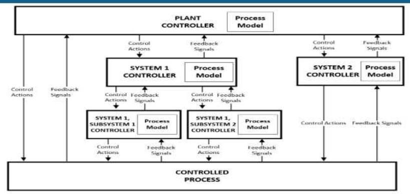
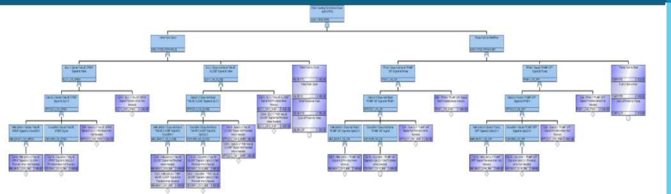
SAND2018-13449PE

Hazard and Consequence Analysis for Digital Systems





PRESENTED BY

Mitch McCrory, Sandia National Laboratories

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.

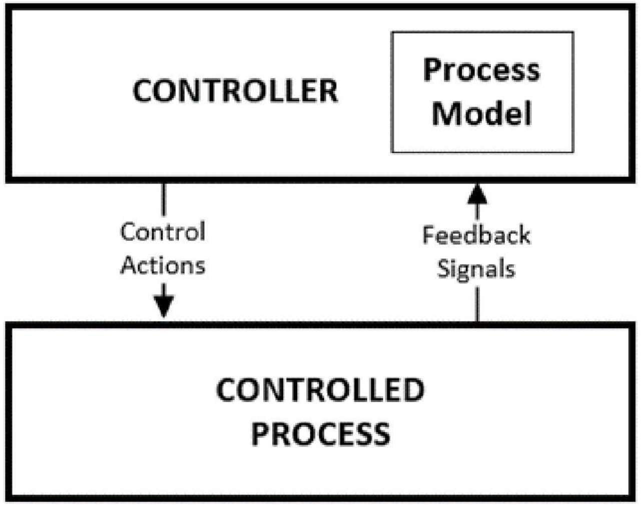
Risk-Informed Approach to Critical Digital Assets

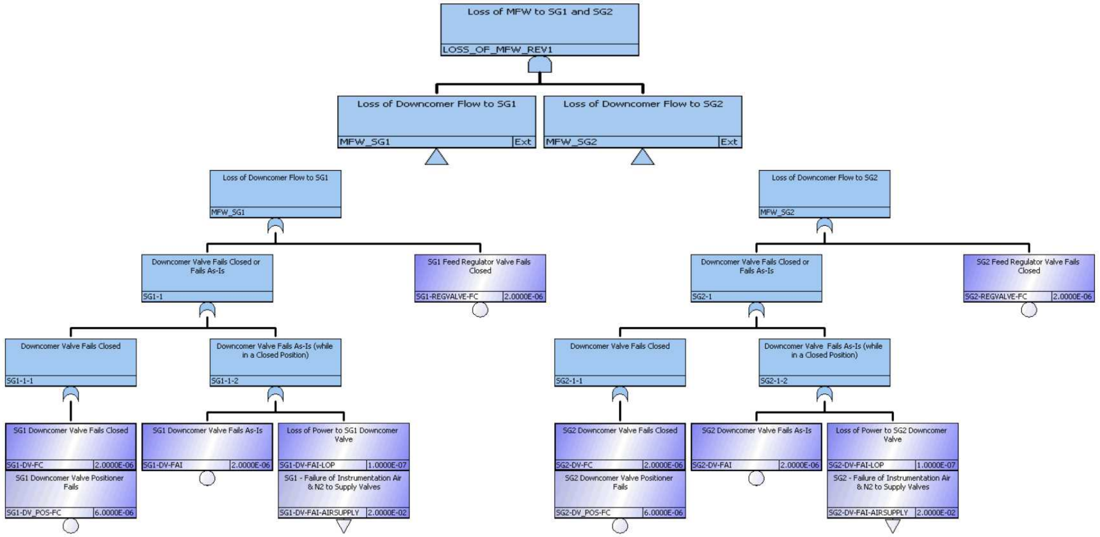
10 CFR 73.54 requires that each licensee submit a cyber security plan.

- Regulatory Guide 5.71, NEI 08-09, and NEI 13-10 provide guidance on developing a cyber security plan.
- However, these guides do not provide effective methods for a risk-informed approach to cyber security plans.

SNL and EPRI have developed an methodology that provides a risk-informed approach to assessing digital I&C.

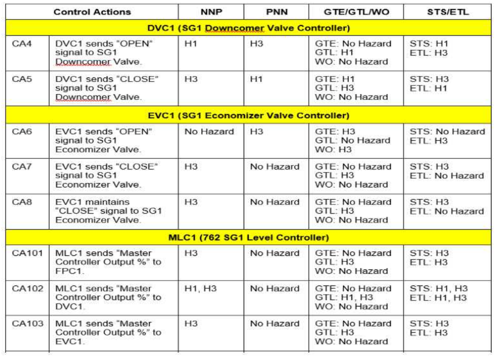
- The method combines Systems-Theoretic Process Analysis (STPA) and fault tree analysis.
- This method incorporates potential hazardous control signals into existing PRA models. The as-built PRA models are not altered in this method, but new basic events are added.
- The developed methodology gives transparency as to the effects a digital component has on safety and may remove unnecessary burden placed on licensees.



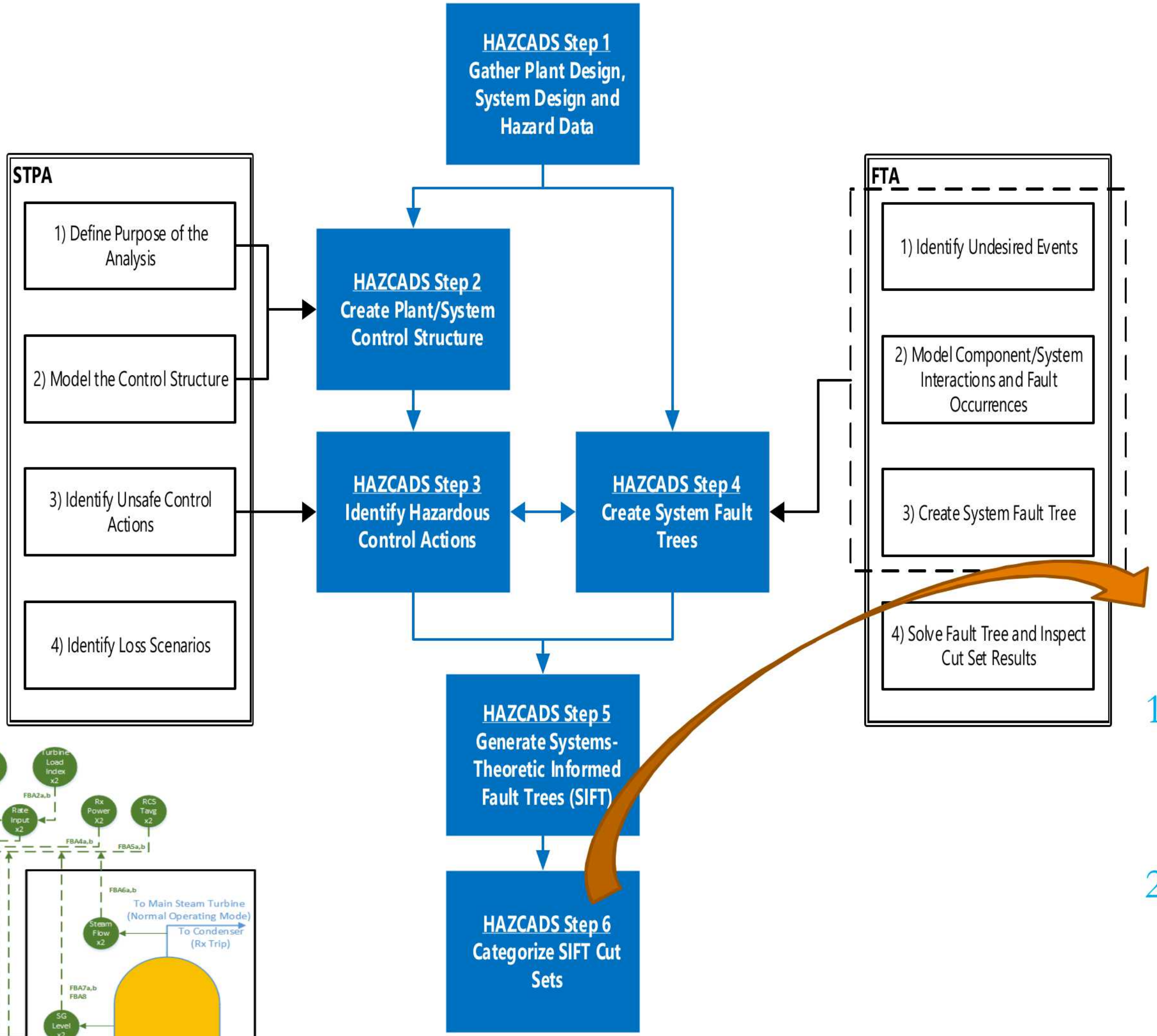


Loss of MFW to SG1 and SG2
LOSS_OF_MFW_REV1
Loss of Downcomer Flow to SG1
MFW_SG1
Ext
Loss of Downcomer Flow to SG2
MFW_SG2
Ext
Loss of Downcomer Flow to SG1
MFW_SG1
Downcomer Valve Fails Closed or Fails As-Is
SG1-1
SG1 Feed Regulator Valve Fails Closed
SG1-REGVALVE-FC
2.0000E-06
Downcomer Valve Fails 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
Loss of Downcomer Flow to SG2
MFW_SG2
Downcomer Valve Fails Closed or Fails As-Is
SG2-1
SG2 Feed Regulator Valve Fails Closed
SG2-REGVALVE-FC
2.0000E-06
Downcomer Valve Fails Closed
SG2-1-1
Downcomer Valve Fails As-Is (while in a Closed Position)
SG2-1-2
SG2 Downcomer Valve Fails Closed
SG2-DV-FC
2.0000E-06
SG2 Downcomer Valve Positioner Fails
SG2-DV_POS-FC
6.0000E-06
SG2 Downcomer Valve Fails As-Is
SG2-DV-FAI
2.0000E-06
Loss of Power to SG2 Downcomer Valve
SG2-DV-FAI-LOP
1.0000E-07
SG2 - Failure of Instrumentation Air & N2 to Supply Valves
SG2-DV-FAI-AIRSUPPLY
2.0000E-02

Hazard and Consequence Analysis for Digital Systems (HAZCADS)



Control Actions		NNP	PNN	GTE/GTL/WO	STS/ETL
DVC1 (SG1 Downcomer Valve Controller)					
CA4	DVC1 sends "OPEN" signal to SG1 Downcomer Valve.	H1	H3	GTE: No Hazard GTL: H1 WO: No Hazard	STS: H1 ETL: H3
CA5	DVC1 sends "CLOSE" signal to SG1 Downcomer Valve.	H3	H1	GTE: H1 GTL: H3 WO: No Hazard	STS: H3 ETL: H1
EVC1 (SG1 Economizer Valve Controller)					
CA6	EVC1 sends "OPEN" signal to SG1 Economizer Valve.	No Hazard	H3	GTE: H3 GTL: No Hazard WO: H3	STS: No Hazard ETL: H3
CA7	EVC1 sends "CLOSE" signal to SG1 Economizer Valve.	H3	No Hazard	GTE: No Hazard GTL: H3 WO: No Hazard	STS: H3 ETL: No Hazard
CA8	EVC1 maintains "CLOSE" signal to SG1 Economizer Valve.	H3	No Hazard	GTE: No Hazard GTL: H3 WO: No Hazard	STS: H3 ETL: No Hazard
MLC1 (762 SG1 Level Controller)					
CA101	MLC1 sends "Master Controller Output %" to FPC1.	H3	No Hazard	GTE: No Hazard GTL: H3 WO: No Hazard	STS: H3 ETL: H3
CA102	MLC1 sends "Master Controller Output %" to DVC1.	H1, H3	No Hazard	GTE: No Hazard GTL: H1, H3 WO: No Hazard	STS: H1, H3 ETL: H1, H3
CA103	MLC1 sends "Master Controller Output %" to EVC1.	H3	No Hazard	GTE: No Hazard GTL: H3 WO: No Hazard	STS: H3 ETL: H3



HAZCADS Step 1
Gather Plant Design, System Design and Hazard Data

STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

HAZCADS Step 2
Create Plant/System Control Structure

HAZCADS Step 3
Identify Hazardous Control Actions

HAZCADS Step 4
Create System Fault Trees

FTA

1) Identify Undesired Events

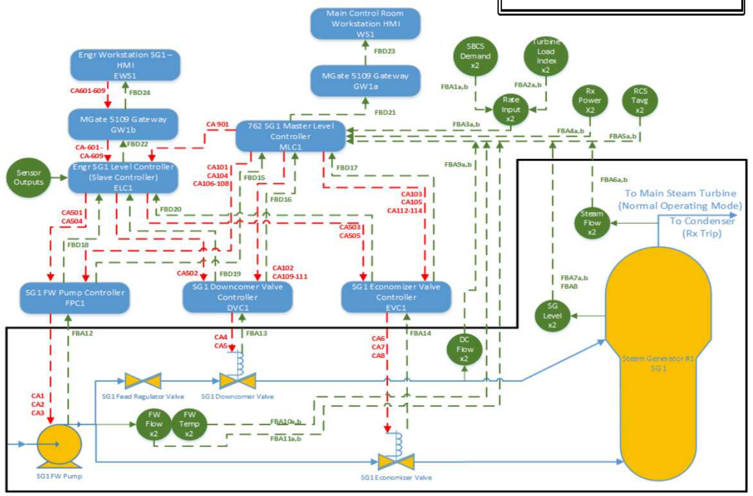
2) Model Component/System Interactions and Fault Occurrences

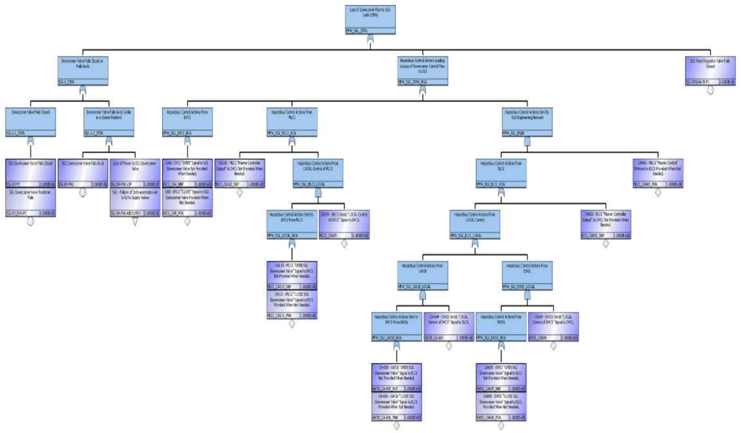
3) Create System Fault Tree

4) Solve Fault Tree and Inspect Cut Set Results

HAZCADS Step 5
Generate Systems-Theoretic Informed Fault Trees (SIFT)

HAZCADS Step 6
Categorize SIFT Cut Sets

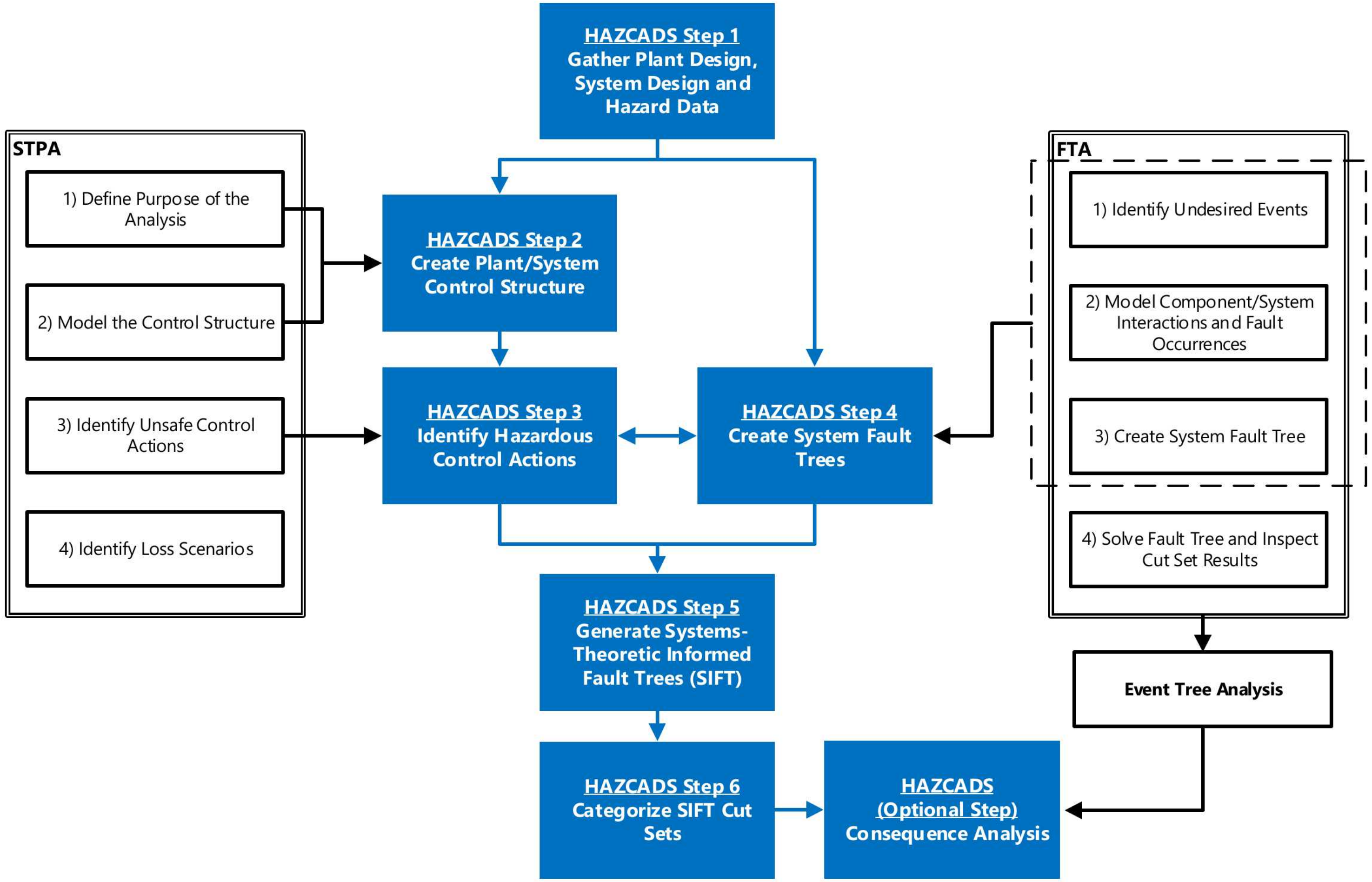




Three Categories of SIFT Cut Set Results:

1. Non-digital (traditional) hardware component failures.
   - Cut sets currently produced in PRAs.
2. Combinations of hazardous control actions with non-digital hardware component failures.
   - *Potential* cyber attacks.
3. Comprised only of hazardous control actions.
   - Hazards that can be achieved strictly from digital/cyber attacks.

HAZCADS Consequence Analysis



HAZCADS Step 1
Gather Plant Design, System Design and Hazard Data

STPA

1) Define Purpose of the Analysis

2) Model the Control Structure

3) Identify Unsafe Control Actions

4) Identify Loss Scenarios

HAZCADS Step 2
Create Plant/System Control Structure

HAZCADS Step 3
Identify Hazardous Control Actions

HAZCADS Step 4
Create System Fault Trees

FTA

1) Identify Undesired Events

2) Model Component/System Interactions and Fault Occurrences

3) Create System Fault Tree

4) Solve Fault Tree and Inspect Cut Set Results

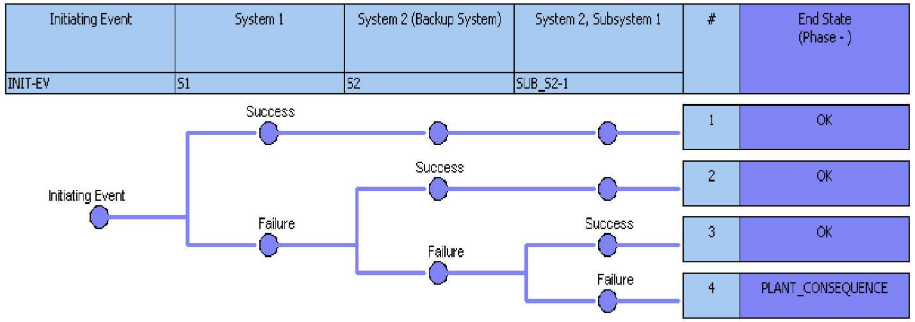
Event Tree Analysis

HAZCADS Step 5
Generate Systems-Theoretic Informed Fault Trees (SIFT)

HAZCADS Step 6
Categorize SIFT Cut Sets

HAZCADS (Optional Step)
Consequence Analysis

Utilization of fault trees allows event trees to be used for consequence analysis (i.e., assessing the impact of digital components on core damage states).



Initiating Event	System 1	System 2 (Backup System)	System 2, Subsystem 1	#	End State (Phase -)
INIT-EV	S1	S2	SUB_S2-1		
				1	OK
				2	OK
				3	OK
				4	PLANT_CONSEQUENCE

Similar to the three categories of cut sets for fault trees, we may uncover new categories of cut sets contributing to core damage.

HAZCADS Further Analysis

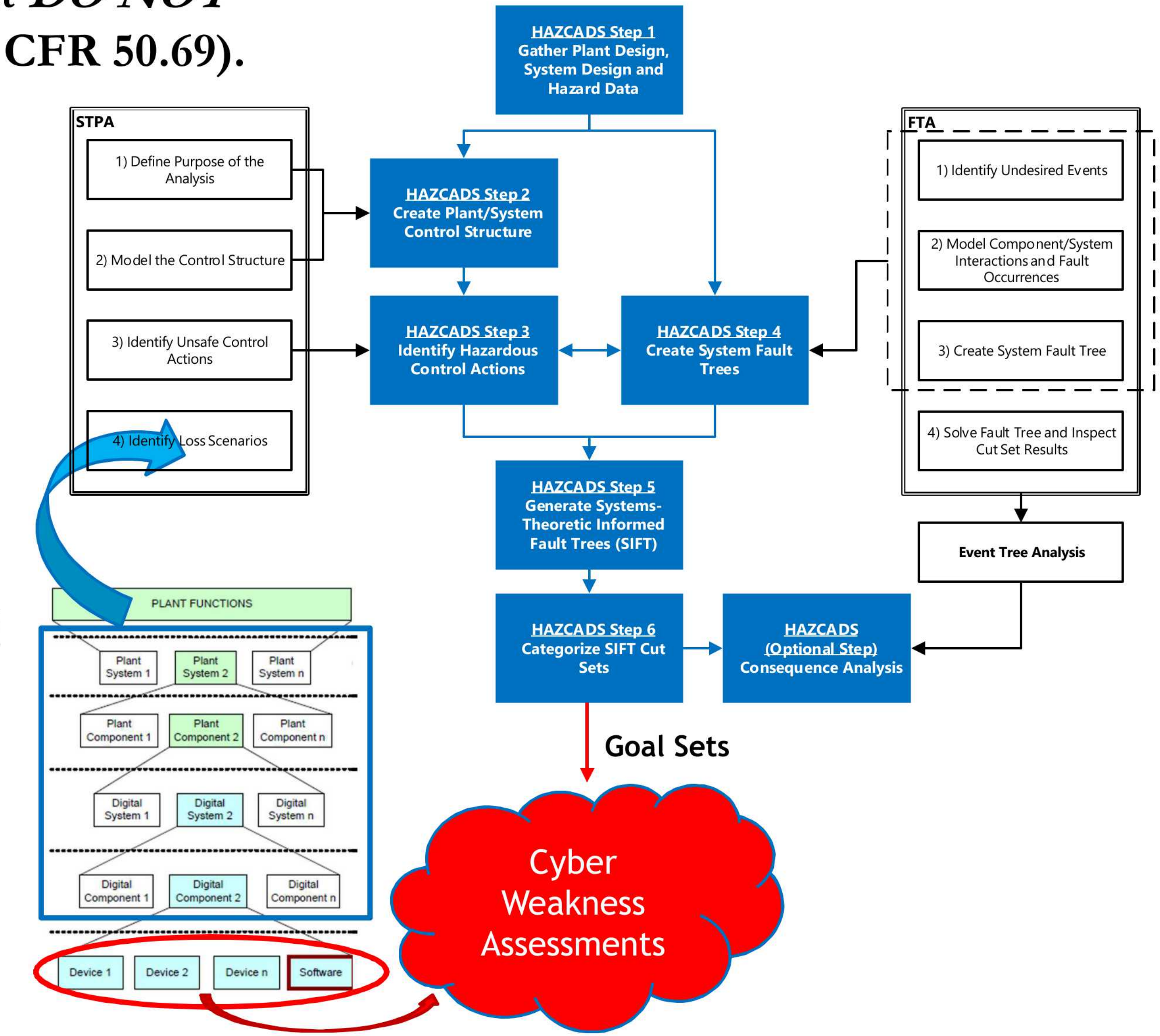
HAZCADS can identify digital components that *DO NOT* perform any safety significant functions (see 10 CFR 50.69).

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

The Type 2 and Type 3 SIFT cut sets can be treated as goal sets in cyber weakness assessments.

- Cyber weakness assessments provide contextual descriptions for the hazardous control actions.



HAZCADS Step 1
Gather Plant Design, System Design and Hazard Data

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

HAZCADS Step 2
Create Plant/System Control Structure

HAZCADS Step 3
Identify Hazardous Control Actions

HAZCADS Step 4
Create System Fault Trees

FTA
1) Identify Undesired Events
2) Model Component/System Interactions and Fault Occurrences
3) Create System Fault Tree
4) Solve Fault Tree and Inspect Cut Set Results

Event Tree Analysis

HAZCADS Step 5
Generate Systems-Theoretic Informed Fault Trees (SIFT)

HAZCADS Step 6
Categorize SIFT Cut Sets

HAZCADS (Optional Step)
Consequence Analysis

Goal Sets

Cyber Weakness Assessments

Future Research Using HAZCADS

Applied to vital area identification of digital components.

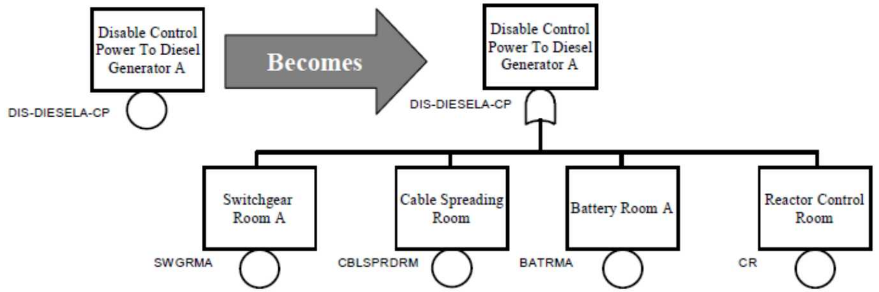
DI&C system hazard inputs into accident analysis computer codes, such as MELCOR.

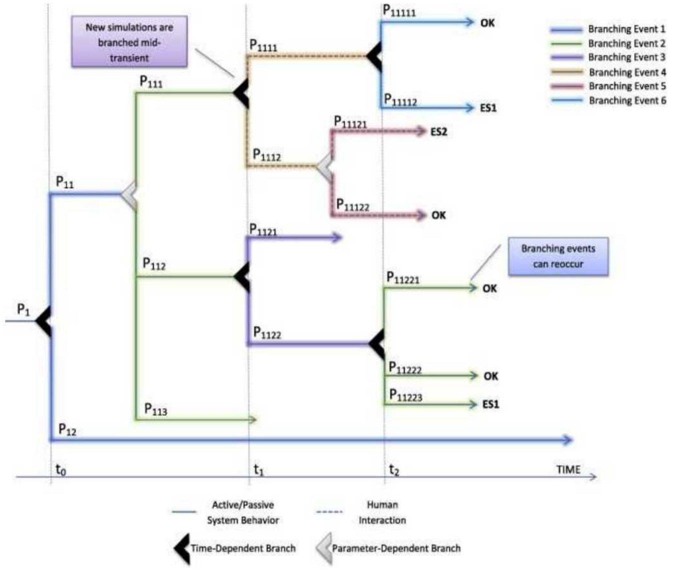
Integrated with cyber attack simulators, such as EMULYTICS™.

Coupled with dynamic probabilistic risk assessment tools.

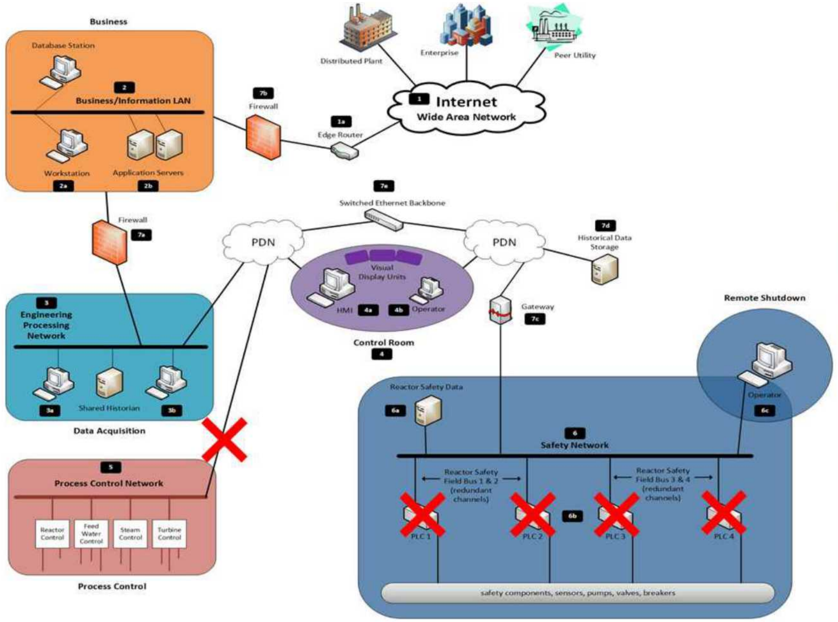
G. B. Varnado and D. W. Whitehead. *Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants*. SAND2008-5644, Sandia National Laboratories, Albuquerque, NM, 2008.

Disable Diesel Generator Control Power





Z.K. Jankovsky, M.R. Denman, T. Aldemir, *Dynamic Event Tree Analysis with the SAS4A/SASSYS-1 Safety Analysis Code*, Annals of Nuclear Energy, May 2018.


Business
Database Station
2
Business/Information LAN
Workstation
2a
Application Servers
2b
7b
Firewall
1a
Edge Router
1
Internet
Wide Area Network
Distributed Plant
Enterprise
Peer Utility
7e
Switched Ethernet Backbone
Firewall
7a
PDN
PDN
7d
Historical Data Storage
Visual Display Units
HMI
4a
4b
Operator
Control Room
4
Gateway
7c
3
Engineering Processing Network
3a
Shared Historian
3b
Data Acquisition
5
Process Control Network
Reactor Control
Feed Water Control
Steam Control
Turbine Control
Process Control
Remote Shutdown
Operator
6c
Reactor Safety Data
6a
6
Safety Network
Reactor Safety Field Bus 1 & 2 (redundant channels)
Reactor Safety Field Bus 3 & 4 (redundant channels)
PLC 1
PLC 2
6b
PLC 3
PLC 4
safety components, sensors, pumps, valves, breakers