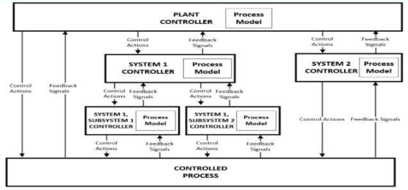
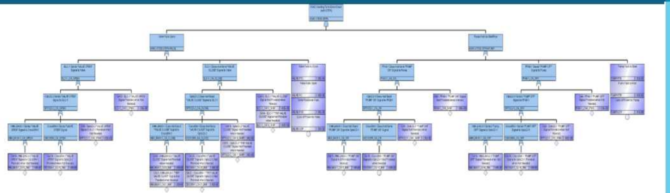
SAND20XX-XXXX

SAND2019-10586PE

HAZCADS – Hazard and Consequence Analysis for Digital Systems



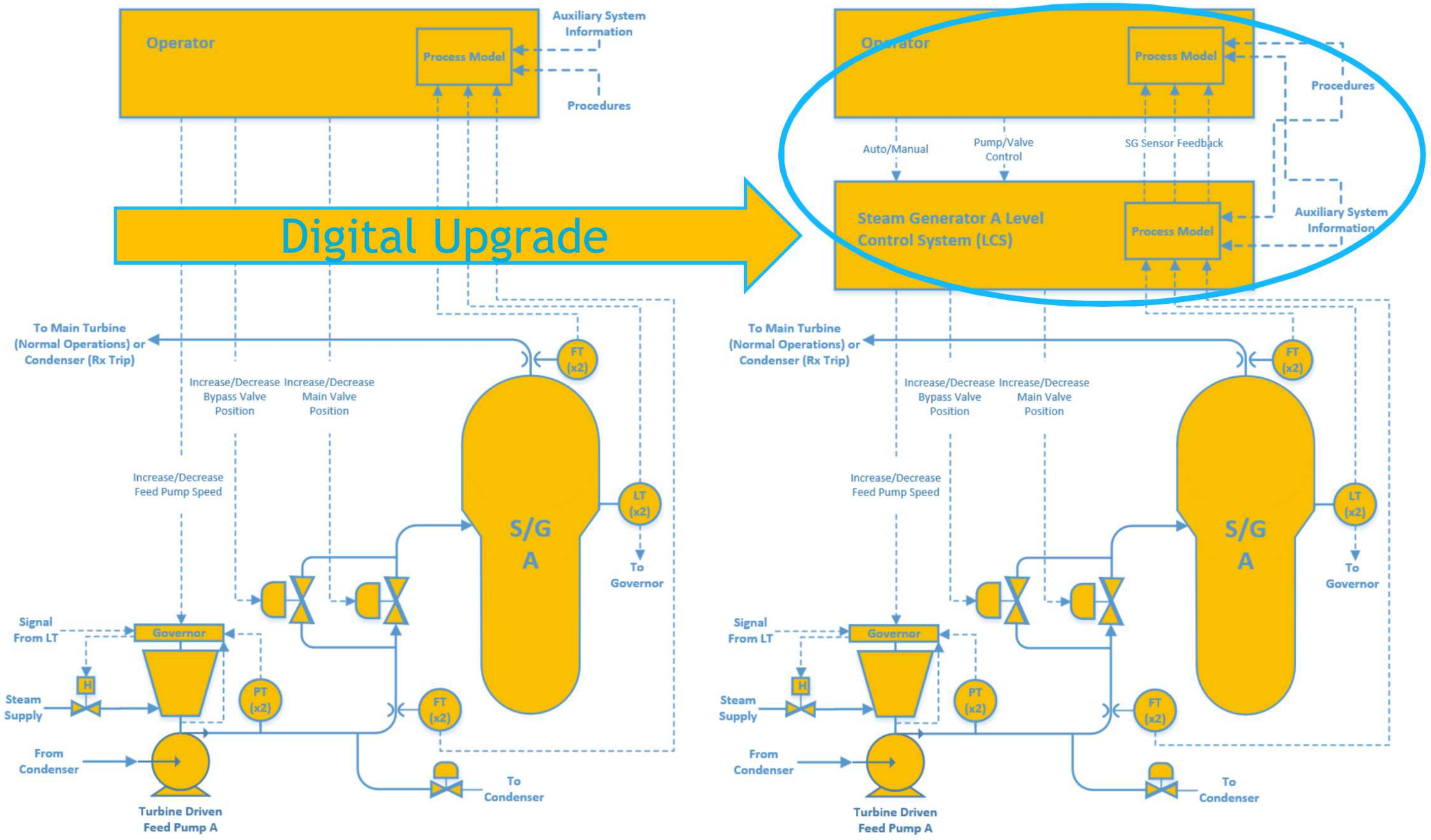


PRINCIPAL INVESTIGATORS

Andrew J. Clark and Adam D. Williams

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

The Need for Digital I&C Risk Management Tools


Digital Upgrade
Operator
Process Model
Auxiliary System Information
Procedures
To Main Turbine (Normal Operations) or Condenser (Rx Trip)
FT (x2)
Increase/Decrease Bypass Valve Position
Increase/Decrease Main Valve Position
Increase/Decrease Feed Pump Speed
S/G A
LT (x2)
To Governor
Signal From LT
Governor
H
Steam Supply
PT (x2)
FT (x2)
From Condenser
Turbine Driven Feed Pump A
To Condenser
Operator
Process Model
Procedures
Auto/Manual
Pump/Valve Control
SG Sensor Feedback
Steam Generator A Level Control System (LCS)
Process Model
Auxiliary System Information
To Main Turbine (Normal Operations) or Condenser (Rx Trip)
FT (x2)
Increase/Decrease Bypass Valve Position
Increase/Decrease Main Valve Position
Increase/Decrease Feed Pump Speed
S/G A
LT (x2)
To Governor
Signal From LT
Governor
H
Steam Supply
PT (x2)
FT (x2)
From Condenser
Turbine Driven Feed Pump A
To Condenser

The nuclear power industry is modifying the types of components and systems in their plants:

Active & *Analog* → *Passive* & *Digital*

With these changes come new and unknown types of component and system "failures".

- ***Traditional risk assessment tools struggle to assess "failure modes" in passive and digital components and systems***

The incorporation of digital I&C in NPPs introduces new control modes (e.g., main feedwater controller), which implicitly introduces potential new failure modes.

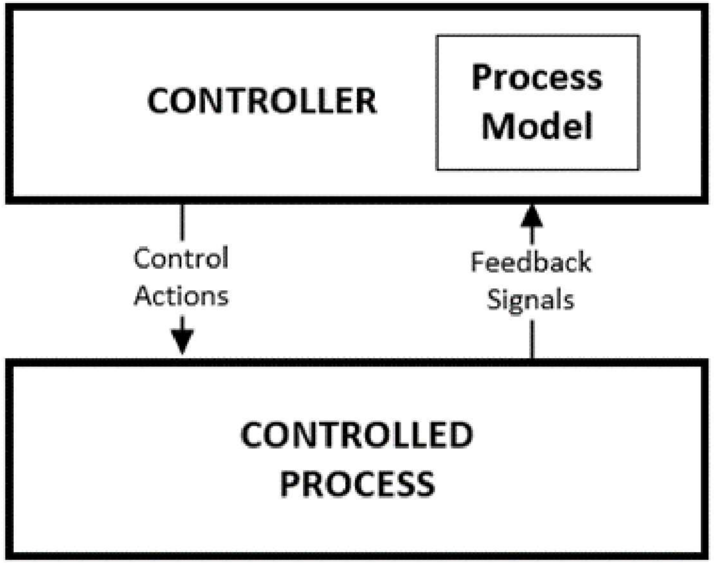
Addressing Digital I&C Issues

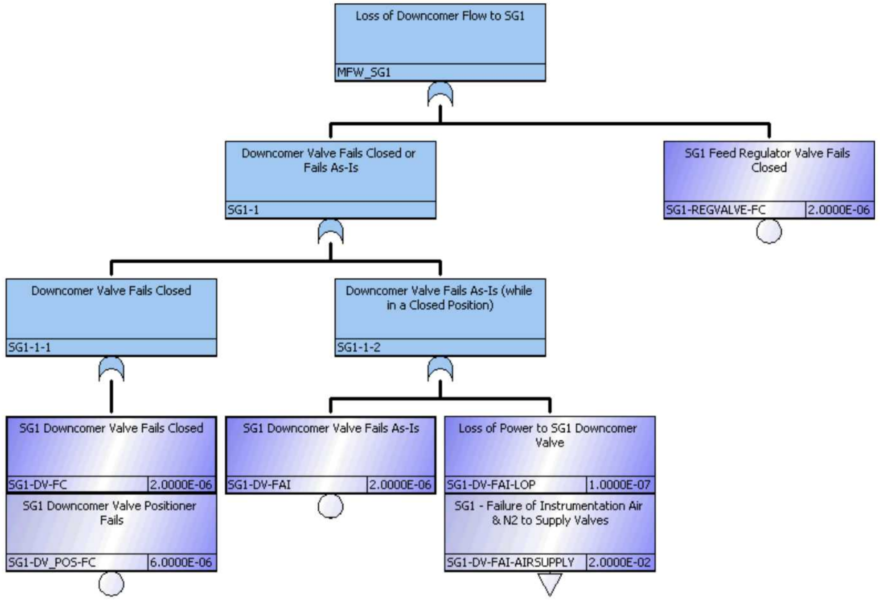
SNL and EPRI have teamed together in the last few years to address issues related to digital I&C and cyber security.

- SNL initially developed a methodology that combined multiple hazard analysis methods into a single methodology.
- The methodology has since been transferred to EPRI to further develop, mature, and validate.

The methodology combines Systems-Theoretic Process Analysis (STPA) and Fault Tree Analysis (FTA) into a unified and systematic framework.

- STPA uncovers *potential* failure modes that could occur on digital I&C components and systems (these failure modes are agnostic of the failure mechanisms).
- FTA provides the models for how systems fail by capturing system redundancy and diversity. The fault tree models predicts the combinatorial failures that ultimately lead to a system failure.




Loss of Downcomer Flow to SG1
MFW_SG1
Downcomer Valve Fails Closed or Fails As-Is
SG1-1
SG1 Feed Regulator Valve Fails Closed
SG1-REGVALVE-FC
2.0000E-06
Downcomer Valve Fails Closed
SG1-1-1
Downcomer Valve Fails As-Is (while in a Closed Position)
SG1-1-2
SG1 Downcomer Valve Fails Closed
SG1-DV-FC
2.0000E-06
SG1 Downcomer Valve Positioner Fails
SG1-DV_POS-FC
6.0000E-06
SG1 Downcomer Valve Fails As-Is
SG1-DV-FAI
2.0000E-06
Loss of Power to SG1 Downcomer Valve
SG1-DV-FAI-LOP
1.0000E-07
SG1 - Failure of Instrumentation Air & N2 to Supply Valves
SG1-DV-FAI-AIRSUPPLY
2.0000E-02

HAZCADS Overview

Hazard and Consequence Analysis for Digital Systems (HAZCADS) is a blended hazard analysis methodology that combines Systems-Theoretic Process Analysis (STPA) and Fault Tree Analysis (FTA).

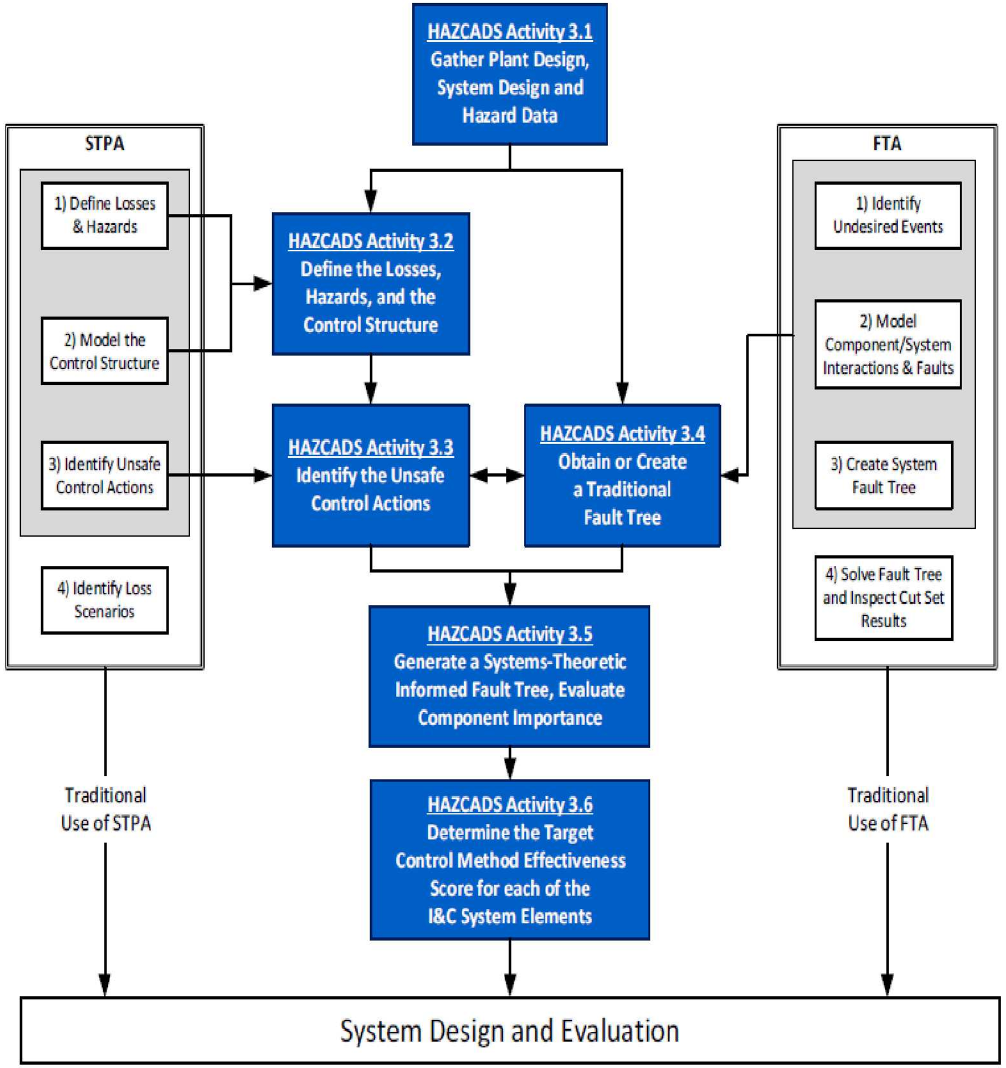
- *HAZCADS: Hazards and Consequences Analysis for Digital Systems*. EPRI, Palo Alto, CA: 2018. 3002012755.

HAZCADS is intended to be one of a suite of tools used for ***risk-informed decision-making*** for digital modifications, digital reliability, and cyber security.

- HAZCADS systematically identifies emergent and complex digital I&C "failures" that may occur – referred to as systematic failure modes.
- Incorporation of the systematic failure modes into existing PRA models provides a method for predicting how these failure modes *potentially* impact plant risk.

HAZCADS is a qualitative approach that incorporates digital I&C systematic failures into fault tree models.

- Cut set/Path set analysis – inspect the cut sets or path sets failure or success paths, respectively.
- Importance analysis – true/false event occurrence sensitivity analysis (FV-Bi importance analysis) of the systematic failure modes.
  - Importance analysis used for digital control method classes.


HAZCADS Activity 3.1
Gather Plant Design, System Design and Hazard Data
STPA
1) Define Losses & Hazards
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
FTA
1) Identify Undesired Events
2) Model Component/System Interactions & Faults
3) Create System Fault Tree
4) Solve Fault Tree and Inspect Cut Set Results
HAZCADS Activity 3.2
Define the Losses, Hazards, and the Control Structure
HAZCADS Activity 3.3
Identify the Unsafe Control Actions
HAZCADS Activity 3.4
Obtain or Create a Traditional Fault Tree
HAZCADS Activity 3.5
Generate a Systems-Theoretic Informed Fault Tree, Evaluate Component Importance
HAZCADS Activity 3.6
Determine the Target Control Method Effectiveness Score for each of the I&C System Elements
Traditional Use of STPA
Traditional Use of FTA
System Design and Evaluation

[*HAZCADS: Hazards and Consequences Analysis for Digital Systems*. EPRI, Palo Alto, CA: 2018. 3002012755.]

HAZCADS “Sales Pitch”

HAZCADS can be applied to systems that contain analog and/or digital equipment to understand how normal, yet *complex*, plant operations can lead to abnormal plant operating states (e.g., plant trips, transient analysis, and accident analysis).

HAZCADS’ novelty is its ability to systematically, efficiently, and accurately identify cyber/physical actions that could be exploited.

- Systematically – It considers the system as whole by considering how individual components contribute to the intended system function.
- Efficiently – HAZCADS does not spend large amounts of resources (relatively speaking) identifying all possible vulnerabilities – it identifies the <u>most important</u> vulnerabilities.
- Accurately – Results of HAZCADS exercises have been performed on actual plant systems with known issues and compared to root cause analyses.
    - HAZCADS’, thus far, has always uncovered the root cause, plus many more *potential* failure modes that could have occurred.

HAZCADS can be performed at any stage (i.e., design-phase, construction-phase, operating-phase).

Workshops and validations performed across the nuclear power plant fleet for cyber security.

- Performed across a wide spectrum of hazards/losses (e.g., Inadequate cooling of reactor; Economic Loss)

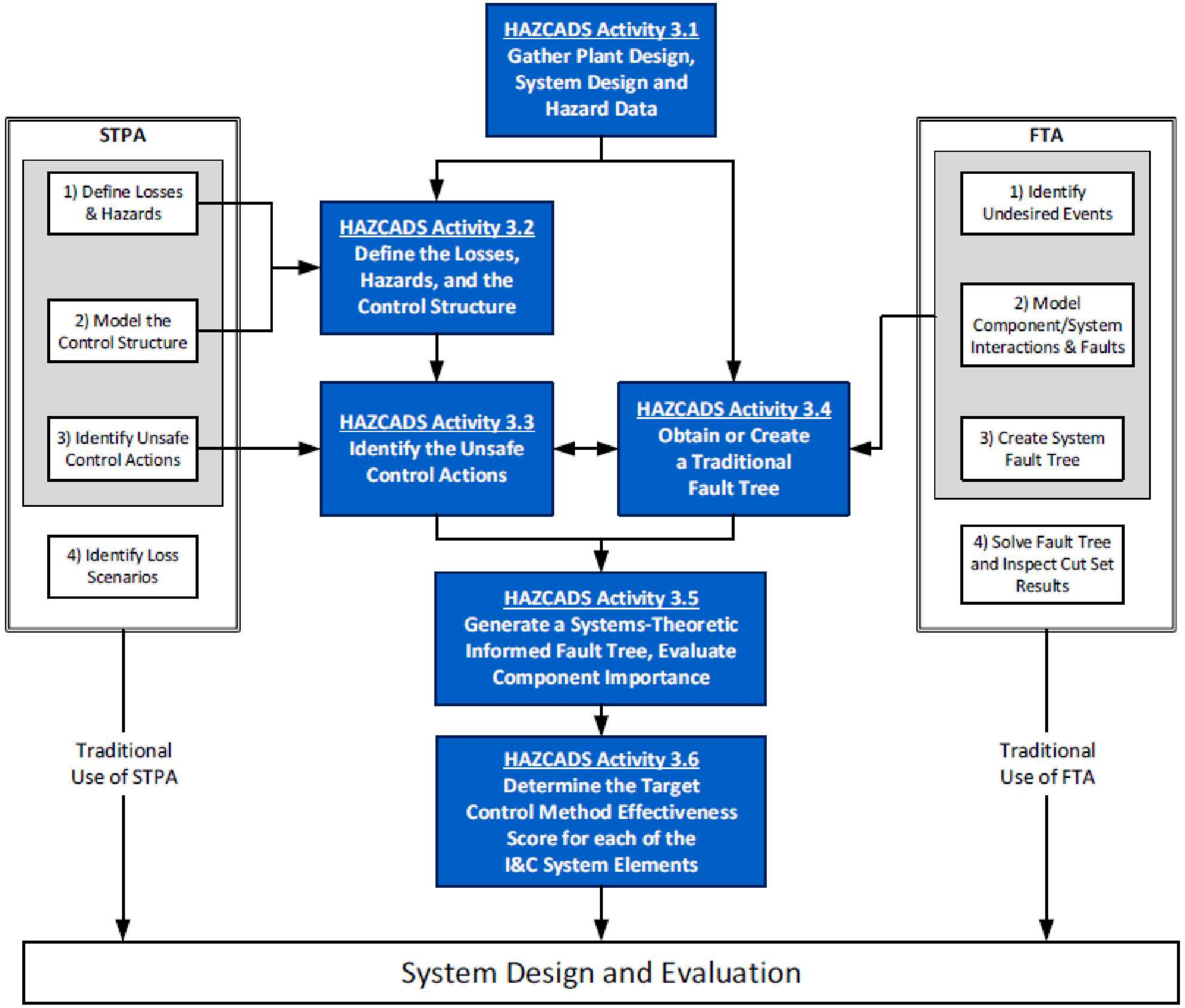
SNL and EPRI Continuing Efforts

EPRI's continuation of efforts is to use HAZCADS to inform digital engineering and modifications.

- HAZCADS Step 6 is used to transfer important results to subsequent digital and cyber security methods.
- Ongoing workshops throughout the nuclear industry to improve the HAZCADS method and ensure seamless training to engineers in the future.

SNL's efforts in FY19 is in applying HAZCADS to several BWR systems (HPCI, ADS, Core Sprays, and LPCI) to understand how system-to-system (e.g., HPCI → ADS → LPCI) interactions influence component behavior.

- FY20 (collaborating with INL) goals are: incorporate HAZOP elements into HAZCADS, apply HAZCADS to pilot systems, and further develop defense-in-depth and common cause failure identification.


HAZCADS Activity 3.1
Gather Plant Design, System Design and Hazard Data
STPA
1) Define Losses & Hazards
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
FTA
1) Identify Undesired Events
2) Model Component/System Interactions & Faults
3) Create System Fault Tree
4) Solve Fault Tree and Inspect Cut Set Results
HAZCADS Activity 3.2
Define the Losses, Hazards, and the Control Structure
HAZCADS Activity 3.3
Identify the Unsafe Control Actions
HAZCADS Activity 3.4
Obtain or Create a Traditional Fault Tree
HAZCADS Activity 3.5
Generate a Systems-Theoretic Informed Fault Tree, Evaluate Component Importance
HAZCADS Activity 3.6
Determine the Target Control Method Effectiveness Score for each of the I&C System Elements
Traditional Use of STPA
Traditional Use of FTA
System Design and Evaluation

[*HAZCADS: Hazards and Consequences Analysis for Digital Systems.* EPRI, Palo Alto, CA: 2018. 3002012755.]

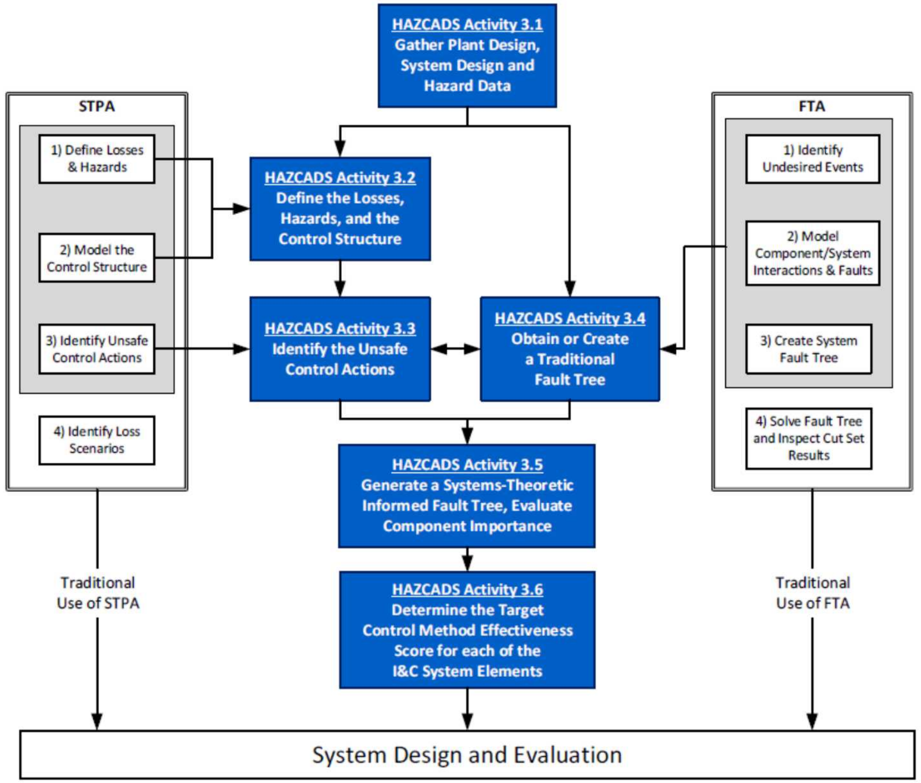
HAZCADS System Analysis

Additional System Analysis Using HAZCADS

We have a systematic framework for addressing hazards initiated by DI&C systems that can expand to:

- Common-cause failures
- Single point digital threats
- Defense-in-depth
- Dependencies between safety and non-safety systems

HAZCADS allows a systematic and formalized methodology for risk-informed assessments.


HAZCADS Activity 3.1
Gather Plant Design, System Design and Hazard Data
STPA
1) Define Losses & Hazards
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios
HAZCADS Activity 3.2
Define the Losses, Hazards, and the Control Structure
HAZCADS Activity 3.3
Identify the Unsafe Control Actions
HAZCADS Activity 3.4
Obtain or Create a Traditional Fault Tree
FTA
1) Identify Undesired Events
2) Model Component/System Interactions & Faults
3) Create System Fault Tree
4) Solve Fault Tree and Inspect Cut Set Results
HAZCADS Activity 3.5
Generate a Systems-Theoretic Informed Fault Tree, Evaluate Component Importance
HAZCADS Activity 3.6
Determine the Target Control Method Effectiveness Score for each of the I&C System Elements
Traditional Use of STPA
Traditional Use of FTA
System Design and Evaluation

EPRI's Digital Engineering Guide (DEG)

The DEG is used to further evaluate:

- Digital Reliability Analysis Methodology (DRAM)
- Technology Assessment Methodology (TAM)
- Human Factors Engineering (HFE).
- EM/RF Interference.

Risk Insights from Main Feedwater Control System Example

Digital I&C Common-Cause Failures - Using STPA to identify unsafe control actions, HAZCADS can identify CCFs between digital components.

- Multiple CCFs were identified for the S/G A and S/G B controllers.

Single Point Vulnerabilities – In the cut set analysis, HAZCADS identifies single point vulnerabilities.

- In some scenarios, S/G controllers were identified as single point vulnerabilities.

Defense-in-Depth and Redundancy – HAZCADS also models and identifies where defense-in-depth and redundancy are captured on digital I&C systems.

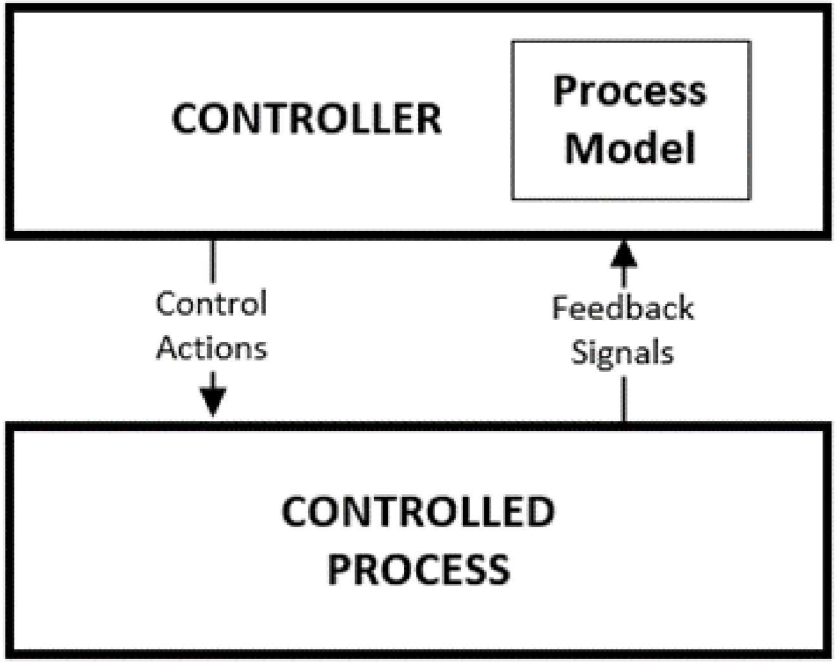
- In some scenarios, defense-in-depth and redundancy was captured with multiple controllers on separate data networks.

System-to-System Interactions – The hierarchical control structure systematically models system-to-system interactions.

- In one workshop, the condensate system was found to impact the MFWCS. These interactions were readily identified using STPA and HAZCADS.

Systems Theoretic Process Analysis (STPA) Methodology

System-Theoretic Process Analysis (STPA)



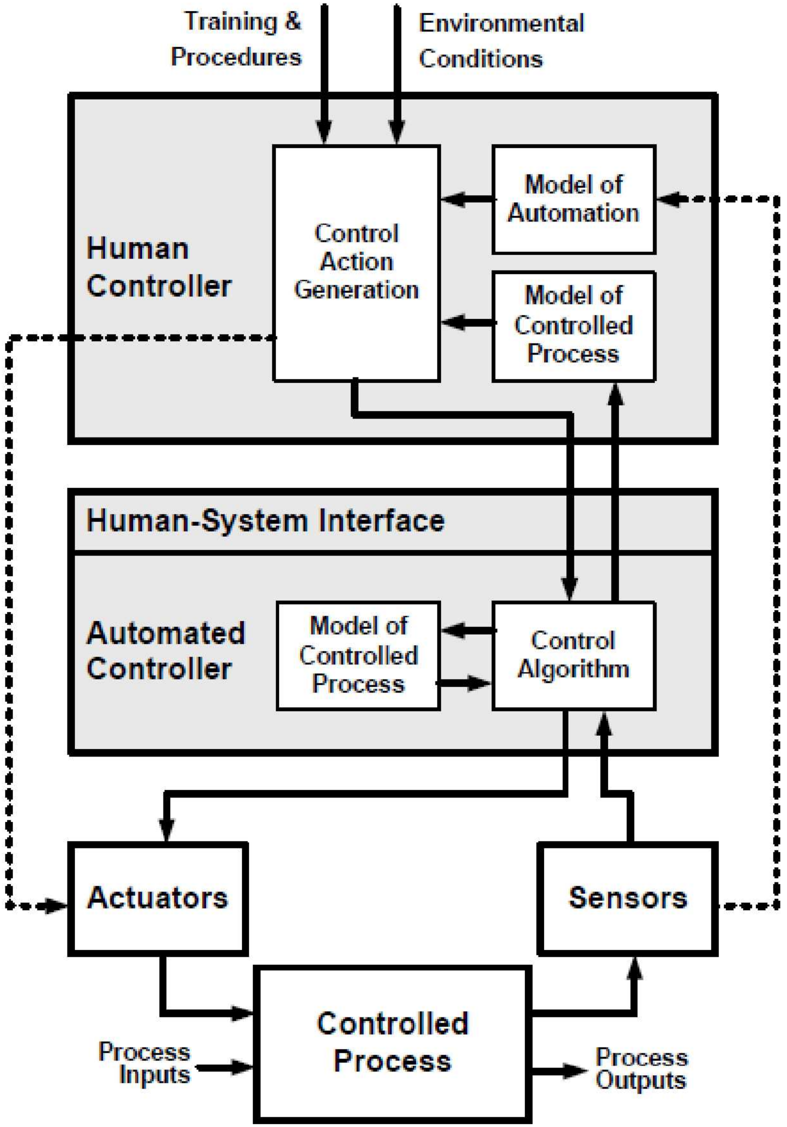
STPA is part of a relatively new set of system safety methods being developed at MIT (see Leveson 2018).

STPA describes how undesired outcomes (e.g., losses) can result from inadequate enforcement of control on design, development, and operation of systems to achieve desired objectives.

STPA can identify nontraditional failure modes (aka, causal factors) that are not identified using traditional hazard techniques (e.g., FMEA, FTA, HAZOP). For example:

- Design errors
- Software flaws
- Component interaction faults
- Social, organizational, and management factors contributing to accidents.

STPA Overview and Objectives



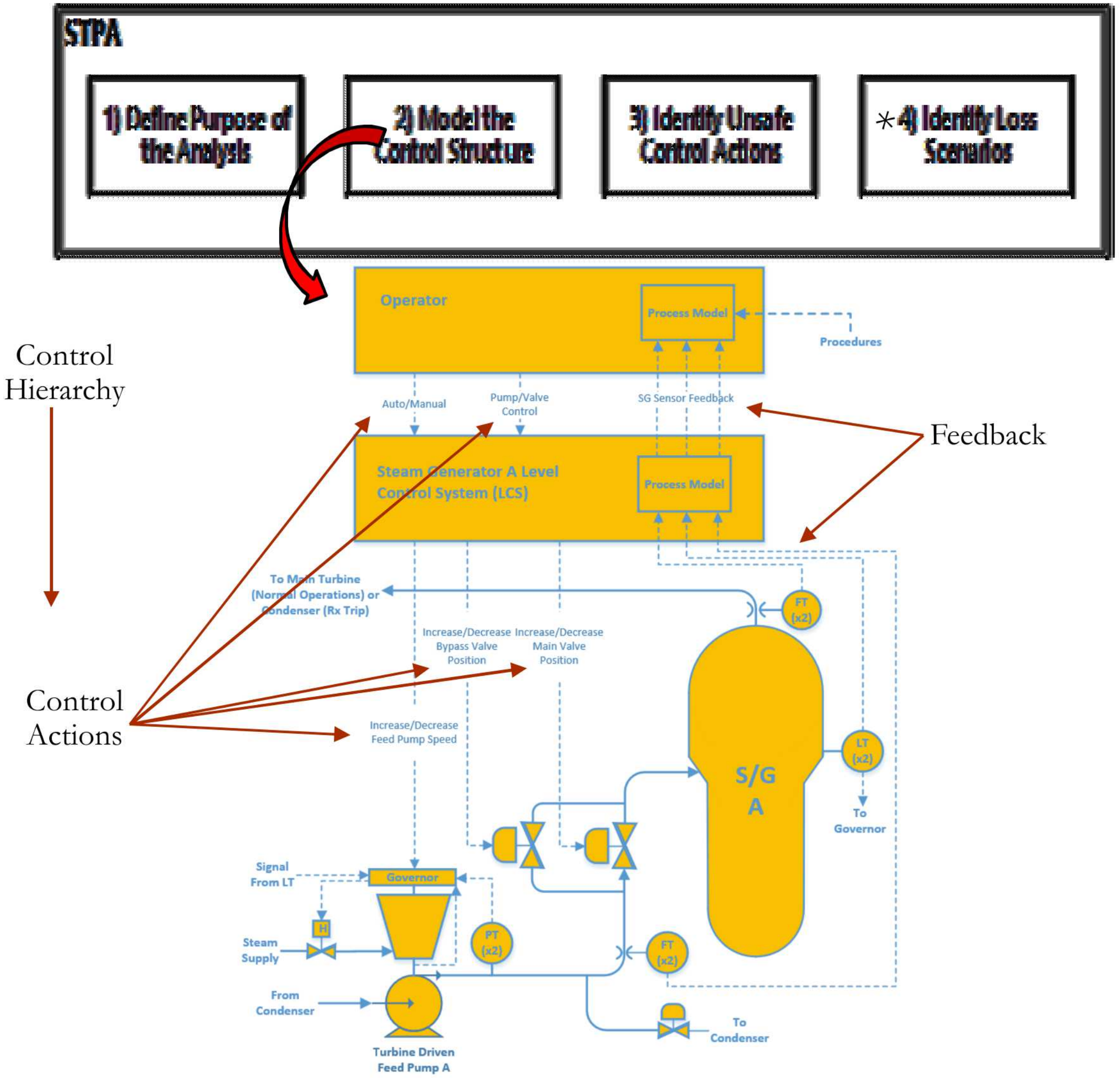
The goal is to identify accident scenarios that encompass the entire accident process, not just the electromechanical components.

Control Action – describes the effect that a controller (human, machine, or both) has on an actuator and ultimately the controlled process. Can be safe or unsafe and may depend on their context.

- For example, an unplanned, automatic main turbine trip may be considered *safe* in the context of protecting the main turbine/generator set, but it may also be considered *unsafe* in the context of nuclear safety because it is an initiating event that can challenge safety systems.

The control structure can include humans, machines, and process components, thus making it a useful model for analyzing a wide range of systems, from functionally simple plant control systems to complex technical and organization systems that interact with each other.

STPA Methodology


STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
*4) Identify Loss Scenarios
Operator
Process Model
Procedures
Auto/Manual
Pump/Valve Control
SG Sensor Feedback
Steam Generator A Level Control System (LCS)
Process Model
To Main Turbine (Normal Operations) or Condenser (Rx Trip)
FT (x2)
Increase/Decrease Bypass Valve Position
Increase/Decrease Main Valve Position
Increase/Decrease Feed Pump Speed
S/G A
LT (x2)
To Governor
Signal From LT
Governor
H
Steam Supply
PT (x2)
FT (x2)
From Condenser
Turbine Driven Feed Pump A
To Condenser

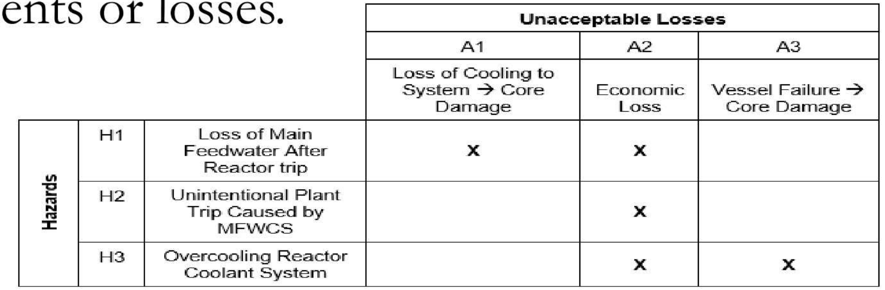
Control Hierarchy

Feedback

Control Actions

STPA systematically identifies hazardous control actions (including failures) that can lead to the identified hazards.

STPA, like FTA, starts with a focus on identified accidents or losses.



			Unacceptable Losses		
			A1	A2	A3
			Loss of Cooling to System → Core Damage	Economic Loss	Vessel Failure → Core Damage
Hazards	H1	Loss of Main Feedwater After Reactor trip	x	x	
	H2	Unintentional Plant Trip Caused by MFWCS		x	
	H3	Overcooling Reactor Coolant System		x	x

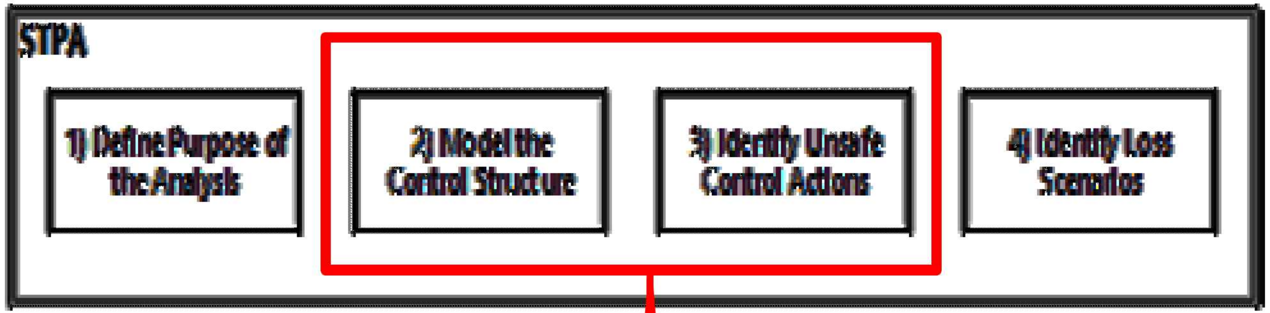
STPA creates a hierarchical view of the system.

Similar to HAZOP and FMEA usage of guide words, STPA classifies control action behaviors as follows:

- Control Action is **Provided**
- Control Action is **Not Provided**
- Control Action is **Provided Too Early**
- Control Action is **Provided Too Late**
- Control Action is **Stopped Too Soon**

**Note –STPA Step 4 greatly expands the analysis and can lead to significant efforts. EPRI's Digital Engineering Guide (DEG) transfers STPA Step 4 analysis to separate digital analysis methods).*

STPA Constraint/Requirements Slide


STPA
1) Define Purpose of the Analysis
2) Model the Control Structure
3) Identify Unsafe Control Actions
4) Identify Loss Scenarios

Identify losses → Loss of cooling systems (potential core damage)

Identify States of Higher Risk → Loss of Main Feedwater after Reactor Trip

Derive Requirements → *MUST* maintain flow of main feedwater

Define Control Actions → FW pump controller *MUST* send “increase speed” signal after reactor trip

Identify *Unsafe* Control Actions →

Control Actions		NNP	PNN	GTE/GTL/WO	STS/ETL
CA1	FPC1 sends “INCREASE SPEED” signal to SG1 FW Pump.	No Hazard	H3	GTE: H3 GTL: No Hazard WO: H3	STS: No Hazard ETL: H3