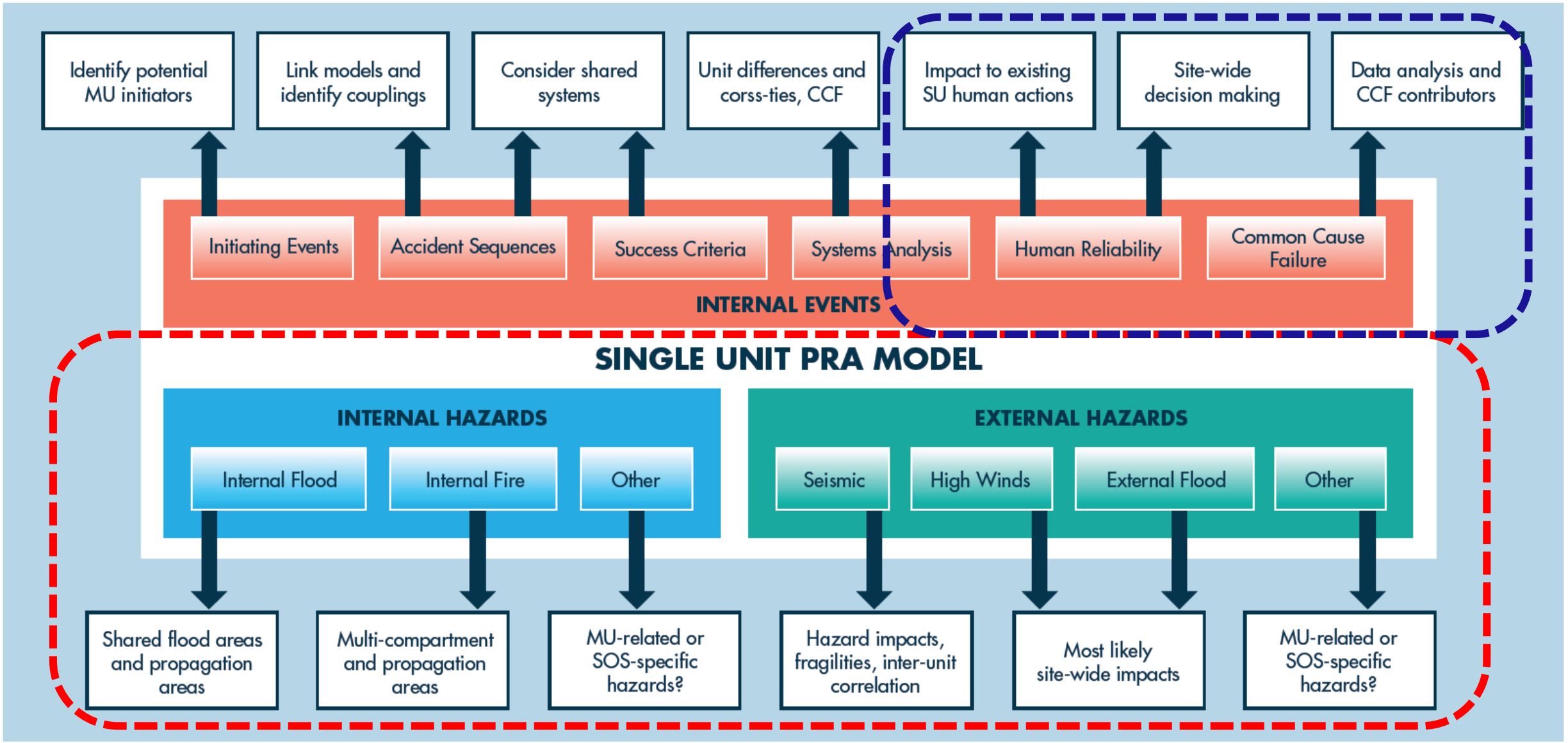
Multi-Unit Risk Assessment Framework Overview

Considerations on CCF and HRA

Andrea Maioli
Consulting Engineer | Westinghouse Electric Company

IAEA Workshop on Multi-unit Probabilistic Safety Assessment (MUPSA)
February 10-14, 2025

Presentation Focus



CCF

See also the ANS PSA 2023 paper
"Common Cause Failures – The Good, the Bad and the Ugly"
Kenneth Kiper, Mark Wishart, Fernando Ferrante, Matthew Degonish

Overview of the Task

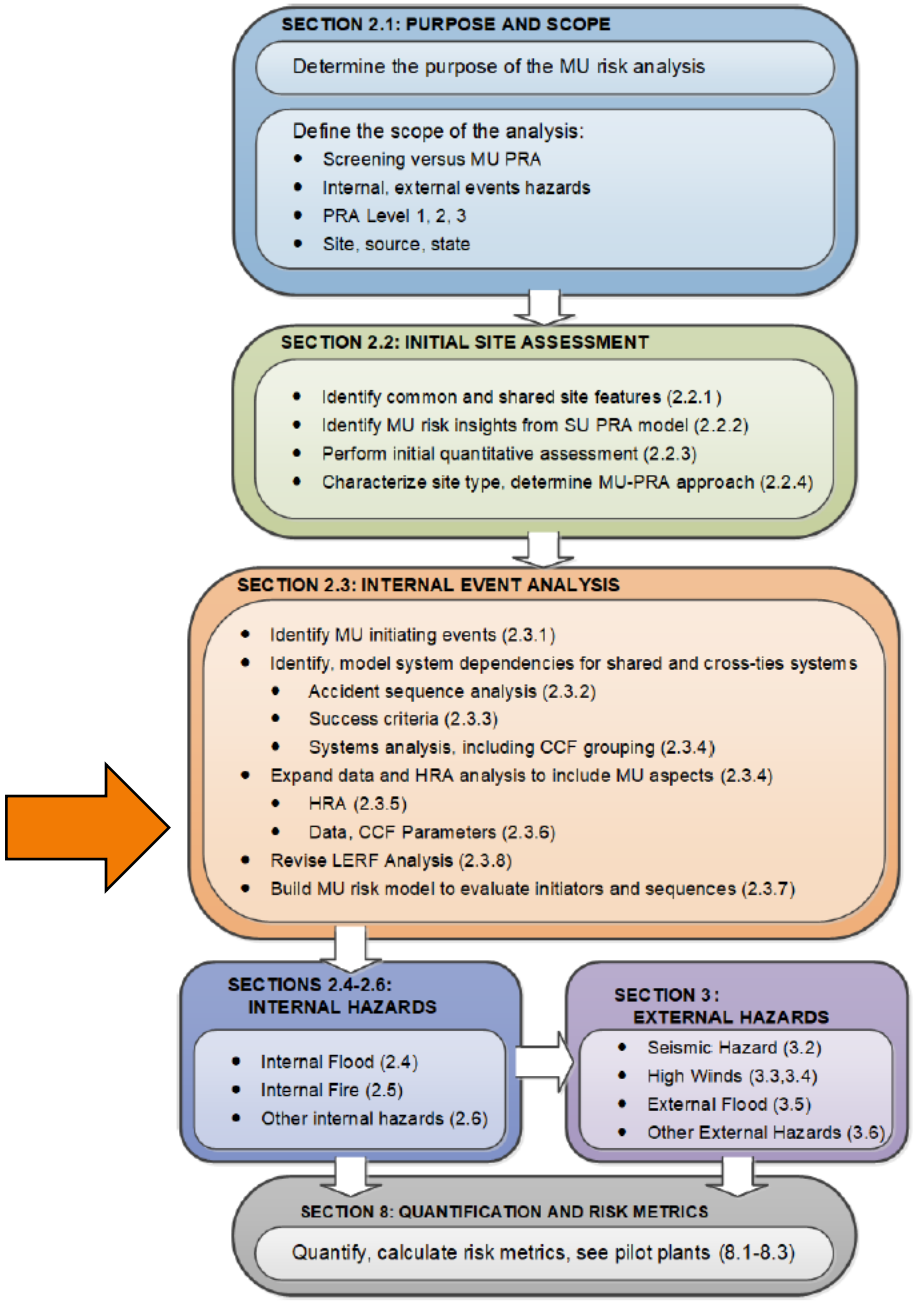
- CCF Modeling is part of the systems analysis process.

- CCF Data considerations are as follows:
  - The screening criteria to be used.
  - The limitations of using CCF data.
  - Issues to be considered when CCF data is applied to multi-unit risk models.

Common Cause Failure (CCF)

- CCF data and modeling are part of the general multi-unit risk analysis framework:
  - The current framework is limited to internal events for dual-unit sites, with both units initially at power.
  - The general process for multi-unit CCF data & modeling should be applicable to a broader scope.
  - See EPRI Technical Report 3002020764 for additional information related to common cause failures.

- Two Key Steps to address CCF:
  - For CCF **modeling**, systems analysis is used to determine the appropriate component common cause groups (CCCGs) to include in systems fault tree models.
  - For CCF **data**, data analysis is used to determine appropriate CCF parameters for the CCCGs.



Systems Analysis for Multi-Unit CCF

Single-unit systems analyses should be appropriate for multi-unit applications, with the following exceptions:

ASME/ANS PRA Standard, SY-01

Identify differences in system design and operation between units. Determine whether the differences require additional modeling.

ASME/ANS PRA Standard, SY-02

Identify all cross-unit dependencies in shared or cross-tied systems and account for cross-unit dependencies in systems analyses (applicable to sites with shared or cross-tied systems).

ASME/ANS PRA Standard, SY-03

Identify potential multi-unit CCF groups for components in shared systems and in identical systems across units:

- Start with CCCGs in existing single-unit models.
- Verify (if applicable) that CCCGs in shared systems include components from both units.
- Consider new multi-unit CCF groups that may not be applicable to single-unit models.
- Provide a clear basis for screening out some CCCGs from the multi-unit CCF analysis.

See the next slide for additional detail

Process for Multi-Unit CCF Modeling

Identify potential MU CCF groups for components in shared systems and in identical systems across units.

Single-Unit CCCGs

- The multi-unit framework assumes that a single-unit model has the necessary depth and detail of CCF modeling as a starting point for MU modeling.

New Multi-Unit CCF Modeling

- Consider new multi-unit CCF groups that may not be applicable to the single-unit analysis.
- For example, consider components typically modeled in CCCGs that do not have redundancy in a single unit (e.g., turbine-driven auxiliary feedwater pumps).

Review Shared Systems

- Verify (if applicable) that CCCGs in shared systems include components from multiple units.
- Shared systems are expected to be important contributors to multi-unit risk.

Screen Out CCCGs

- Screening process is critical to the success of the multi-unit modeling because of the challenges incurred by including large CCCGs in the analysis.
- Provide a clear basis for screening out any CCCGs from the multi-unit CCF analysis.
- Also consider the CCF data limitations for large CCCGs.

Screening CCCGs in Multi-Unit CCF Models

- Requirement SY-B1 of the ASME/ANS PRA Standard states:

> "Model intra-system common-cause failures when supported by generic or plant-specific data."

- The data source of interest is the NRC/INL CCF Dataset (2020). In the US, plant-specific CCF data is captured in the generic data. Thus, requirements could be stated more generally:

Model common-cause failures when supported by generic data.

- The following screening criterion can be inferred from this requirement:

Screen out common-cause failures when supported by generic data.

Criteria for Scoping of the CCF Data

Active Failures

Model component-types with active failure modes in CCCGs.

This is a broad inclusion criterion (active failure modes) that accounts for most of the recent CCF evidence and addresses components beyond those in the NRC CCF dataset (as of 2020).

Function and Environment

Limit CCCGs to identical components with the same function and in the same environment.

This provides a constraint to the first broad criterion, based on the limited evidence of recent CCF events.

This places the focus of CCF modeling on smaller groups of components with the most in common.

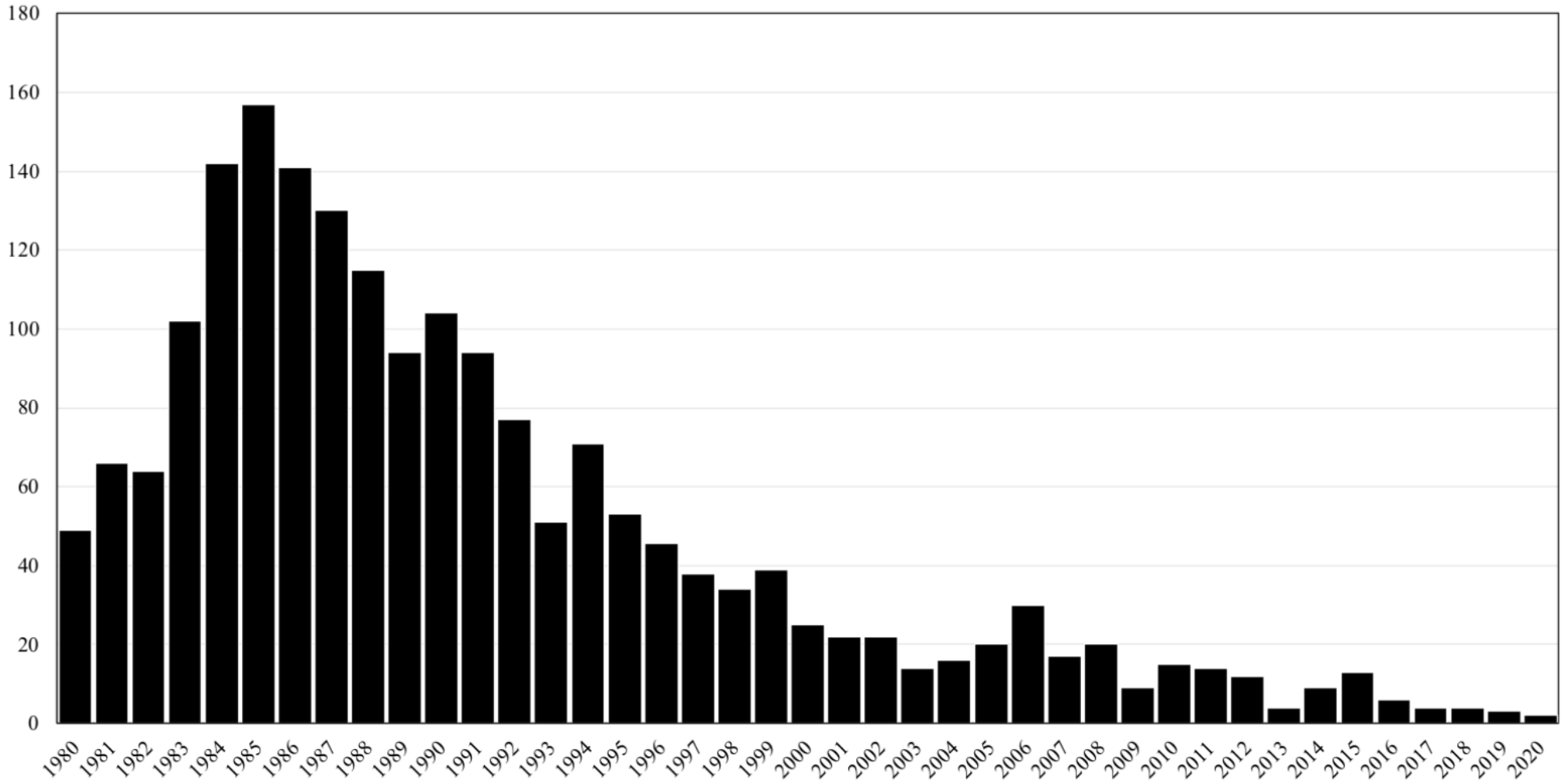
Standby and Passive Failure Modes

Screen out component-types with standby or passive failure modes.

Standby Failure Mode:
The failure of an active component to operate while in standby mode

Passive Failure Mode:
The failure of either an active or passive component due to rupture, leakage, or plugging.

Common Cause Failure Trending – Number of Events



Based on US industry experience

Good News / Bad News…

Good News

Fewer CCF events – The number of CCF events per year for US nuclear power plants has significantly decreased over the last 40 years. A positive sign of increased reliability and performance.

In recent decades, CCF events occurring within the United States nuclear power industry has decreased, from over 1,000 in the 1980s to only 53 in the 2010s.

Bad News

Less data – Fewer events means less data for estimating CCF failure rates. This is especially problematic when estimating the failure of large common cause failure groups (i.e., groups with multiple components).

Failure data related to multi-unit configurations are not tracked consistently.

Evidence for Multi-Unit CCF Events

The NRC/INL NROD database of CCF events includes a field to indicate whether an event is classified as a multi-unit CCF event.

Limitations

Not clear how systematic the identification of multi-unit CCF events is being performed.

For events that impacted only one unit, it is not clear that the same component-types in the other unit(s) were included.

For example, a 2 of 2 EDG CCF event in one unit might be more accurately identified as a 2 of 4 CCF event if the EDGs in the other unit (assuming a 2-unit site) were not failed or degraded.

Conclusions

The most common multi-unit CCF event are plugged circulating water traveling screens.

This results in a full or partial loss of condenser cooling, power reduction or plant trip.

These events would be better modeled as Loss of Condenser Vacuum (LCV) initiating events.

From the lack of multi-unit CCF evidence, common-cause coupling between units seems to be weak.

The Problem with Treatment of Multi-Unit CCF Events

- How a CCF event is classified can dramatically impact the resultant impact vectors. For example:
  - Two-unit site, with 2 EDGs on each unit (4 EDGs total).
  - CCF event: 2 EDGs on Unit 1 fail to start, Unit 2 EDGs are not impacted by this event.
  - Two possible ways to classify this event, in the form of event impact vectors:
    - Single unit event, CCCG-2 (2|2): impact vector [0,1]
    - Dual unit event, CCCG-4 (2|4): impact vector [0,1,0,0]
  - Single unit event can be mapped up (2→4): impact vector [0, 0.25, 0.50, 0.25]
  - Dual unit event can be mapped down (4→2): impact vector [0.67, 0.17]
- Results depend on the event classification:

Evidence	Impact Vector (CCCG-2)	Impact Vector (CCCG-4)
Single unit event (2 of 2)	0.00, 1.00	0.00,1.00, 0.00, 0.00
Dual unit event (2 of 4)	0.67, 0.17	0.00, 0.25, 0.50, 0.25

Multi-Unit CCF Process Steps

1

Risk Significant

Model CCCGs across dual units only if the CCCG is risk significant in the "reduced single-unit model."

Reduced Single-Unit Model:
The single-unit model that parallels the multi-unit model (i.e., limited to only the initiating events included in the multi-unit model.)

2

Active Failures

Limit modeling of component-types to active failure modes in CCCGs.

This is a broad inclusion criterion that accounts for most of the recent CCF evidence and addresses components beyond those in the NRC CCF dataset (as of 2020).

Pooled data (rather than system-specific data) should be considered as a source of CCF parameter values where the system-specific component-types have limited data.

3

Function and Environment

Limit CCCGs to identical components with the same function and in the same environment.

This places the focus of CCF modeling on smaller groups of components with the most in common, as supported by the data.

Conclusions

- Overly-conservative CCF modeling could distort the multi-unit risk results and insights. Realistic modeling approaches are recommended.
- The EPRI methodology limits the number of CCF groups that are expanded in the multi-unit risk analysis.
- Selected CCF groups should be fully modeled using available CCF data.
- Review the multi-unit risk results to:

Identify where even the limited CCCG modeling may be a dominant contributor to multi-unit risk.

Identify where independent failures to be important (i.e., where additional CCCGs should be considered).

Understand limitations and uncertainties in the CCF parameter data when extended to multi-unit.

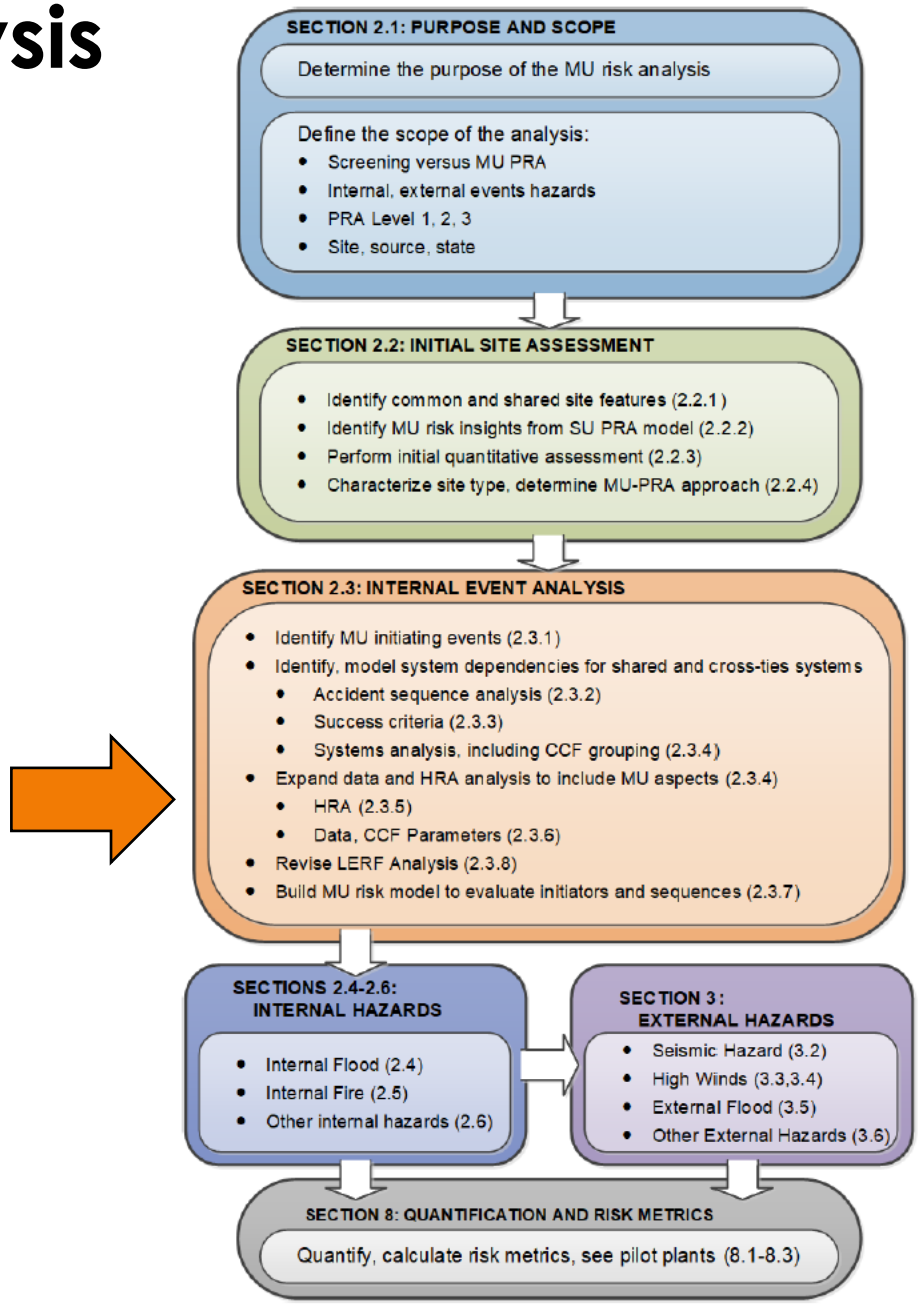
HRA

Overview of the Task

- Multi-unit human reliability analysis (HRA) is part of the general framework for addressing multi-unit risk.
- Multi-unit HRA uses the same general methodology used in single-unit HRA (e.g., the EPRI HRA Calculator tool and methods).
- Multi-unit HRA emphasizes unique aspects of the analysis that are due to multi-unit accidents.

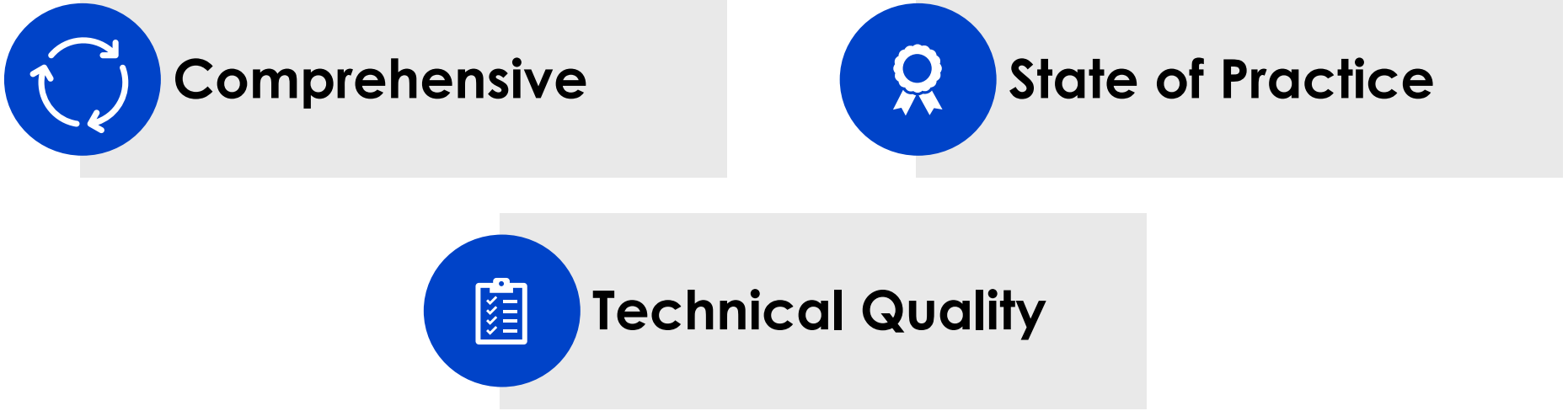
General HRA Screening and Analysis

- Understand the distinct plant contexts created by multi-unit accidents (e.g., unique cross-unit dependencies).
- Review and revise the single-unit HRA to reflect multi-unit specific actions and performance influencing factors.
- Address specific issues of human failure events (HFEs) associated with shared support systems.
- Evaluate HRA dependencies between units, including explicit and implicit dependencies.



Assumptions

- A comprehensive single-unit HRA model and documentation.
- Single-unit analysis developed using HRA methodologies that represent the current state of practice.
- The single-unit HRA meets the requirements in the technical element of the ASME/ANS PRA standard, including requirements related to multi-unit aspects.



Outline of Multi-Unit HRA Framework Tasks

1. Understand the **distinct plant contexts** created by multi-unit accidents, especially the cross-unit dependencies unique to multi-unit accidents.
2. Evaluate **HRA dependencies** between units, including both explicit and implicit dependencies.
3. Address the complexities of **Command & Control** created by multi-unit accidents.
4. Review and revise the single-unit HRA to reflect **multi-unit specific actions** and performance influencing factors.
5. Address the specific issue of operator actions associated with **shared support systems**.

Focus of this presentation

Task 1: Understanding the Context for MU-HRA

Plant contexts are created by a common MU initiator and the units' responses to the initiators.

Explicit Dependencies

Unit response can be linked due to physical attributes stemming from specific site designs that create explicit dependencies, such as:

- Shared or connected systems and structures.
- Similar plant designs that cause similar plant responses to the common initiator (e.g., requiring standby safety systems, sequence timing).
- Shared location – common external hazards.

Implicit Dependencies

Unit responses can be linked due to implicit dependencies due to the increased likelihood of failures of common component types (CCFs) across units.

Context: Accident Sequences and the Impact on HRA

Initiating events and accident sequences generally come from a small set of initiators:

- For example, a loss of off-site power, the loss of a secondary heat sink, and a shared support system).

Site-Level

Initiators that impacts multiple units at (or about) the same time and provide an initial correlating factor between the units.

Example:
LOOP due to loss of grid would typically be a site-level initiator, requiring both units' EDGs to start and load at about the same time.

Cascading

Initiators that involve an event in one unit leading to impacts in other units, which may cause additional trips.

Example:
A cascading event caused by the failure or incorrect alignment of a shared support systems.

Context: Key Site Features and the Impact on HRA

Shared or Connected Structures

Allow a hazardous environment created in one unit to impact the second unit, challenging the feasibility of specific local actions.

Cross-tied Systems

Systems that are normally unit-specific but with off-normal alignment capability to serve other units (e.g., unit-specific diesel generator that can be cross-tied by back-feeding through a main transformer).

Connected Main Control Rooms

Potentially both beneficial and adverse influences on actions in multi-unit scenarios.

Shared Components

Components that can support either, but only one, unit (e.g., a swing DG).

Shared Systems

Systems with components that are designed to support multiple units (e.g., service water system configured with pumps that can be aligned to multiple units).

Task 2: Evaluate Cross-Unit Dependencies

HRA dependencies across units refer to the potential for the failure of an action in one unit to make a related action in another unit less reliable.

Dependency (Negative)

For related human actions, actions taken in one unit could be less reliable based on the failure to perform the same action in another unit.

Positive Dependency

For related human actions, actions taken in one unit could be more reliable based on feedback from other units at the site.

Note: Other dependencies may exist between units that impact operator action reliability. For example, the accident sequence in the first unit might create environmental conditions that make actions in the second unit more difficult or impossible. **Such dependencies must be addressed explicitly.**

Complexities Regarding HRA Dependencies

- The evaluation of HRA dependencies between units can be complex due to the multi-dimensional nature of multi-unit events.
- Must consider the intra-unit (i.e., same unit) HRA dependencies and then the additional inter-unit (i.e., cross-unit) dependencies.
- The modeling of cross-unit HRA dependencies should be limited to "related" actions (for example):

Explicit cross-unit hardware dependencies

Implicit/indirect dependencies due to shared plant contexts

Sources of Implicit Dependencies

Accident Sequences

- Multi-unit accidents start with a common initiating event.
- The most probable condition for multiple units is that they are on the accident sequence path.
- As such, the required operator actions are expected to occur in each unit with approximately the same plant context (e.g., time window, cues, competing demands) and the same resources (process, training, experience).

Control Room

- A shared control room and the shared environment - alarms and activity - would be sensed by all within the space.
- Crew management (e.g., shift manager, unit shift supervisors) would communicate and coordinate their actions early and often during a multi-unit accident.
- Dependencies across crews in a shared environment may be positive (e.g., shared crew members) or negative (e.g., group think).

Command and Control

- Site-level command and control becomes more challenging due to competing demands for resources and the “fog of war” that may accompany severe accidents.
- The site-level command and control structure creates high-level dependencies, both positive and negative, depending on the multi-unit event (e.g., a LOOP vs. a severe external event).

Task 3: Address Command & Control Challenges

A review of command & control functions can help identify challenges to successful actions during a multi-unit accident.

Command

Authority and responsibility for decision-making and directing actions to accomplish a goal, in this case, the safe operation of the nuclear power plant site.

Control

Manipulating control board switches or local controls in response to commands.

Control is generally limited to licensed operators, reactor operators in the main control room and auxiliary operators in the field.

Normal Command & Control (C2)

- For normal operation and “anticipated” transients, C2 is generally clear and straightforward – a **formal chain of command** as defined in station policies.
- Most actions at this level are constrained by procedural direction:

COMMAND
Actions are based on procedures driven by the assessment of information (cues) present in the control room of the plant condition.

CONTROL
Communication of commands based on procedural steps is typically from the unit supervisor to reactor operators on the main control board.

CONTROL
Communication to local auxiliary operators may be through the unit supervisor or reactor operators.

Severe Accident Command & Control Issues

For more severe multi-unit accidents (e.g., extreme external hazards), the command & control function **is more complex:**

- Additional layers of command, with the **need for coordination and collaboration**.
- The true conditions of the reactors and mitigation systems may not be clearly understood by all layers of command.
- The accident may limit the options and place other constraints on personnel and equipment.
- The standard command & control function may confront outside influences and ad hoc command structures may develop in response to a severe accident.

Command & Control in Accident Stages

The multi-unit HRA framework is built around six stages of severe accidents:

Stage	Title	Time Frame	Command / Control (C2)
1	Initial Response to Multi-Unit Initiator	0 to 15 min	**U1, U2:** The initial response for each unit is led by a unit supervisor, following applicable EOPs and/or AOPs.
2	Initial Collaboration	15 to 60 min	**U1 + U2:** For a site-level initiator, the crews would communicate between units regarding their specific status and begin to coordinate their responses once the initial plant actions were taken. This collaboration would be through the shift manager(s) and unit supervisors.
3	Technical Support Center (TSC) Activation	1 hr. +	**U1 + U2 + TSC:** Activation of the TSC brings significantly greater personnel resources to the site but also creates a more complex command & control structure. Communication occurs between the TSC leadership and the shift manager(s).
4	Deployment of Portable Equipment	2 hr. +	**TSC + U1 + U2:** Once the TSC is fully functional, it takes over the higher level C2 functions. The MCR crew would still take procedural actions in response to indications on the main control board.
5	Initiation of Severe Accident Management Guidelines (SAMGs)	4 hrs. +	**TSC + EOF + U1 + U2:** Entry into SAMGs implies the onset of core damage for at least one unit.
6	Regional Center Response	24 hrs. +	**EOF + TSC + U1 + U2:** Procuring equipment from the regional center would require control from the Emergency Operations Facility (EOF).

Conclusions – General

- Multi-unit HRA follows the same general approach for identifying, defining, and quantifying human failure events as used in current single-unit PRAs.

- Multi-unit HRA requires expanded investigation and analysis related to shared structures, systems, and components.

- Multi-unit HRA complexity may be reduced for sites with limited or no coupling between units.

Conclusions – HRA Uncertainties

- Increase in HRA uncertainty may depend on the degree of coupling between units.
- For sites with limited unit coupling, the multi-unit HRA may have similar ranges of uncertainties as the single-unit HRA.
- For sites with significant coupling, the ranges of uncertainties may be significantly higher based on implicit and explicit dependencies across the units.

Conclusions – HRA Scope

- For larger sites, the potential complication of dependencies among units makes multi-unit site HRA more difficult to address.
- Although more complex, the underlying multi-unit HRA logic should generally apply to internal and external hazards (e.g., internal fire, seismic).
- Command & control challenges may become more important for severe external hazard events.

Conclusions – Operating States

- Different site operational states with one or more units shut down create unique site contexts for multi-unit accidents.
- Different operational states in each unit may effectively decouple the actions in each unit since the units will not share as much of a common plant context.
- For sites with connected control rooms, an operating state with one unit in an outage may cause distractions and confusion.
- For sites with shared support systems, an operating state with one unit in an outage may require the system to be aligned differently to support shutdown cooling or to allow component maintenance.

Research Acknowledgments

- Fernando Ferrante (EPRI)
- Mark Wishart (EPRI)
- Ken Kiper (WEC, retired)
- Carroll Trull (former at WEC)
- Adriana Sivori (WEB)
- Fred Grant (SGH)

TOGETHER…SHAPING THE FUTURE OF ENERGY®

www.epri.com