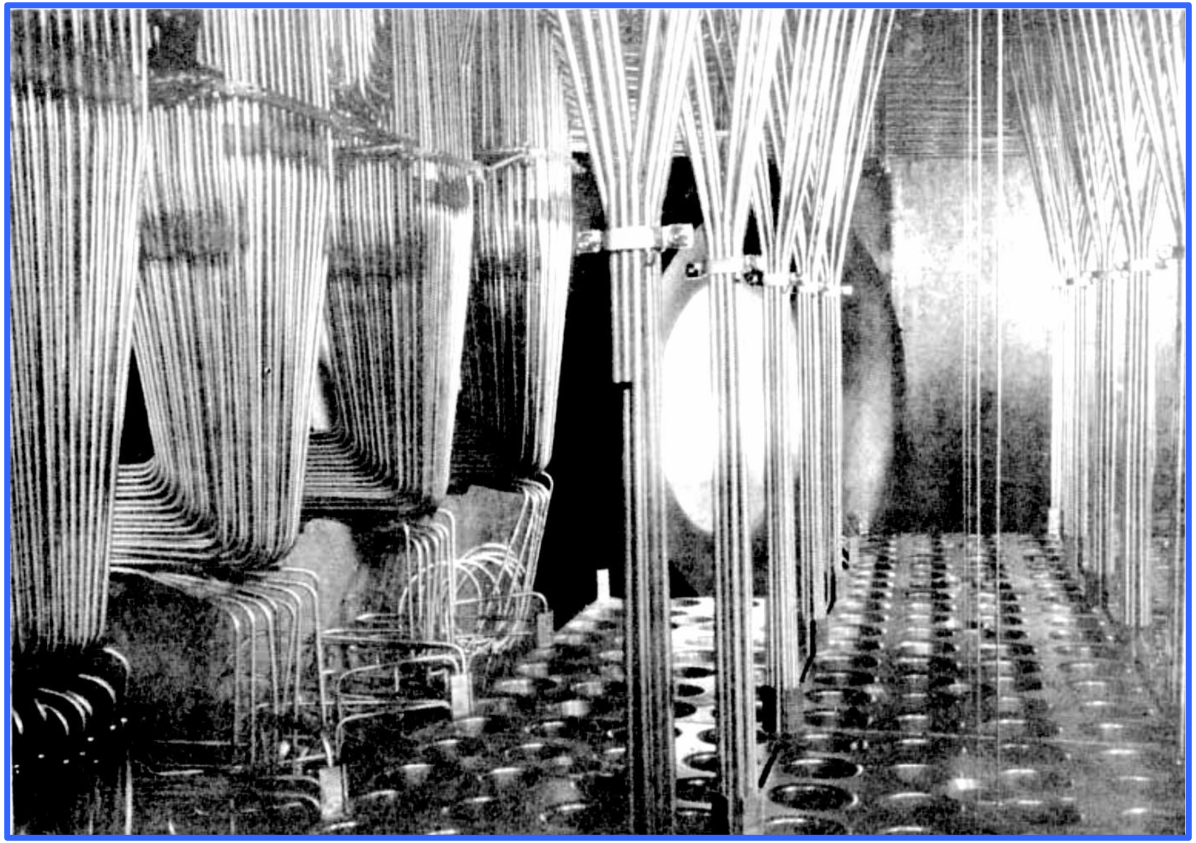
Chapelcross Unit 2



The Engineer, Oct 5, 1956. pp 464

Some of the actors in this story

Sampling tubes for fission product monitors



This and previous slide, Reactor Core Design Principles, Air-Cooled and Magnox, B. J. Marsden, The University Of Manchester.

The Chapelcross 2 event

Unknown

In 1964 experimental fuel assemblies were loaded into a fuel channel having a damaged sleeve. The damage partially blocked coolant flow, but there was still enough flow to cool the fuel.

Known but unrecognized

No outlet temperature sensors for the affected fuel channel.

Fission product detectors meant to identify leaking channels had a long response time.

→

Trigger

In 1967 new hotter fuel replaced most of the reactors fuel, but fuel in the damaged channel was left in place.

The new fuel raised the coolant temperature enough that flow in the damaged channel was insufficient to cool the fuel assemblies

→

Consequences

Six fuel assemblies melted

No significant radiological release

Consider the TMI-2 Accident

Poor maintenance procedure for condensate polishers → Condensate polisher isolates

No bypass for tripped polishers → Turbine trip, Reactor trip

Safety system automatically initiated high pressure injection

- Pressurizer Power Operated Valve (PORV) position indication “lied”
- Operators not informed of the hazards of high point LOCA
- Encouragement to avoid solid pressurizer
- Inadequate procedures for LOCA and Pressurizer operation

→ Operators didn’t recognize the event as a small break LOCA (SBLOCA) and they shutdown safety injection

- Prior operation with leaky PORV masked temperature indications that PORV was stuck open
- Displays for important secondary parameters inaccessable
- Poor training for SBLOCA and thermodynamic principles
- Inadequate range of core exit temperature display
- No RPV level measurement

→ Operators failed to recognize that they had a SBLOCA for at least 2 1/2 hours

By that time recovery was very difficult

Severe accidents were generally not caused by random failures

- The events resulted from
  - Unrecognized hazards (11 instances)
  - Plant design issues (13 instances)
  - I&C design issues (13 instances)
  - Operator training issues (7 instances)
  - Operating procedure issues (9 instances)
  - Maintenance issues (7 issues)
- The likely root causes are inadequate:
  - Safety analysis
  - Equipment specification
  - Communication between designers and operators

Severe accidents involved bypass of multiple “independent” layers of <u>defense in depth</u>

- Here I speak of the INSAG defense in depth model
  - See INSAG 10 and 12
- INSAG is a “greybeard” committee that advises IAEA on high level safety topics

Strategy	Accident prevention			Accident mitigation	
Operational state of the plant	Normal operation	Anticipated operational occurrences	Design basis and complex operating states	Severe accidents beyond the design basis	Post-severe accident situation
Level of defence in depth	Level 1	Level 2	Level 3	Level 4	Level 5
Objective	Prevention of abnormal operation and failure	Control of abnormal operation and detection of failures	Control of accidents below the severity level postulated in the design basis	Control of severe plant conditions, including prevention of accident progression, and mitigation of the consequences of severe accidents, including confinement protection	Mitigation of radiological consequences of significant releases of radioactive materials
Essential features	Conservative design and quality in construction and operation	Control, limiting and protection systems and other surveillance features	Engineered safety features and accident procedures	Complementary measures and accident management, including confinement prodection	Off-site emergency response
Control	Normal operating activities		Control of accidents in design basis	Accident management	
Procedures	Normal operating procedures		Emergency operating procedures	Ultimate part of emergency operating procedures	
Response	Normal operating systems		Engineered safety features	Special design features	Off-site emergency preparations
Condition of barriers	Area of specified acceptable fuel design limit		Fuel failure; Severe fuel damage	Fuel melt; Uncontrolled fuel melt	Loss of confinement
Colour code	NORMAL		POSTULATED ACCIDENTS		EMERGENCY

INSAG-10 Defense in Depth Levels

(Level 1 | Level 2 | Level 3 | Level 4 | Level 5)

Events ordered by date	INSAG-10 Defense in Depth Levels			Event termination
Fukushima Daiichi 1,2,3	Inadequate design basis for external hazards & large tsunami	Accident management couldn't deal with effects of extreme external hazards		Operators provide cooling of corium
Chernobyl 4	Operators unaware of design's hazards. Inadequate procedures poor operational discipline	SCRAM inserted reactivity		Core disassembly
Saint Laurent A2	Lack of loose parts monitoring.	Loose part in the core blocks flow in several fuel channels	Trip set point error	Automatic trip: High Fission Product Activity
TMI-2	Poor training, procedures, operational discipline, MCR design, & I&C design	Operators fail to recognize plant condition		Operators restore core cooling
KS 150	Inadequate QA for fuel assembly	Unreliable core exit temperature indicators delayed reactor trip.		Manual trip: High Fuel Temperature
Lucens	Unexpected condition partially blocks fuel channel	Sensitivity of exit thermocouples and flow meters not sufficient to detect partial fuel blockage		Automatic trip: High Fission Product Activity
Chapelcross U2	Fuel channel damaged, inadequate provisions for detecting damage	New fuel assemblies increase fuel channel temperatures	Procedure delays SCRAM	Manual trip: High Fission Product Activity
Saint Laurent A1	Inadequate feedback for why refueling machine wouldn't load element	Operator overides interlock	Trip set point error	Automatic trip: High Fission Product Activity
Fermi 1	Inadequate analysis of core retention plates. No loose parts monitoring. Core monitors can't detect blockage	Corium retention plates come loose and block fuel channels		Manual trip: High containment radiation
WTR	Inadequate operating procedures & training.	No trip on fuel failure		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 combines with reactor coolant and blocks fuel channels	Operators failed to investigate causes of reactor trips		Manual shutdown to investigate fuel condition
HTRE-3	Incorrect location and voltage settings for neutron detectors. New power control system not tested before use			Beneficial of high fuel temperature trip
Windscale U1	Incorrect location of fuel temperature sensors. Fission product detection systems inoperable			Burning fuel removed from core
EBR-I	Inadequate test procedure. Inadequate fuel temperature measurement channels.	Trip set point error. Confusion about manual trip actions.		Manual trip: Short period
105 KW	Inadequate control of temporary changes and instrument calibration. 1 out of one 1 reactor trip on low flow in fuel channel			Automatic trip: high flow in channel (rupture)
NRX	Inadequate procedures & I&C. Operation with sticky control rods	Operator errors actuating reactor trip		Manual trip: diverse shutdown system

Most severe accidents had minimal effect on the surrounding area

Chernobyl Unit 4	Major Accidents
Fukushima Daiichi Units 1, 2, & 3	
Windscale Unit 1	Accidents with Wide Consequences
Three Mile Island 2	
NRX	Accidents with Local Consequences
Heat Transfer Reactor Experiment-3	
Fermi Unit 1	
KS 150	
Sodium Reactor Experiment	
Saint Laurent Unit A2	
SL-1	
Westinghouse Testing Reactor	
Saint Laurent Unit A1	
Lucens	
Experimental Breeder Reactor 1	
Chapelcross Unit 2	Serious Incidents
105 K-West	

Gen 2 US LWR
Other power reactors
Production reactors
Test Reactors

Severe accidents haven't caused <u>the expected levels of public radiation exposure</u>

- Five events involved significant off-site radiological release
  - Windscale, Chernobyl, Fukushima Daiichi X 3
- No member of the public is known to have suffered deterministic effects of radiation exposure from a severe accident.
- Only Chernobyl had identifiable stochastic effects
  - ~ 6000 additional thyroid cancers
  - ~ 15 fatalities

Severe accidents have harmed the public because of long term relocation

	Fukushima Daiichi	Chernobyl
People displaced from their homes	210,000	335,000
People still displaced as of 2015	80,000	
Land excluded from human use	1000 km^2	15,000 km^2
Long term no-return area	330 km^2	
Deaths during evacuation	≈ 50	

Depression was common

- Depression and post traumatic stress were common among the affected, and even some of the unaffected, in both areas.
- A 2013 study of Fukushima-Daiichi evacuees found
  - 16,000 people were still living in evacuation shelters
  - 8,000 considered themselves socially disabled due to traumatic symptoms,
  - 17,000 thought that they or their offspring would suffer health effects from radiations exposure
- A 2016 study of determined that mortality rates of evacuated elderly increased by 2 to 3 times during the four months after the accidents.

Instrumentation and control issues almost always contributed to the causes of severe accidents

I&C & HSI Contributions	Number of Instances
Lack of needed functions	8
Systems unavailable	10
Inadequate design	16
Inadequate human system interface	10
Inadequate lifecycle implementation	6

Most events involved several I&C and HSI contributions

Generally these were failures of the design not of the I&C equipment

Safety systems failed, but failure of non-safety systems strongly contributed

Conclusions

- While many of the events considered are old, I think that the fundamental causes are still relevant today
- We should expect future severe accidents
    - A optimistic estimate of the severe accident occurrence frequency at this time is about 10^{-4}/reactor year
- Severe accidents look to me like black swans
    - Unknown unknowns or incompletely understood known unknowns lead to severe accidents

Conclusions

- Severe accidents have generally resulted from “high level” errors, not equipment failures
- Severe accidents involve bypass of multiple levels of defense in depth.
- We’ve done a good job of protecting the public from radiation exposure
- But we should have the further goal of never making our neighbors move at least not for a long time

You may download the EPRI Report at

https://www.epri.com/#/pages/product/000000003002005385/

It is free and public.

The IAEA reports and videos should be available to universities

If you want these, I prefer that you get them from IAEA

Contact Ashok Ganesan

A.Ganesan@iaea.org

If that fails, let me know

Short bibliography

- Slide 2: Definition of Severe Accident - IAEA Safety Glossary, https://www.iaea.org/resources/safety-standards/safety-glossary
- Slide 4: See list of event references at end
- Slide 5: Reactor Years – World Nuclear Association, http://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/safety-of-nuclear-power-reactors.aspx
- Slide 6: Black Swans – The Black Swan: The Impact of the Highly Improbable, Nassim Nicholas Taleb, (2007)
- Slide 10: Chaplecross accident – See list of event references
- Slide 11: TMI event – See list of event references
- Slide 13: Defense in Depth concept – INSAG-10 Defense in Depth in Nuclear Safety, https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1013e_web.pdf, also Basic Safety Principles for Nuclear Power Plants, https://www-pub.iaea.org/MTCD/Publications/PDF/P082_scr.pdf

- Slide 17: Displaced from home
  - Fukushima. Fallout of fear, Brumfiel, G, Nature, Vol. 493, pp 290-293, (2013)
  - Chernobyl, UNSCEAR Report 2008 Annex D.pdf, http://www.unscear.org/docs/reports/2008/11-80076_Report_2008_Annex_D.pdf

  Still displaced

  - Finding a place to call home still plagues Japanese displaced by quake and tsunami, Whietfield, M, Miami Herald (2015),

  Land excluded from human use

  - Fukushima. Estimated from Progress of Off-Site Cleanup Efforts in Japan, Ministry of Environment, (2015)
  - Chernobyl's Legacy: Health, Environment and Socio-Economic Impacts and Recommendations to the Governments of Belarus, the Russian Federation, and Ukraine, The Chernobyl Forum: 2nd revised version (2006), https://www.iaea.org/sites/default/files/chernobyl.pdf

  No long term return

  - Estimated from Progress of Off-Site Cleanup Efforts in Japan, Ministry of Environment, (2015)

  Deaths due to evacuation

  - UNSCEAR_2013_Annex_A_Ebook_website.pdf http://www.unscear.org/docs/reports/2013/13-85418_Report_2013_Annex_A.pdf

Slide 18

- 2013 Study – Psychological Distress after the Great East Japan Earthquake and Fukushima Daiichi Nuclear Power Plant Accident: Results of a Mental Health and Lifestyle Survey through the Fukushima Health Management Survey, Yabe, H, et. al., Fukushima Journal of Medical Science, Vol. 60, No. 1 (2014), https://www.jstage.jst.go.jp/article/fms/60/1/60_2014-1/_pdf
- Clinical Oncology 28 (2016) pp. 240

Accident Reports

105 KW	Investigation of the KW reactor incident	http://www.osti.gov/scitech/servlets/purl/10124432/
Chapelcross	Interim report of the board of inquiry set up to investigate the incident in No. 2 Reactor at Chapelcross on 11 May, 1967	UK national archives, Kew
KS 150	Jaslovské Bohunie KS 150	Personal correspondence Rudolf Burcl (former plant operator)
EBR-1	Analysis of the EBR-1 core meltdown	https://www.osti.gov/servlets/purl/4305038
Chernobyl 4	Safety series No.75-INSAG-1 Summary Report on the post-accident review meeting on the Chernobyl accident	No longer available from IAEA, but the UC Berkeley library has a copy.
Chernobyl 4	The Chernobyl Accident: Updating of INSAG-1	http://www-pub.iaea.org/MTCD/publications/PDF/Pub913e_web.pdf
Fermi-1	Report on the fuel melting incident in the Enrico Fermi Atomic Power Plant on October 5, 1966	http://www.osti.gov/scitech/servlets/purl/4766757/
HTRE-3	Summary report of the HTRE No. 3 nuclear excursion	https://www.osti.gov/servlets/purl/4643464
Lucens	Accident at the Experimental Nuclear Power Station in Lucens	Nuclear Safety volume 22:1 Available at Northern Regional Library Facility in Richmond

Accident Reports

NRX	The accident to the NRX reactor on December 12, 1952	http://www.osti.gov/scitech/servlets/purl/4379334
NRX	The accident to the NRX reactor on December 12, 1952 (Part II)	http://www.nuclearfaq.ca/NRX_Accident_%20partII-AECL-233.pdf
St. Laurent 1	Fuel Meltdown at St. Laurent 1	https://babel.hathitrust.org/cgi/pt?id=umn.31951d03526370t;view=1up;seq=45
St. Laurent 2	Les accidents de 1969 et 1980 à la centrale de Saint-Lucens-des-Eaux	https://www.irsn.fr/FR/connaissances/Environnement/expertises-incidents-accidents/rejets-plutonium-accident-Saint-Laurent/Pages/1-accident-Saint-Laurent-des-Eaux-1969-1980.aspx#.W3DGPS2ZPUJ
SL-1	IDO-19302 IDO report on the nuclear incident at the SL-1 Reactor on January 3, 1961 at the National Reactor Testing Station	http://www.id.doe.gov/foia/PDF/IDO-19302.pdf
SL-1	IDO-19300, SL-1 Reactor Accident on January 3, 1961, Interim Report	http://www.id.doe.gov/foia/PDF/IDO-19300a.pdf, retrieved 20141106
SL-1	IDO-10311 Final report of SL-1 recovery operations	http://www.id.doe.gov/foia/PDF/IDO-19300a.pdf
SRE	NAA-SR-5898 Analysis of SRE power excursion of July 13, 1959	http://www.etec.energy.gov/Library/Main/Doc._No._34_Analysis_of_SRE_Power_Excursion_of_7-13-59_NAA-SR-5898.pdf

Accident Reports

TMI-2	Report of the President's commission on the accident at Three Mile Island – The need for change: The Legacy of TMI	https://catalog.hathitrust.org/Record/007418765
TMI-2	Staff reports to the President's commission on the accident at Three Mile Island, Report of the technical task force (four volumes)	https://catalog.hathitrust.org/Record/011328952
Windscale-1	Report on the accident at Windscale No. 1 Pile on 10th October 1957	Available as an appendix in the book, "Windscale 1957, Anatomy of a Nuclear Accident", Lorna Arnold
Windscale-1	A revised transcript of the proceedings of the board of enquiry into the fire at Windscale Pile No. 1, October, 1957	https://www.hep.phy.cam.ac.uk/~lester/teaching/LiteratureReviews/Windscale/05_10_07_ukaea.pdf
WTR	Report on WTR fuel element failure April 3, 1960	http://pbadupws.nrc.gov/docs/ML0217/ML021780374.pdf
WTR	Personal impressions of WTR incident investigation	http://pbadupws.nrc.gov/docs/ML0217/ML021780235.pdf

Note: the complete set of references and bibliographic documents is 506 documents. The full set can be found in the IAEA summaries, or by contacting me.

The following slides are unused.

Consider the TMI-2 accident for example

Unrecognized Hazard	Instrument & Control	Operator training	Operating procedures	Maintenance
Hazards of high point LOCA Operation with a leaky PORV caused operators to ignore high PORV tail pipe temperature	No automatic polisher bypass Indirect indication of PORV position No RPV level measurement Core temp display too narrow Operators can't see secondary parameters important to the event	Thermodynamic principles poorly covered Encouragement to avoid solid pressurizer Training didn't cover SBLOCA	Inadequate LOCA and Pressurizer procedures	Poor maintenance of a condensate polisher blocked a polisher

Severe accidents almost always involved of instrument and control safety systems

Means that brought plant to a controlled state	Number of Instances
Operators initiated reactor trip or shutdown	8
Automatic reactor trip	5
Operators restored core cooling	4
Core disassembly	5
Operators removed fuel from core and added water	1

Number of instances > 19 because sometimes multiple causes were possible
Three events involved diverse shutdown functions
In one of these three CCF of the diverse function caused the trip

The Sodium Reactor Experiment for example

Unknown
RCP coolant mixed with reactor coolant could produce sodium/hydrocarbon solids

Known but Unrecognized
RCP coolant had leaked into reactor vessel
and
Reactor trip system subject to spurious SCRAMs

→

Trigger

↓

Normal Operation
Solids block fuel channels

Operators ignore multiple reactor rate trips

→

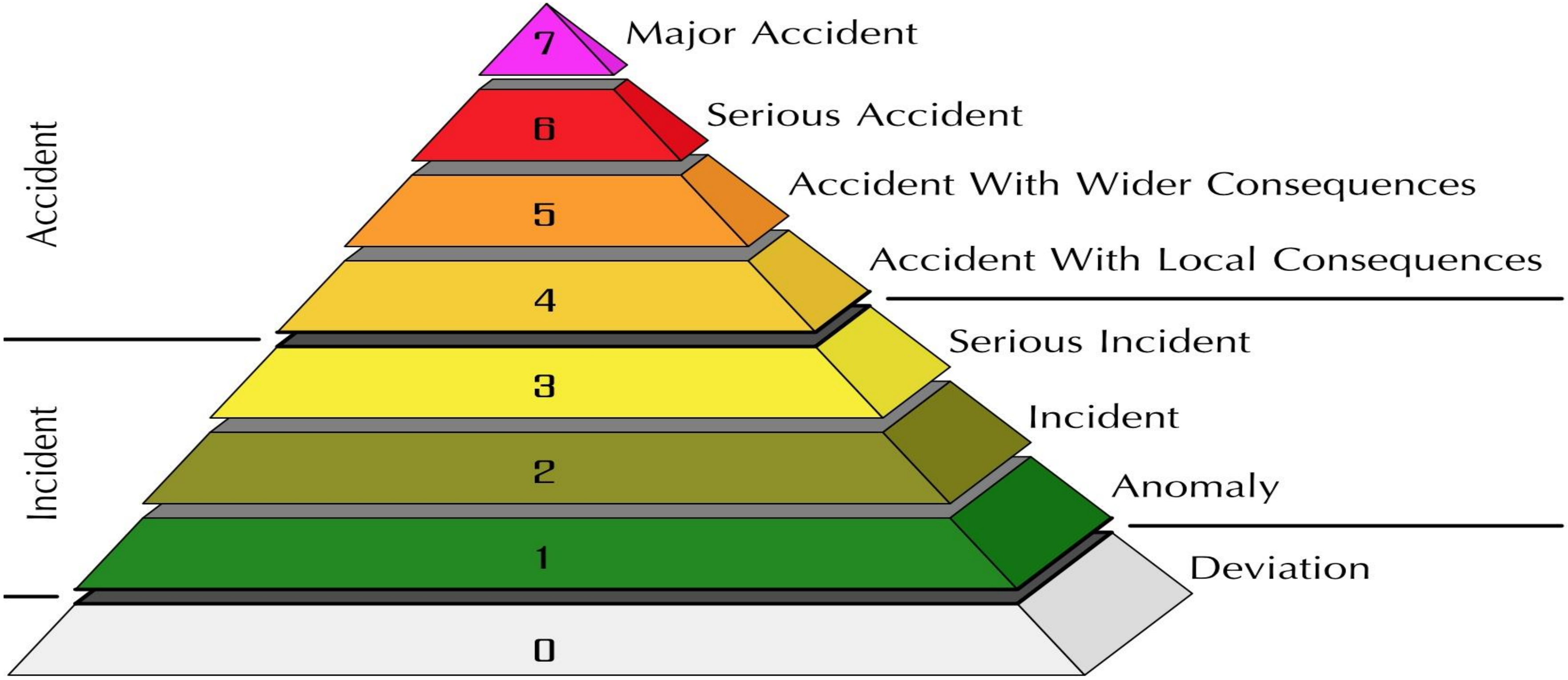
Conquences

30% of fuel damaged

Insignificant radiological release

In 1964 a number of experimental fuel assembles were loaded into the core During loading graphite holding one experimental assembly fractured partially blocking the fuel chanel

International Nuclear Event Scale



See http://www-ns.iaea.org/tech-areas/emergency/ines.asp

Image source: Silver Spoon

Depression was common

- Many thousands at Chernobyl were “caught in a downward spiral of isolation, poor health, and poverty.”
- Depression and post traumatic stress were common among the affected, and even some of the unaffected, in both areas.