NAVAL
POSTGRADUATE
SCHOOL

A Graph Theory Approach to Functional Failure Propagation in Early Complex Cyber-Physical Systems (CCPSs)

Bryan M. O' Halloran, Ph.D.

Nikolaos Papakonstantinou , Ph.D.

Kristin Giammarco , Ph.D.

Douglas L. Van Bossuyt, Ph.D.

Where do failures occur in the system?

- Many years ago…Component failures
- This is the reason for MIL-HDBK-217f, and other component-based methods
- Suppliers are getting better
  - Failure rates: Factor of 1000 better over 17 year period
- Since components make up the system, where do failures occur?

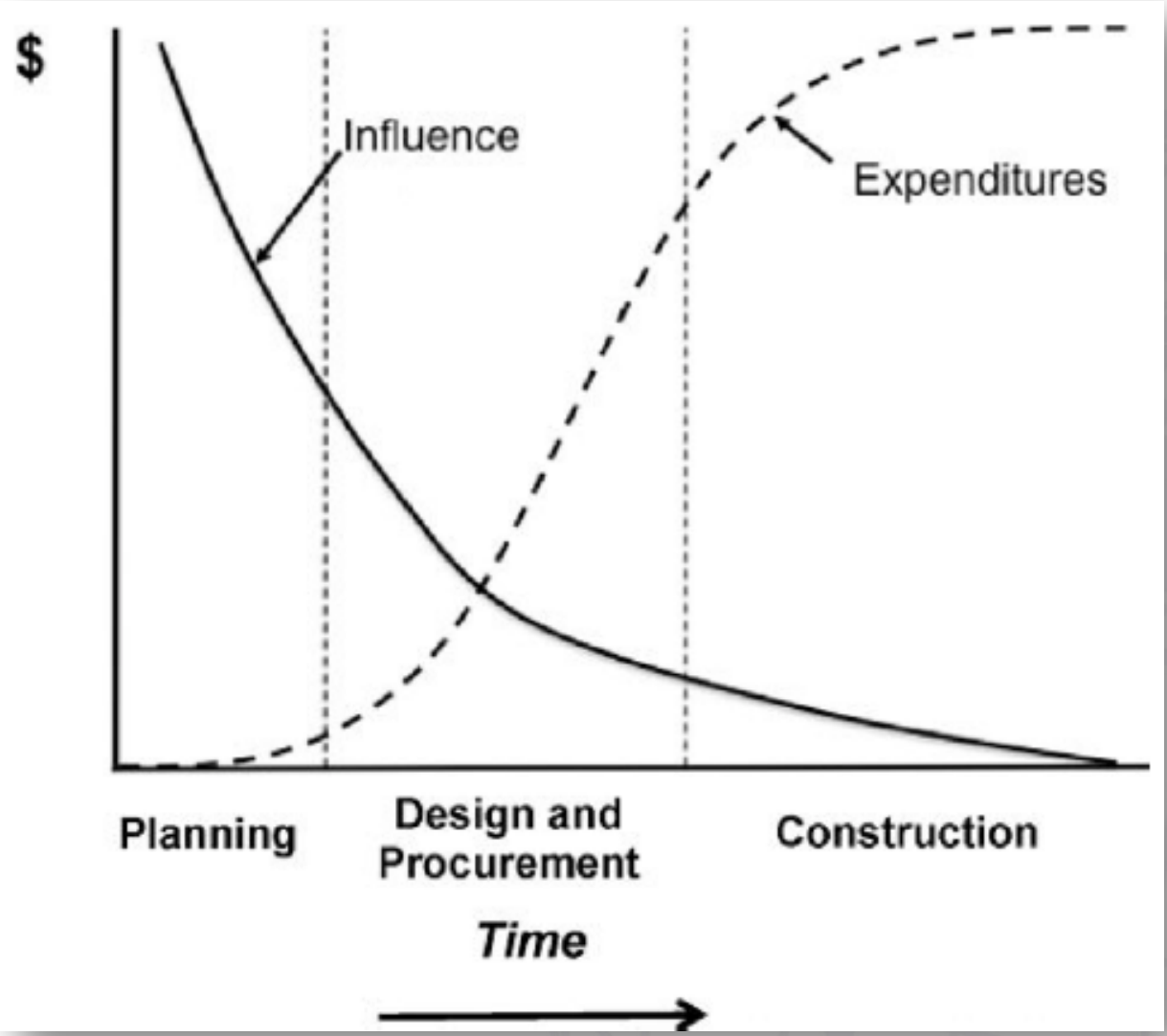
Where do failures occur in the system?

- **Connections**
- Reliable components connected unreliably = unreliable system
- There are many more connections in a system than components, so they are critical to get right during design.
- This **motivates** investigating the connectivity of the system

Constraints of modern design

- Have you ever heard?
  - Feel free to deliver the system late, or
  - We're hoping to relax the requirement of the next generation system.
- Modern systems are developed on shorter schedules, smaller budgets…and, the systems are being expected to do more
- Modern systems are highly connected and therefore have a high degree of failure propagation potential
- Where's the opportunity to make big changes?

Introduction



What is being solved?

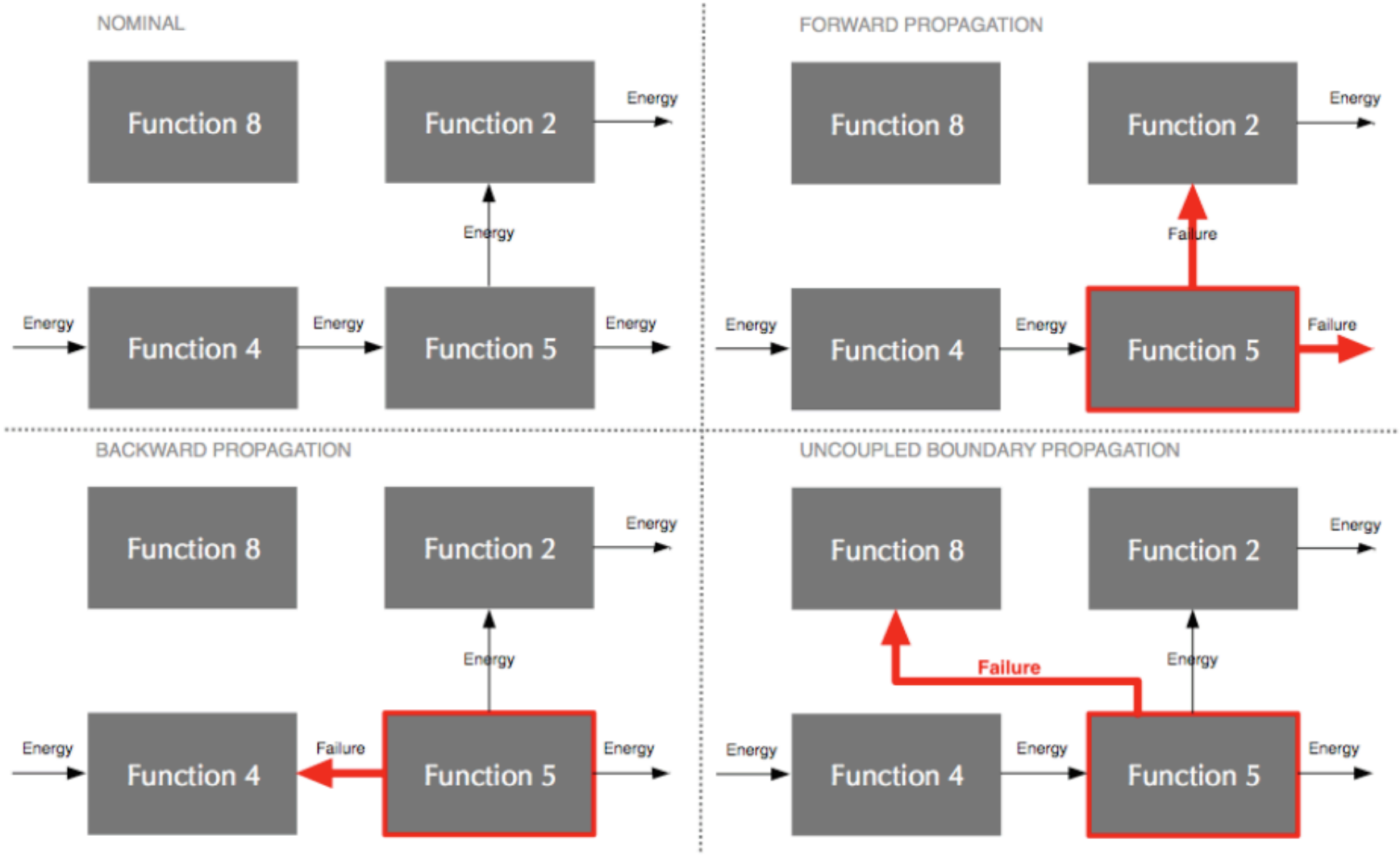
Research Question:

How can failure propagation be quantified during the early stages of complex systems design?

Approaches that already exist

- Most research is concerned with identifying propagation pathways, identifying/quantifying risk, etc.
- Also most research is only applicable once components have been selected.
  - The progression of decisions during design reduce the system's flexibility to maneuver throughout the design space
- This work uses the system's functional architecture, and network theory, to investigate the connectivity of a system, and then to propose a failure propagation metric.

How do failures propagate?

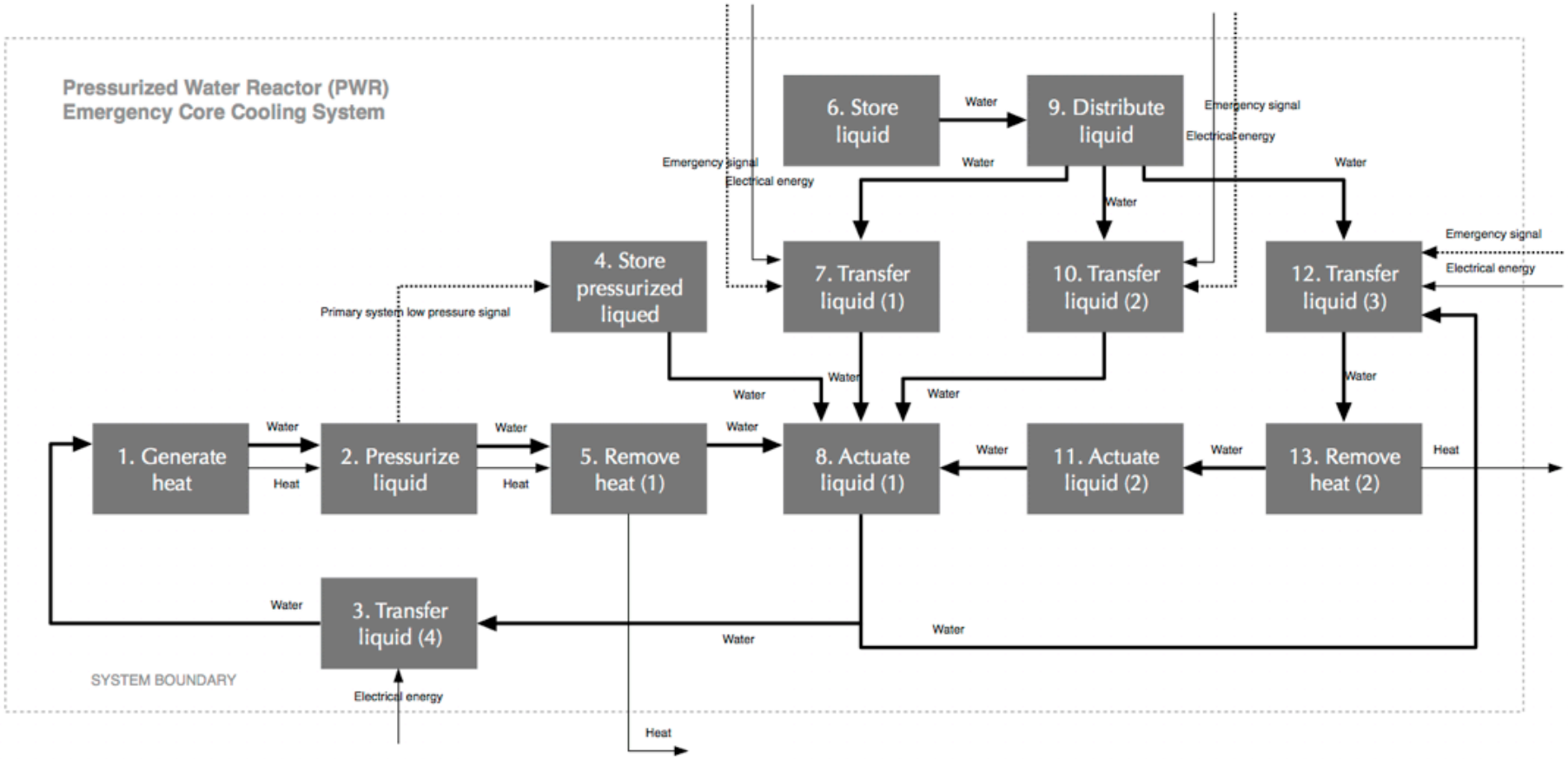


Function Failure Propagation Potential Methodology (FFPPM)

- Function Failure Propagation Potential Methodology (FFPPM)
- 1) Functional Block Diagrams (FBDs) are expressed as graphs
- 2) Identify functional failure modes
- 3) Identify failure's effected variables
- 4) Update the graph with failures
- 5) Quantifying Graph Failure Propagation Potential

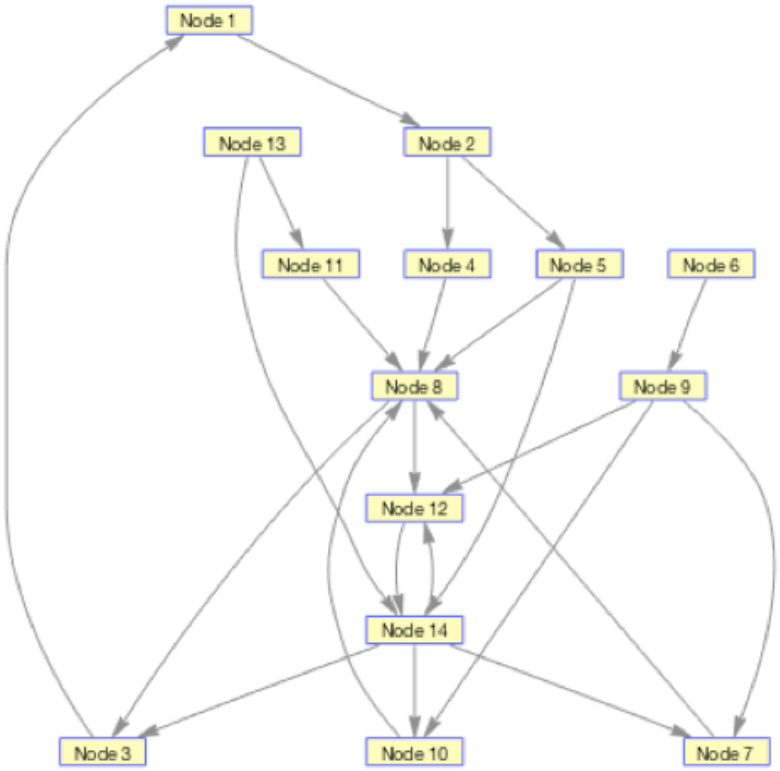
Function Failure Propagation Potential Methodology (FFPPM)

- FFPPM begins with a functional block diagram (FBD)



Function Failure Propagation Potential Methodology (FFPPM)

- **1) FBDs are expressed as graphs**
- The FBD needs to be quantifiable using methods in network science



Nominal connections have values of 1

$$FBD : PWR_{Nominal} = \begin{bmatrix} 0&2&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&2&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&1&0&0&1&0&1&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&1 \\ 0&0&1&0&0&0&2&0&0&2&0&2&0&0&0 \end{bmatrix}$$

Function Failure Propagation Potential Methodology (FFPPM)

- **2) Identify functional failure modes**
- Remember that the physical architecture does not yet exist
- Past research, FFRDM, connections functions to failure modes
- FFRDM includes failure rates, not just occurrences

	Store liquid (includes 'store pressurized liquid')	Distribute liquid	Transfer liquid (x4)	Actuate liquid (x2)	Remove heat (x2) (export thermal energy)	Generate heat (import thermal energy)	Pressurize liquid (regulate pneumatic energy)
Failure	**Failure Rate (Failure per Million Hours)**						
Breakdown, time dependent dielectric	0	2.0E-04	0	0	0	0	0
Contamination	0	0	0	0	2.0E-04	1.0E-04	0
Control issue	5.0E-03	0	0	1.2E-03	1.3E-02	6.0E-04	0
Corrosion	4.0E-03	5.8E-03	4.0E-04	0	1.3E-02	3.0E-04	0
Cracking	2.0E-04	4.0E-04	1.2E-03	0	1.5E-02	6.0E-03	1.1E-03
Creep	0	7.0E-04	2.4E-03	6.0E-04	1.0E-02	4.1E-03	4.0E-03
Direct chemical attack	0	0	4.8E-03	0	2.6E-03	1.3E-03	4.9E-03
Failure mechanism	2.0E-04	1.2E-03	4.4E-03	0	1.3E-02	6.1E-03	6.2E-03
Fatigue	0	3.0E-04	0	0	0	0	0
Fretting	0	7.0E-04	4.0E-04	0	6.0E-04	3.0E-04	1.0E-04
Galling and seizure, seizure	0	2.0E-04	0	8.0E-04	1.3E-02	5.9E-03	0
Impact, deformation	0	0	0	0	2.0E-04	1.0E-04	0
Latch-up	6.0E-04	0	0	0	1.2E-03	0	0
Noise	0	1.0E-04	0	0	8.0E-04	0	0
Other	6.0E-04	3.0E-04	8.0E-04	4.0E-04	1.0E-02	3.3E-03	1.2E-03
Overstress of incorrect current magnitude	8.0E-04	1.0E-04	0	4.0E-04	1.0E-02	3.5E-03	0
Rupture	0	2.0E-04	4.0E-04	0	2.0E-04	0	4.0E-04
Unknown	0	1.1E-03	2.0E-03	3.6E-03	3.5E-02	1.5E-02	5.7E-03
Wear	4.0E-04	3.6E-03	1.2E-02	5.2E-03	2.0E-01	9.2E-02	1.2E-02

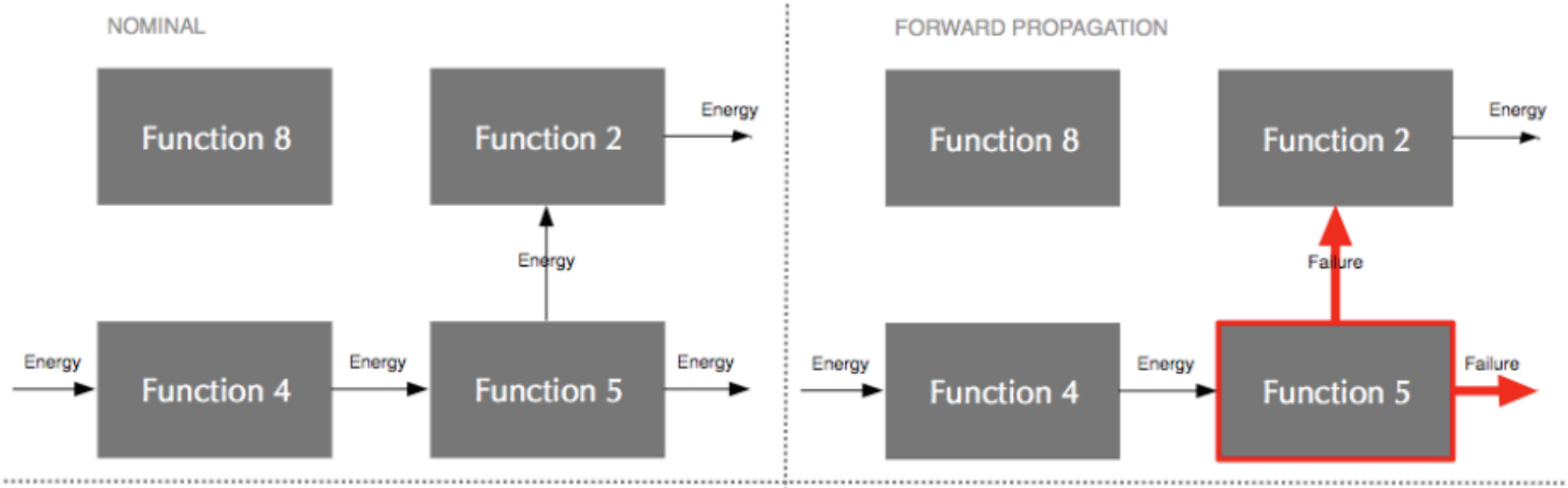
Function Failure Propagation Potential Methodology (FFPPM)

- **3) Identify failure's effected variables**
- The Functional Basis Naming Taxonomy is used to determine the variables affected in a propagation path.

FBED flow hierarchy	FBED flow and definition	Behavior variable (*New)	Variable des.
Material	**Human**. All or part of a person who crosses the device boundary.	*volume, *location	
	Gas. Any collection of molecules characterized by random motion and the absence of bonds between the molecules.	*volume, *location, *chemical elements	V, L, Ce
	Liquid. A readily flowing fluid, specifically having its molecules moving freely with respect to each other, but because of cohesive forces, not expanding indefinitely.	*volume, *location, *chemical elements	V, L, Ce
	Solid. Any object with mass having a definite, firm shape.	*volume, *dimensions, *location, *chemical elements	V, L, D, Ce
	Plasma. A collection of charged particles that is electrically neutral exhibiting some properties of a gas, but differing from a gas in being a good conductor of electricity and in being affected by a magnetic field.	*volume, *location, *chemical elements	V, L, Ce
	Mixture. A substance containing two or more components which are not in fixed proportions, do not lose their individual characteristics and can be separated by physical means.	*volume, *location, *chemical elements	V, L, Ce
	Human. Work performed by a person on a device.	force, velocity	F, Ve
	Acoustic. Work performed in the production and transmission of sound.	pressure, particle velocity	P, Pv
	Biological. Work produced by or connected with plants or animals.	pressure, volumetric flow	P, Vf
	Chemical. Work resulting from the reactions by which substances are produced		

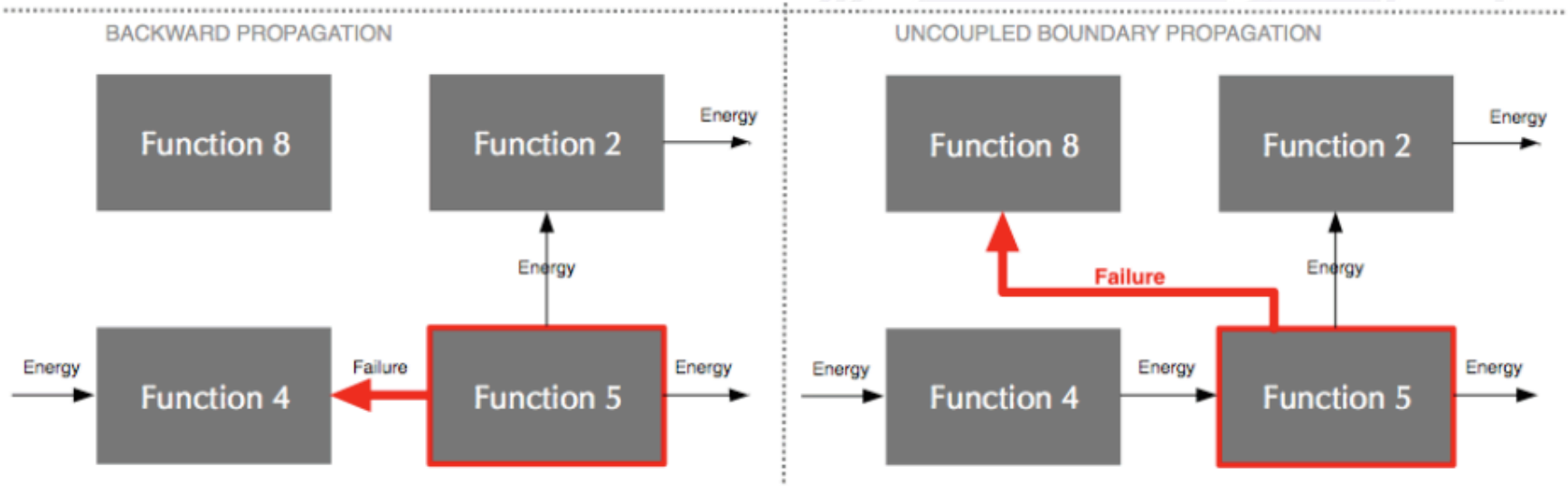
How do failures propagate?

- *Forward propagation:* This propagation is in the direction of the flow (e.g., SW command not sent, inadvertent software command, no flow due to failed pump, etc.)



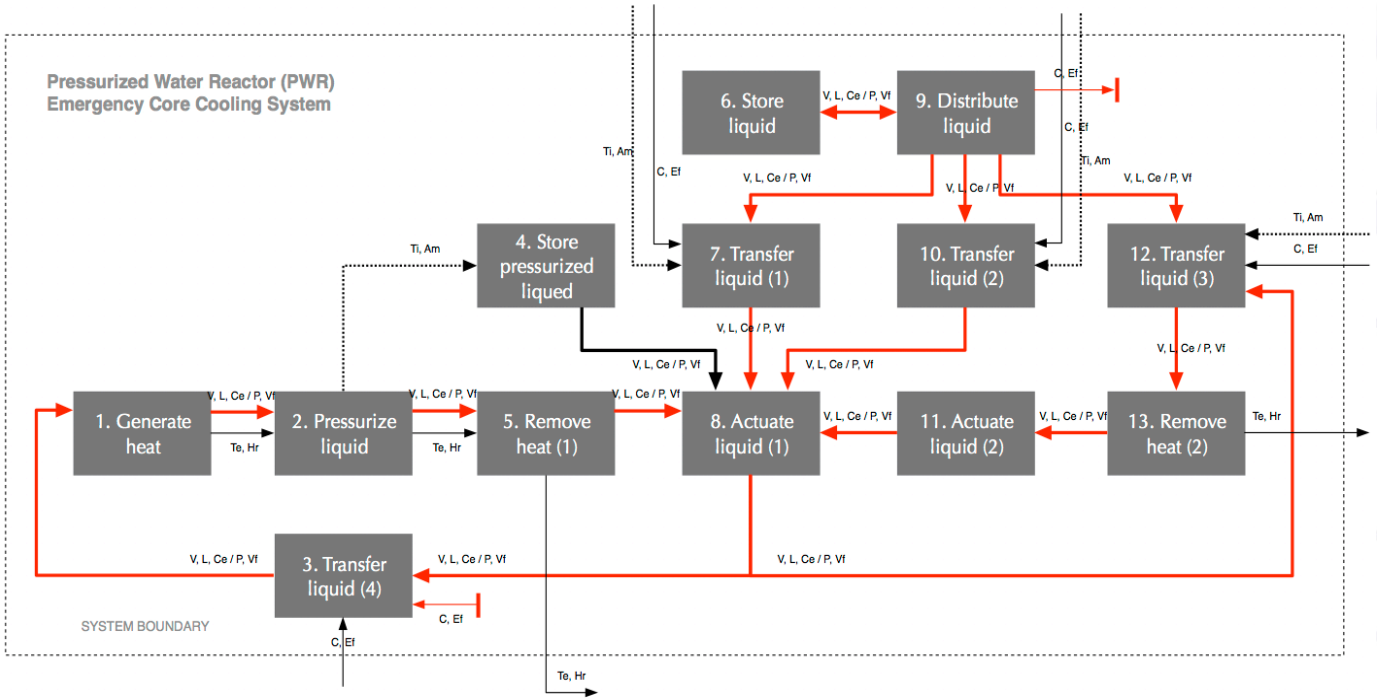
How do failures propagate?

- *Backward propagation:* Failure propagates against the nominal direction of the material, energy, and signal flows (e.g., pressure from valve stuck closed).
- *Uncoupled boundary propagation:* failure propagates between functions that were not intended to interact (e.g., shrapnel or debris from explosion, heat, vibration, etc.)



Function Failure Propagation Potential Methodology (FFPPM)

- **3) Identify failure's effected variables (continued)**
- The variables that a failure mode effects should first be determined, then these are traced throughout the system



Function Failure Propagation Potential Methodology (FFPPM)

- **4) Update the graph with failures**
- Two types of connections (1. was done in step 1)
- 1. *Nominal connections:* Connections that are present in the nominal FBD (i.e., provided prior to applying this method) have a weight equal to 1.
- 2. *Failure propagation paths* that are likely to occur have a weight equal to λ of the failure.
  - Note: λ is distributed to all connections along the path
  - Promotes mitigating longer propagation paths

Function Failure Propagation Potential Methodology (FFPPM)

- **4) Update the graph with failures**

Step 1 to Step 4

$$FBD:PWR_{Nominal}=\begin{bmatrix}
0&2&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&2&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&1&0&0\\
0&0&0&0&0&0&1&0&0&1&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&0&1&0&0&0&2&0&0&2&0&2&0&0
\end{bmatrix}$$

$$FBD:PWR_{FailProp}=\begin{bmatrix}
0&2.5&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1.0&2.5&0&0&0&0&0&0&0&0&0\\
1.5&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1.0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1.5&0&0&0&0&0&1.0\\
0&0&0&0&0&0&0&0&1.0&0&0&0&0&0\\
0&0&0&0&0&0&0&1.0&0.5&0&0&0&0&0\\
0&0&1.5&0.5&0&0&0.5&0&0&0.5&0&1.5&0&0\\
0&0&0&0&0&0.5&1.0&0&0&1.0&0&1.0&0&0\\
0&0&0&0&0&0&0&1.0&0.5&0&0&0&0&0\\
0&0&0&0&0&0&0&1.5&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0.5&0&0&0&0.5&1.0\\
0&0&0&0&0&0&0&0&0&0&1.5&0&0&1.0\\
0&0&1.0&0&0&0&2.0&0&0&2.0&0&2.0&0&0
\end{bmatrix}$$

Function Failure Propagation Potential Methodology (FFPPM)

- **5) Quantifying Graph Failure Propagation Potential**
- Quantifications use the following;
  - (1) the number of paths between functions i and j.
  - (2) the reachability between functions i and j, and

Function Failure Propagation Potential Methodology (FFPPM)

- **5) Quantifying Graph Failure Propagation Potential**
- The figure below shows the total number of paths between two nodes (i.e., functions)
  - Highly connected nodes represent more paths *(expected)*

To node \ From node	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	n/a	373	1	179	194	179	80	68	68	80	223	95	183	126
2	1	n/a	1	179	194	179	80	68	68	80	223	95	183	126
3	27	373	n/a	179	194	179	80	68	68	80	223	95	183	126
4	27	27	27	n/a	131	198	71	35	78	71	198	110	175	112
5	1	1	1	179	n/a	179	80	68	68	80	223	95	183	126
6	79	79	79	89	96	n/a	27	47	1	27	157	75	142	77
7	130	130	130	187	205	336	n/a	137	186	123	173	139	299	160
8	72	72	72	135	97	198	51	n/a	78	51	173	105	159	112
9	79	79	79	89	96	209	27	47	n/a	27	157	75	142	77
10	130	130	130	187	205	336	123	137	186	r/a	329	139	299	160
11	55	55	55	75	90	110	49	37	44	49	n/a	1	1	89
12	55	55	55	75	90	110	49	37	44	49	191	n/a	280	89
13	55	55	55	75	90	110	49	37	44	49	191	1	n/a	89
14	61	61	61	145	39	215	98	70	84	98	273	47	166	n/a

Function Failure Propagation Potential Methodology (FFPPM)

- **5) Quantifying Graph Failure Propagation Potential**
- A cell Xi, j in R(G) represents the number of "steps" required to traverse the graph from function i to j
- Note that fractions are used because the previous matrix was not whole numbers

$$R(G): PWR_{FailProp} = \begin{bmatrix} 0 & 2.5 & 3.5 & 3.5 & 5.1 & 4.6 & 3.5 & 4.5 & 4.0 & 3.5 & 5.6 & 3.5 & 4.1 & 4.5 \\ 2.5 & 0 & 1.0 & 1.0 & 2.5 & 2.0 & 1.0 & 2.0 & 1.5 & 1.0 & 3.1 & 1.0 & 1.5 & 2.0 \\ 1.5 & 4.1 & 0 & 5.1 & 6.6 & 6.1 & 5.1 & 6.1 & 5.6 & 5.1 & 7.1 & 5.1 & 5.6 & 6.1 \\ 1.5 & 4.1 & 0 & 0 & 6.6 & 1.0 & 0 & 1.0 & 0.5 & 0 & 2.1 & 0 & 0.5 & 1.0 \\ 3.5 & 6.1 & 2.0 & 2.0 & 0 & 3.1 & 2.0 & 1.5 & 2.5 & 2.0 & 4.1 & 2.0 & 2.6 & 1.0 \\ 1.5 & 4.1 & 0 & 1.5 & 6.6 & 0 & 0 & 1.0 & 0.5 & 0 & 2.1 & 0 & 0.5 & 1.0 \\ 2.0 & 4.6 & 0.5 & 1.5 & 7.1 & 1.0 & 0 & 1.0 & 0.5 & 1.0 & 3.1 & 1.0 & 1.6 & 2.0 \\ 2.0 & 4.6 & 0.5 & 0.5 & 7.1 & 1.5 & 0.5 & 0 & 1.0 & 0.5 & 2.6 & 0.5 & 1.0 & 1.5 \\ 1.5 & 4.1 & 0 & 2.0 & 6.6 & 0.5 & 0.5 & 1.5 & 0 & 0.5 & 2.6 & 0.5 & 1.0 & 1.5 \\ 2.0 & 4.6 & 0.5 & 1.5 & 7.1 & 1.0 & 1.0 & 1.0 & 0.5 & 0 & 3.1 & 1.0 & 1.6 & 2.0 \\ 1.5 & 4.1 & 0 & 1.5 & 6.6 & 1.0 & 0 & 1.0 & 0.5 & 0 & 0 & 0 & 0.5 & 1.0 \\ 2.0 & 4.6 & 0.5 & 2.5 & 7.1 & 1.0 & 1.0 & 2.0 & 0.5 & 1.0 & 2.1 & 0 & 0.5 & 1.0 \\ 3.1 & 5.6 & 1.5 & 3.1 & 8.1 & 2.6 & 1.5 & 2.5 & 2.0 & 1.5 & 1.5 & 1.5 & 0 & 1.0 \\ 2.5 & 5.1 & 1.0 & 3.5 & 7.6 & 3.0 & 2.0 & 3.0 & 2.5 & 2.0 & 4.1 & 2.0 & 2.5 & 0 \end{bmatrix}$$

Function Failure Propagation Potential Methodology (FFPPM)

- **5) Quantifying Graph Failure Propagation Potential**
- How does *R(G)* quantify relative to other graphs (theoretically)

Graph	sum(R(G))	Norm sum(R(G))	Interpretation
Complete graph	182	0%	Max failure propagation potential
Ring graph	1274	100%	Min failure propagation potential
Nominal PWR FBD	489	28%	Baseline failure propagation potential for nominal PWR FBD
FailProp PWR FBD	436	23%	Failure propagation potential for PWR FBD with added failure propagation

Function Failure Propagation Potential Methodology (FFPPM)

- **5) Quantifying Graph Failure Propagation Potential**
- Why are both metrics necessary?
- There are many paths between function 2 and 8, e.g., [2 5 8], [2 4 8], [2 4 7 8], […]
- The first metric captures the connection between function 2 and 8, it quantifies this with a value of 2 since the shortest path between these is 2 steps.
- In the event that function 5 has failed, one of the shortest paths are eliminated.
  - Other paths will propagate the failure. e.g., [2 4 8], and [2 4 7 8]
- Thus, the metrics address different aspects of the failure propagation potential.

Limitations of the work

- This work…
  - says nothing about the ***severity*** or ***timing*** of the failure
  - is derived based on historical data, which has (as always) uncertainty
  - assumes the FBD precedes the physical architecture

Summary of this work

- Due to how systems are being designed, the FFPPM has been developed to quantify failure propagation.
- The method is specific to early design when no physical architecture has been developed.
- The importance of the method is in being used to develop metrics – thus steer the design.

Future development of this work

- Since not all connections in the FBD are equally used during the system's operation, this work will move toward a more rigorous determination of the initial connection weights.
- The inclusion of failure severity will also be included.

Thanks for your time

QUESTIONS