RELIABILITYFIRST

Annual Reliability and Compliance Workshop: Embracing the Transformation

Day 2

Wednesday, September 28, 2022

8 a.m. – 12 p.m. Eastern

PUBLIC

Welcome and Logistics

- Safety and Logistics
- This WebEx event is not being recorded
- Please submit all questions through Slido
- We will provide the workshop survey live at the end of today
- Today's presentations (minus the FERC presentation) are posted on the RF website

Join the conversation at

Slido.com

#RFWorkhshop

Slido – Share What You've Learned!

In a few words, what did you learn from yesterday's presentations?

Join the conversation at

Slido.com

#RFWorkhshop

Today's Agenda

Wednesday, Sept. 28		
Presentation	**Presenter(s)**	**Time**
Opening Remarks	Brian Thiry, Director of Entity Engagement, RF	8 – 8:05 a.m.
Day 2 Keynote	Heather Baldwin, Vice President of Indirect Procurement, Micron Technology, Inc.	8:05 – 8:45 a.m.
Compliance Excellence – Raising the Bar	Jim Kubrak, Operations and Planning Compliance Monitoring Manager, RF; and Matt Di Maggio, Principal Reliability Assurance Analyst, ITC Holdings Corp.	8:45 – 9:30 a.m.
Break		9:30 – 9:40 a.m.
State Outreach Update	Michelle Cross, Manager Entity Engagement, RF	9:40 – 10:05 a.m.
IEEE/NERC Technical Report: Integrating Cyber and Physical Security Concepts into Transmission Planning	Johnny Gest, Manager Engineering and System Performance, RF; and JP Skeath, Engineer II, BPS Security and Grid Transformation, NERC	10:05 – 10:45 a.m.
Break		10:45 – 10:55 a.m.
FERC NOPR – Internal Network Security Monitoring	Cesar Tapia, Cyber-Security Specialist, Office of Electric Reliability, FERC	10:55 – 11:35 a.m.
RF Resources Available and Getting Involved	Sam Ciccone, Principal Reliability Consultant, RF	11:35 – 11:50 a.m.
Closing Remarks	Brian Thiry, Director of Entity Engagement, RF	11:50 a.m. – 12 p.m.
Lunch		12 – 1 p.m.

Trivia Giveaways

RF is offering the opportunity to win a $50 Amazon gift card at the end of each workshop day for five participants!

To Enter: Use Slido (Slido.com, Slido app or the QR code). At the closing of each workshop day, we will announce that a content-based trivia question is coming. You will have one minute to enter your name into Slido before the questions are asked. You must enter your first and last name; anonymous responders are not eligible to win.

To Win: A skill-based question will be visible in Slido. You must answer correctly and be the fastest respondent, as recorded in Slido, to win. We will announce the winners who will then email Jody Tortora to receive the $50 Amazon gift card.

Join the conversation
at **Slido.com**
#RFWorkshop

NO COST TO ENTER. Governed by the rules of Ohio. Registrants and Entrants hold RF harmless from any associated claim and RF is not responsible nor may be held liable for any technical errors or events that may prevent the promotion from running smoothly. Must be over the age of 18 with a valid US address and not an Employee of ReliabilityFirst to win. Any resulting taxes are the responsibility of the winner.

RF Anti-Trust Statement

It is ReliabilityFirst's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct which violates, or which might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every ReliabilityFirst participant and employee who may in any way affect ReliabilityFirst's compliance with the antitrust laws to carry out this policy.

Keynote Speaker

Heather Baldwin
Vice President of Indirect Procurement, Micron Technology, Inc.

Embracing the Reliability Transformation

Heather Baldwin
Micron Vice President of Indirect Procurement

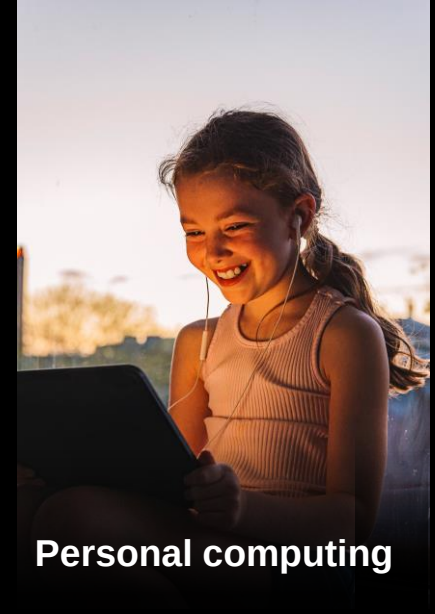
Safe Harbor Statement

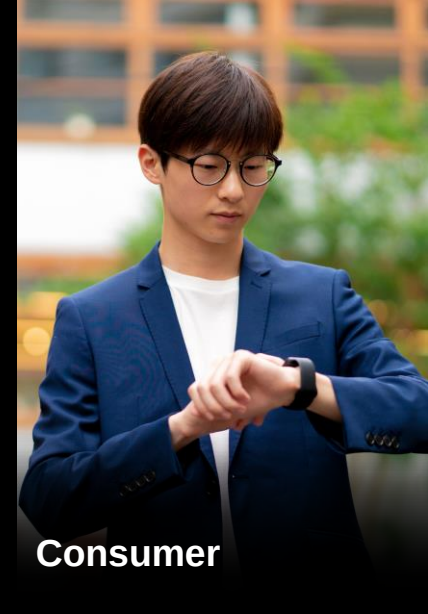
During the course of this meeting, we may make projections or other forward-looking statements regarding future events or the future financial performance of the Company and the industry. We wish to caution you that such statements are predictions, and that actual events or results may differ materially. We refer you to the documents the Company files from time to time with the Securities and Exchange Commission, specifically the Company's most recent Form 10-K and Form 10-Q. These documents contain and identify important factors that could cause the actual results for the Company to differ materially from those contained in our projections or forward-looking statements. These certain factors can be found at http://www.micron.com/certainfactors. Although we believe that the expectations reflected in the forward-looking statements are reasonable, we cannot guarantee future results, levels of activity, performance, or achievements. We are under no duty to update any of the forward-looking statements after the date of the presentation to conform these statements to actual results.

Heather Baldwin

VP, Indirect Procurement

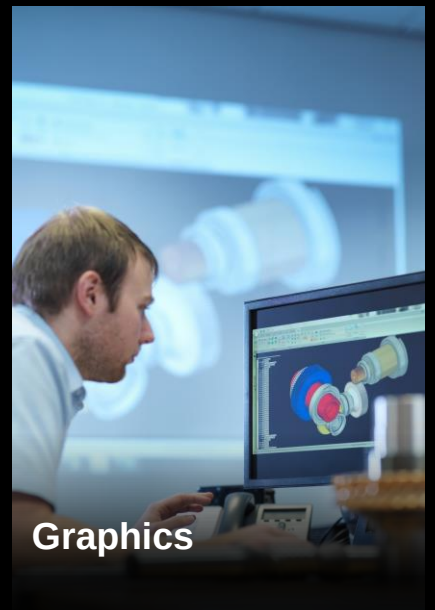
- 18+ years in the semiconductor industry
- Micron renewable and non-renewable energy leader
- Sustainability goal champion

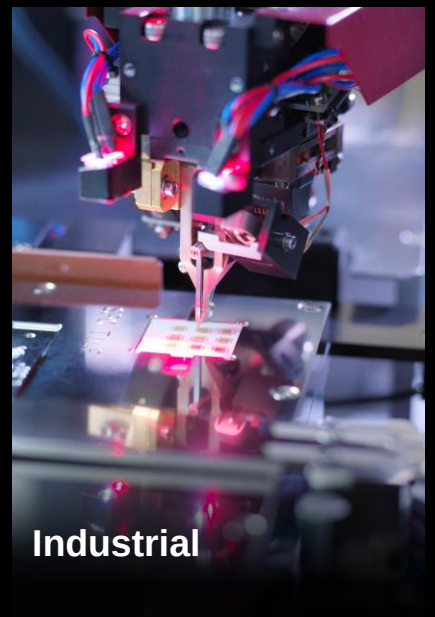


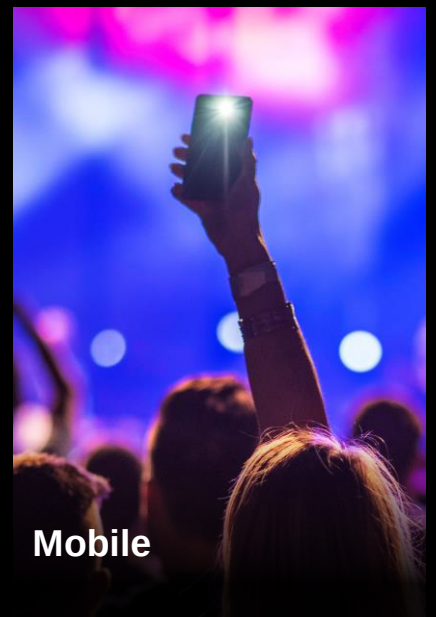


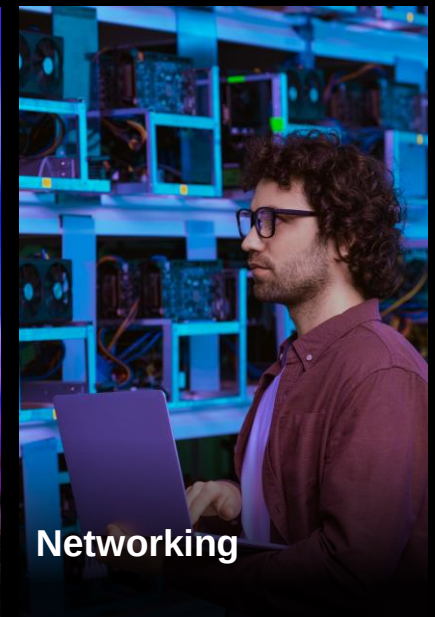
Micron is at the center of the data economy

… and everything we do requires POWER





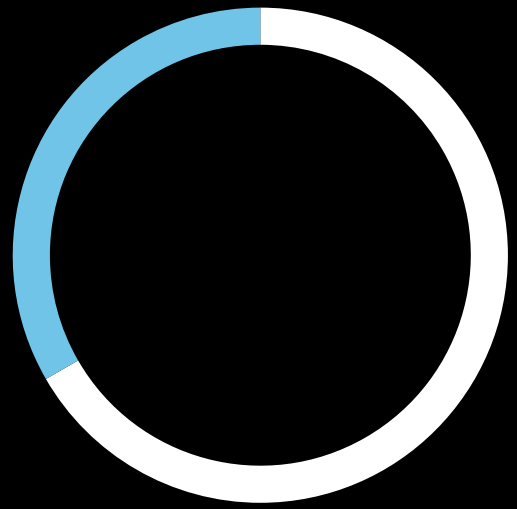




2022 world memory market

$195B

(+17% Y/Y)



Semiconductor market overall

$639B

DRAM

$112B

Mobile $37B
Non-mobile $75B

NAND

$77B

SSD $37B
Non-SSD $41B

Non-memory markets

$443B

Analog	Logic	Discrete	Other
$33B (+6% Y/Y)	$321B (+6% Y/Y)	$30B (+7% Y/Y)	$59B (+9% Y/Y)

Source: Gartner Semiconductor Forecast, CQ4-21 Update, Dec. 2021
[1]Memory includes DRAM, NAND and NOR, emerging and other

Founded on
October 5, 1978

Headquartered in
Boise, Idaho, USA

$27.7B
FY2021 revenue

4th
largest semiconductor company in the world

127
on the 2022 Fortune 500

50,000+
patents granted and growing

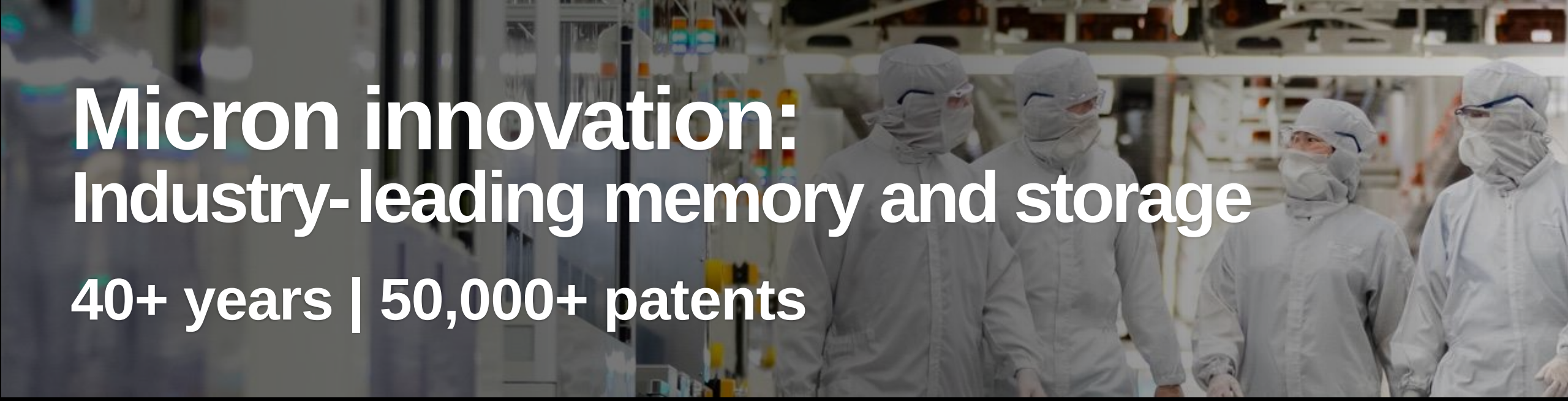
17
countries

11
manufacturing sites and 18 customer labs

~45,000
team members

Micron manufacturing sites

Micron's global footprint map highlight's locations that include our manufacturing sites, centers of excellence, customer labs and large offices.



Micron innovation:
Industry-leading memory and storage

40+ years | 50,000+ patents

1979
Designed world's smallest 64K DRAM

1984
Introduced world's smallest 256K DRAM

1987
Reached 1-megabit DRAM milestone

1999
Shipped industry's first DDR memory

2004
Invented high-density $6F^2$ memory cell architecture

2006
Delivered industry's densest server memory module (16GB)

2007
Developed industry's first pitch-doubled NAND

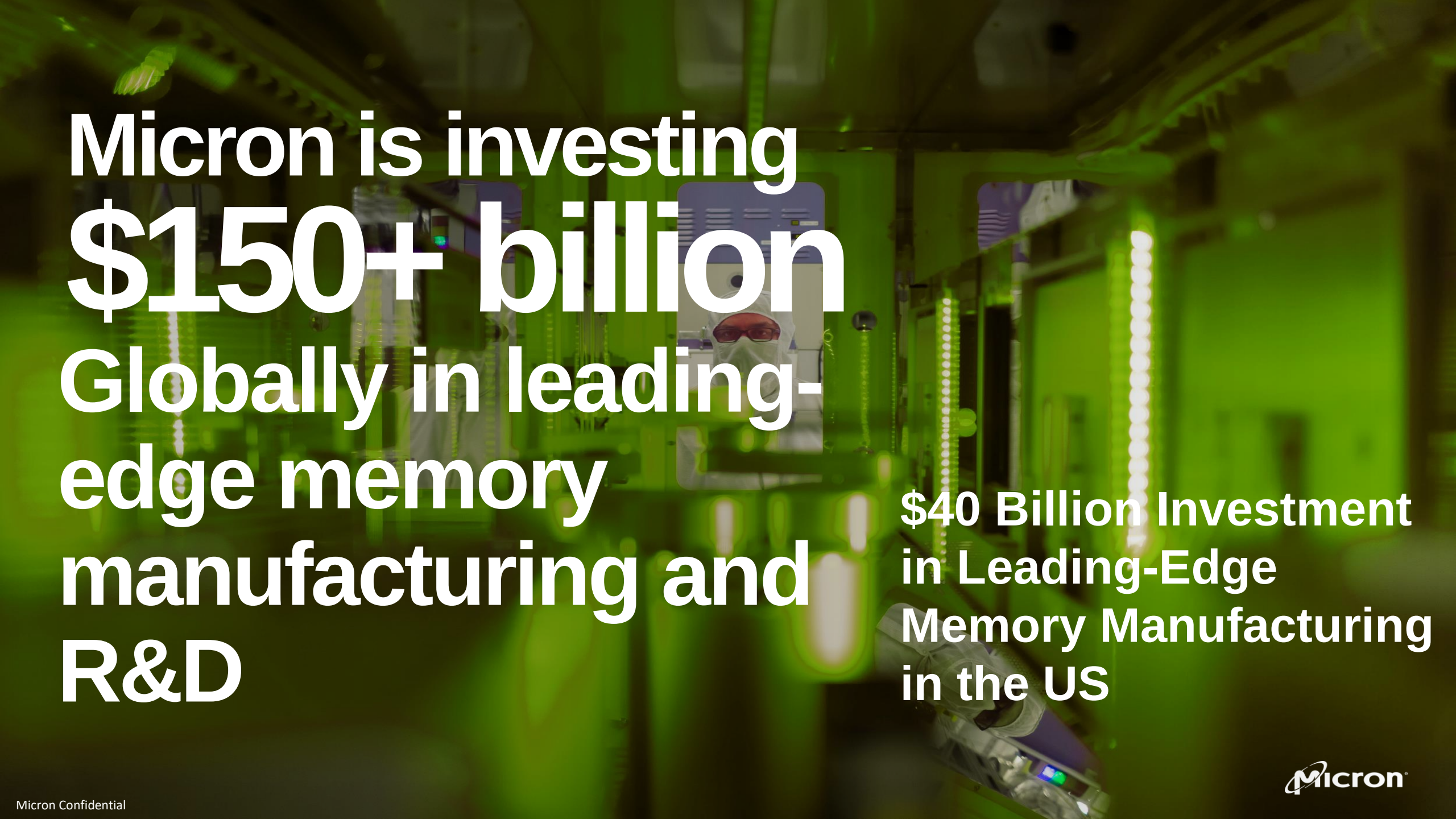
2015
Created 3D XPoint™ technology (with Intel)

2018
Shipped industry's first QLC NAND SSD

2020
Launched GDDR6X, first memory with PAM4 multi-level signaling

Shipped industry's first 176-layer NAND flash

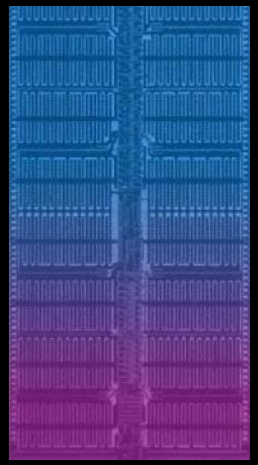
2021
Shipped industry's first 1α DRAM process technology



Micron technology leadership

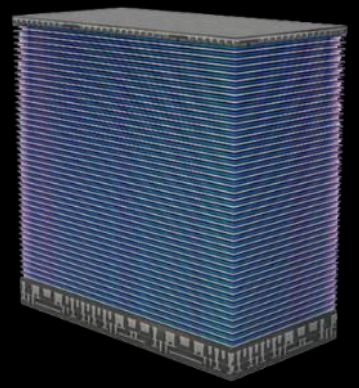
Achieved with leading design efficiency and process technology

1α nm: Industry's most advanced DRAM



- Lowest-power mobile DRAM with 15% improvement vs. prior generation[1]
- Roadmap for highest-speed DRAM available across comprehensive portfolio
- Now in volume production

World's first 176-layer NAND

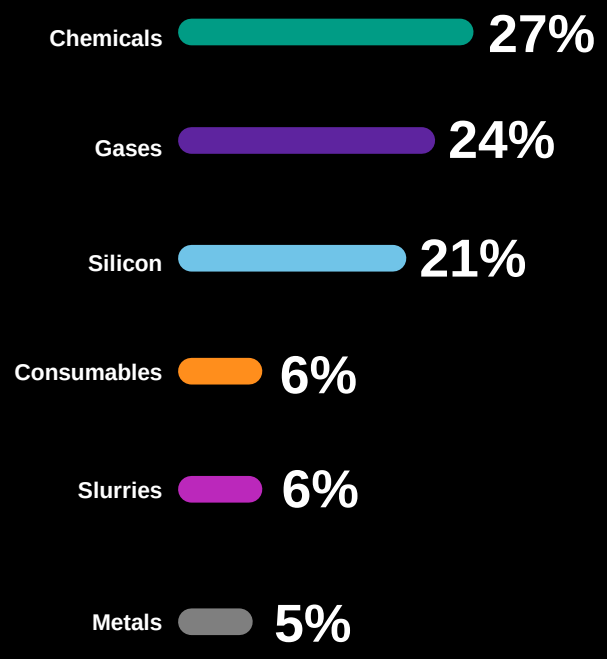


- ~1.5x cost reduction vs. previous Micron generation of 3D NAND[2]
- >2x improved power efficiency[3]
- >2x better write times[3]
- 33% higher data transfer rate[3]

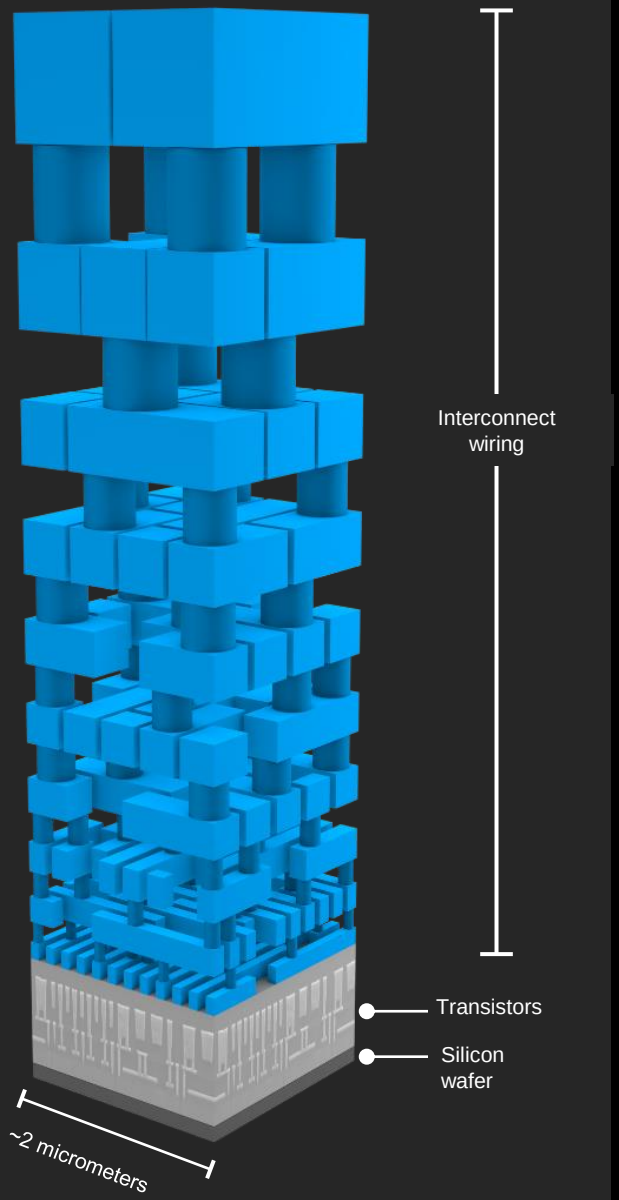
1 15% power savings when compared to the previous 1z generation of Micron mobile DRAM
2 Cash cost per Gb vs. Micron 64L/96L transition
3 Versus Micron's high-volume, floating-gate 96-layer 3D NAND

What's in a chip?

General material content for 3D Flash Memory



500+ unique materials

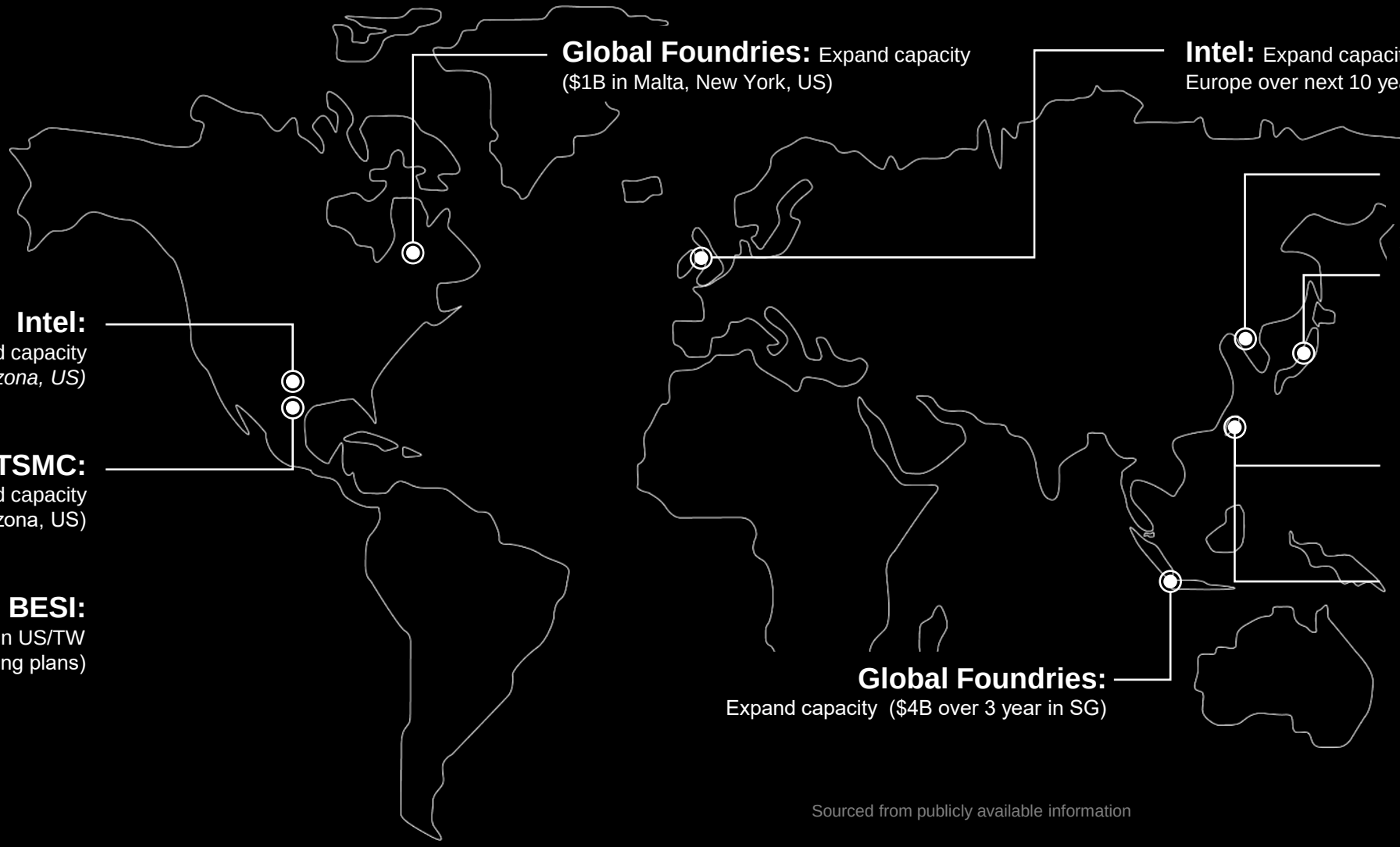


Did you know?

- Micron makes about 10 quintillion bytes of memory and storage each year
- It takes 1,000+ process steps over several months time and a journey of 100s of miles through a factory to make a chip
- Data from nearly 500,000 sensors pours into our 10-petabyte smart manufacturing system
- We feed 1,000,000+ images every day through our AI inspection systems
- Over 2,000 metric tons of sand is consumed to make the silicon wafers used in our factories each year

Semiconductor industry expansions

Cumulative investment announced over next decade: >$350 Billion



Global Foundries: Expand capacity ($1B in Malta, New York, US)

Intel: Expand capacity ($100B in Europe over next 10 years)

Samsung: Expand foundry (~$115B over next 10 years)

TSMC: New plant in JP ($7B over next 3 years)

Kioxia: R&D expansion ($0.2B over next 3 years)

Powerchip: expand Capacity (>$9B over next 10 years)

TSMC: Expand capacity ($100B over next 3 years)

UMC: Expand capacity ($5B over next 3 years)

Intel: Expand capacity *($20B in Arizona, US)*

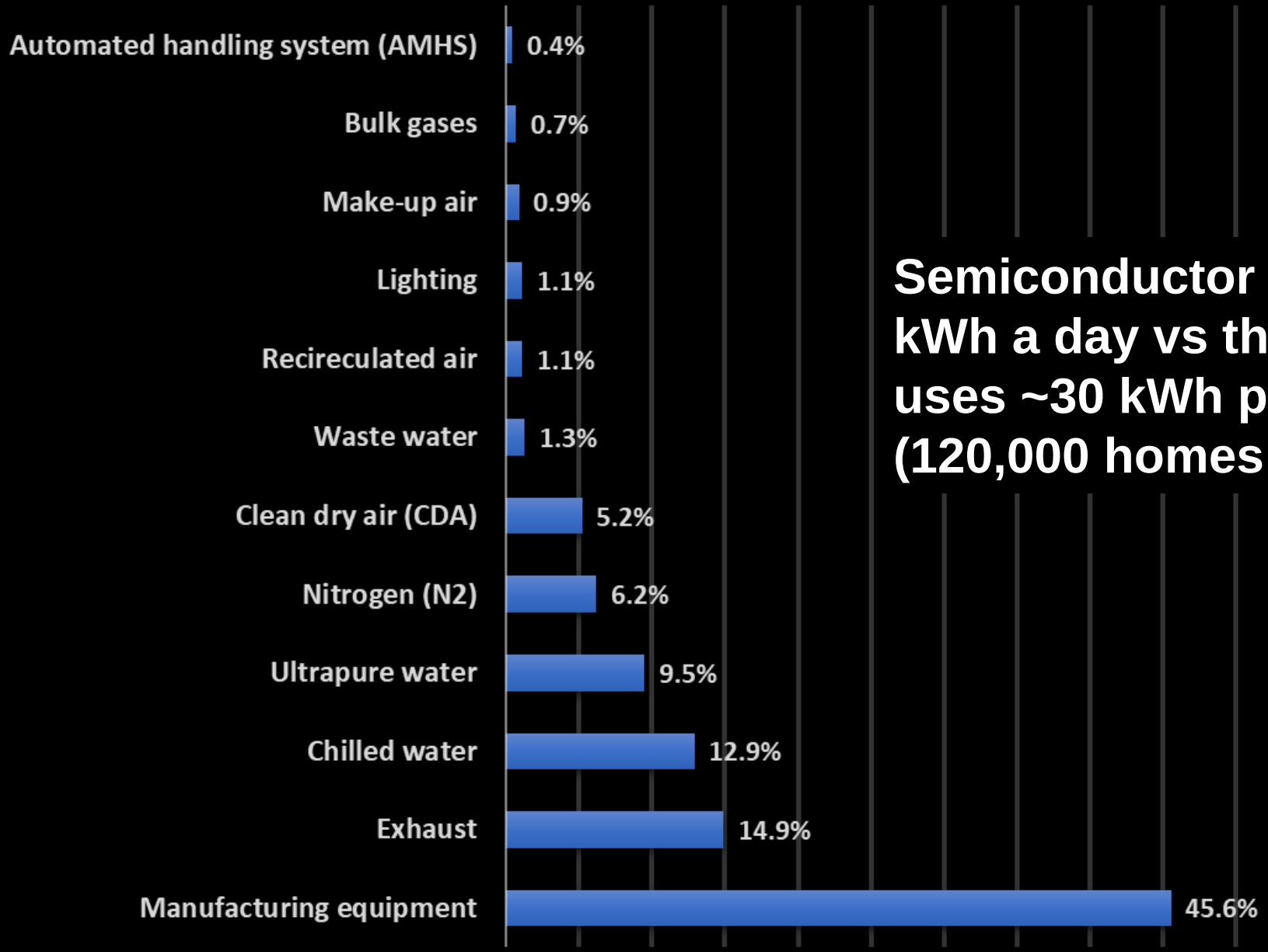
TSMC: Expand capacity ($12B in Arizona, US)

BESI: Expansion plans in US/TW (developing plans)

Global Foundries: Expand capacity ($4B over 3 year in SG)

Sourced from publicly available information

Power Consumption in a Fab

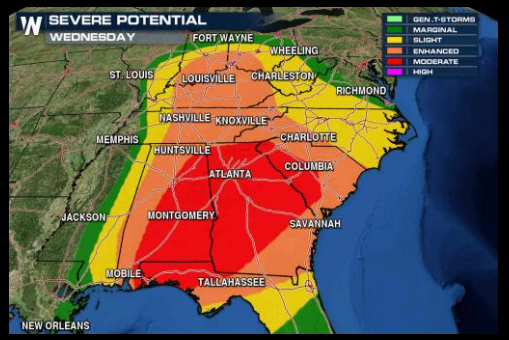


Semiconductor fabs use up to 3.6M kWh a day vs the average home that uses ~30 kWh per day (120,000 homes per 1 Fab`s usage)

Micron

Power Outage Causes, Impact to a Fab & the Economy

Potential Causes



Impacts

Power bumps lasting only seconds can trigger large global supply chain impacts

Power Outage Recovery

STABILIZE

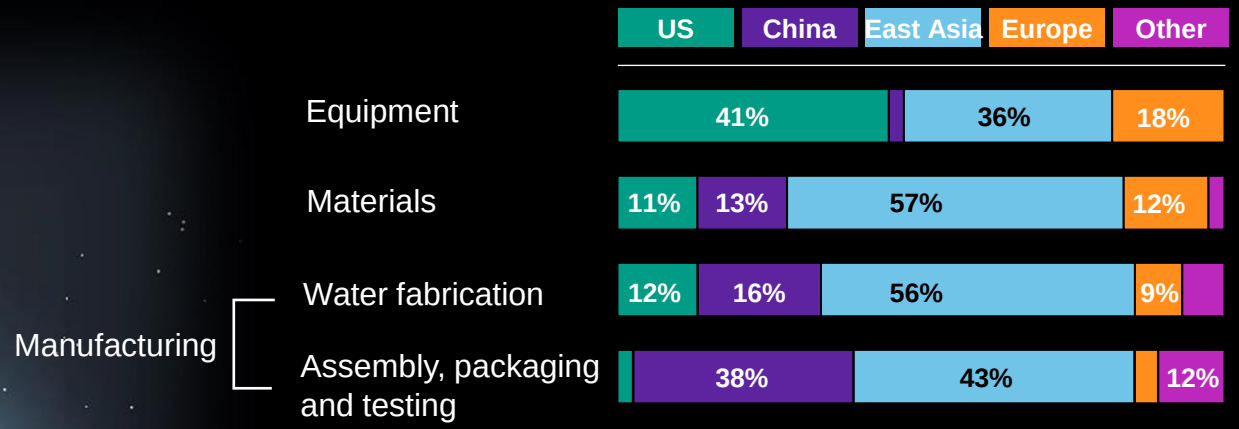
ASSESS

RECOVER

Supply Chain Impacts

Semiconductor supply chain

Share by region (% of worldwide total, 2019)



Due to the global supply chain complexity, we need to regionalize and focus on improved quality, reliability, and IP protection

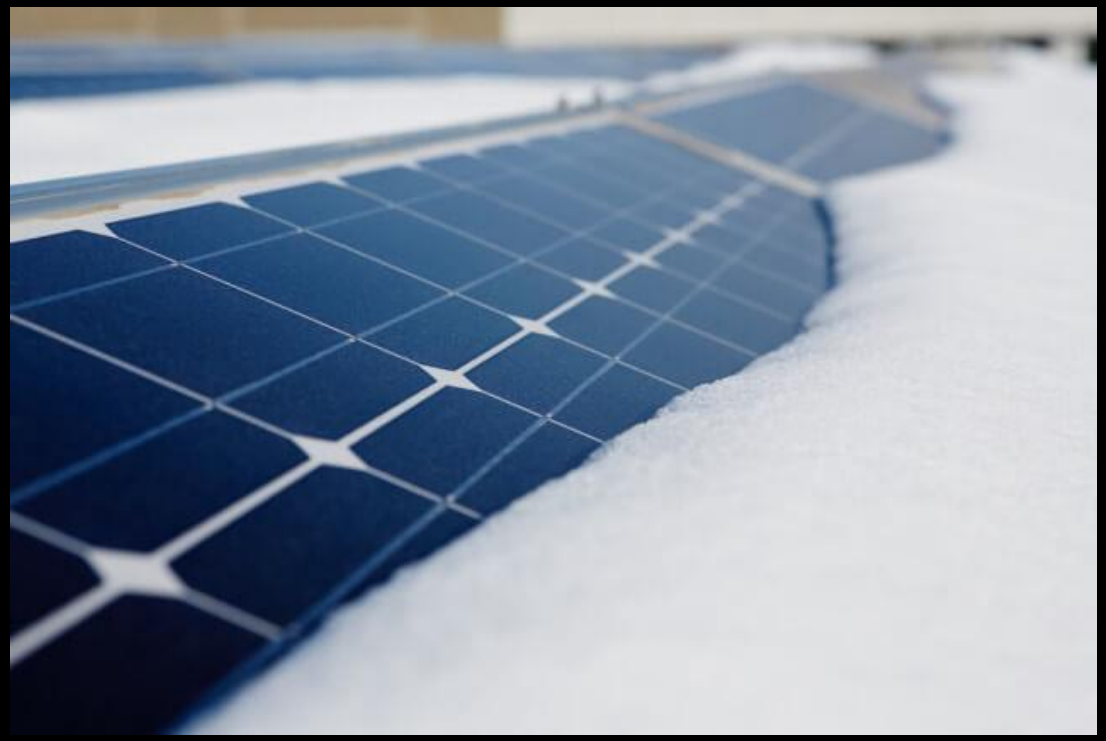
SIA: Local supply chains in each region to meet its current levels of semiconductor consumption would have required at least $1 trillion in incremental upfront investment, resulting in a 35% to 65% overall increase in semiconductor prices and ultimately higher costs of electronic devices for end users.

Power Grid Integration

We must work together to overcome the challenges

Energy is the largest contributor to our carbon neutral goals… Integration of solar and other green sources of power are a necessity to achieve ESG goals

Power Grid Volatility & Reliability



Stable and reliable sources of power are critical for manufacturing due to the cost of power events

Cyber Security

Risks are growing each year and the methods to thwart them must keep pace with those seeking to disrupt.

- Ransomware cost the world **$20 billion in 2021**. That number is expected to rise to **$265 billion by 2031**.
- In 2021, **37 percent of all businesses and organizations** were hit by ransomware.
- Only **57 percent of businesses** are successful in recovering their data using a backup.
- Recovering from a ransomware attack cost businesses **$1.85 million on average in 2021**.

*Source: Forbes.com

Environmental Goals

We are in this together

Emissions

42%
absolute reduction in scope 1 emissions by CY30 from CY20 baseline

Net zero
scope 1 and 2 emissions by CY50

Energy

100%
renewable energy in the United States in CY25

100%
renewable energy in Malaysia in CY22

Water

75%
water conservation in CY30

Waste

95%
reuse, recycling and recovery, and zero hazardous waste to landfill in CY30**

Early in calendar year 2022 (CY22), we set new aspirational commitments to reach net zero greenhouse gas (GHG) emissions in our operations (scope 1) and purchased energy (scope 2) by 2050.

Wrap up

- Semiconductor factories rely heavily on highly stable sources of power and are significantly impacted by disruptions that create ripple effects across the global supply chain
- We look to partner on efforts to improve the stability of power grids and the integration of green energy, driving for favorable regulations, lower costs, and overall stability/reliability will be key
- Environmental Sustainability initiatives require reduced consumption, better material development, improved waste management and recapture
- Cyber security is a necessity, we must be vigilant


Micron®

Compliance Excellence: Raising the Bar

Jim Kubrak, Manager Operations and Planning Monitoring
Matt Di Maggio, Principal Reliability Assurance Analyst, ITC
September 28, 2022






The Bar

Engagements Last 3 Years: CIP & O&P		
Determination	**Total**	**Total Percentage**
Positive Observations	**252**	9.7%
Recommendations	541	20%
Areas of Concern	184	7%
Potential Noncompliance (PNC)	201	7.7%

35%

What Does Success Look Like

1. Understanding the Role of Compliance
2. Sustainability Mindset
3. Ready to talk Recommendations and AOC's
4. What entity is achieving compliance at a high level?

Theodore Roosevelt – "The Man in the Arena"
Paris, France April 23, 1910

Role of Compliance

- **People Matter**
  - Service based organization
    - Considerate of time and resources
- **Getting Involved and Communicating with SMEs**
  - Sharing compliance issues/trends/tools at program level
  - Keeping SOs/SMEs up to date with industry developments at standards level (News You Can Use)
- **Going above Compliance**
  - Implementing best practices
    - Going over and above – beyond the minimum - helps mitigate risk
  - Internal mock audits
  - Industry participation
    - Peer reviews
    - Leveraging others review/audit experience

Sustainability Mindset

- How did we prepare?
  - SO/SMEs updated Reliability Standard Audit Worksheet (RSAWs) and evidence
  - Performed mock audits utilizing internal resources
    - Past
      - Used external resources
        - Less focused approach/detail/nuances
        - Knowledge of company and processes wasn't there
          - Administrative exercise
        - Costly

Sustainability Mindset

- Current
  - Mock audits performed in-house
  - Resources are selected based on knowledge and role
    - Fresh set of eyes
      - Perform review of RSAW and evidence
  - All individuals involved with a particular standard are invited to mock audit (SO and SMEs)
    - Able to ask more in-depth questions/challenge due to company knowledge and understanding of business
    - SMEs being asked questions are more open in their answers
      - Additional discussion around the response can take place
  - Performing mock audits internally has been well-received
    - Knowledge is retained in-house (employee development)

Sustainability Mindset

- What did we do differently this time?
  - Involved field support crews in preparation
    - Limited previous audit experience
    - Set expectations for auditors
      - No safety/procedural exceptions for audit team
        - Safety debriefs at each location prior to walk down
        - Maintaining safe distances
        - Opening of cabinets
      - Answering questions completely and truthfully
        - If you don't know, "say that"
          - Get back with auditors
      - Locations and times
        - Had to remain flexible as schedule was uncertain
        - COVID-19 issues

Sustainability Mindset

- Controls
  - In 2021, started adding controls to RSAWs
    - Not able to test all controls for NERC responsible departments
      - Wanted to document where controls exist
        - If there is a Potential Non-Compliance (PNC), able to see if a control exists or not
          - If there is a control, identify where breakdown occurred
  - In several instances, implementation of controls resulted in self-reported violations

AOCs and Recommendations

- Continuous improvement
  - AOCs and recommendations from previous audits
    - Are taken seriously
      - Ready to discuss and forthcoming with mitigations

Self-Report Promptly

- Self-reports not viewed negatively
  - No retaliation for reporting a PNC
    - Goal internally is 30 days from identification
  - How do we prepare?
    - Ready to discuss the PNC with RF
      - Open dialogue/establish trust
    - Have the appropriate SMEs engaged to provide documentation/answer questions
  - Developing mitigation plans that will prevent reoccurrence including new/revised controls

Achieving Compliance at a High-Level

- Has become harder in the current environment
  - Challenge - Retention of employees
    - Opportunities elsewhere not just utility industry
      - Increased remote work and competitive market
  - Negative impacts
    - Loss of highly trained and knowledgeable employees
    - New employees increase likelihood of PNCs due to unfamiliarity
- Resources that are available to entities to help improve programs
  - RF Tech Talks
  - RF CUG
  - Develop contacts with other regions
    - Other entities
  - Social events
  - NATF

Questions & Answers

Forward Together ReliabilityFirst

Break

See you back at 9:40 for a presentation from Michelle Cross on State Outreach

Join the conversation at

Slido.com

#RFWorkhshop

ReliabilityFirst State Outreach

Michelle Cross

Manager, Entity Engagement

September 28, 2022

PUBLIC



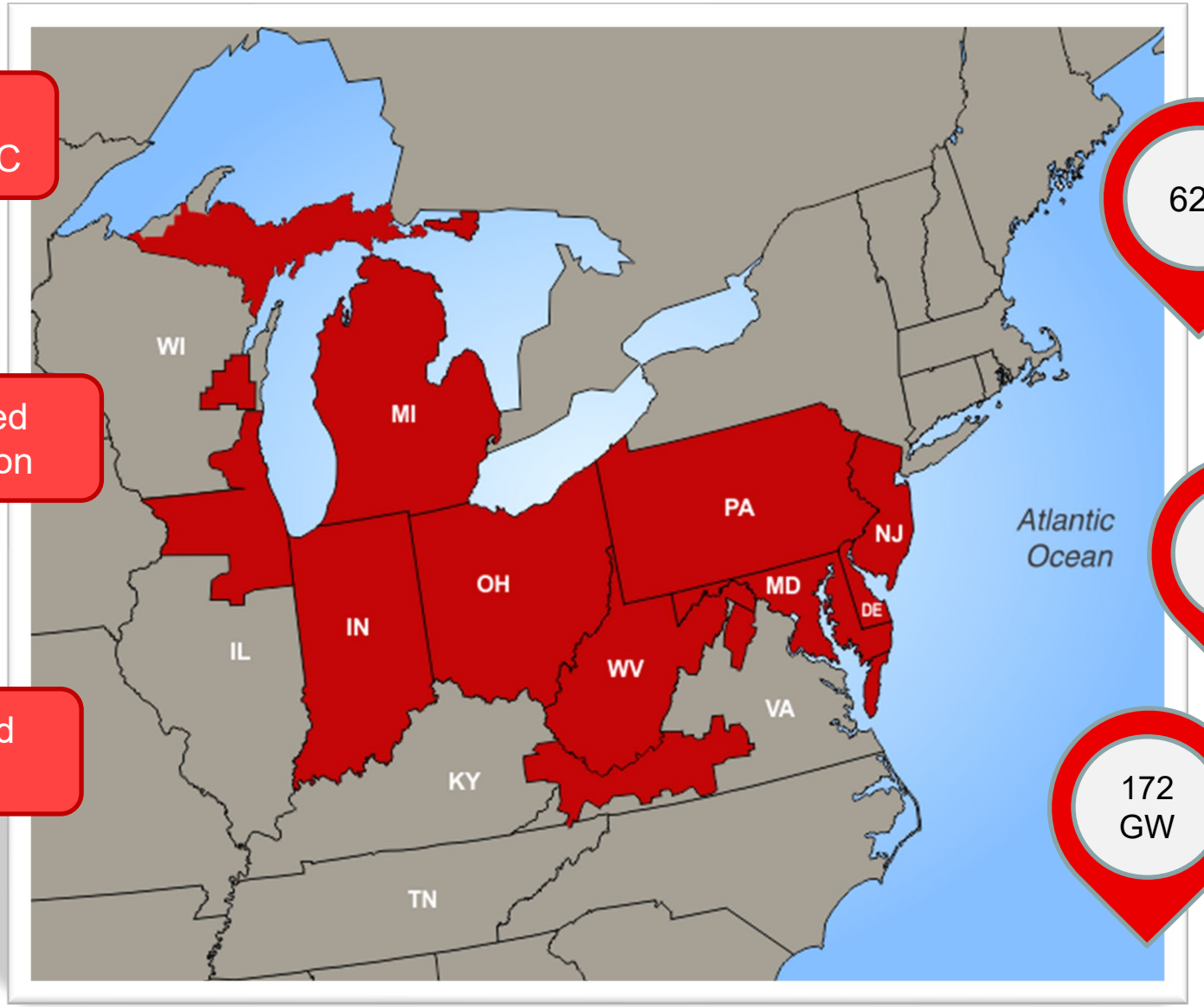



RF Footprint

13 Number of States and DC

73M Estimated Population

270 Registered Entities



62K Miles of BES Lines

1300 Generating Units

172 GW Forecasted Load

Purpose

RF's mission is to preserve and enhance the reliability and security of the bulk power system

Regulatory Outreach Principles for Engagement

Unbiased Information Resource

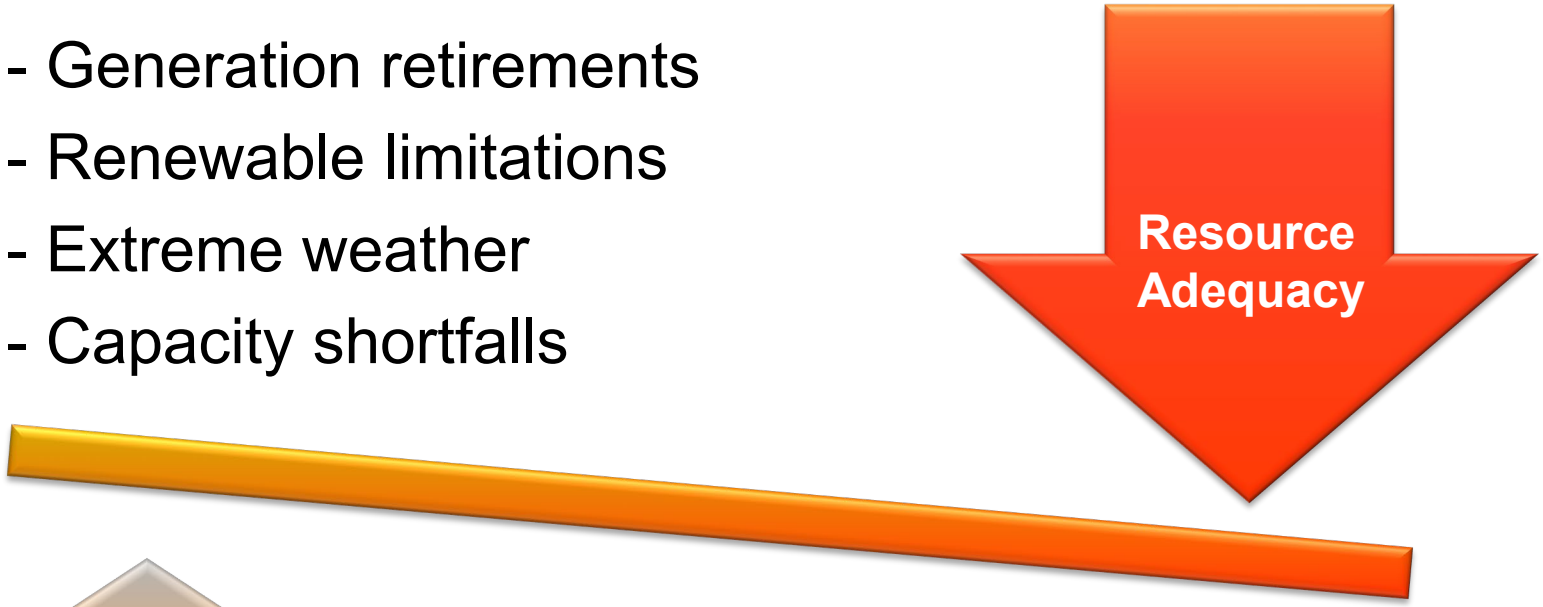
Resource & Technology Agnostic

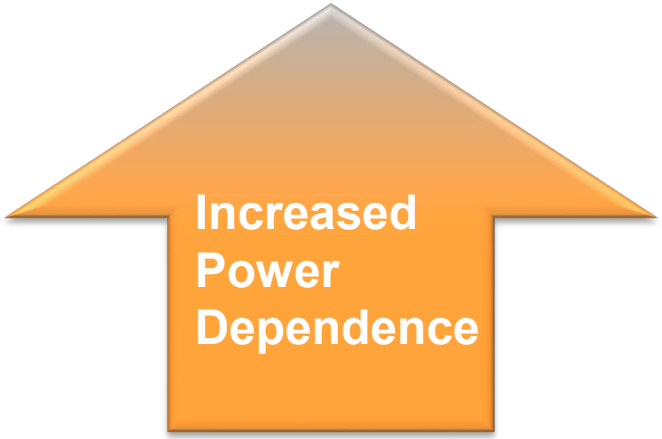
No Political Affiliation

Reliability Focused

Why State Outreach?

- Generation retirements
- Renewable limitations
- Extreme weather
- Capacity shortfalls





- Economic reliance
- Societal dependency
- Transportation
- Logistics/Supply chain

Why State Outreach Continued

The Energy Policy Act of 2005

Specifically prohibits the ERO from "ordering the construction of additional generation or transmission capacity or to set and enforce compliance standards for adequacy or safety of electric facilities."

What can we do?

- **We use our flashlights to shine a light on areas of concern**

- **We analyze data**
- **We share information**
- **We help States ask the right questions**
- **We help States make informed decisions**

RF's State Outreach Strategies

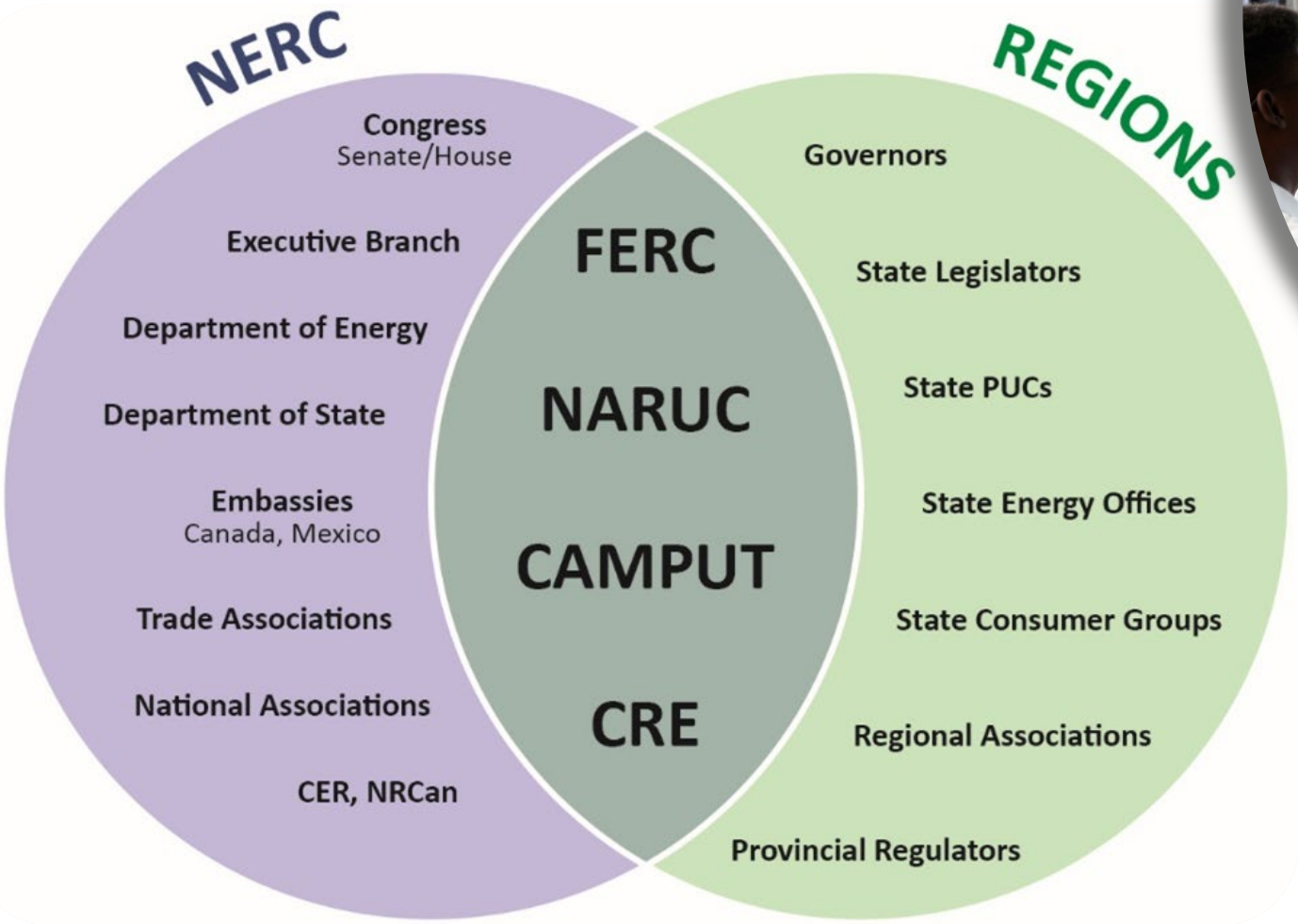
01 Engage Conversation
States have been prioritized to Increase reliability and security awareness

02 Share Knowledge
Present on new technologies and emerging threats

03 Distribute and Discuss Public Reports
Facilitate discussion around public ERO reports

04 Gather Information
Provide Data Analytics on public information or data in aggregate

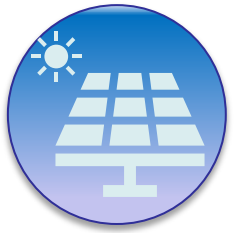
Who Are We Meeting?



Key Reliability Topics for State Outreach

Transmission Planning

Historical Events



Changing Resource Mix

Cyber and Physical Security

Inverter Based Resources

System Resilience and Restoration

Questions & Answers

Forward Together ReliabilityFirst

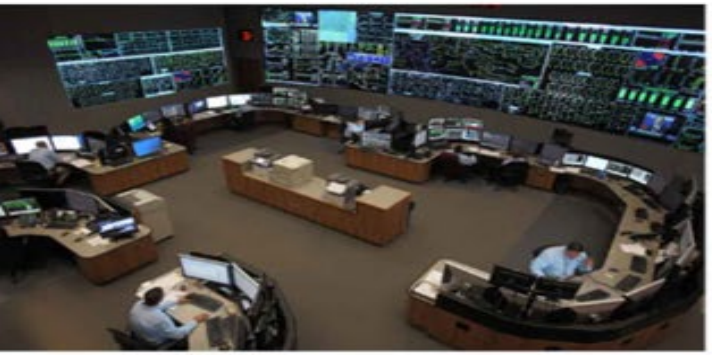
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RELIABILITYFIRST

IEEE-NERC Security Integration Project

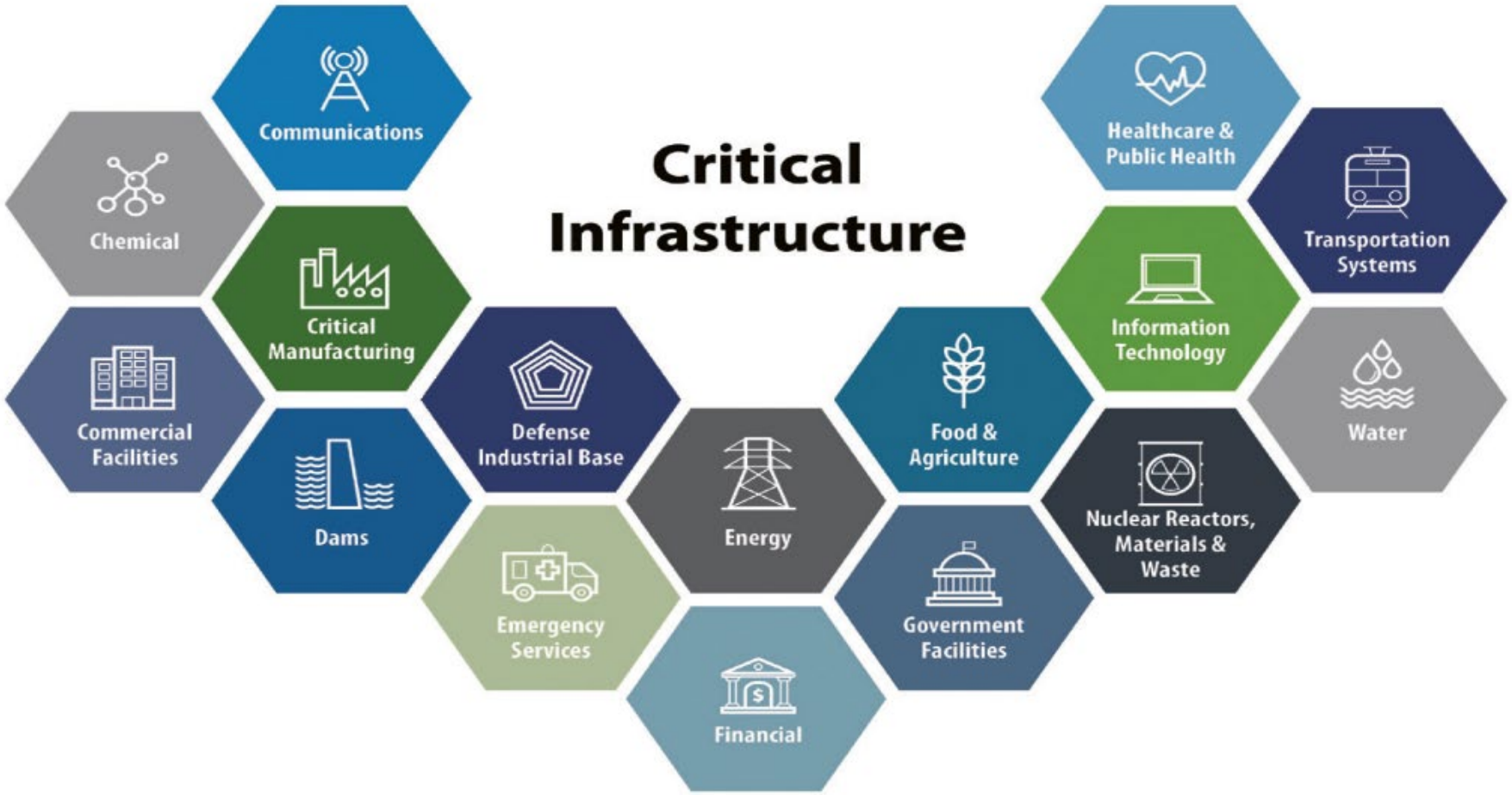
JP Skeath, Engineer II, North American Electric Reliability Corporation
Johnny Gest, Manager Engineering & System Performance, ReliabilityFirst
September 28, 2022

RELIABILITY | RESILIENCE | SECURITY




Reliability, Resilience, and Security

Critical Infrastructure



© US Cybersecurity & Infrastructure Security Agency (CISA)

Risks to the Bulk Power System

Starting with the Basics

Continuous Scanning and Assessment: Are all the door and window locks functioning? Is your security camera functioning properly?

Continuous Monitoring: Do you get notifications on your phone of motion or noise when the alarm is armed? What is your baseline “normal” and how do you determine “abnormal”?

Asset Inventory: If someone breaks into your home and steals everything, your homeowners insurance will require an itemized list of assets in your home for the claim. Do you have that?

Identity and Access Management: Who has physical keys to the home? How do you handle vendors doing repairs? Are there electronic access points and how are those controls managed?

Incident Response: Does your alarm system notify the police of a security breach? Can you quickly call the neighbors? Are you prepared to protect yourself?

Recovery: How would you respond if someone had broken into your home? Do you have a place to go to feel safe? Do you need to lock your credit report or report stolen weapons?

Securing Operational Technology

- Control centers
- Power plants
- Substations
- Distribution networks
- Renewable energy resources
- Communications infrastructure
- Fuel supply systems
- Inverters
- Distributed energy resources
- Grid edge technology
- Cloud computing networks
- Synchronized timing sources
- Etc.

History

Security Integration

Security Integration: *The integration of cyber and physical security aspects into conventional planning, design, and operations engineering practices.*

- Can we mutually understand ***threats*** posed to the electric grid?
- Can we ***plan*** a grid more resilient to cyber and physical attack?
- Can we ***design*** a grid with security as a critical consideration up front rather than at the end?
- Can we ***operate*** the grid in a way that can easily identify, detect, and respond to security incidents?
- Can we ***restore*** the grid effectively following any compromise?
- Can we integrate ***emerging technologies*** with the electricity ecosystem in a secure manner?

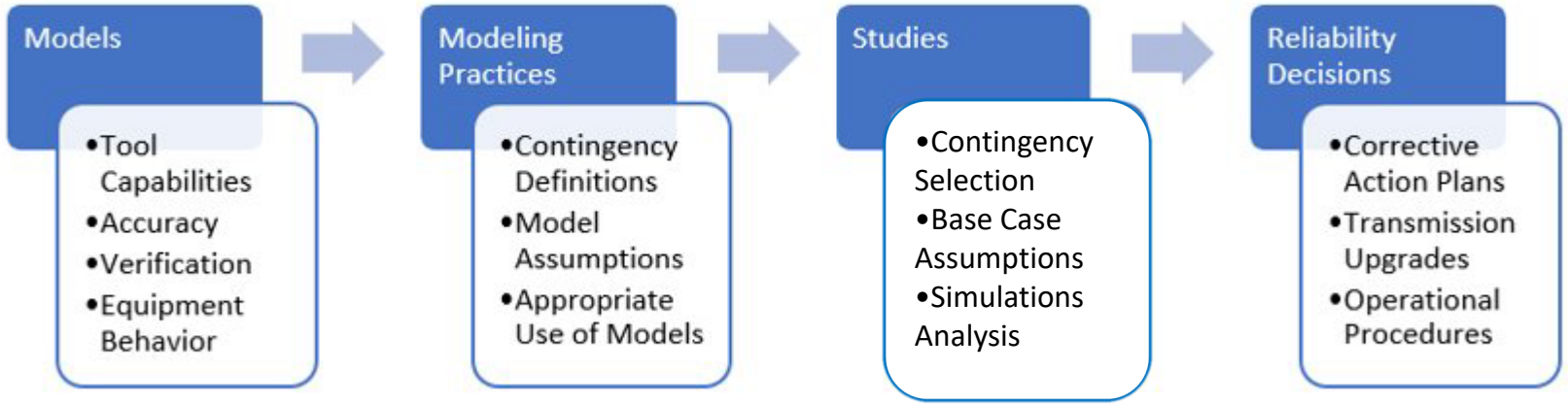
Project Updates & Logistics

- Report coming later in 2022
- Industry expert team meeting regularly
- Discussing security integration topics specifically
- Broad range of expertise and engagement

Planning Integration

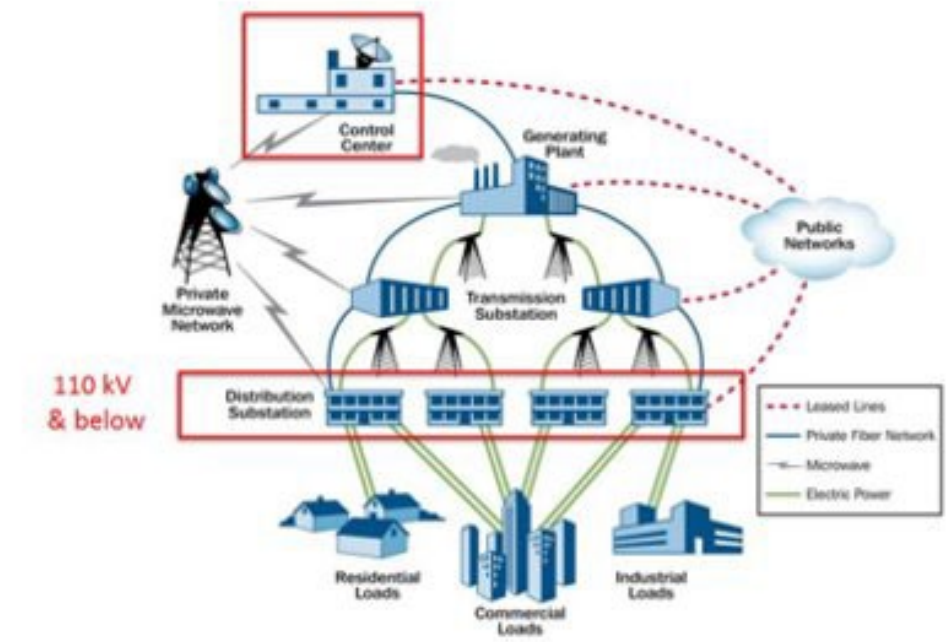
- Integrate cyber and physical security concepts into conventional transmission planning practices

General Transmission Planning Process



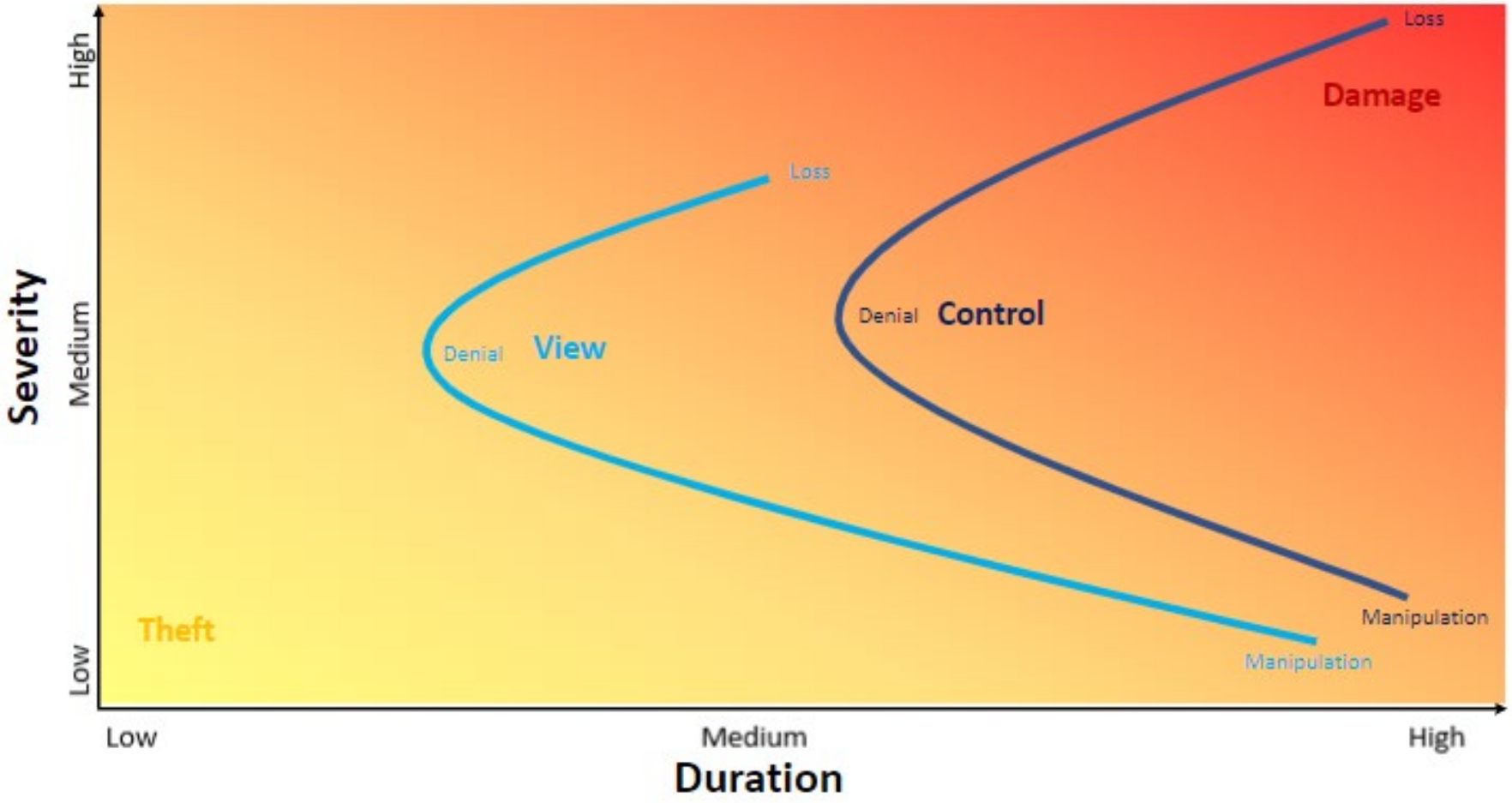
Transmission Planning – Gap Analysis

- Impacted Environments
- Attacker Actions/Manipulations
- Grid Impact
- MITRE ATT&CK Framework
  - Damage to Property
  - Impact to Control
  - Impact to View
  - Theft
  - Safety
  - Loss of Revenue



Source: Modification to the DHS Energy Sector-Specific Plan 2010

Gap Analysis – Main Takeaways



Existing Planning Processes

Do existing studies typically performed by transmission planning already represent cyber/physical security events?

CIP-014-2 Physical Security

- Facilities below 200 kV not required to be reviewed
- Encourage both prevention and security enhancements

EOP-005-3 System Restoration from Blackstart Resources

- Lack of contingency planning during restoration
- Identify units that are blackstart capable

TPL-001-4 Transmission System Planning Performance Requirements

- Lack required system reinforcement for cyber/physical attacks
- Improvement of stress scenarios and contingency definitions

Identified Gaps

Compromise of control center functionality is very challenging to simulate with conventional planning tools.

- Loss of control for multiple random elements
- Manipulation of alarms, displays, or data inputs

Recommendations

- Review the impact of losing multiple elements simultaneously and coordinate results with system operators – lead to actions like design segmentation and prioritization in emergency response plans
- Improve data quality measures and monitoring for manipulation threats

Planning Contingencies

Identified Gaps

- Contingencies mainly represent conventional outage of elements on electric grid
- Historically driven from environmental impacts to electric grid

Recommendations

- Redefine contingencies based on cyber and physical security relationships between elements
  - shared electric security perimeter
  - communications
  - physical location/ownership

Planning Models

Identified Gaps

- Improvements required associated with unauthorized access/data theft and data corruption/manipulations
- Manipulation of model parameters may mask the need for system reinforcements to mitigate reliability issues for anticipated future system conditions

Recommendations

- Develop more sophisticated model access practices and data quality measures
- Enhance existing checks performed against the planning models and inputs into the studies
- More emphasis on the development of uniform industry modeling practices used to represent transmission elements within models

Reliability Decisions

Identified Gaps

- Recommendation of system reinforcements based on conventional planning assessments may not adequately mitigate cyber and physical security risks

Recommendations

- Develop more comprehensive list of potential root causes associated with an outage to ensure recommended system reinforcements are effective for security-based threats

Additional Considerations

- Build and develop relationships with cyber/physical security and communication experts within industry
- Increase education related to cyber and physical security concerns
- Participation in tabletop exercises or simulation events
- Effectively communicate planning study results and recommended system reinforcements to other engineering groups like design, communications, cyber/physical security
- Track and trend cyber and physical security related outages
- Encourage the development of new tools with operational flexibility that allows integration into existing conventional planning tools

Questions and Answers

Break

See you back at 10:55 for a presentation from Cesar Tapia on the FERC NOPR on Internal Network Security Monitoring

Join the conversation at

Slido.com

#RFWorkhshop

FERC NOPR
Internal Network Security Monitoring

Cesar Tapia
Cybersecurity Specialist, OER, FERC

ISNM and FERC Resources

- Docket No. RM22-3-000 Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems (Issued 1/20/2022)
- Executive Order on Improving the Nation's Cybersecurity (5/12/2021)
- National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (1/28/2021)
- ERO Enterprise CMEP Practice Guide – Network Monitoring Sensors, Centralized Collectors, and Information Sharing (6/4/2021)
- FERC Events Calendar
- FERC Open Meetings
- FERC Sunshine Notice – July Commission Meeting

RF Resources Available and Getting Involved

ReliabilityFirst Fall Workshop

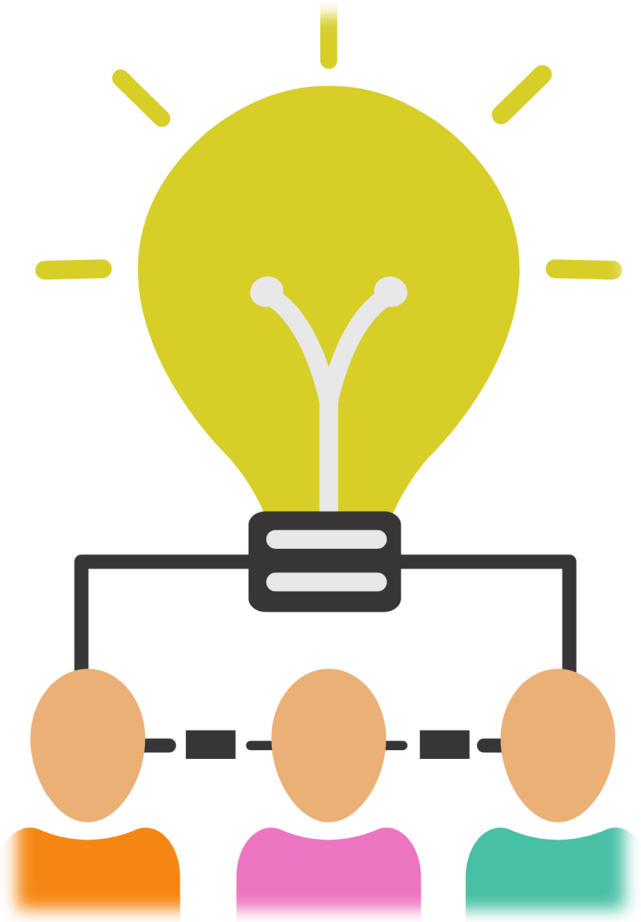
September 28, 2022






Agenda

- RF Outreach Offerings
- Questions and Answers



RF Outreach – Assist Visits

➢ Assist Visits

rfirst.org/ProgramAreas/EntityEngage/AssistVisits/Pages/AssistVisits.aspx

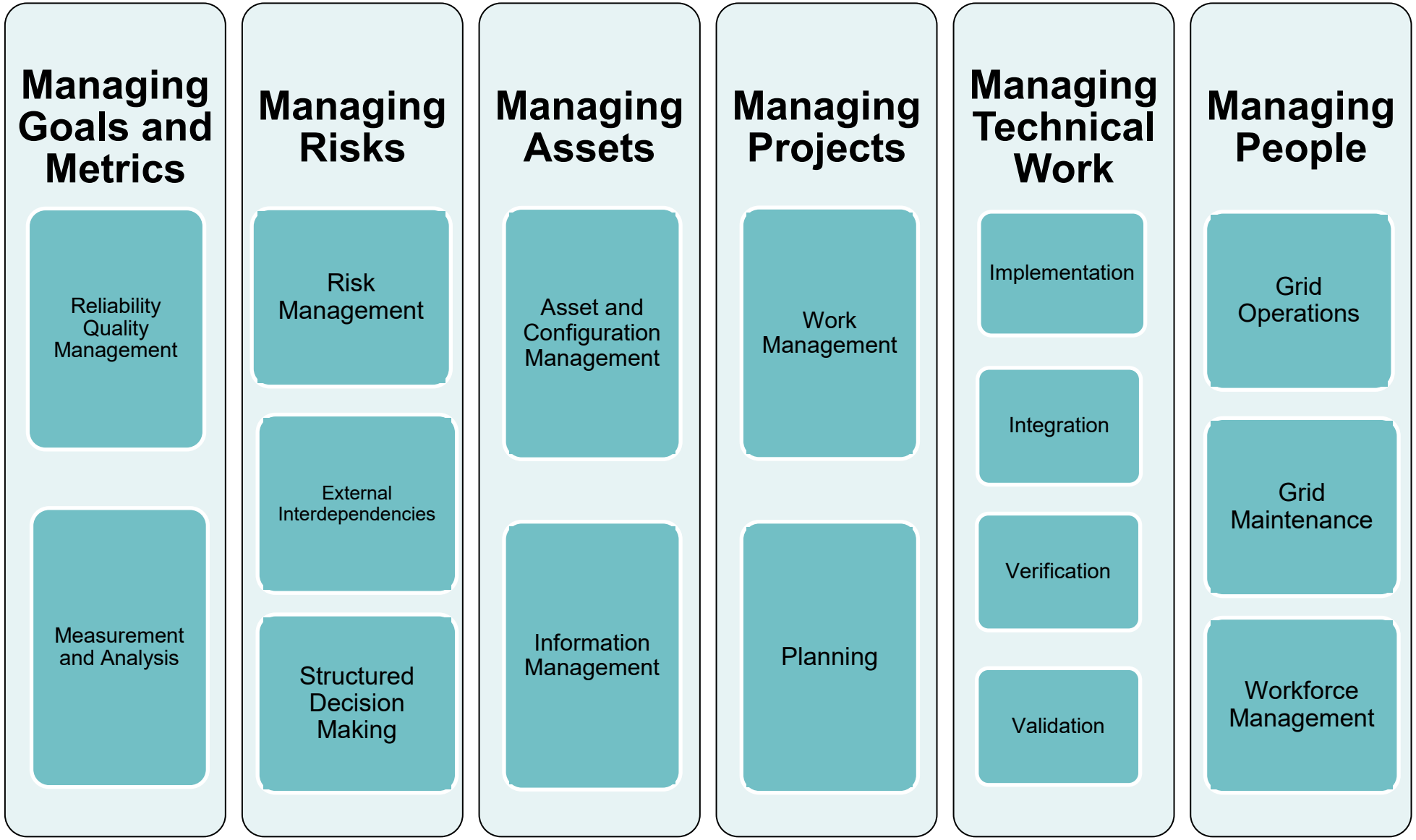
- Single and Extended
- Questions can go to other regional entities and the ERO (CCTF, OPCTF)

RF Outreach – Appraisal

➢ Appraisals

- RF review of entity's internal controls and 16 management practices
- Focused review of business processes and procedures, risks, and organizational maturity
- Based on a grid reliability maturity model developed by RF

RF Outreach – Appraisal Management Practices



RF Outreach – Appraisal Implementation Levels

Implementation Level	Criteria
Managed Practices that are Fully Implemented (FI) (90% < Level)	Sufficient evidence and/or affirmations are present and judged to be adequate to demonstrate process has no significant weaknesses
Defined Practices that are Largely Implemented (LI) (70% ≤ Level < 90%)	Sufficient evidence and/or affirmations are present and judged to be adequate to demonstrate that practices have one or more significant weaknesses

Implementation Level	Criteria
Partially Implemented Practices (PI) (30% ≤ Level < 70%)	Data supplied to the team (evidence and/or affirmations) conflict – some data indicate the Management Practices are implemented and some data indicate the practice is not implemented, and one or more significant weaknesses
Not Implemented (NI) (Level < 30%)	Some or all data required are absent or judged to be inadequate, data supplied does not support the conclusion that the process is implemented, and one or more significant weaknesses

RF Outreach Tools

Self-Assessments – Capability Assessment Management Platform (CAMP)

- **Maturity model evaluation**
  - An appraisal but assessed by the Entity
  - Self-guided assessments to determine maturity of internal controls and management practices
  - RF will help with scope, questions, and after assessment improvement roadmap

RF Outreach Tools

Self-Assessments – "CAMP"

- **Cyber Resilience Assessment Tool (CRAT)** rfirst.org/ProgramAreas/Resilience/
  - Self-assessment tool that allows entities to evaluate and benchmark their cyber resilience (CR) posture, as well as measure effectiveness
  - Four overarching domains
    - Robustness
    - Resourcefulness
    - Rapidity
    - Redundancy

Self-Assessments – "CAMP"

- **Insider Threat Program Maturity Assessment (InTP)**
  - A web-based self-assessment based on 21 best practice areas under SEI CERT's Common-Sense Guide to Mitigating Insider Threats

Self-Assessments – "CAMP"

➢ Incident Response Assessment Tool (IRPAT)

- Self-assessment tool to help test incident response and preparedness capabilities to improve resiliency throughout the ERO
- The IRPAT helps characterize an Entity's ability to gather and analyze threat intelligence and information

More RF Outreach

- **Continuous Improvement Services**
  - Kaizen events
  - Value Stream Mapping
  - Facilitation
- **Recurring Newsletter Articles**
  - Lighthouse (CIP)
  - Continuous Improvement

- **Tech Talk with RF**
  - Typically, on the third Monday of every month
  - Open to everyone; if you want to be invited, please let us know

More RF Outreach

➢ Workshops

- RF Compliance Workshop
- Other workshops as hot topics arise

➢ Matchmaking

- Discuss issues/lessons learned with other entities
- Standards, Processes, Technology

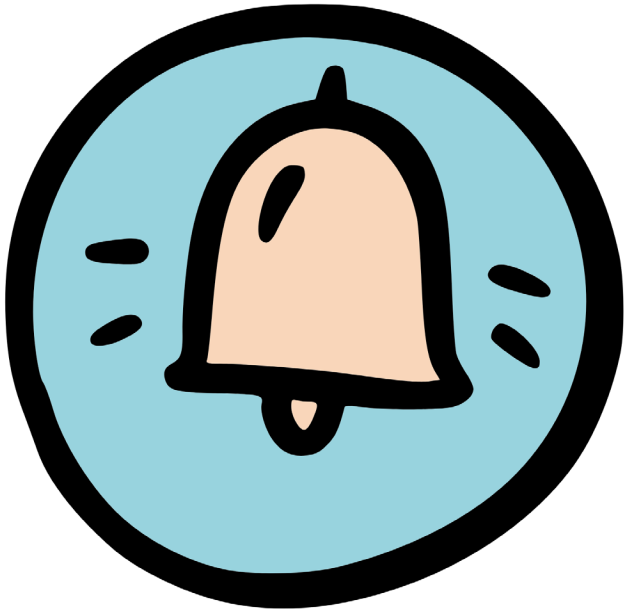
Reminder on Certifications/Reviews

- **NERC Rules of Procedure Section 500 Appendix 5A**

  nerc.com/AboutNERC/RulesOfProcedure/Appendix%205A%20effective%2020210119.pdf

  - Section IV discusses full certifications
  - Section V discusses Certification Reviews
    - See the triggers for Certification Reviews: New EMS, new Controls Center, Footprint changes

For NERC Certified TOP, BA, and RC



- **Please contact Entity Engagement ideally 12 months prior to your change to allow time for a review**
  - Please use the application and questionnaire document on Rfirst.org to start the review. It is found at this location: rfirst.org/ProgramAreas/RegCert/Certifications/Pages/Certifications.aspx

Questions & Answers

Forward Together ReliabilityFirst

Trivia Giveaway Day 2

Please log into Slido now for the opportunity to win a $50 Amazon gift card!

- You have one minute from the time this slide is shown to enter your name into Slido before the question is asked.
- You must enter your first & last name; anonymous responders are not eligible to win.
- To win, you must answer the questions correctly and be the fastest respondent, as recorded in Slido.
- Prizes for the top five participants.

Slido.com
#RFWorkshop

Trivia Giveaway Winners

Thank you and congrats to today's five trivia winners!

To claim your $50 Amazon gift card, please email Jody Tortora at Jody.Tortora@rfirst.org.

Closing Remarks

Thank you for attending our Annual Reliability and Compliance Workshop! Your feedback is extremely important to us and allows RF to continuously improve our webinars, workshops and outreach efforts.

Take the survey at

Slido.com

#RFWorkhshop

Thank You

Thank you for attending!

See you next year!