

# Demystifying ICS Cyber Risk

ICS Cyber Security Conference 2018

Mike Radigan, Director, OT Strategy

Leidos Cyber, Inc.

radiganm@Leidos.com



# Demystifying ICS Cyber Risk – How much \$\$ should you care?

**Table B.5: Relative Risk of TADS AC Circuit 200 kV+ Events by ICC (2013–2017)**

Group of TADS events	Probability that an Event from a Group Starts during a Given Hour	Expected Impact (Expected TOS of an Event)	Risk Associated with a Group per Hour	Relative Risk by Group
All TADS events 200 kV+	0.427	0.119	0.051	100.0%
Lightning	0.085	0.121	0.010	20.2%
Unknown	0.090	0.113	0.010	20.1%
Weather, Excluding Lightning	0.062	0.109	0.007	13.4%
Misoperation	0.030	0.141	0.004	8.4%
Failed AC Circuit Equipment	0.032	0.107	0.0034	6.8%
Failed AC Substation Equipment	0.023	0.139	0.0032	6.4%
Contamination	0.024	0.132	0.0031	6.2%
Foreign Interference	0.026	0.094	0.0025	4.9%
Human Error (w/o Type 61 OR Type 62)	0.018	0.129	0.0023	4.5%
Fire	0.012	0.141	0.0017	3.4%
Power System Condition	0.010	0.133	0.0013	2.6%
Other	0.009	0.115	0.0010	2.0%
Combined Smaller ICC groups	0.006	0.099	0.0006	1.1%

Top Risk Issues for TADS Outage Events\*

\*Source: NERC State of Reliability Report 2018

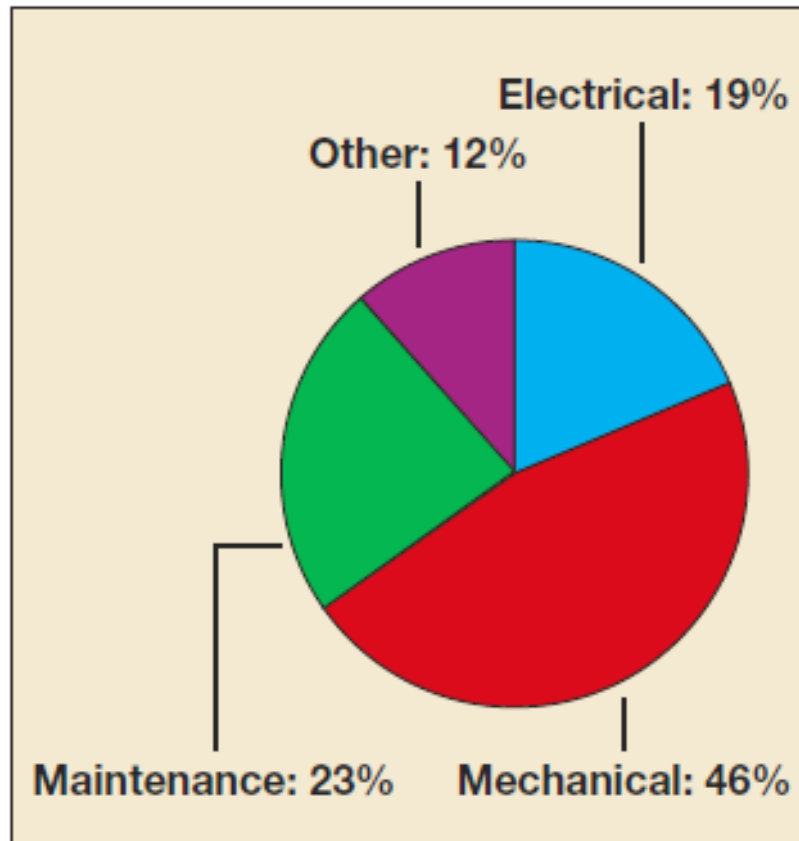
# Demystifying ICS Cyber Risk – How much \$\$ should you care?

**Table C.5: Recurring Top 10 Cause Codes**

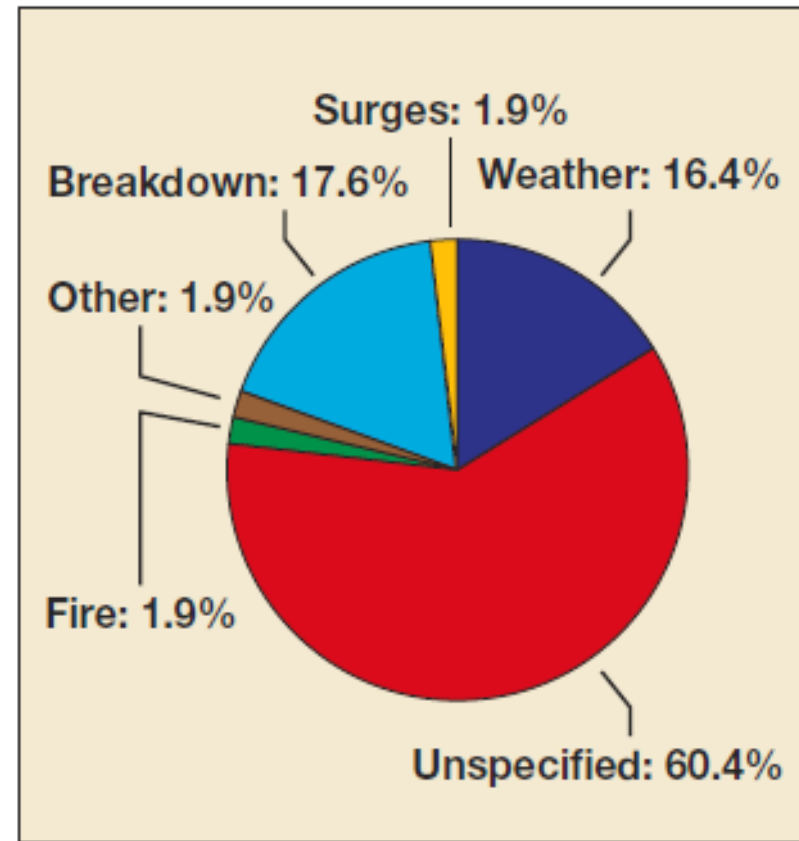
Code	Description	Number of Years in Top 10 Causes
1000	Waterwall (Furnace wall)	5
1050	Second Superheater	5
3620	Main Transformer	5
1060	First Reheater	4
4609	Other Exciter Problems	3
4520	Stator Windings, Bushings, and Terminals	3
1040	First Superheater	2
9131	Lack of Fuel (interruptible supply of fuel)	2
1090	Other Boiler Tube Leaks	2
1999	Boiler–Miscellaneous	2

\*Source: NERC State of Reliability Report 2018

# Demystifying ICS Cyber Risk – How much \$\$ should you care?



**Figure 1** Overall shutdowns  
2009-2012, %



**Figure 2** Causes of power disruptions  
2009-2012, %

Causes of Refinery Shutdowns, Source: Hydrocarbon Publishing Co.

© Leidos. All rights reserved.

# Demystifying ICS Cyber Risk

## Agenda:

- 1) Why & how it is possible to quantify cyber risk in financial terms
- 2) Prove this method is credible and enhances decision making
- 3) Case study overview & results
- 4) Q&A

# Demystifying ICS Cyber Risk: Conclusions

**You will demystify cyber risk when quantifying and normalizing it with other operational risk issues.**

- 1) Enable optimal risk management decisions
  - 1) Effective comparisons & prioritization with operational risk issues
  - 2) Results in safe, reliable & profitable operations
- 2) Enhanced communication between OT & IT
- 3) Enhanced credibility with plant / OT decision makers

# Demystifying ICS Cyber Risk

## Agenda:

- 1) **Why & how it is possible**
- 2) Prove it is credible and useful to decision making
- 3) Case study overview & results
- 4) Q&A

This presentation and white paper will be made available upon request: [radiganm@leidos.com](mailto:radiganm@leidos.com)

# Demystifying ICS Cyber Risk



## Premise:

The fundamental value (or outcome) of cyber security in an operational environment is its **effect on risk.**

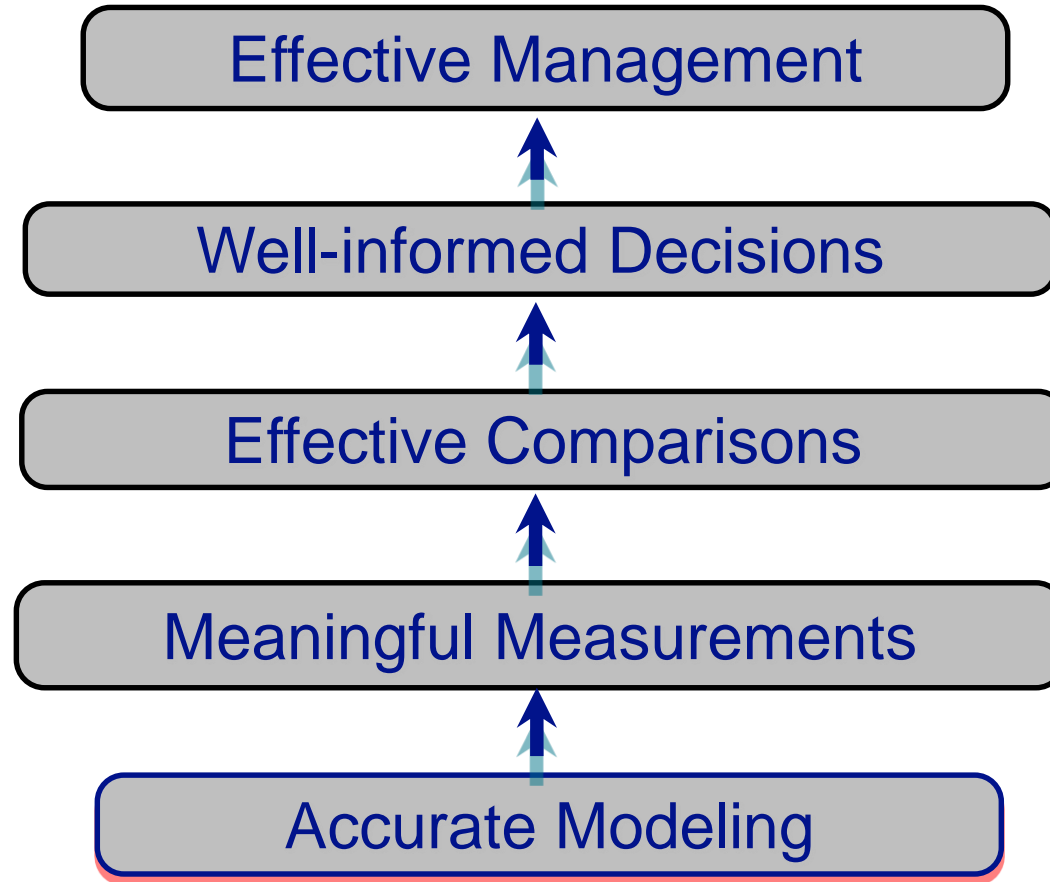
How much less risk will exist if the cyber security initiative is undertaken?

Reduction in the **probable loss event frequency**

Reduction in the **probable loss magnitude**

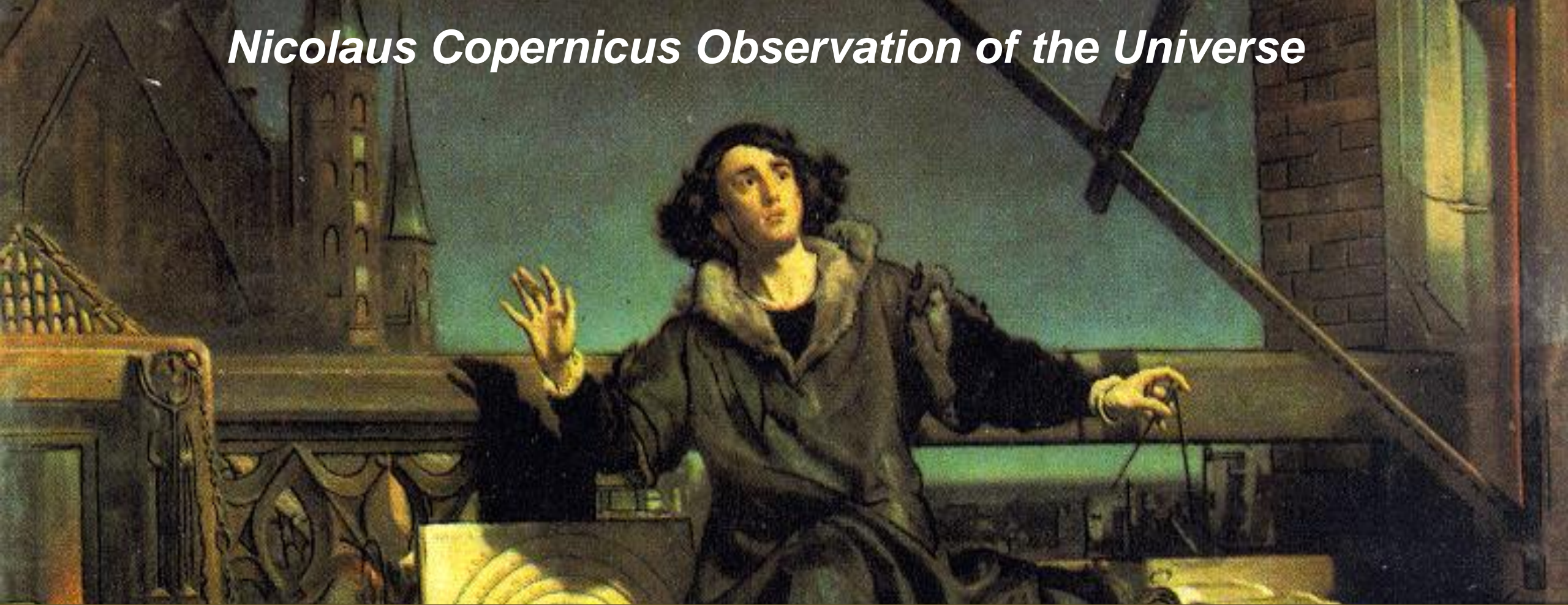


# Demystifying ICS Cyber Risk: The Objective ...



Source: Open FAIR, Risk Taxonomy (O-RT), Version 2.0

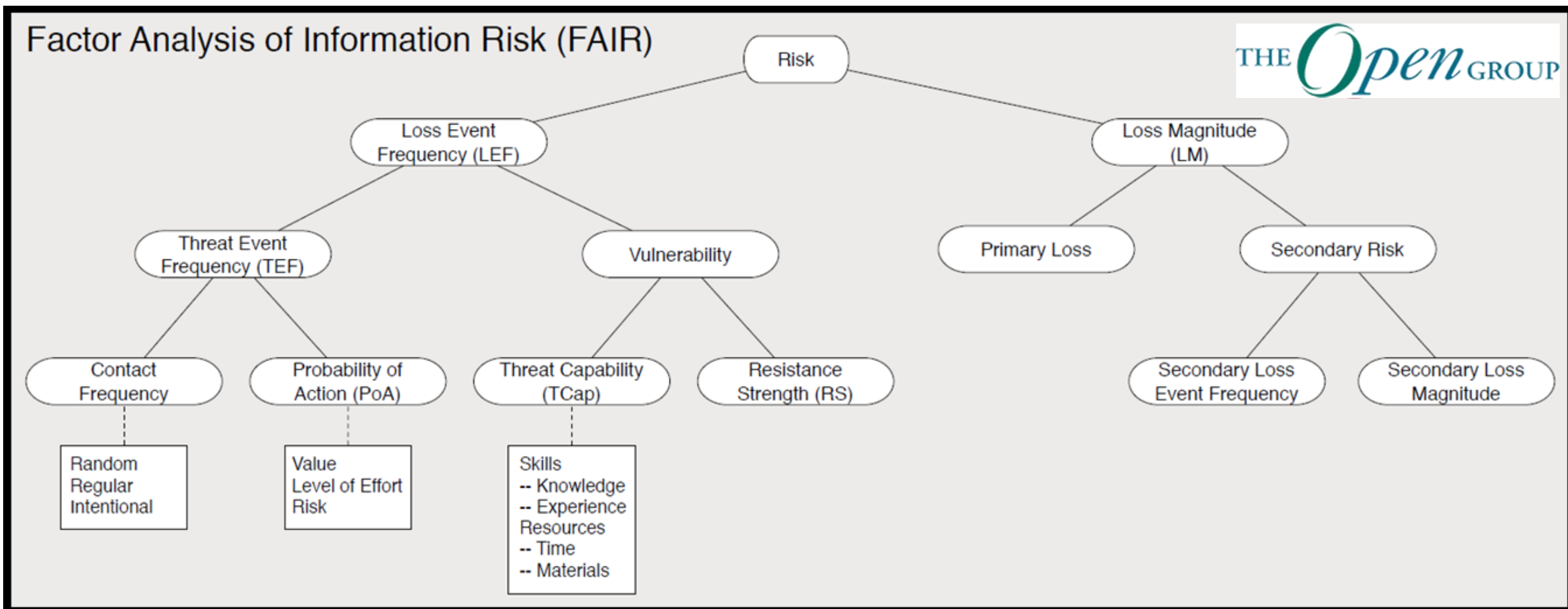
# *Nicolaus Copernicus Observation of the Universe*



FAIR is the first model to decompose risk down to its basic elements and define the effect each element has on the other.

FAIR is how risk works! It is an evolutionary understanding of risk.

# Open FAIR = “makes cyber risk quantification possible”



# Open FAIR = “makes cyber risk quantification possible”

## Factor Analysis of Information Risk (FAIR)



**Risk = the probable frequency and probable magnitude of future loss**



# Demystifying ICS Cyber Risk: Why it is possible



- Risk Taxonomy Standard (O-RT v2.0)
- Risk Analysis Standard (O-RA v2.0)
- Risk Analysis Tool (spreadsheet)



- Owns & advancing intellectual property
- RiskLens software & analytic engine

Accredited as an Industry Standard by



Complementary to Risk Frameworks



Supported by a Fast Growing Community

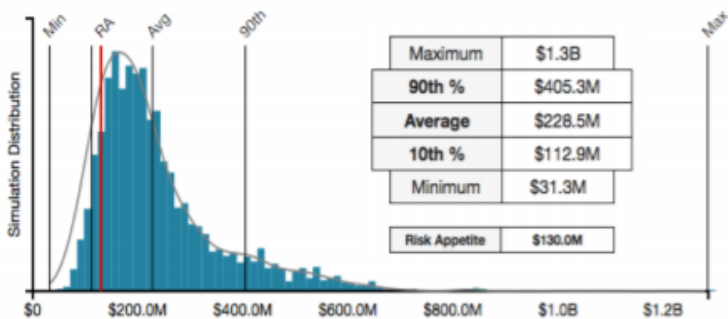


FAIR Book Inducted in Cybersecurity Canon

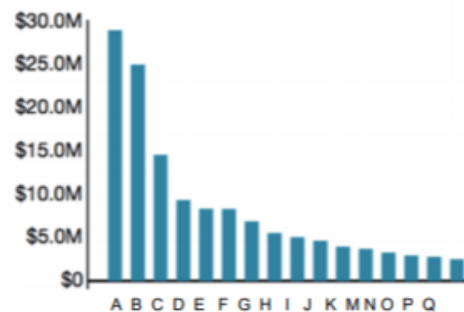


# COMMUNICATING RISK IN FINANCIAL TERMS

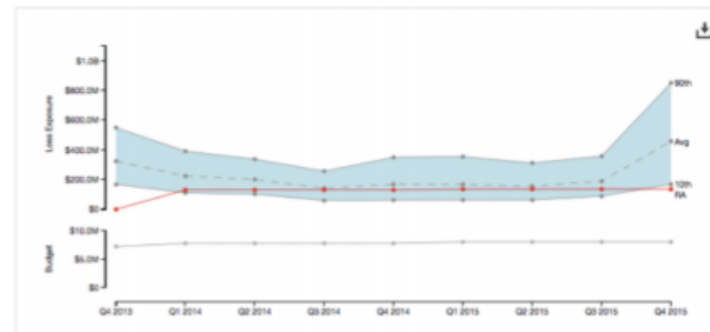
## “HOW MUCH RISK DO WE HAVE?”



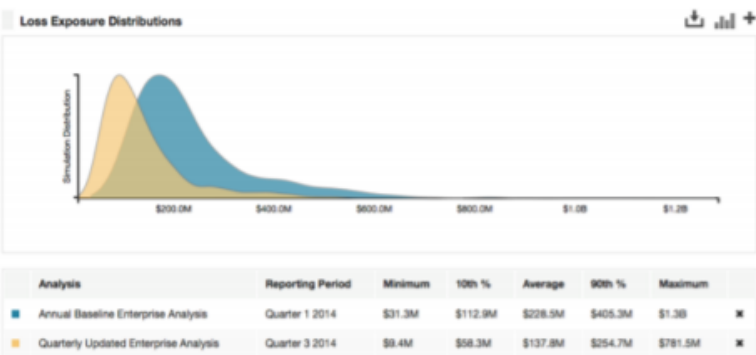
## “WHAT ARE OUR TOP RISKS?”



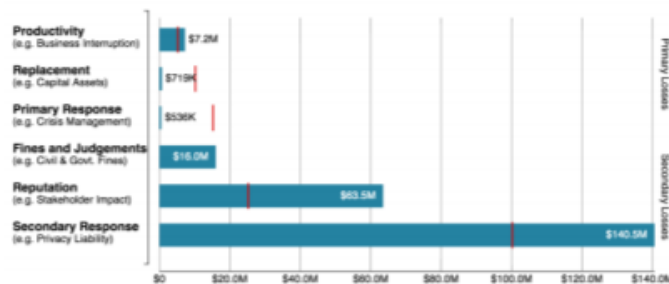
## “HOW IS RISK TRENDING VS. APPETITE?”



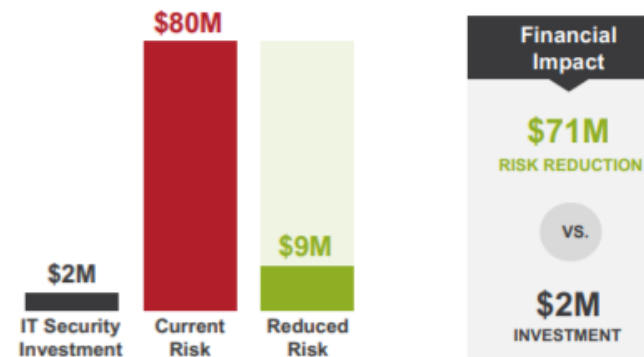
## “HAVE WE REDUCED RISK?”



## “WHAT TYPE OF LOSS CAN WE EXPECT?”

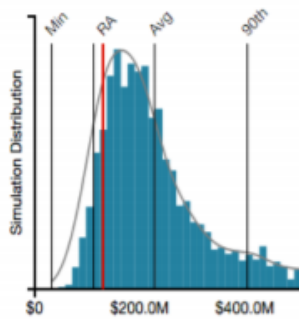


## “WHAT IS THE COST/BENEFIT OF THIS PROJECT?”

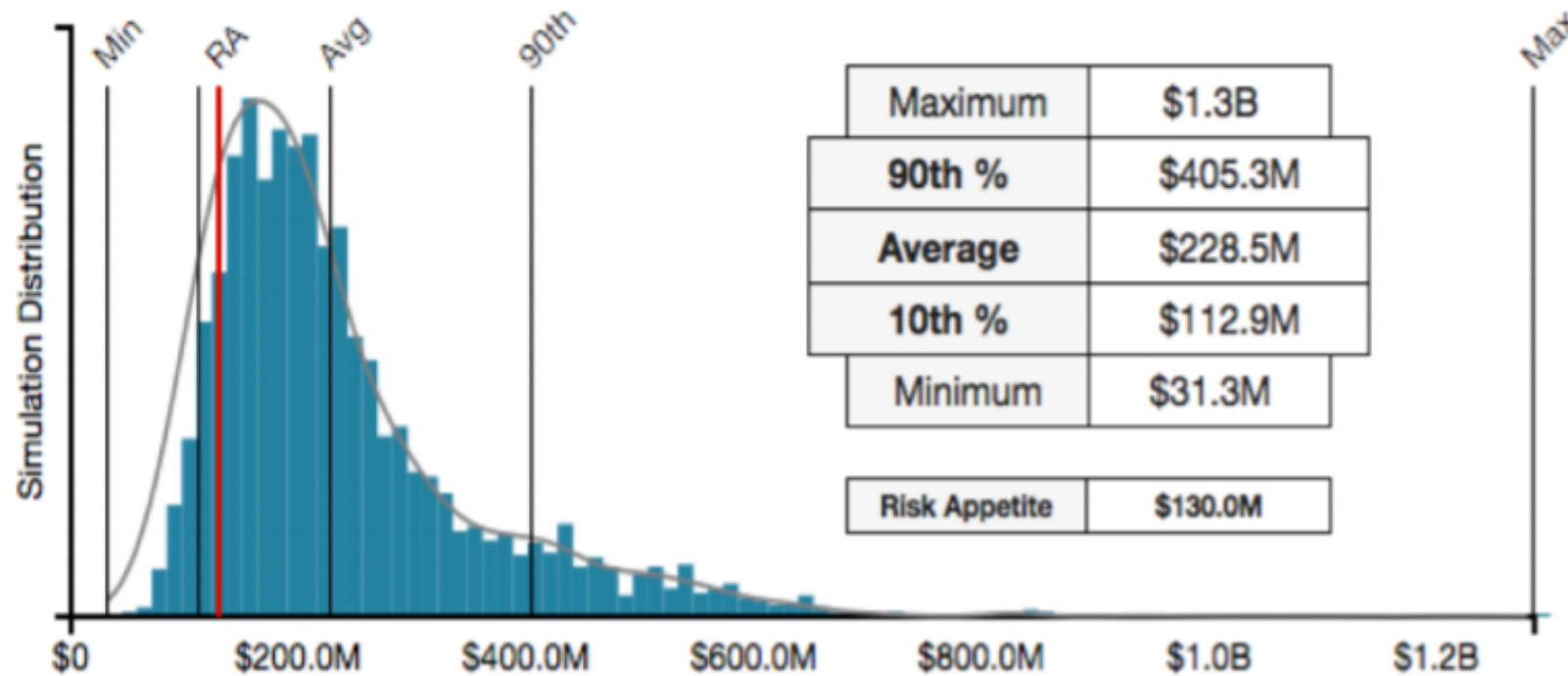


# COMMUNICATING RISK IN FINANCIAL TERMS

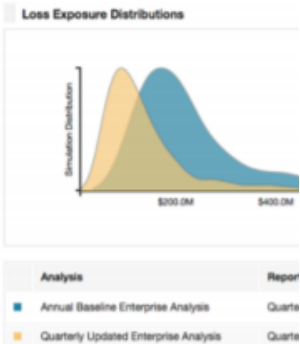
“HOW MUCH



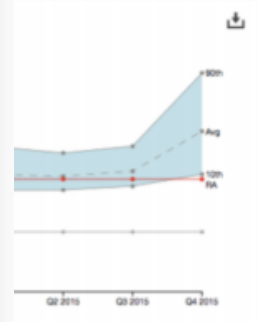
“HOW MUCH RISK DO WE HAVE?”



“HAVE W



“APPETITE?”

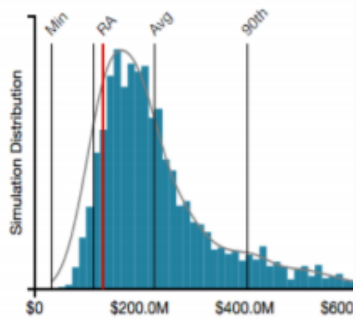


“THIS PROJECT?”



# COMMUNICATING RISK IN FINANCIAL TERMS

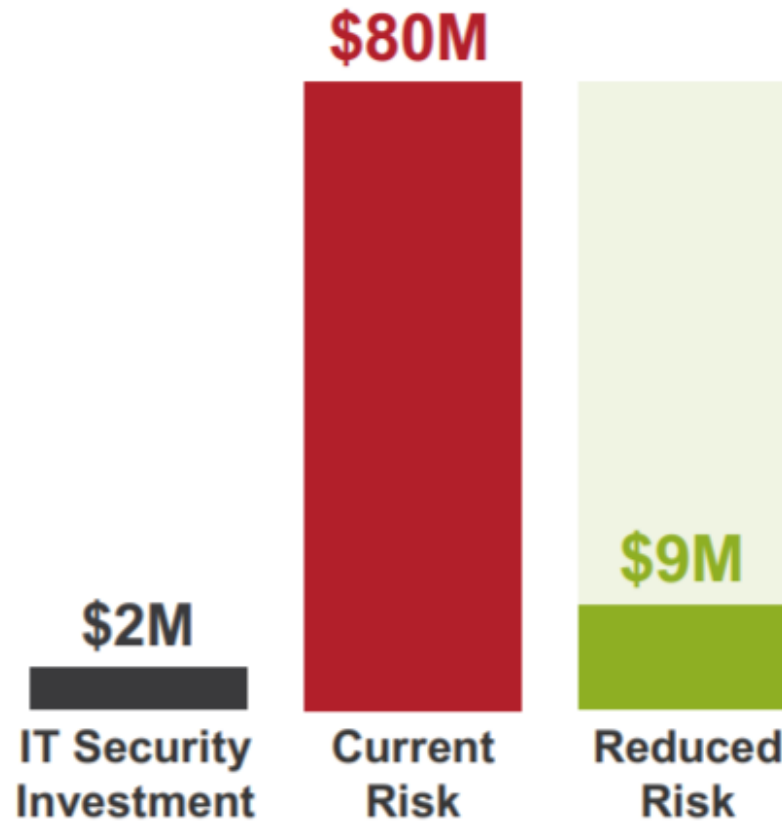
“HOW MUCH RISK?”



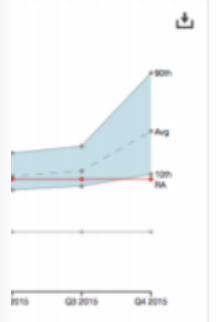
“HAVE WE RISKED?”



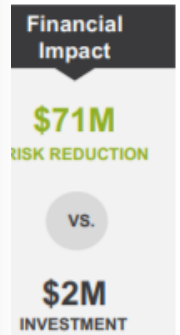
“WHAT IS THE COST/BENEFIT OF THIS PROJECT?”



“APPETITE?”



“IS PROJECT?”





# Demystifying ICS Cyber Risk

## Agenda:

- 1) Why & how it is possible to quantify cyber risk in financial terms
- 2) **Prove the FAIR method is credible**
- 3) Case study overview & results
- 4) Q&A

This presentation and white paper will be made available upon request:

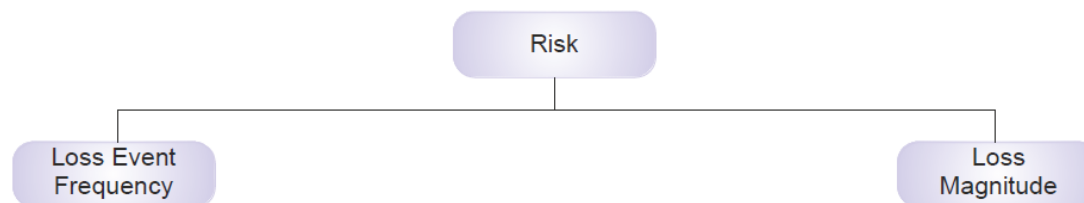
[radiganm@leidos.com](mailto:radiganm@leidos.com)

# Demystifying ICS Cyber Risk: Prove the FAIR risk model is credible

## Plant Cyber Risk Assessment Project Objective:

Demonstrate how cyber risk can be quantified and normalized with other plant operational risk issues to enable well informed decisions.

- Quantify select operational risk issues at the power plant
- Quantify select cyber risk scenarios at the power plant
- Demonstrate value: prioritization, cost-benefit of mitigation options



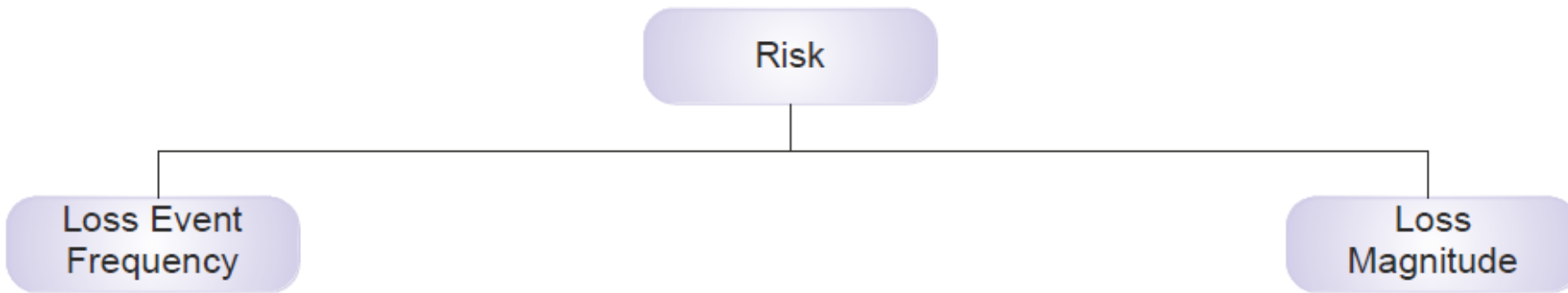
# Demystifying ICS Cyber Risk: Prove the FAIR risk model is credible

## Operational Risk Assessment Scope:

How much risk is there due to Top 4 historical failures that result in a forced outage (revenue loss)?

- Waterwall (Furnace Wall) Leaks
- First and Second Superheater Leaks
- Feedwater Pump Failure
- Generator Failure





Failure Description	Frequency Est (Failures/YR)		
	MIN	MOST LIKELY	MAX
U3 & U4 WATERWALL (FURNACE WALL) LEAKS	0.2	0.6	1
U1 & U2 WATERWALL (FURNACE WALL) LEAKS	0.2	0.4	0.8
U3 & U4 First & Second Superheater / Backpass,	0.6	0.8	1.4
U1 & U2 First & Second Superheater / Backpass,	0.4	0.5	1
U3 & U4 FEEDWATER PUMP	0.6	0.8	1.2
U1 & U2 FEEDWATER PUMP	0.2	0.8	1.2
Generator Failure	0	0.1	0.2



# Waterwall U3/U4: Physical / Mechanical Operational Risk for Power Plant A

Back

Threat Event Frequency

Vulnerability

Primary Loss Magnitude

Secondary Loss Magnitude

Guided  off

Workshop Progress

## Mechanical: Undetermined, Availability

### Loss Event Frequency -

What is the Loss Event Frequency for **Mechanical** for an event affecting **availability**?

Minimum

0.2

per year

Maximum

1

per year

Curve Shape



Confidence: High

Most Likely

0.6

per year

#### Rationale

Operations Manager provided estimates based on his experience and interpretation of cause code data. Cause code data from the past 5 years was used as a point of reference;. Event Types that resulted in a loss of revenue were included. Only Event Type "PO" was excluded. Assumption made that a % of waterwall leaks will be detected and addressed during a planned maintenance outage. This reduced the estimated number of waterwall leaks resulting in Forced Outage.

Threat Event Frequency +



# Waterwall U3/U4: Physical / Mechanical Operational Risk for Power Plant A

Back

Threat Event Frequency

Vulnerability

Primary Loss Magnitude

Secondary Loss Magnitude

Guided

 off

Workshop Progress



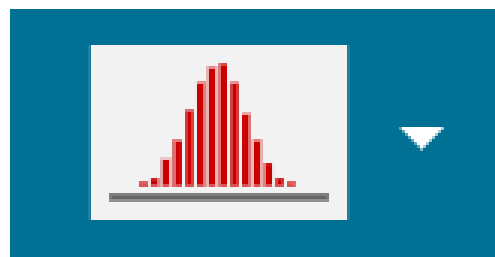
### Minimum

per year ▾

### Maximum

per year ▾

### Curve Shape



Confidence: High

Confidence: High

### Most Likely

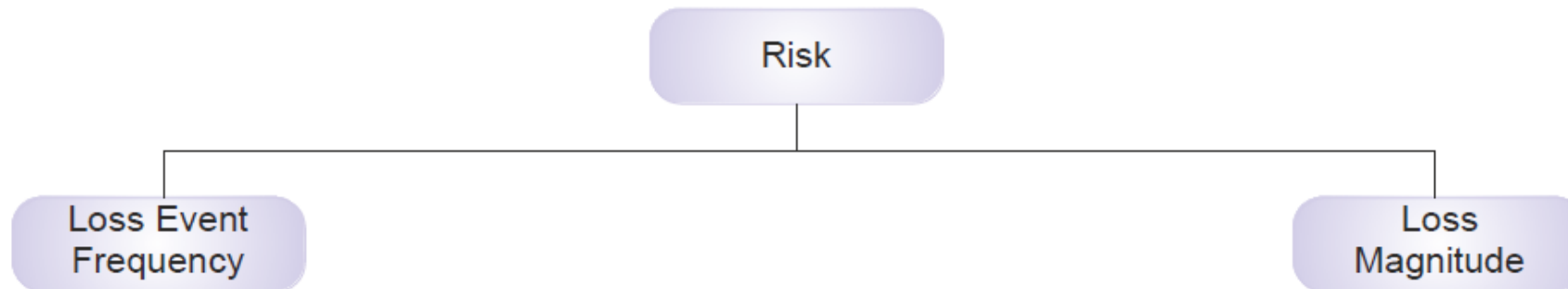
per year ▾

Rationale

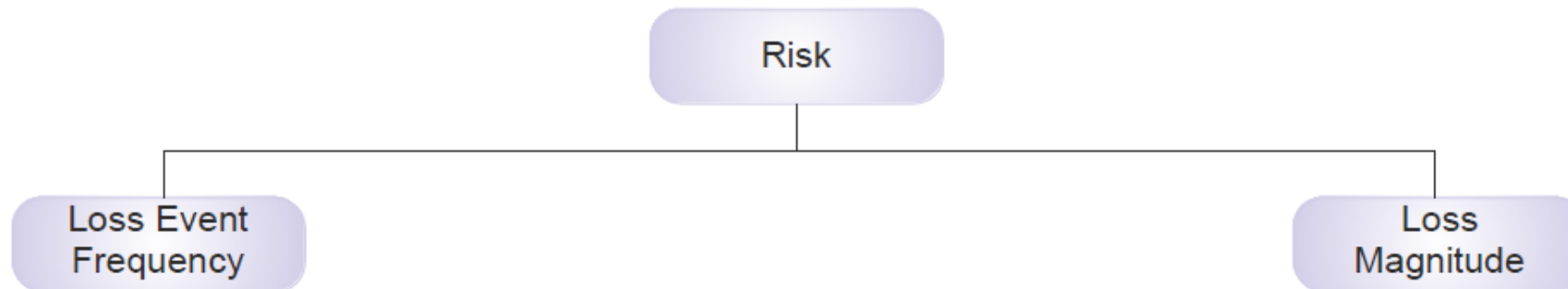
Operations Manager provided estimates based on his experience and interpretation of cause code data. Cause code data from the past 5 years was used as a point of reference;.Event Types that resulted in a loss of revenue were included. Only Event Type "PO" was excluded. Assumption made that a % of waterwall leaks will be detected and addressed during a planned maintenance outage. This reduced the estimated number of waterwall leaks resulting in Forced Outage.

Threat Event Frequency



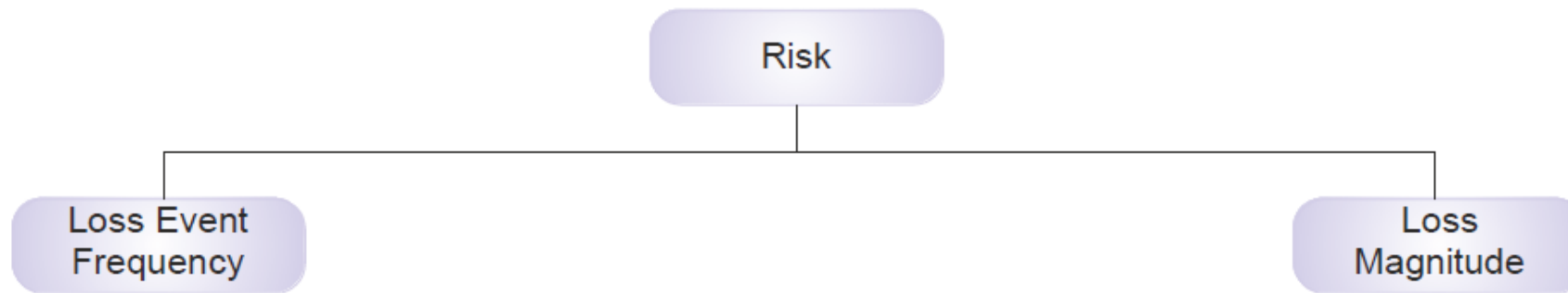


Failure Description	Duration Est (Days)			Labor Costs		
	MIN	MOST LIKELY	MAX	Minimum	Most Likely	Maximum
U3 & U4 WATERWALL (FURNACE WALL) LEAKS	5	7	9	\$ 75,000	\$ 150,000	\$ 250,000
U1 & U2 WATERWALL (FURNACE WALL) LEAKS	2	3	5	\$ 5,000	\$ 50,000	\$ 100,000
U3 & U4 First & Second Superheater / Backpass,	3	5	7	\$ 75,000	\$ 150,000	\$ 250,000
U1 & U2 First & Second Superheater / Backpass,	2	3	5	\$ 5,000	\$ 50,000	\$ 100,000
U3 & U4 FEEDWATER PUMP	1	2	10	\$ 15,000	\$ 30,000	\$ 50,000
U1 & U2 FEEDWATER PUMP	2	6	14	\$ 15,000	\$ 30,000	\$ 50,000
Generator Failure	21	60	180	\$ 500,000	\$ 700,000	\$ 3,200,000



Failure Description	Materials Cost \$		
	Minimum	Most Likely	Maximum
U3 & U4 WATERWALL (FURNACE WALL) LEAKS	\$ 5,000	\$ 10,000	\$ 25,000
U1 & U2 WATERWALL (FURNACE WALL) LEAKS	\$ 5,000	\$ 10,000	\$ 25,000
U3 & U4 First & Second Superheater / Backpass,	\$ 5,000	\$ 10,000	\$ 25,000
U1 & U2 First & Second Superheater / Backpass,	\$ 5,000	\$ 10,000	\$ 25,000
U3 & U4 FEEDWATER PUMP	\$ 60,000	\$ 175,000	\$ 400,000
U1 & U2 FEEDWATER PUMP	\$ 60,000	\$ 175,000	\$ 400,000
Generator Failure	\$ 200,000	\$ 1,200,000	\$ 5,000,000





Failure Description	Revenue Loss		
	Minimum	Most Likely	Maximum
U3 & U4 WATERWALL (FURNACE WALL) LEAKS	\$ 940,037	\$ 1,316,052	\$ 1,692,066
U1 & U2 WATERWALL (FURNACE WALL) LEAKS	\$ 596,292	\$ 894,438	\$ 1,490,730
U3 & U4 First & Second Superheater / Backpass,	\$ 564,022	\$ 940,037	\$ 1,316,052
U1 & U2 First & Second Superheater / Backpass,	\$ 596,292	\$ 894,438	\$ 1,490,730
U3 & U4 FEEDWATER PUMP	\$ 94,004	\$ 188,007	\$ 940,037
U1 & U2 FEEDWATER PUMP	\$ 298,146	\$ 894,438	\$ 2,087,022
Generator Failure *	\$ 5,104,610	\$ 7,292,000	\$ 7,292,000

\* Business Interruption Insurance: Caps revenue loss after 30 days

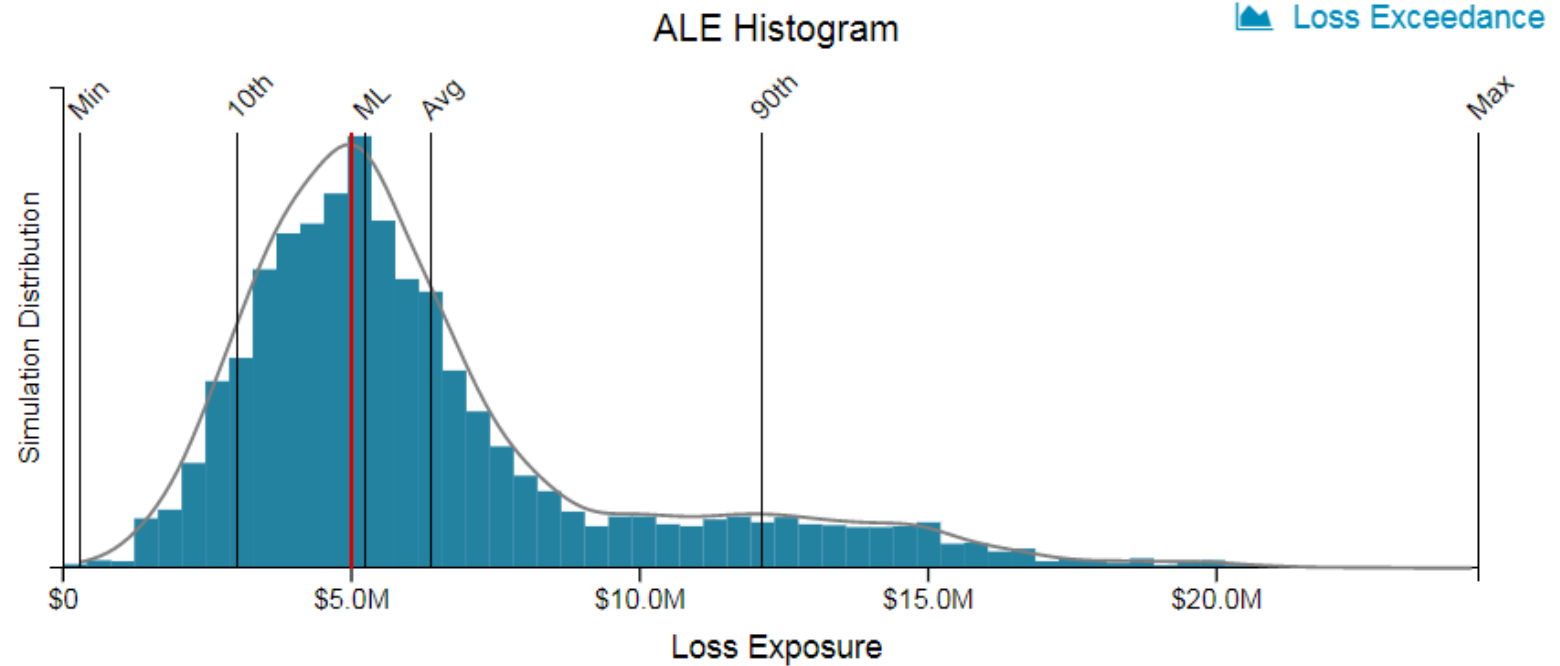
# Mechanical Operational Risk for Power Plant A

## Aggregate Loss Exposure

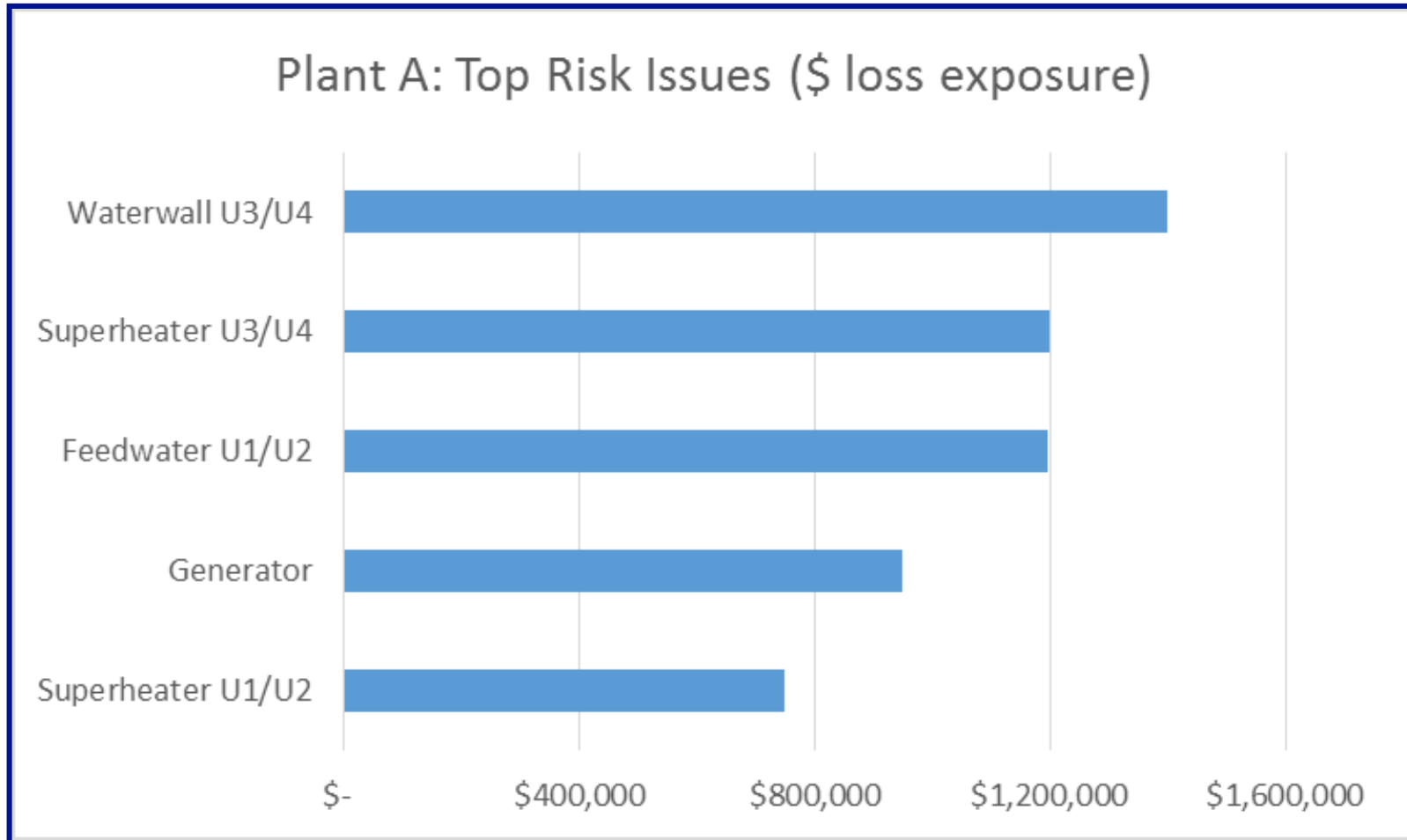
The aggregation of all independently analyzed risk scenarios.

Based on the analysis, the average loss exposure for this analysis is \$1.4M above the risk appetite.

Maximum	\$24.5M
90th %	\$12.1M
Most Likely	\$5.2M
Average	\$6.4M
10th %	\$3.0M
Minimum	\$287K
Risk Appetite	\$5.0M



# Demystifying ICS Cyber Risk: Prove FAIR risk model is credible



# Demystifying ICS Cyber Risk: FAIR model applied to cyber risk

## Proposed Project Scope:

### Cyber risk analysis at Power Station A

- Cyber incident, loss of availability, resulting in a forced outage (criminal)
- External threat communities, multiple threat vectors:
  - Criminal Level 1: non-targeted (malware, ransomware)
  - Criminal Level 2: targeted attack (malware, ransomware)
- High Level Assessment: Assets are Control System / Functional Systems



# Demystifying ICS Cyber Risk: FAIR model applied to cyber risk

## Cyber risk analysis at Power Station A

- Network isolation (“air-gapped”)
- DCS - Generator, Boiler, Air Quality, Turbine U1 & U2
- OEM Turbine controls for U3 & U4
- Obsolete HMI, Windows XP, very static system
- PI Server in former DMZ
- **Thumb drives in use for file exports / imports**
- IDE drive for backups
- Malwarebytes is the corp scanning engine
- All electronic contact w/ ICS considered threat vectors



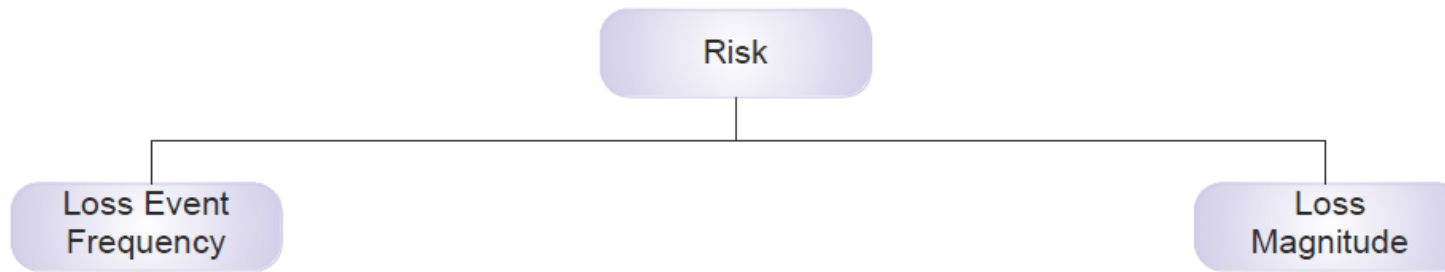
# Demystifying ICS Cyber Risk: FAIR model applied to cyber risk

## Must have visibility

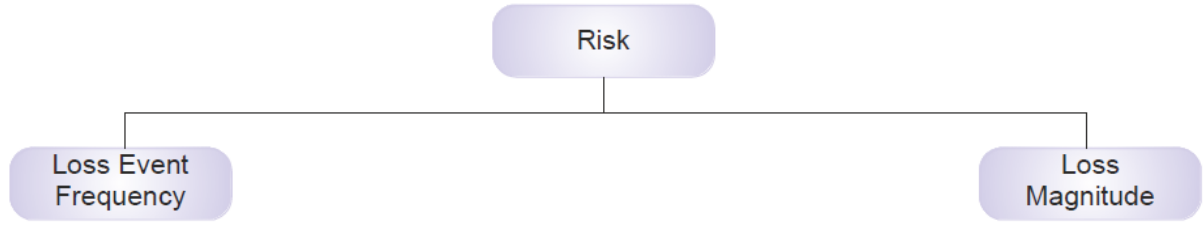
- ▶ Cyber asset inventory accuracy
- ▶ Configuration policy
- ▶ Resistive control strength
- ▶ Asset value characteristics
- ▶ Relevant threats

## Where do I get data inputs?

- ▶ All electronic access & interaction with cyber assets
- ▶ File import / export process
- ▶ Firmware updates
- ▶ Backup process
- ▶ OEM / contractor access



Failure Description	Frequency Est (Failures/YR)		
	MIN	ML	MAX
U3 & U4 WATERWALL (FURNACE WALL) LEAKS	0.2	0.6	1
U1 & U2 WATERWALL (FURNACE WALL) LEAKS	0.2	0.4	0.8
U3 & U4 First & Second Superheater / Backpass,	0.6	0.8	1.4
U1 & U2 First & Second Superheater / Backpass,	0.4	0.5	1
U3 & U4 FEEDWATER PUMP	0.6	0.8	1.2
U1 & U2 FEEDWATER PUMP	0.2	0.8	1.2
Generator Failure	0	0.1	0.2
Plant DCS, Criminal Malicious	0.2	0.35	0.5
Plant DCS, Criminal Targeted, Malicious	0.2	0.5	1
U3 & U4 Turbine Controls, Criminal Malicious	0.01	0.11	0.2
U3 & U4 Turbine Controls, Crim Targeted, Mal	0.01	0.11	0.2



Loss Event / Failure Description	Primary Revenue Loss		
	Minimum	Most Likely	Maximum
U3 & U4 WATERWALL (FURNACE WALL) LEAKS	\$ 940,037	\$ 1,316,052	\$ 1,692,066
U1 & U2 WATERWALL (FURNACE WALL) LEAKS	\$ 596,292	\$ 894,438	\$ 1,490,730
U3 & U4 First & Second Superheater / Backpass,	\$ 564,022	\$ 940,037	\$ 1,316,052
U1 & U2 First & Second Superheater / Backpass,	\$ 596,292	\$ 894,438	\$ 1,490,730
U3 & U4 FEEDWATER PUMP	\$ 94,004	\$ 188,007	\$ 940,037
U1 & U2 FEEDWATER PUMP	\$ 298,146	\$ 894,438	\$ 2,087,022
Generator Failure *	\$ 5,104,610	\$ 7,292,000	\$ 7,292,000
Plant DCS, Criminal Malicious	\$ 94,004	\$ 488,015	\$ 20,418,441
Plant DCS, Criminal Targeted, Malicious	\$ 94,004	\$ 488,015	\$ 20,418,441
U3 & U4 Turbine Controls, Criminal Malicious	\$ 94,004	\$ 244,008	\$ 10,209,221
U3 & U4 Turbine Controls, Crim Targeted, Mal	\$ 94,004	\$ 244,008	\$ 10,209,221

\* Business Interruption Insurance: Does not cover due to cyber attack



# Demystifying ICS Cyber Risk: FAIR model applied to cyber risk

## Secondary Risk Factors

- Targeted attack and/or ransomware incident causing high impact drives Secondary Risk
- Secondary loss frequency = 10%
- Organizational response would be multi-year, fleet-wide, 5 plants
  - CEO whiplash effect “Not again on my watch!”
- Investments in cyber security strategy, program, projects
- Reputational loss mitigation




# Primary Loss Data - PERT Distribution

Threat Event Frequency	Vulnerability	Primary Loss Magnitude	Secondary Loss Magnitude
------------------------	---------------	------------------------	--------------------------

Guided  Off Workshop Progress

### Primary Productivity Loss

What is the Productivity Loss for the Primary Loss Magnitude?

Minimum	Maximum	Curve Shape	Most Likely
\$94,000	\$20,418,000	 Confidence: High	\$488,000 <input checked="" type="checkbox"/>

Rationale

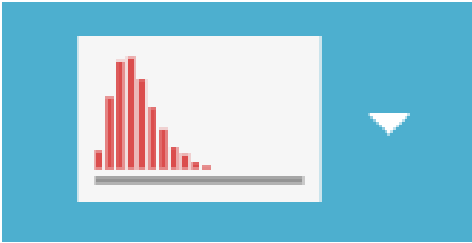
Revenue loss from a failure is calculated with an average of \$29.23 per MWH. The 2016 PJM demand mwh. Revenue Loss is limited due to the ability of the plant to operate several weeks without the Engineering Workstation (EWS) that is the most likely point of attack. The operator workstations will be unaffected, the malware cannot propagate across proprietary connectivity; The EWS can be taken off-line and remediation performed.

Last Updated by Mike Radigan, Aug 26, 2018 at 3:07pm

# Primary Loss Data - PERT Distribution

Threat Event Frequency   Vulnerability   Primary Loss Magnitude   Secondary Loss Magnitude

Guided  Off   Workshop Progress

Minimum	Maximum	Curve Shape	Most Likely
\$94,000	\$20,418,000	 Confidence: High	\$488,000 <input checked="" type="checkbox"/>

Revenue loss from a failure is calculated with an average of \$29.23 per MWh. The 2016 PJM demand mwh. Revenue Loss is limited due to the ability of the plant to operate several weeks without the Engineering Workstation (EWS) that is the most likely point of attack. The operator workstations will be unaffected, the malware cannot propagate across proprietary connectivity; The EWS can be taken off-line and remediation performed.

Last Updated by Mike Radigan, Aug 26, 2018 at 3:07pm

# Quantifying ICS Cyber Risk : DCS / Turbine Controls

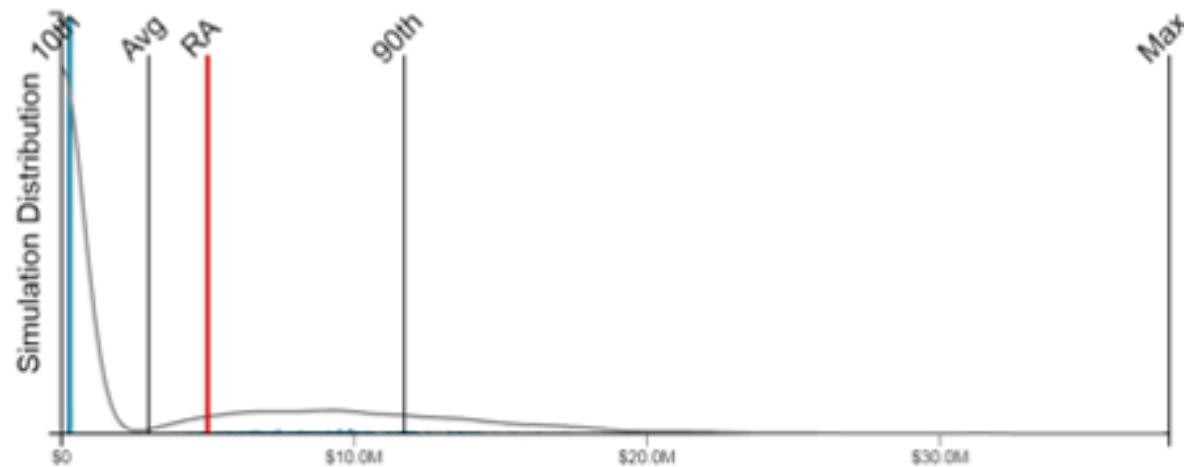
## Cyber Risk for Plant A: Summary

### Aggregate Loss Exposure

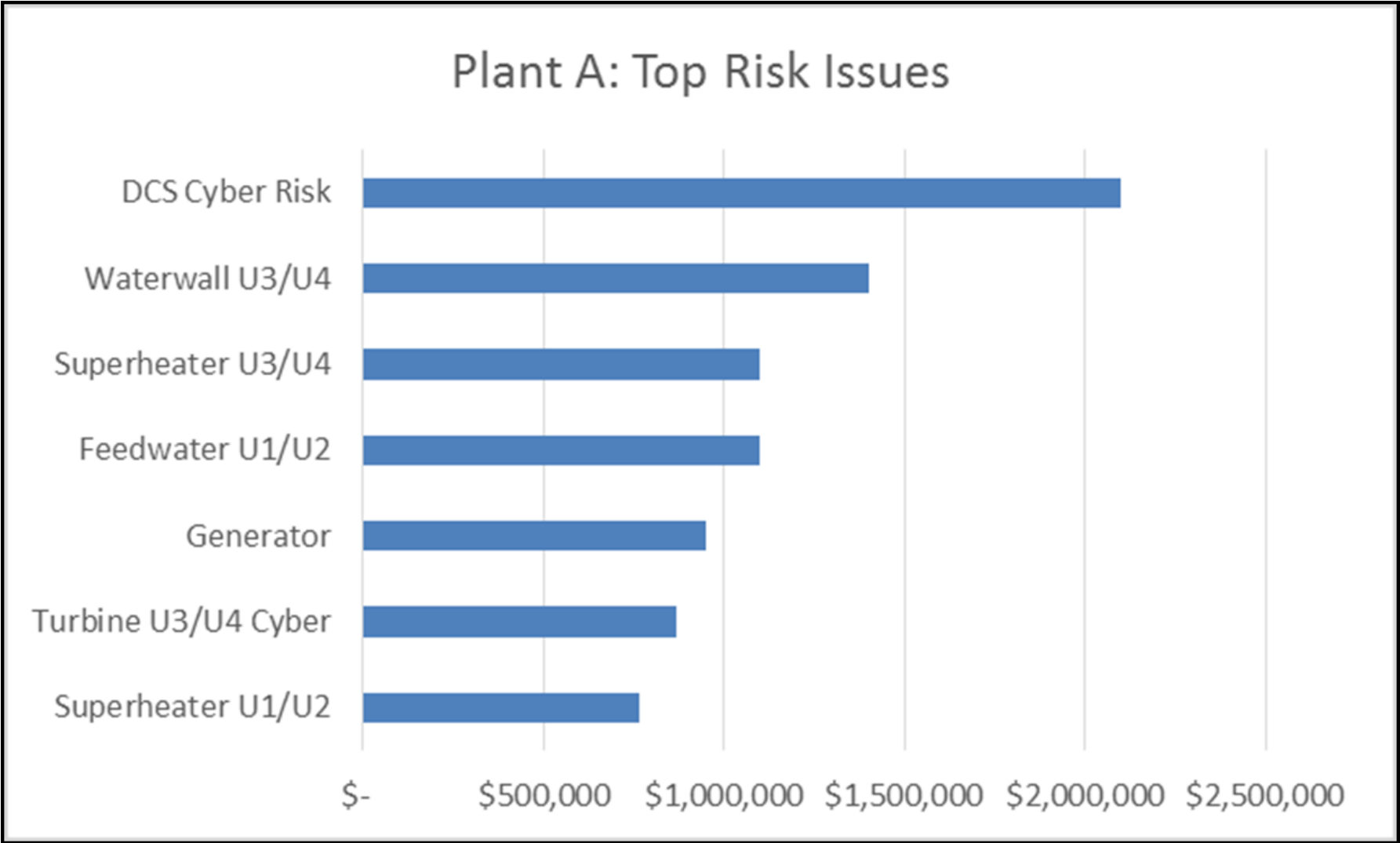
The aggregation of all independently analyzed risk scenarios.

Based on the analysis the average loss exposure for this analysis is \$2.0M below the risk appetite.

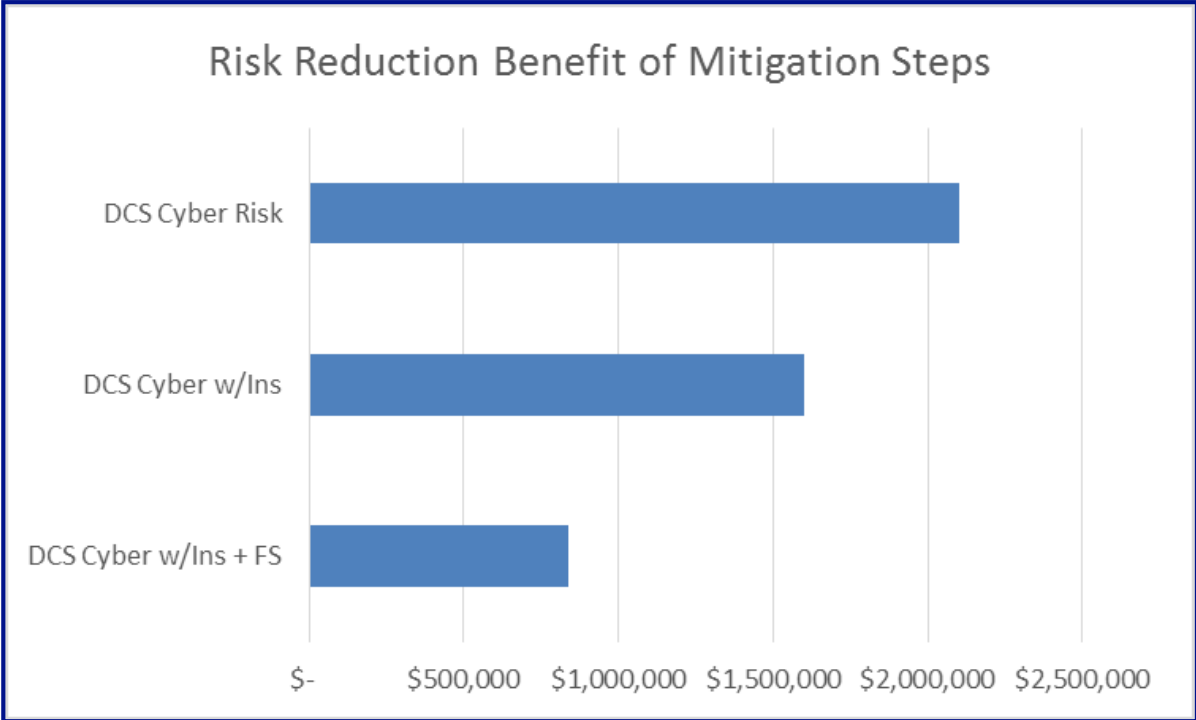
Maximum	\$37.8M
90%	\$11.7M
Average	\$3.0M
10%	\$0
Minimum	\$0



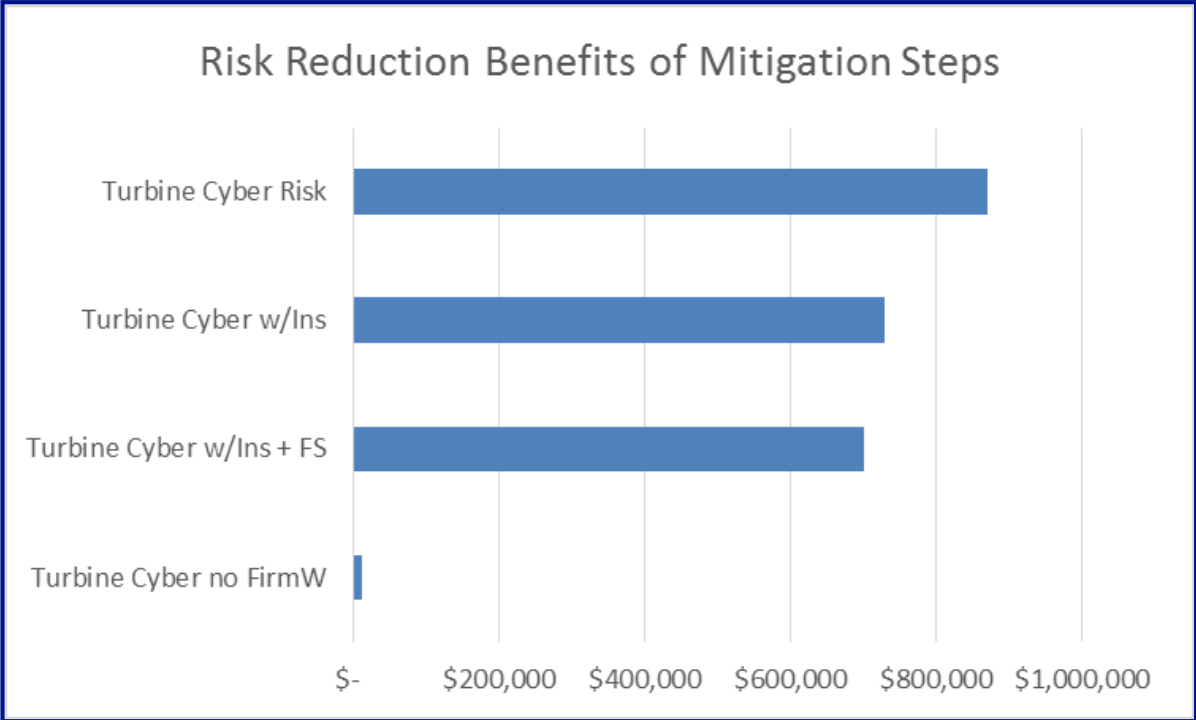
# Quantifying ICS Cyber Risk: FAIR model applied to cyber risk



# Quantifying ICS Cyber Risk: FAIR model applied to cyber risk

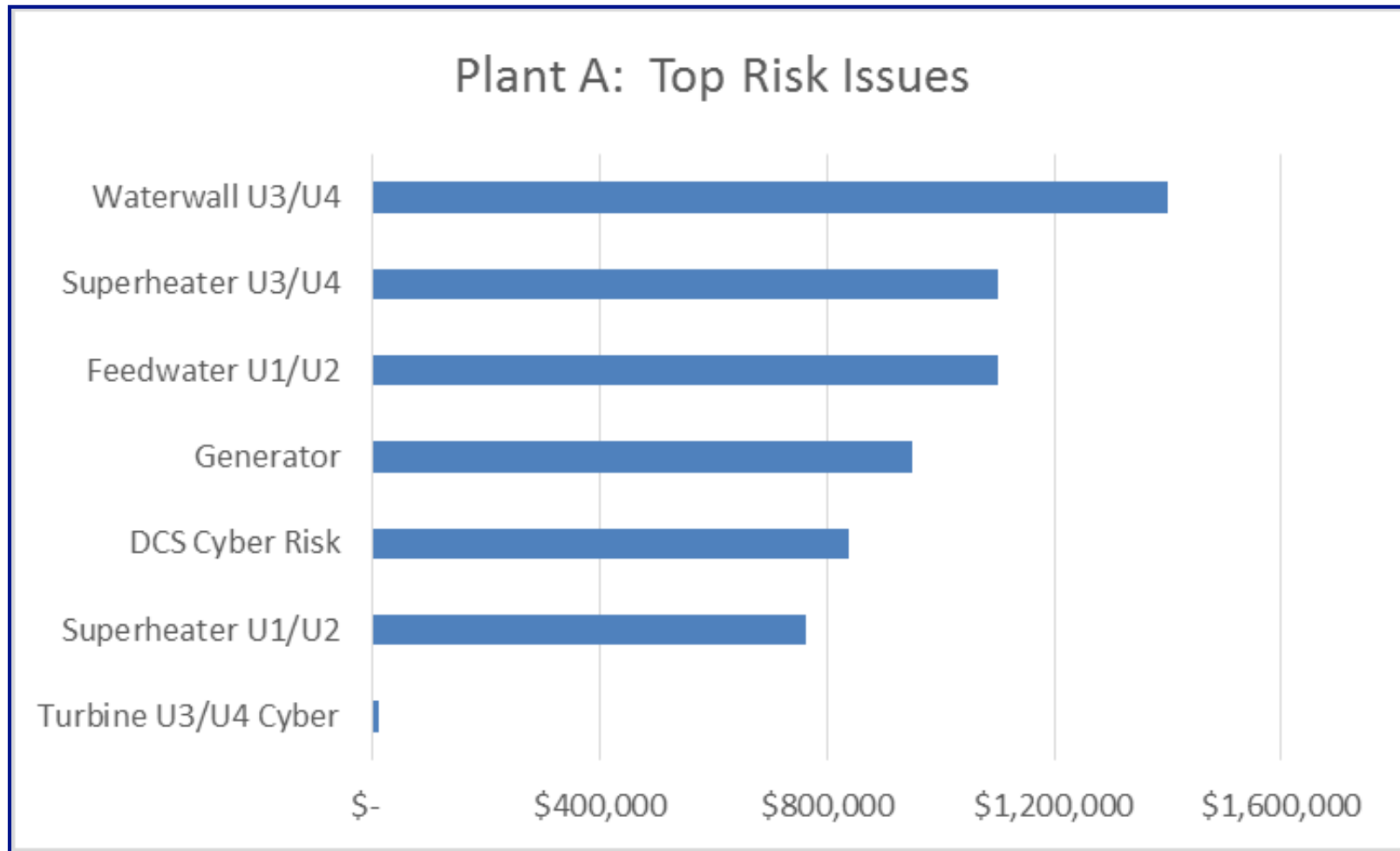


**DCS Cyber Risk Reduction:  
\$2.1M => \$841K**



**Turbine Cyber Risk Reduction:  
\$869K => \$10K**

# Demystifying ICS Cyber Risk: FAIR model applied to cyber risk



# Recommendations Supported by Cost-Benefit Analysis

**Current State:** The cyber risk associated with current state for ICS is \$2.7M.

**Mitigation Plan C:** Revise file transfer policies, implement new controls, purchase cyber insurance

**Results:** Achieve a 52% reduction in annualized loss exposure; a 38% reduction in “worst case” scenario

**Resource Requirement:** First year cost to implement plan is \$140k with annual renewal of \$90k

**Cost-Benefit Ratio:** Annual risk reduction benefit of \$1.4M. First year ratio 1:10 Second year ratio 1:15

Cost/Benefit Analysis	Ave Loss Exposure (Risk)	90% Loss Exposure	Max Loss Exposure	% Decrease (Ave)	1st Yr Cost	Ratio
Cyber Risk	\$2.7M	\$10.7M	\$45.3M			
Mitigation Plan A: Cyber Insurance	\$2.2M	\$7.6M	\$30.1M	18%	\$80k	1:6
Mitigation Plan B: File Sanitizer	\$1.5M	\$6.9M	\$35.0M	44%	\$60k	1:20
Mitigation Plan C: A&B	\$1.3M	\$6.1M	\$28.0M	52%	\$140k	1:10



# Demystifying ICS Cyber Risk: Conclusions

You will demystify cyber risk when quantifying and normalizing with other operational risk issues.

1. Enable optimal risk management decisions
  1. Effective comparisons & prioritization with operational risk issues
  2. Safe, reliable & profitable operations
2. Enhanced communication between OT & IT
3. Enhanced credibility with plant / OT decision makers

# Demystifying ICS Cyber Risk: Resources



*Established FAIR as an International Standard*

- **Standard for Risk Analysis**
- **Standard for Risk Taxonomy**
- **Certification for FAIR Analyst in Nov 2013**
- **FAIR Computational Engine (Beta in 2018)**



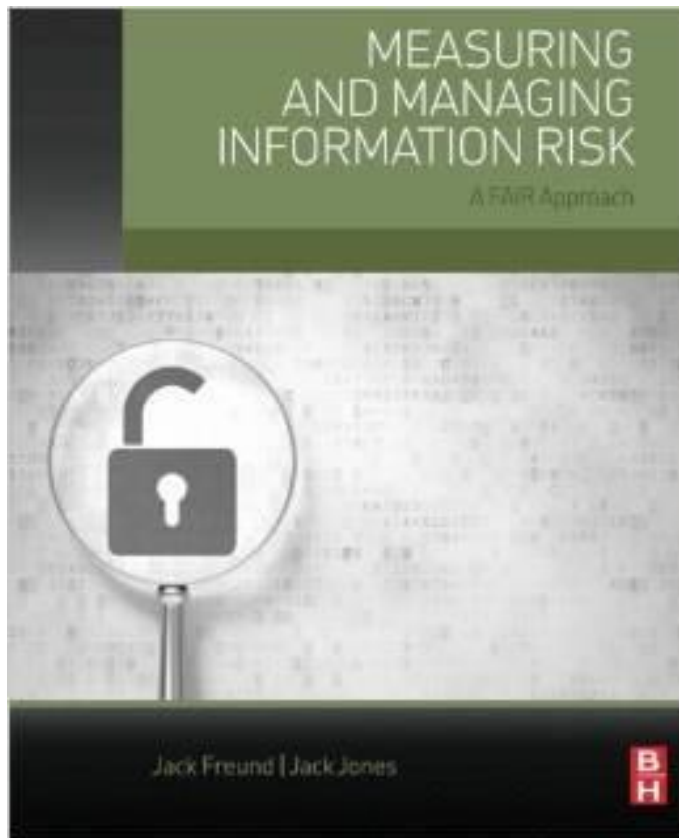
*Commercialized FAIR & provides SaaS*

- **What is FAIR?**
- **FAIR on a Page**
- **Introduction to FAIR**

# Demystifying ICS Cyber Risk: Resources

## Valuable Resource

- Provides a practical and credible framework for understanding, measuring and analyzing information risk of any size and complexity
- Shows how to deliver financially derived results tailored for enterprise risk management
- Intended for organizations that need to build a risk management program from the ground up or strengthen an existing one
- Covers key areas such as risk theory, risk calculation, scenario modeling and risk communication within the organization
- Measuring and Managing Information Risk is an essential tool to help business executives of the digital age make smarter business decisions.
- <http://www.amazon.com/Measuring-Managing-Information-Risk-Approach/dp/0124202314>





Thank You!  
Mike Radigan  
Director, OT Strategy  
Leidos Cyber, Inc.  
[Radiganm@leidos.com](mailto:Radiganm@leidos.com)  
508-330-2553

# Mechanical Operational Risk for Power Plant A

## Loss Exceedance Curve

Maximum	\$24.5M
90th %	\$12.1M
Most Likely	\$5.2M
Average	\$6.4M
10th %	\$3.0M
Minimum	\$287K

Risk Appetite	\$5.0M
---------------	--------

