Aurora Maximum Credible Accident: Review and Discussion

August 4, 2020

Online public meeting

In summary

- Oklo utilized the NUREG 0800 event categories that LWRs do, *and* a range of other non-LWR events and heat pipe specific events. Oklo surveyed all external event hazard space
- Ultimately the Oklo Aurora plant is analyzed and safe against events that no existing (and safe) plant could withstand today, including a complete loss of everything outside the module (building, heat sink, power, etc), as well as simultaneous failure of a shutdown system
- In audit, this is a plant for which Oklo even showed NRC what a fully unprotected loss of heat sink would look like, although that is far from credible or reasonable for a regulatory standard of safety.
- This is a 1 MW plant with decay heat within 24 hrs on the order of a riding lawnmower. It produces less heat than the MIT research reactor. It has less material than one fuel assembly at an existing plant surrounded by much more material.

A novel application:

Framing the unique “safety case” for a non-LWR

The challenge

Decades of regulatory guidance predicated on old technology and large light water reactors

Costs and requirements have increased over decades and would disproportionately make advanced and very small plants a “non-starter”

Lack of thousands of reactor-years of data for advanced fission like what light water reactors have means that probabilistic risk analysis has some challenges compared with LWR experience (even with decades of operating advanced fission experience)

Safety case

- The maximum credible accident of the Aurora is mitigated by the inherent features of the design:
  - Small size, low power output, and low power density
  - Low fuel burnup, small inventory of fuel, and limited possibilities for dose
  - Low decay heat term, removed by inherent and passive means
  - Inherent reactivity feedbacks ensure reactor power is controlled during overpower or overtemperature events
  - High thermal conductivity materials reduce temperature hot spots, and large thermal mass provides capacity for heat dissipation
  - Ambient pressure system limits driving forces for release
  - Many boundaries to release

Maximum credible accident

- History of conceptual use by the U.S. NRC for ~70 years
- The worst credible accident(s) caused by any single event or failure
- Oklo performed broad review and analysis of events as categorized in NUREG 0800, historical non-LWR event methodology, and events particular to the Aurora
- Systematic and holistic review and focus on deterministic analysis removes uncertainties introduced through reliance on risk analysis for a FOAK reactor, and insights from risk were still utilized per regulations and for defense-in-depth.
- Further precedent for safety case and EPZ/site boundary for reactors of this size regulated by the NRC is shown through existing non-power reactors

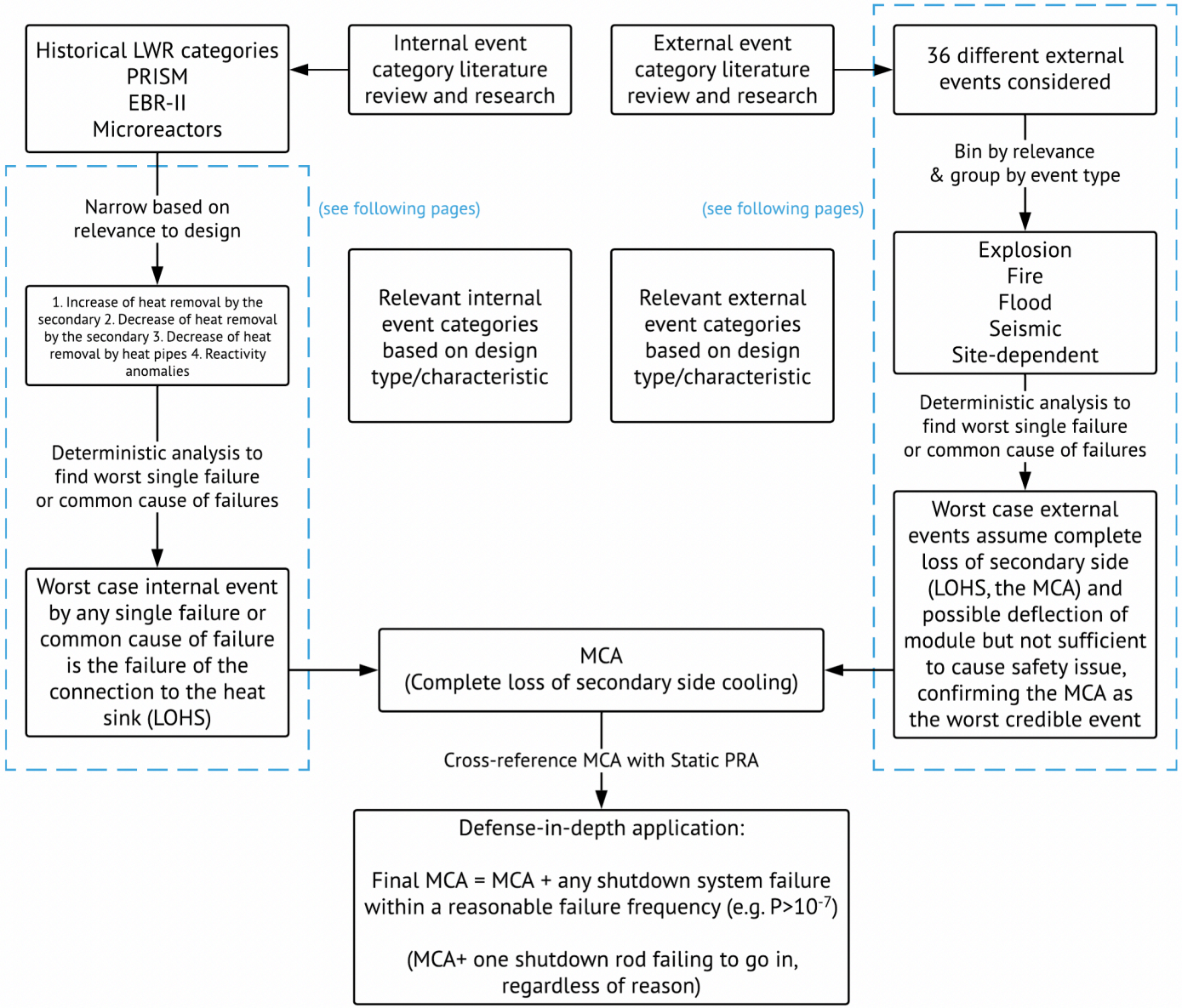
Role of risk insights

- Not “What can go wrong,” ”How likely is it,” and then “What are the consequences…”
  - Challenges of determining ”how likely is it”
- But “What can go wrong?” then “What are the consequences?”
  - And then applying any risk insight on top of what can go wrong, as defense in depth.
  - Oklo provided PRA insights in the application per NRC regulatory requirements

Safety analysis approach:

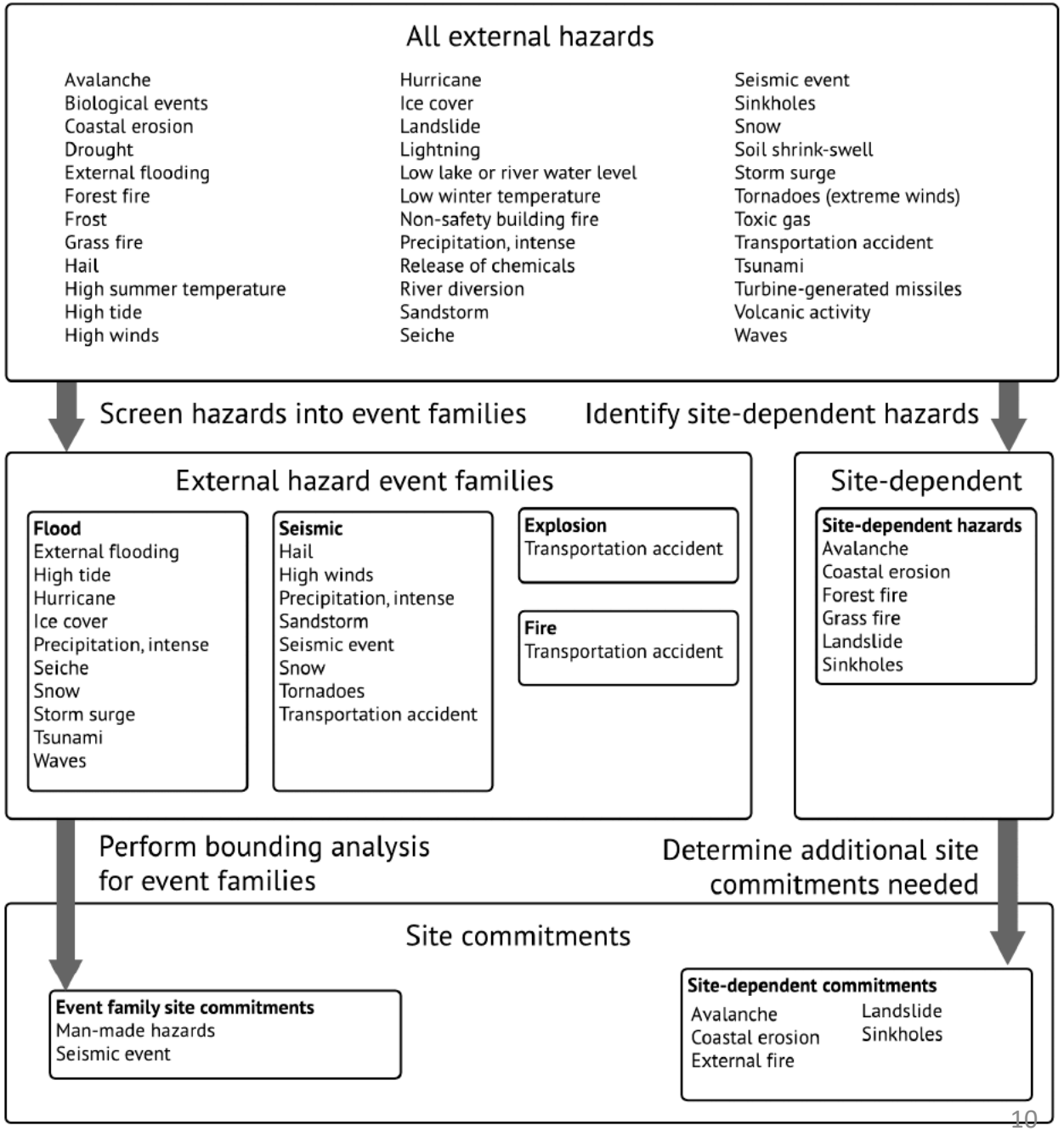
A complete look at an extensive safety analysis

Details on Internal and External event selection/analysis process



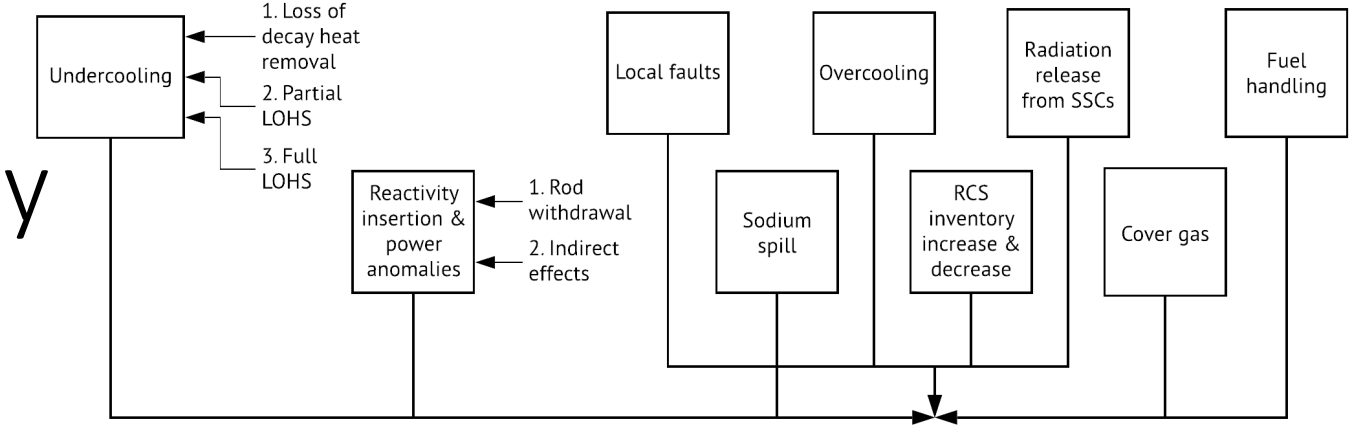
External hazards methodology

- Described in Chapter 1 of the FSAR.
- Set risk-informed metrics, specifically that PRA would be used if the deterministic analysis of the event families resulted in consequences above 1 rem whole-body dose over 4 days as given in the EPA's PAGs manual (2017 edition).
- The 4 external hazard families did not result in any dose
  - This analysis already considered the MCA (i.e., no secondary system heat removal available)
  - Because the set dose metric was not exceeded, PRA was not utilized at all in the external hazards evaluation.
- All external hazards analysis was performed on the Aurora design deterministically.



Maximum credible accident methodology overview

- Chapter 5 of the FSAR describes the initiating event selection process, which was one of the first steps in the determination of the maximum credible accident for the Aurora design.
- **This process was essentially deterministic.**
  - Although the word “credible” is used, it is used in the context of the MCA analysis, not risk analysis.
  - **This approach avoided challenges associated with a risk-informed approach.**
- The initiating event process started by a review of events analyzed by past reactors, specifically focusing on metal-fueled fast reactors and the experience of large light water reactors.



Reviewed LWR events for the Aurora (partial list):

- Operation with a fuel assembly in improper position
- Inadvertent blowdown of RCS
- Loss of feedwater heating
- Trip of any/all recirculation pumps
- Inadvertent pump start in hot recirculation loop
- Condenser tube leak
- Startup of an idle recirculation pump in a cold loop
- Reactor overpressure with delayed scram
- Major rupture of a pipe containing reactor coolant (inc. double ended rupture of the largest pipe)
- Ejection of a control rod assembly
- Control rod drop (BWR)
- Major secondary side rupture (inc. double ended rupture)
- Single RCP locked rotor
- Seizure of one recirculation pump
- Inadvertent control rod/rod group w/d
- Loss/interruption of core flow
- Inadvertent moderator cooldown
- Inadvertent chemical shim dilution
- Depress. By spurious operation of an active element (relief valve)
- Blowdown of reactor coolant through safety valve
- Loss of normal feedwater
- Loss of condenser cooling
- SG tube leaks
- Rx.-turbine load mismatch (inc. loss of load and turbine trip)
- Control rod drop (inadvertent addition of absorber) (PWR)
- Single error of an operator
- Single failure of a control component
- Single failure in the electrical system
- Minor RCS leak/loss of reactor coolant (from small ruptured pipe or crack)
- Minor secondary system break
- LOOP

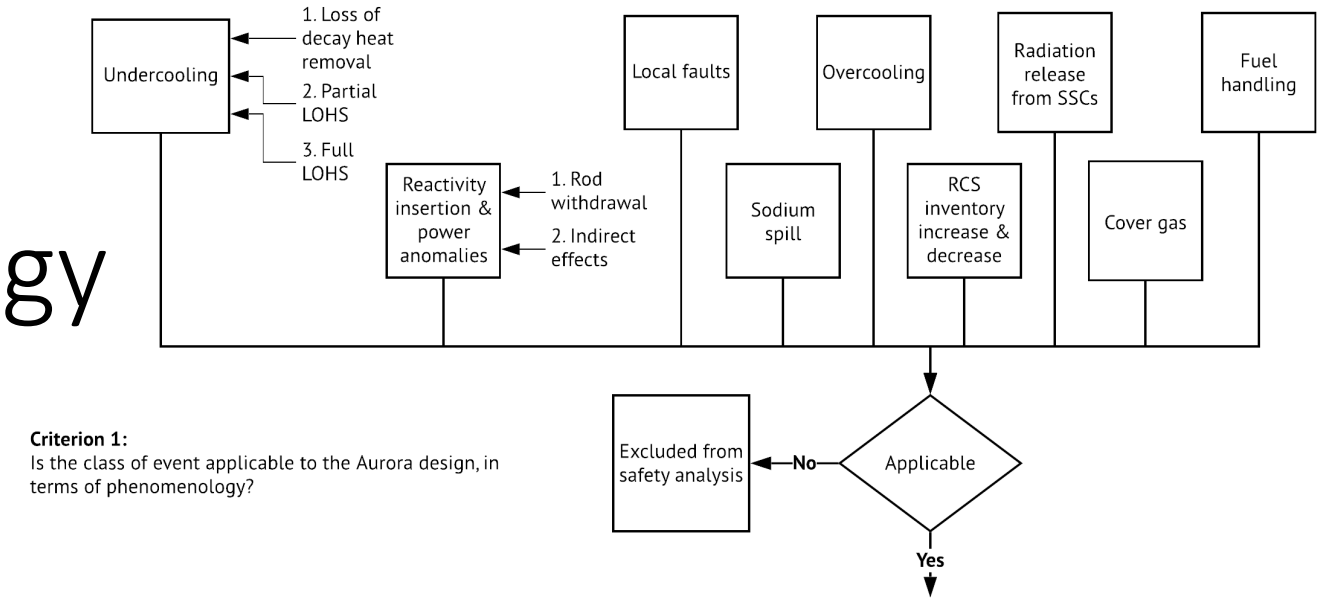
Heat pipe reactors considered:

- SAFE-100
- SAFE-100a
- SAFE-30
- SAIRS
- HP-STMCs
- SNAP-50
- SNAP-2
- SNAP-8
- SNAP-10A
- SP-100
- HP-ENHS
- ENHS
- HOMER
- Martian Surface Reactor
- HPS/HBS

Heat pipe reactor events for the Aurora (partial list):

- Cascading failure
- Delta pattern failure
- 3 adjacent HP failure
- 2 adjacent HP failure
- >3 adjacent HP failure
- 1 HP failure - juvenile
- 1 HP failure - performance based
- 1 HP failure - age related
- Exceeding sonic limit
- Exceeding capillary limit
- Exceeding entrainment limit
- Exceeding boiling limit
- Exceeding the superheating limit of the working fluid (Startup)
- Exceeding the heat rejection limit in the condenser section of the HP
- Insufficient return of the working fluid to the evaporator (startup)
- Inadvertent water/sand/etc. flooding
- Dry out/De priming of the condenser region (startup)
- Condensation zone collapse (startup)

Maximum credible accident methodology



Criterion 1 – Screen out events from an exhaustive, large initial set

→ Events that are not applicable to the Aurora design because no equivalent event can occur.

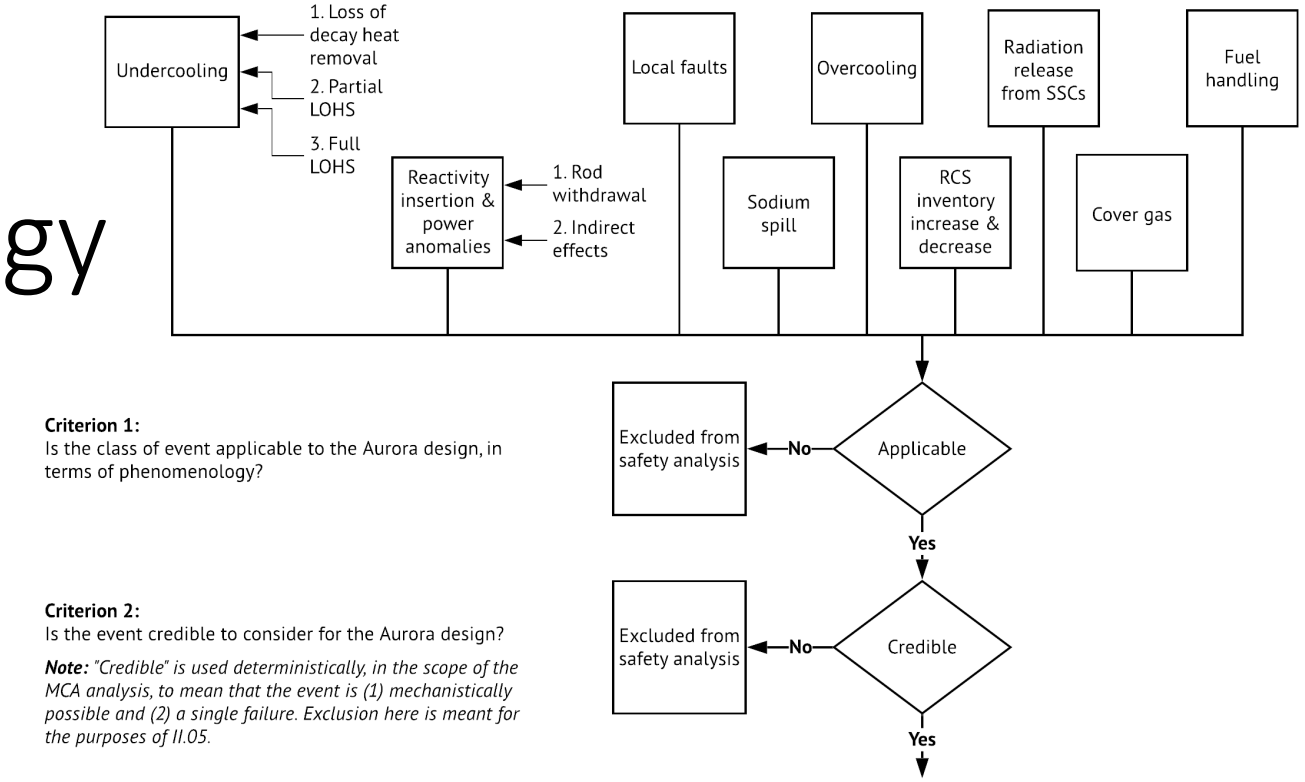
→ Example (SFR): Fire from a backup sodium tank.

Maximum credible accident methodology

Criterion 2 – Screen out events that are not credible in the Aurora design, as defined by the MCA methodology

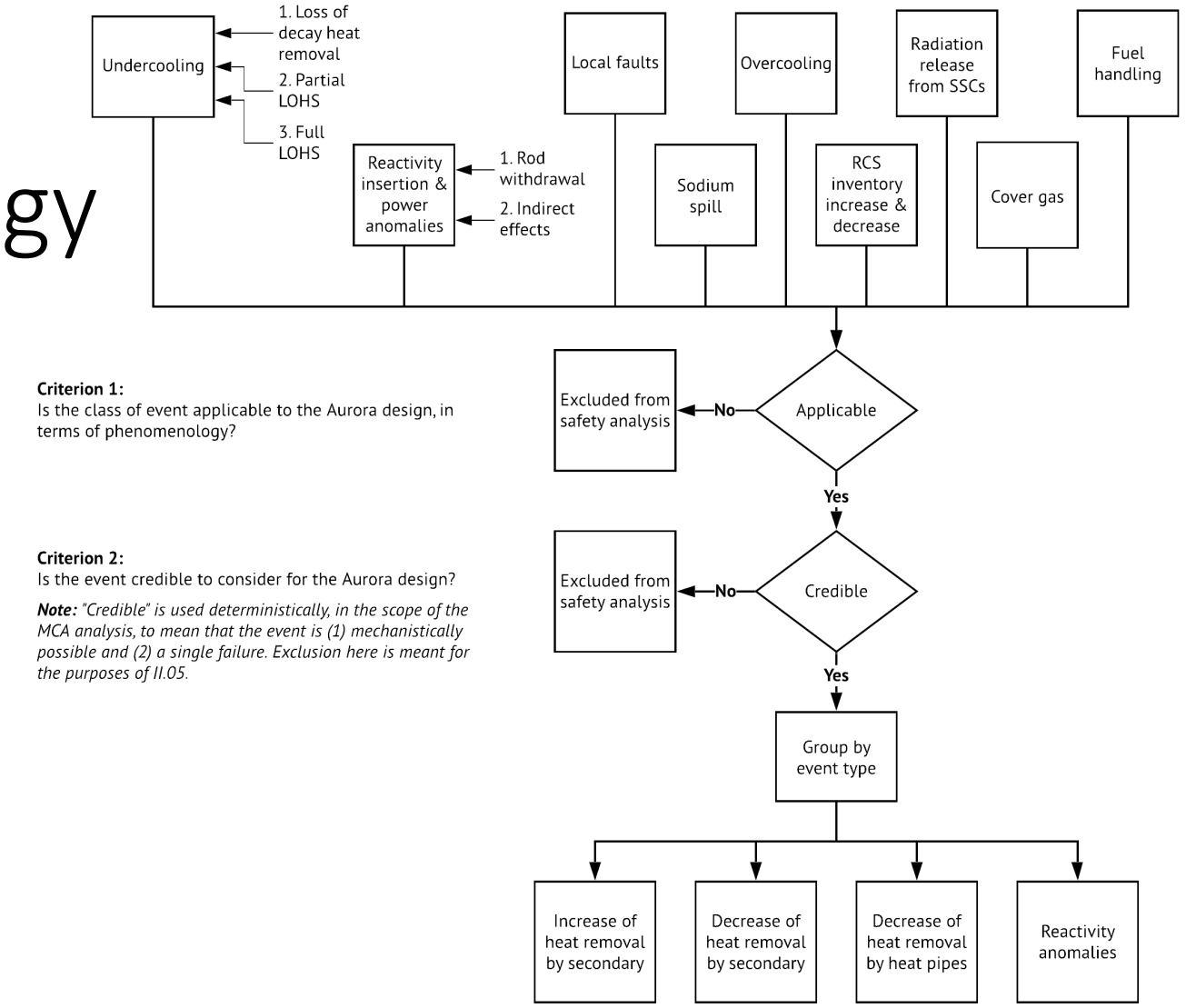
→Must be mechanistically possible

→Must assume a single failure



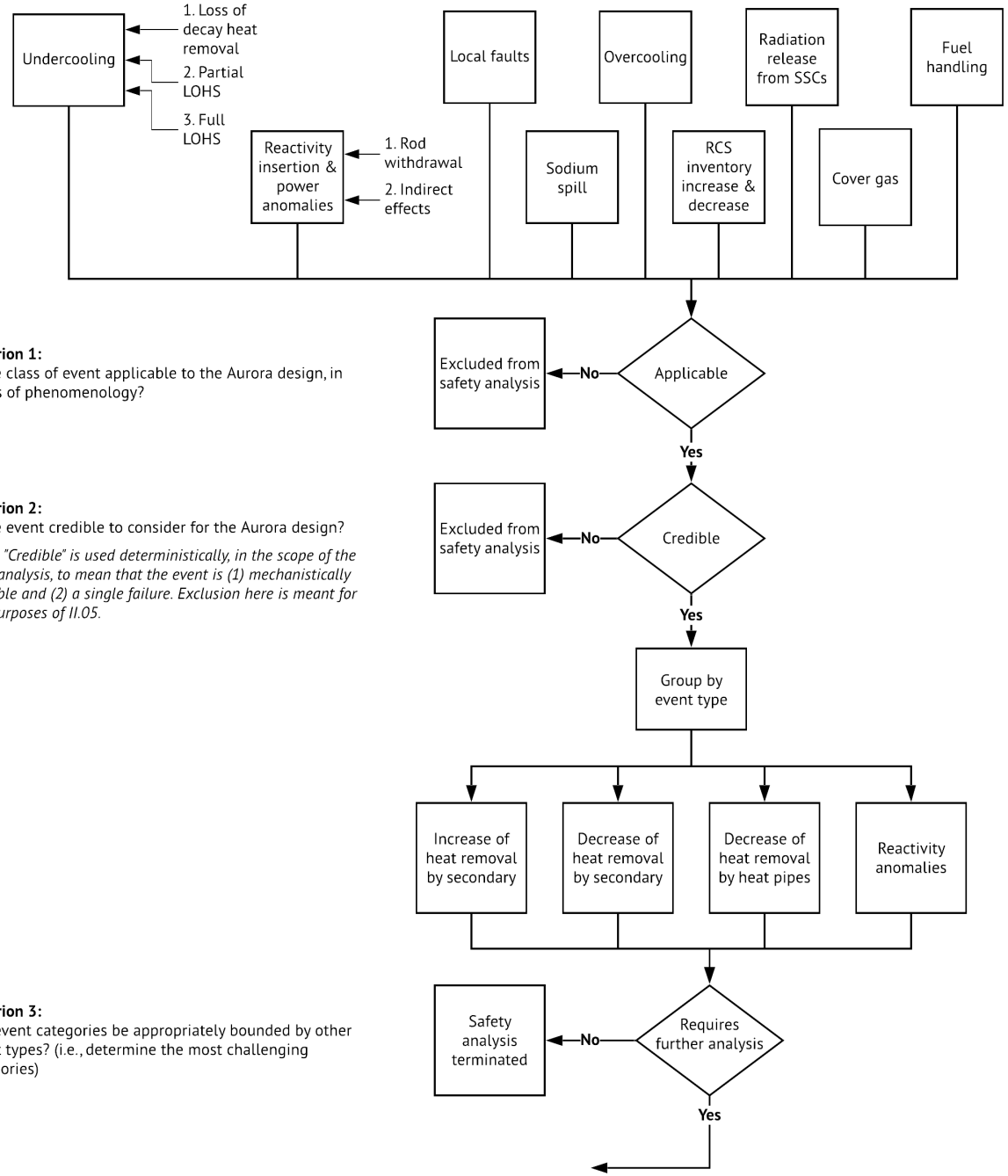
Maximum credible accident methodology

Group events by event category – based on common phenomena



Maximum credible accident methodology

Criterion 3 – Determine if event categories can be bounded or need further analysis



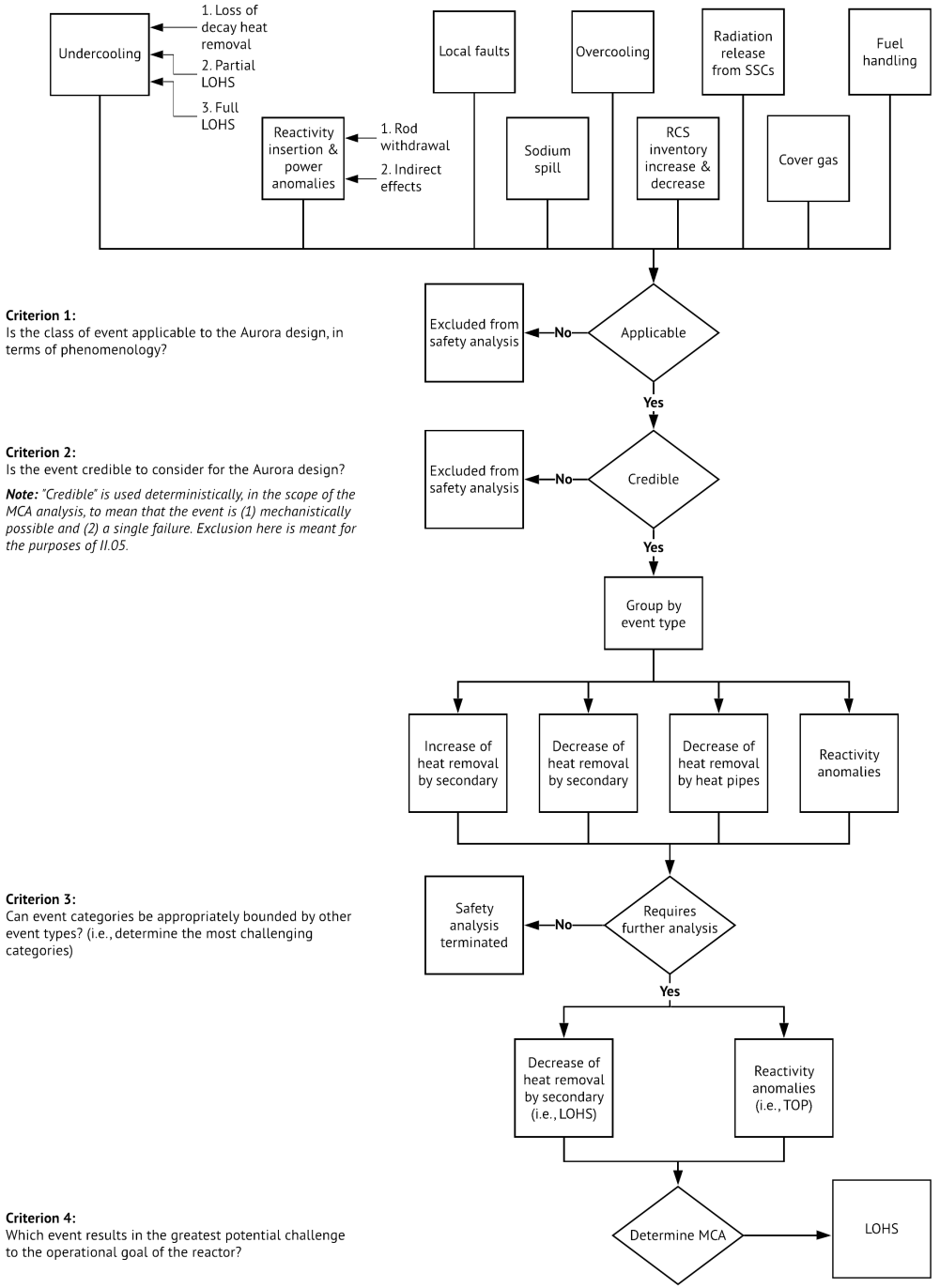
Maximum credible accident methodology

Criterion 4 – Determine the maximum credible accident from event categories

→From the 4 categories of events, only 2 categories were found to require additional analysis

→Specifically, increase of heat removal by secondary (i.e., overcooling) and decrease of heat removal by heat pipes were not found challenging to the reactor, even in extreme cases

→The remaining 2 categories were further analyzed to determine which category challenged the reactor the most



Determining the maximum credible accident

- The “decrease of heat removal by secondary" category (i.e., LOHS) was analyzed through a sensitivity analysis.
  - The sensitivity analysis concluded that a full LOHS is more challenging than a partial LOHS, as the relationship between the degradation in heat removal and increase in fuel temperature is direct.
  - For the Aurora, the degradation of heat removal is directly correlated to the increase in fuel temperature.
    - The challenging effects commonly seen in LWRs for partial loss of cooling are not relevant in the Aurora design.
- The reactivity anomalies category (i.e., TOP) was also analyzed through a sensitivity analysis to the most extreme state allowed physically (mechanically) by the system.
  - The sensitivity analysis concluded that the system response is largely insensitive to the speed of the event because of the rapid overtemperature detection. Consequently, the transient analysis (II.05) assumed the maximum speed of drum insertion maximum for the TOP.
- The results of the TOP and LOHS events are described in Chapter 5 of the FSAR.
- Each of these events assumes a single equipment failure that would result in the most challenged state (as per the MCA philosophy) **and** a failure of one of three shutdown rods to insert (to capture defense-in- depth principles).
- During the LOHS event, peak fuel temperatures are higher than during the transient overpower.
  - This is due to the failure of the PCS, as well as failure of bypass and decay heat removal via the radiators.
  - This leads to a reliance on passive cooling to the air outside of the shell, in comparison to active cooling occurring via the PCS during the TOP.
  - Further, temperatures that exceed steady-state temperatures are experienced for over 17 hours during the LOHS, while temperatures return to steady-state values within minutes during the TOP.
- **Therefore, the loss of heat sink event is considered the more challenging event and is designated as the MCA. The Aurora reactor undergoes this extreme transient without experiencing fuel damage.**
- **This is historic safety analysis, as no other reactor has been licensed by the NRC with such extensive and extreme event analysis.**

Conclusion

- Oklo utilized the NUREG 0800 event categories that LWRs do, *and* a range of other non-LWR events and heat pipe specific events. Oklo surveyed all external event hazard space
- Oklo structured its application based directly off existing regulations for requirements for an application
- Ultimately the Oklo Aurora plant is analyzed and safe against events that no existing (and safe) plant could withstand today, including a complete loss of everything outside the module (building, heat sink, power, etc), as well as simultaneous failure of a shutdown system
- We are proud to be working on a plant that has safety and environmental characteristics and benefits never seen before, and appreciate NRC work to ensure these plants with novel characteristics can be effectively licensed

Background slides

10 CFR 50.77 – (i.e., 10 CFR 50.33)

Section	Short description	Location in COLA
50.33(a)	**Name**	**I.01**
50.33(b)	**Address**	**I.01**
50.33(c)	**Description of business**	**I.01**
50.33(d)	**Business details**	**I.01**
50.33(e)	**Class of license**	**I.02**
50.33(f)	**Financial qualification**	**I.03**
50.33(g)	**Emergency planning governments**	**I.04**
50.33(h)	Construction or alteration	V.03
50.33(i)	Generation and distribution of electric energy	V.03
50.33(j)	Restricted Data or defense information	V.03
50.33(k)	**Decommissioning**	**I.05**

10 CFR 52.79 (part 1/4)

Section	Short description	Location in COLA
52.79(a)(1)	**Site envelope and boundary**	**II.01**
52.79(a)(2)	**Design and analysis of structures, systems, and components**	**II.02**
52.79(a)(3)	**Radioactive materials produced in operation**	**II.03**
52.79(a)(4)	**Principal design criteria**	**II.04**
52.79(a)(5)	**Transient analysis**	**II.05**
52.79(a)(6)	**Fire protection**	**II.06**
52.79(a)(7)	Pressurized thermal shock	V.03
52.79(a)(8)	Combustible gas control	V.03
52.79(a)(9)	Station blackout	V.03
52.79(a)(10)	Environmental qualification of electric equipment	V.03
52.79(a)(11)	Codes and standards	V.03
52.79(a)(12)	Primary containment leakage rate testing program	V.03

10 CFR 52.79 (part 2/4)

Section	Short description	Location in COLA
52.79(a)(13)	Reactor vessel material surveillance program	V.03
52.79(a)(14)	**Operator training program**	**V.04**
52.79(a)(15)	Maintenance rule	V.03
52.79(a)(16)	Effluent monitoring and sampling	V.03
52.79(a)(17)	Three Mile Island requirements	V.03
52.79(a)(18)	Risk-informed treatment of SSCs	V.03
52.79(a)(19)	**Earthquake criteria**	**II.07**
52.79(a)(20)	**Unresolved and generic safety issues**	**II.08**
52.79(a)(21)	**Emergency planning**	**II.09**
52.79(a)(22)	**Emergency planning with state and local governments**	**II.17**
52.79(a)(23)	Reserved	V.03
52.79(a)(24)	**Prototype operational conditions**	**II.11**

10 CFR 52.79 (part 3/4)

Section	Short description	Location in COLA
52.79(a)(25)	**Quality Assurance Program - design**	**II.12**
52.79(a)(26)	**Organizational structure for operations**	**II.13**
52.79(a)(27)	**Quality Assurance Program - operation**	**II.12**
52.79(a)(28)	**Preoperational testing and initial operations**	**II.14**
52.79(a)(29)	**Operational plans**	**II.15**
52.79(a)(30)	Technical Specification	IV
52.79(a)(31)	Multi-unit sites	V.03
52.79(a)(32)	Technical qualifications of the applicant	II.16
52.79(a)(33)	Training Program description	II.17
52.79(a)(34)	Operator requalification	V.04
52.79(a)(35)	**Physical security plans**	**II.18**
52.79(a)(36)	**Safeguards and other security plans**	**II.18**

10 CFR 52.79 (part 4/4)

Section	Short description	Location in COLA
52.79(a)(37)	**Incorporation of operational insights**	**II.19**
52.79(a)(38)	Severe accidents	V.03
52.79(a)(39)	**Radiation Protection Program description**	**II.20**
52.79(a)(40)	**Fire Protection Program description**	**II.21**
52.79(a)(41)	Standard Review Plan evaluation	V.03
52.79(a)(42)	Anticipated transients without scram	V.03
52.79(a)(43)	**Criticality accidents**	**II.22**
52.79(a)(44)	**Fitness-for-Duty Program description**	**II.23**
52.79(a)(45)	**Minimization of contamination**	**II.20**
52.79(a)(46)	**Probabilistic risk assessment summary**	**II.24**
52.79(a)(47)	Aircraft impact assessment	V.03

10 CFR 52.80

Section	Short description	Location in COLA
52.80(a)	**Inspections, tests, analyses, and acceptance criteria**	**VI**
52.80(b)	**Environmental report**	**III**
52.80(c)	Limited work authorization	V.03
52.80(d)	Mitigation of beyond design basis events	V.03

Organization of the Environmental Report

Chapter	Chapter title	Requirement
1	Purpose	None
2	Description of the Aurora site	
	Site description	10 CFR 51.45(b)
		10 CFR 51.45(c)
	Site preparation	10 CFR 51.45(b)
		10 CFR 51.45(c)
	Operational activities	10 CFR 51.45(b)
		10 CFR 51.45(c)
	Status of compliance	10 CFR 51.45(d)
3	Projected impacts	10 CFR 51.45(b)(1)
		10 CFR 51.45(b)(2)
		10 CFR 51.45(b)(4)
		10 CFR 51.45(c)
4	Environmental impacts of alternatives	10 CFR 51.45(b)(3)
		10 CFR 51.45(c)
5	Summary of impacts	
	Irreversible and irretrievable commitments of resources	10 CFR 51.45(b)(5)
	Benefits and cost	10 CFR 51.45(c)
Appendix A	Environmental commitment set	None