RELIABILITYFIRST

2021 Human Performance Workshop

August 12, 2021

RELIABILITYFIRST

Human Performance Workshop

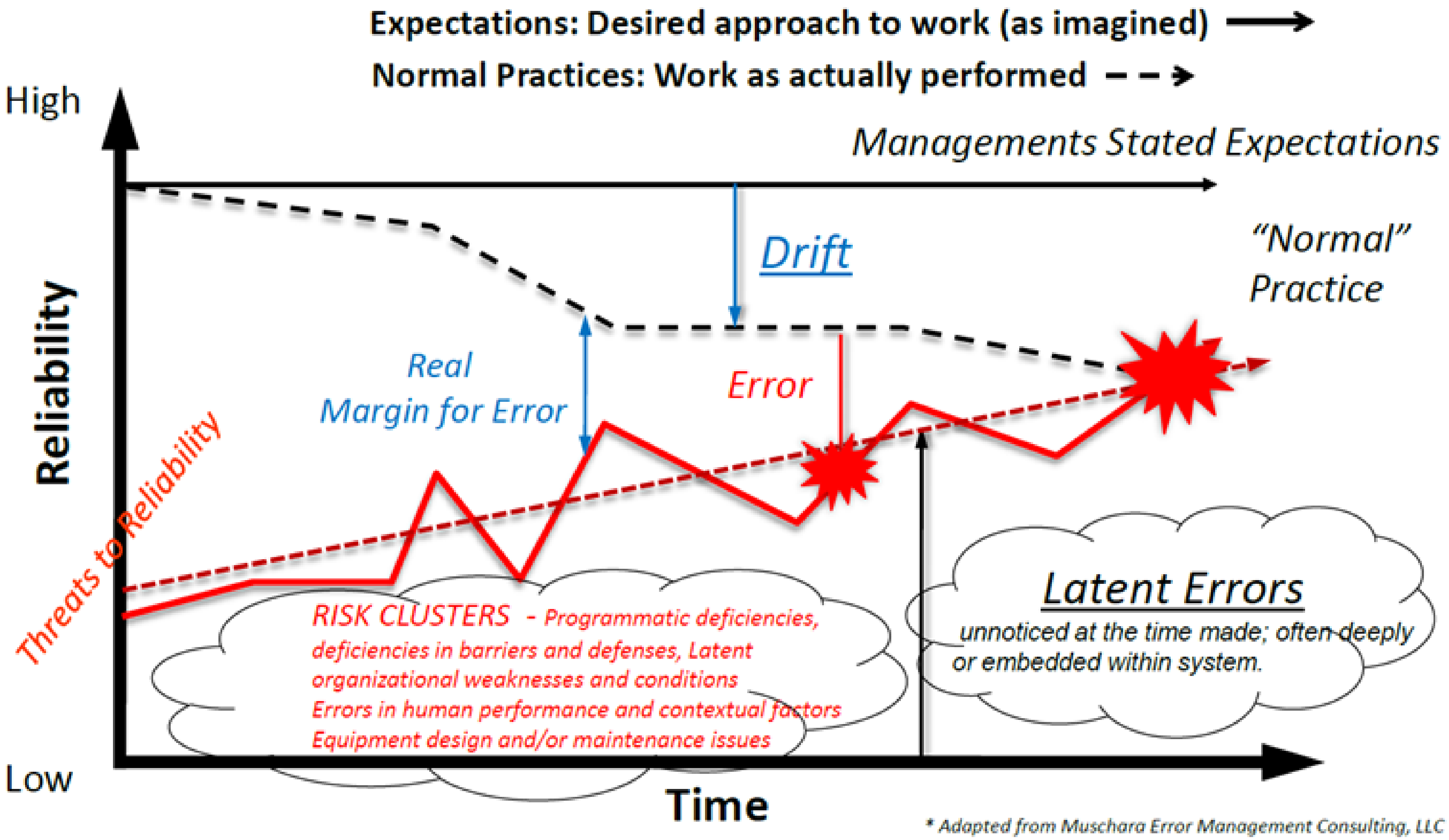
Why Are We Here?

Johnny Gest
Manager, Engineering & System Performance
August 12, 2021

PUBLIC

What is Human Performance?

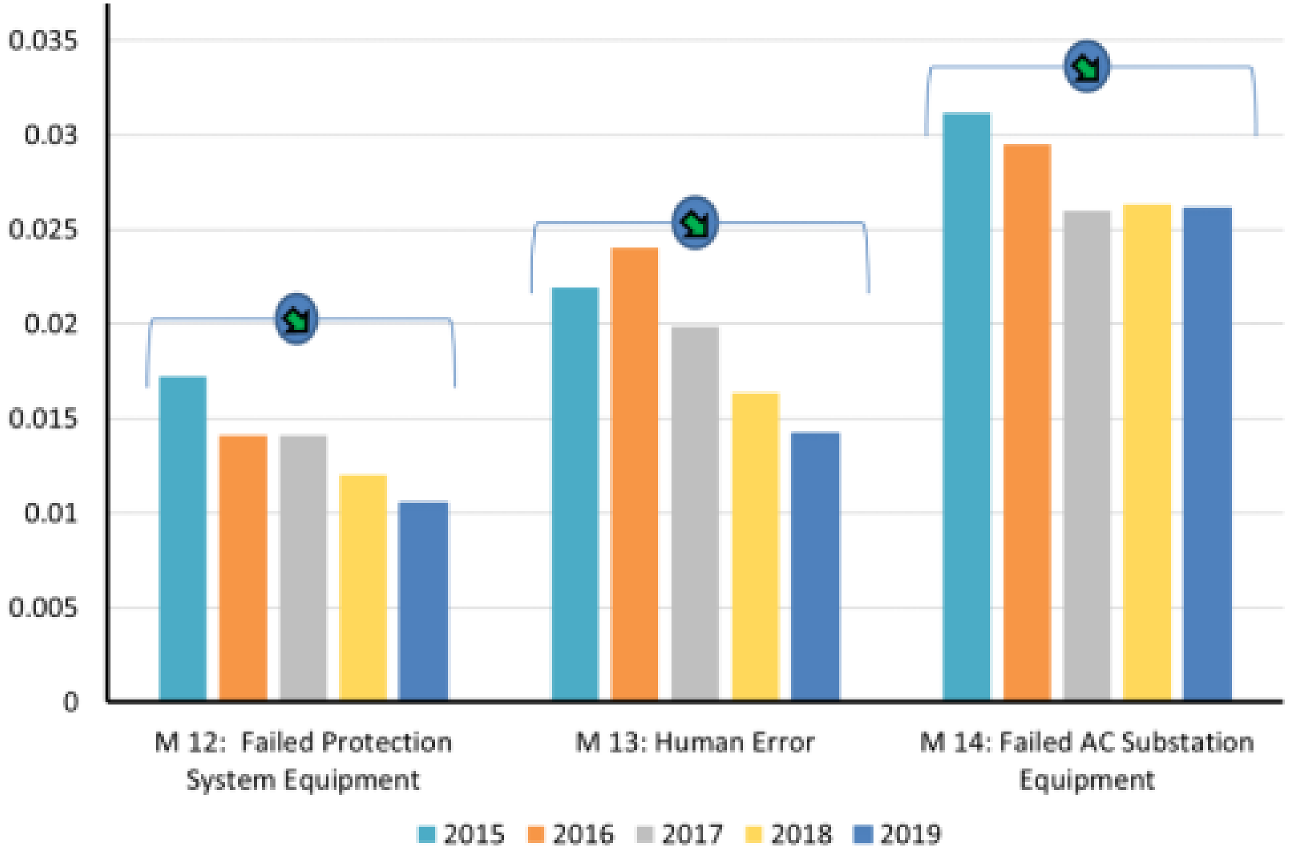
Drifting to Failure Concept


Expectations: Desired approach to work (as imagined)
Normal Practices: Work as actually performed
High
Low
Reliability
Time
Managements Stated Expectations
Drift
"Normal" Practice
Real Margin for Error
Error
Threats to Reliability
RISK CLUSTERS - Programmatic deficiencies, deficiencies in barriers and defenses, Latent organizational weaknesses and conditions Errors in human performance and contextual factors Equipment design and/or maintenance issues
Latent Errors
unnoticed at the time made; often deeply or embedded within system.

* Adapted from Muschara Error Management Consulting, LLC

2015-2019 Outages per Circuit (100 kV+)

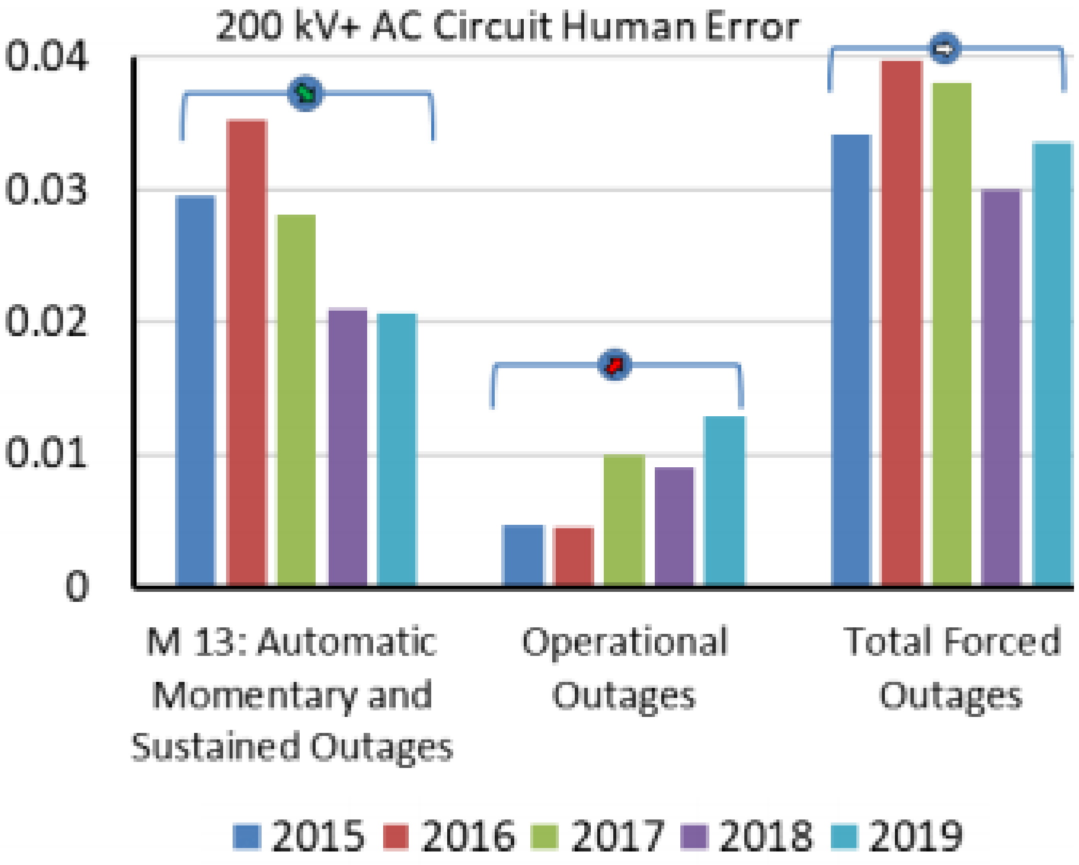
Number of transmission outages from AC circuits and transformers caused by human error is decreasing

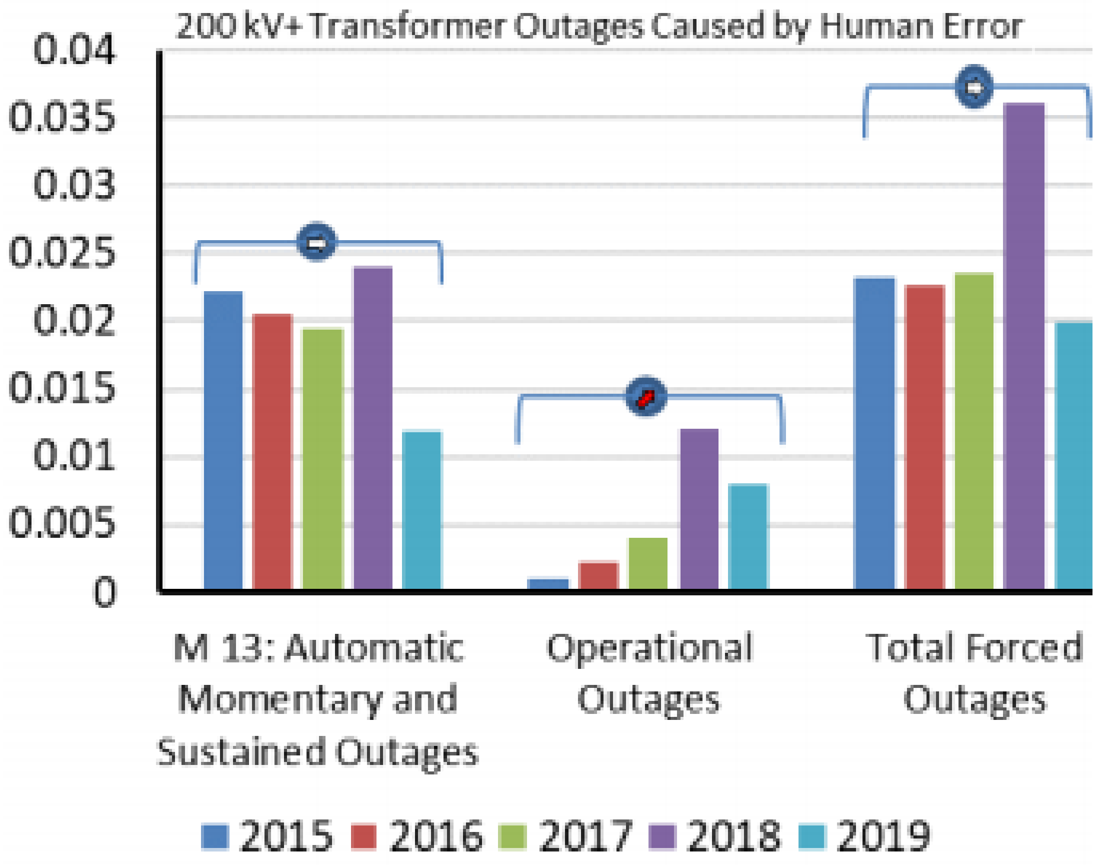


https://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/NERC_SOR_2020.pdf

Human Error Outages (100 kV+)

Number of operational outages from AC circuits and transformers caused by human error are increasing





Events Involving Human Error

- Job scoping did not identify special circumstances and/or conditions
- System interactions not considered or identified
- Inadequate work package preparation
- Risks/consequences associated with change not adequately reviewed/assessed
- Management policy guidance or expectations are not well-defined, understood or enforced

Maximizing Human Performance

We must understand that people will be people!

Make it easy for employees to do the right thing.

Make it hard for employees to do the wrong thing.

**Make it so that when they do the wrong thing,
it doesn’t lead to a catastrophe!**

**Make the system conform to the people,
not the other way around!**

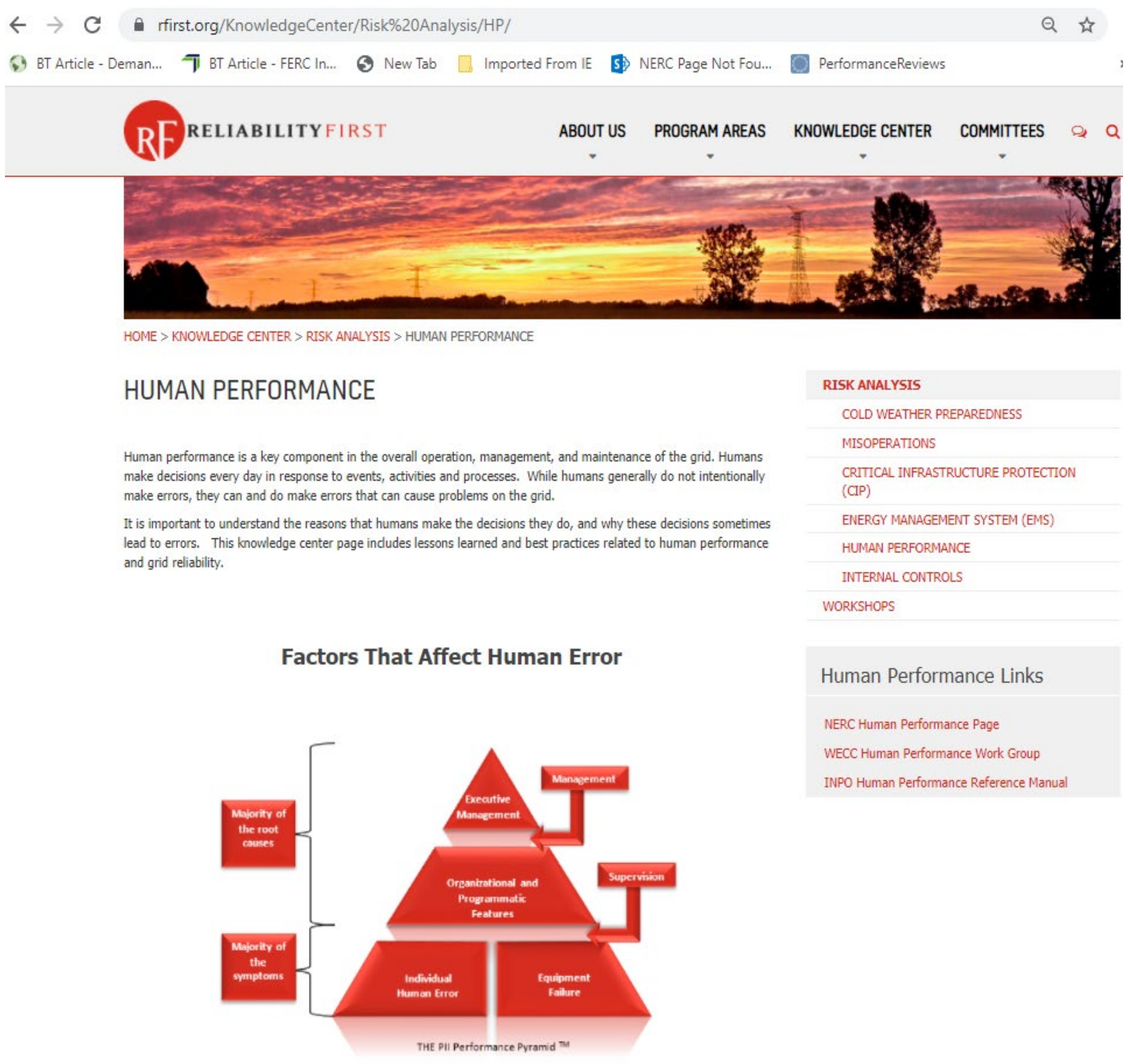
Create an environment that allows feedback and adaptation!

RF Human Performance Community of Excellence

A Community of Excellence (CoE) is a group of people who share an interest or passion for something they do, and learn how to do it better as they interact regularly with other colleagues in their field of expertise.

Intended Audience:
Human Performance Professionals from the ReliabilityFirst Entities

RF Knowledge Center



HOME > KNOWLEDGE CENTER > RISK ANALYSIS > HUMAN PERFORMANCE

HUMAN PERFORMANCE

Human performance is a key component in the overall operation, management, and maintenance of the grid. Humans make decisions every day in response to events, activities and processes. While humans generally do not intentionally make errors, they can and do make errors that can cause problems on the grid.

It is important to understand the reasons that humans make the decisions they do, and why these decisions sometimes lead to errors. This knowledge center page includes lessons learned and best practices related to human performance and grid reliability.

Factors That Affect Human Error

RISK ANALYSIS
- COLD WEATHER PREPAREDNESS
- MISOPERATIONS
- CRITICAL INFRASTRUCTURE PROTECTION (CIP)
- ENERGY MANAGEMENT SYSTEM (EMS)
- HUMAN PERFORMANCE
- INTERNAL CONTROLS

WORKSHOPS

Human Performance Links

- NERC Human Performance Page
- WECC Human Performance Work Group
- INPO Human Performance Reference Manual

https://rfirst.org/KnowledgeCenter/Risk%20Analysis/HP/

Technical Talk with RF

Technical Talk with RF is scheduled the third Monday of each month from 2:00-3:30 p.m.

Save the Date for our next event,
Monday, August 16

NERC’s Dr. Ryan Quint plus RF’s Johnny Gest and David Sopata will be providing an update from the Security Integration and Technology Enablement Subcommittee (SITES) including an update on the upcoming IEEE-NERC Technical Report. Also NERC’s Clayton Calhoun will be presenting with RF’s Brian Thiry on the recently released FERC and ERO Enterprise Joint Report on Real-time Assessments.

Follow us on:

SERC & ReliabilityFirst Joint Webinar on Cold Weather Preparedness

Tuesday, August 24, 9:00 a.m. – 12:00 p.m.

This webinar will utilize the results of the 2020/2021 SERC Winter Weather Survey plus industry experts across the ERO and industry to provide insight into Cold Weather best practices with a focus on exposed equipment, training, documentation, experiences, and lessons learned.

Registration Link

Follow us on:

RF Internal Controls Webinar

Wednesday, August 25, 1:00 – 4:30 p.m. EDT

Building on our last Internal Controls event, this webinar will focus on the importance of culture within the internal control program; how and why the tone at the top, tone at the middle and the acceptance throughout is crucial; and how that can drive the appropriate mitigation of risk, as well as reliability, resilience and security.

This event is especially relevant for C-suite and Vice Presidents, directors, supervisors, managers, primary/alternate compliance contacts, plus SMEs involved in creating and managing internal controls.

Registration Link

Follow us on:

RF Annual Reliability and Compliance (Virtual) Workshop

Wednesday, September 22, 1:00 – 5:00 p.m. EDT
Thursday, September 23, 1:00 – 5:00 p.m. EDT

The theme is Building Sustainable Programs, and the goal is to help Entities and stakeholders establish, improve and maintain their efforts in critical areas. This includes gaining a deeper understanding of why and how sustainable programs (e.g., compliance programs, internal control programs, Facility Ratings, implementing new standards, etc.) significantly contribute to greater grid reliability, security and resilience, as well as risk mitigation.

This event is especially relevant for directors, supervisors, managers, primary/alternate compliance contacts,plus SMEs involved in creating and managing internal controls.

Registration Link

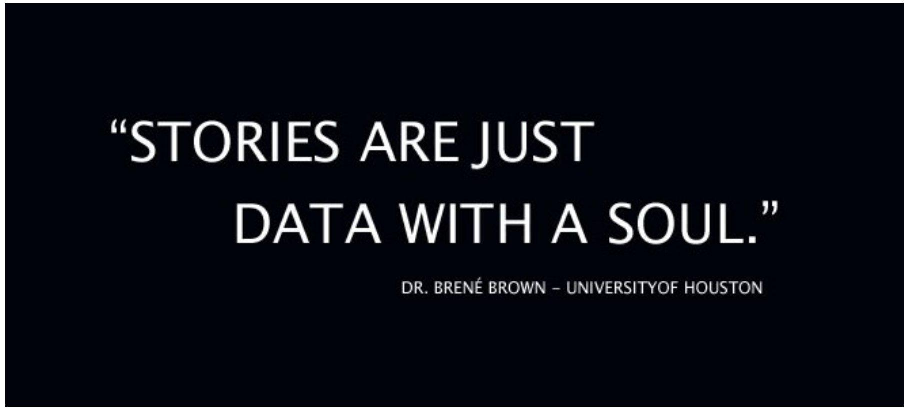
RF

Follow us on:

We Are All Connected!

These engagements are about building relationships with our stakeholders so we are all successful!

Tell Some Stories!



“STORIES ARE JUST
DATA WITH A SOUL.”

DR. BRENÉ BROWN – UNIVERSITYOF HOUSTON

OPG's Total Health Strategy

Do you have a coping crisis?

August 12, 2021

ONTARIO POWER GENERATION

PUBLIC

Agenda

1 | Background

2 | Why a Total Health Strategy

3 | Business Case Model

4 | OPG's Total Health Journey

5 | OPG Successes to Date

6 | Elements of Success

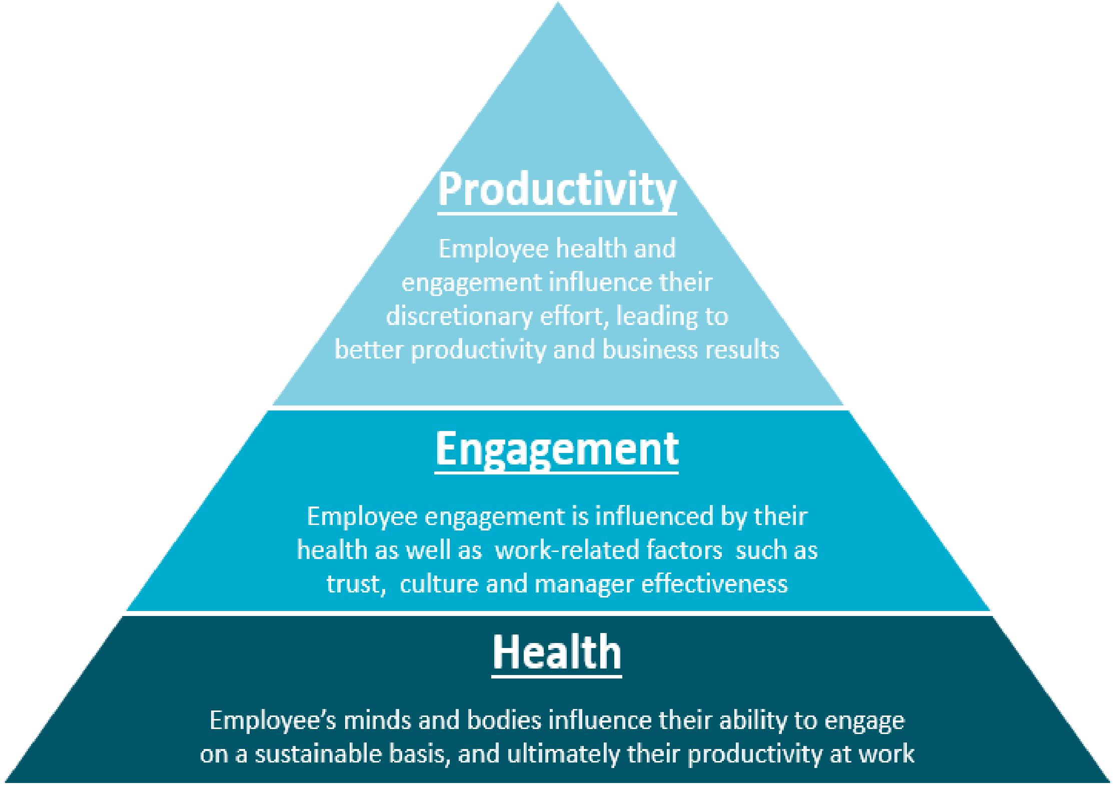
Who is Ontario Power Generation?

- OPG is one of the largest electricity producers in North America. OPG operates/maintains 66 hydroelectric stations, 2 nuclear stations, 1 biomass station, 1 dual-fueled oil and gas station, 1 solar facility and 4 natural gas-fueled stations owned and operated by wholly-owned subsidiary Atura Power.
- OPG also owns or co-owns a number of additional facilities in Ontario and the United States. This includes Eagle Creek Renewable Energy, Brighton Beach, and Portlands Energy Centre.
- OPG has 18 910 MW of in-service generating capacity, 90%+ free of carbon emissions and employs over 9300 skilled workers.

Why A Total Health Strategy?

- Unfavourable Auditor General Report (2013) around employee sick leave statistics.
- The COVID-19 pandemic has had a detrimental effect on the mental health of Canadians.
- Want a health program that mirrors our safety program.
- An understanding of the value of health on engagement and productivity.
- It's the right thing to do.

Health Drives Productivity



Productivity

Employee health and engagement influence their discretionary effort, leading to better productivity and business results

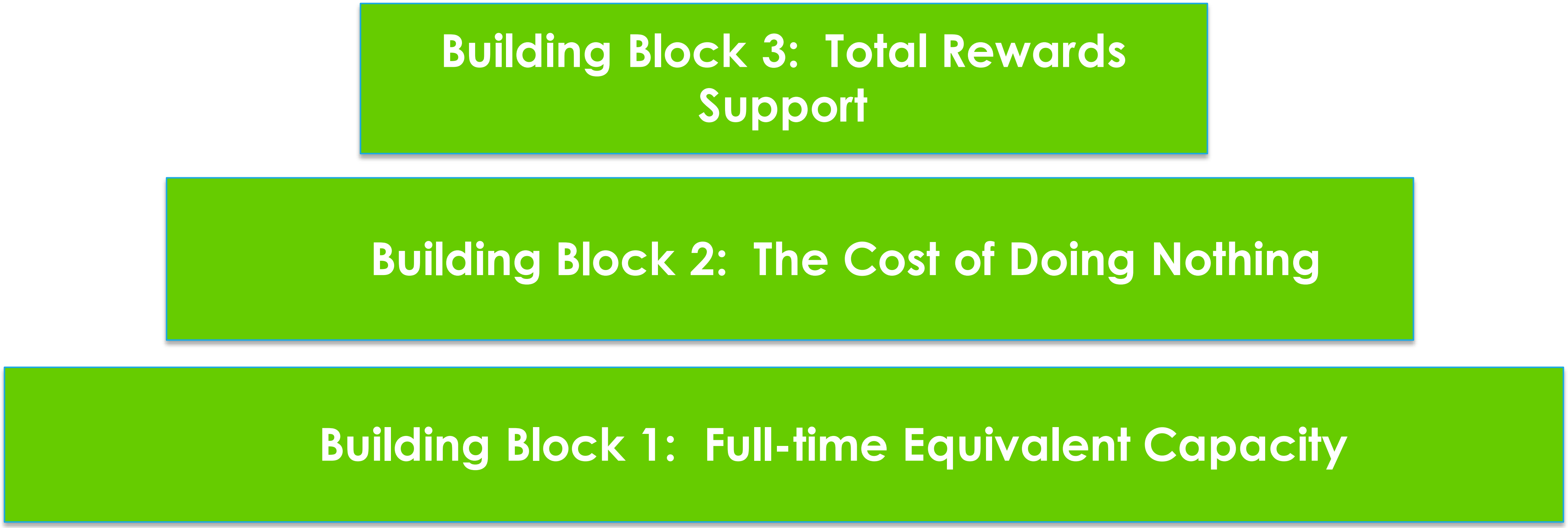
Engagement

Employee engagement is influenced by their health as well as work-related factors such as trust, culture and manager effectiveness

Health

Employee's minds and bodies influence their ability to engage on a sustainable basis, and ultimately their productivity at work

The Total Health business case model consists of 3 building blocks



Building Block 3: Total Rewards Support

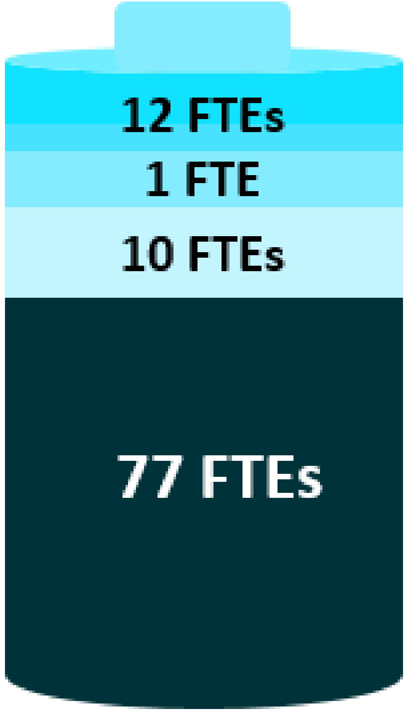
Building Block 2: The Cost of Doing Nothing

Building Block 1: Full-time Equivalent Capacity

Source: Lifespeak THI 2018 (Formerly Morneau Shepell)

Building Block 1: Understanding FTE capacity, a 100 employee example

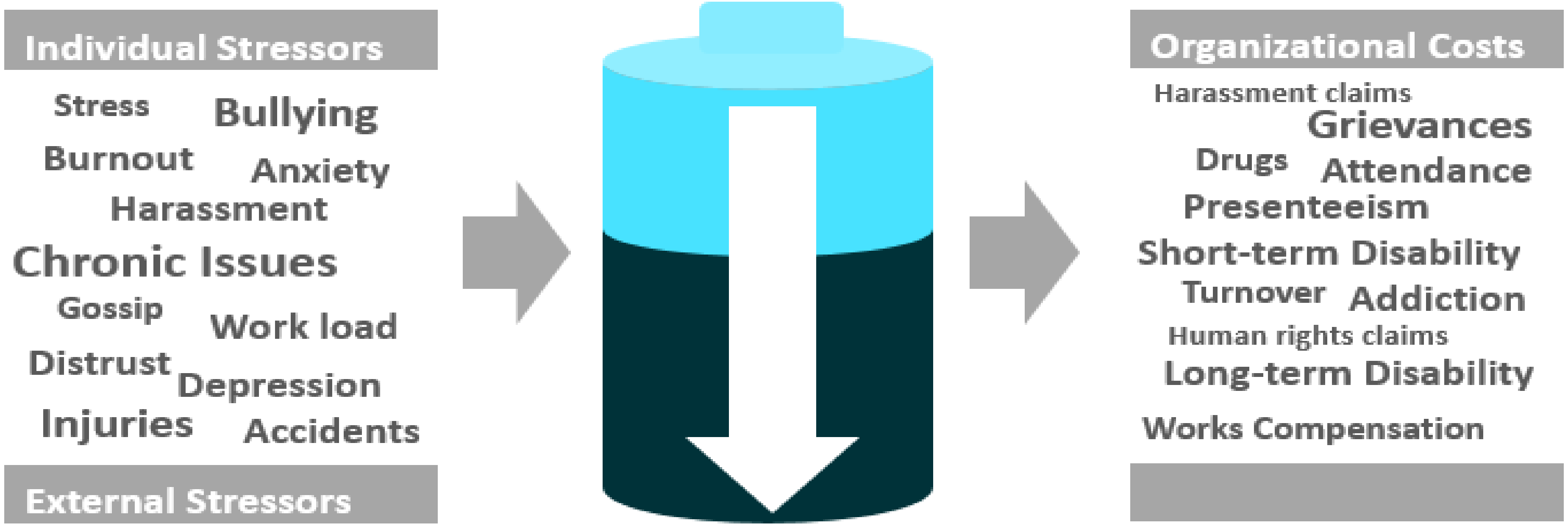
- If we have 100 employees, working at 8 hours per day, this equates to 800 hours of work units per day
- **Discretionary Effort –** this is the human condition and may never be 100%; our benchmarks show an average of 88% or **12** FTEs.
- **Absenteeism –** every day, some employees miss work. Morneau Shepell THI benchmarks show that for every 100 FTEs each day **1** can be expected to miss work.
- **Presenteeism –** every day, some employees come to work feeling unwell. Morneau Shepell THI benchmarks show this is about **10** employees.
- This model suggests that in this 100-FTE organization on a typical day the actual number of FTEs operating is **77**, even though the number of employees on site may be higher.



Source: Lifeworks THI 2018 (formerly Morneau Shepell)

Building Block 2: Understanding the Cost of Doing Nothing (CODN)

- There are factors that can drain an organization's and employee's batteries.
- These drains can result in costs that impact productivity and the bottom line.



Individual Stressors

Stress Bullying Burnout Anxiety Harassment Chronic Issues Gossip Work load Distrust Depression Injuries Accidents

External Stressors

Organizational Costs

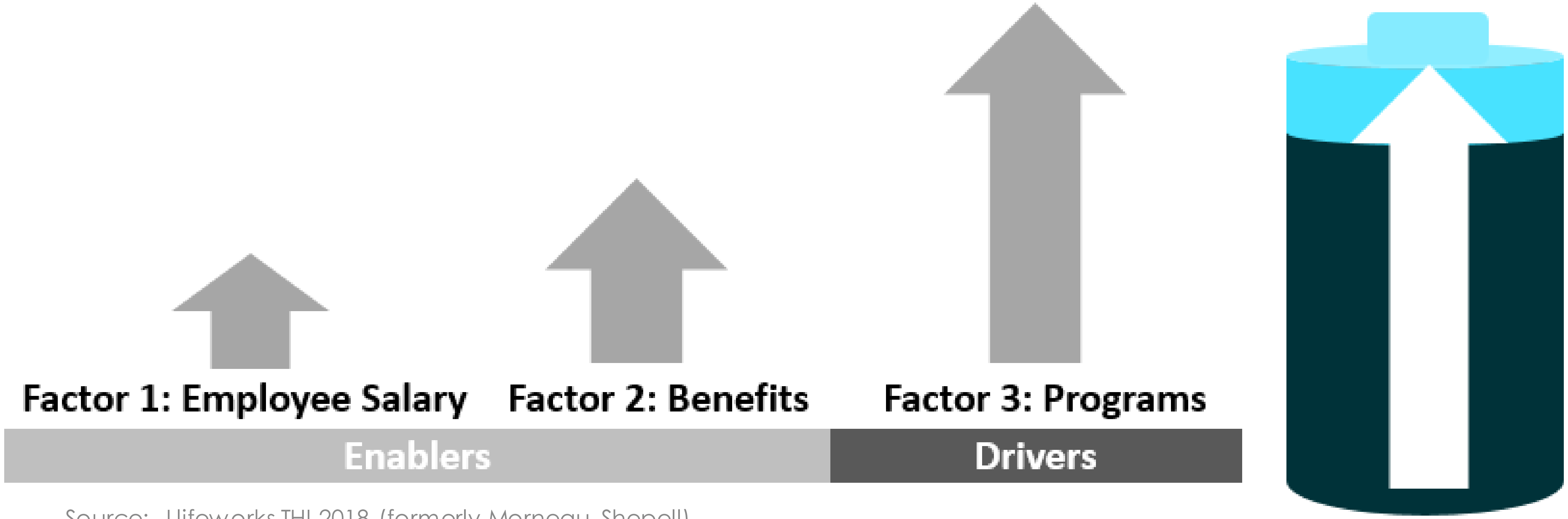
Harassment claims Grievances Drugs Attendance Presenteeism Short-term Disability Turnover Addiction Human rights claims Long-term Disability Works Compensation

Source: Lifeworks THI 2018 (formerly Morneau Shepell)

Building Block 3: Understanding Total Rewards

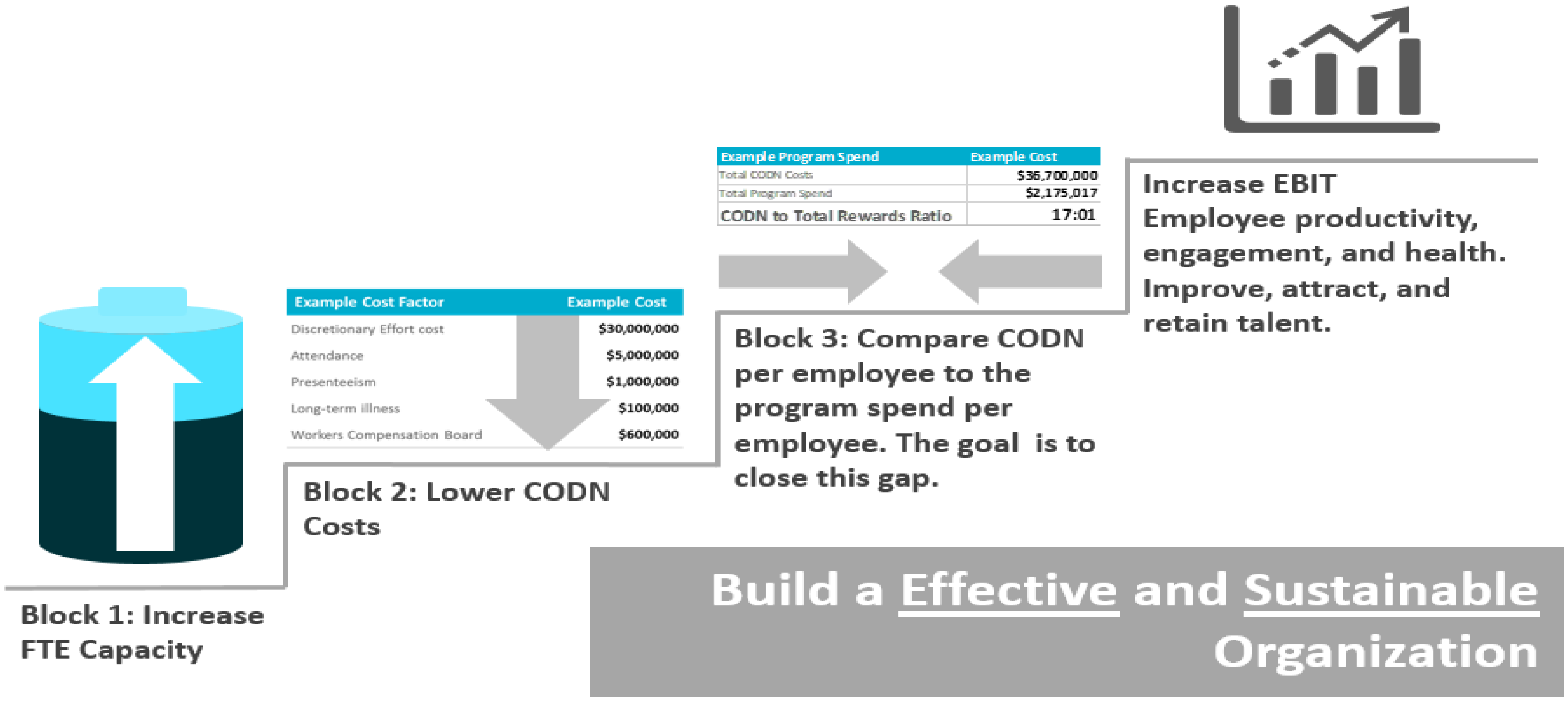
Support, factors that charge employee capacity

- Organizations use three factors to charge the organization's and individuals' batteries. These factors can be divided into enablers and drivers.
- The research suggests that evidence-based programs provide the biggest opportunity to have a major impact on CODN.



Source: Llifeworks THI 2018 (formerly Morneau Shepell)

Laying Your Foundation for a Total Health Strategy



Example Cost Factor	Example Cost
Discretionary Effort cost	$30,000,000
Attendance	$5,000,000
Presenteeism	$1,000,000
Long-term illness	$100,000
Workers Compensation Board	$600,000

Example Program Spend	Example Cost
Total CODN Costs	$36,700,000
Total Program Spend	$2,175,017
CODN to Total Rewards Ratio	17:01

Block 1: Increase FTE Capacity

Block 2: Lower CODN Costs

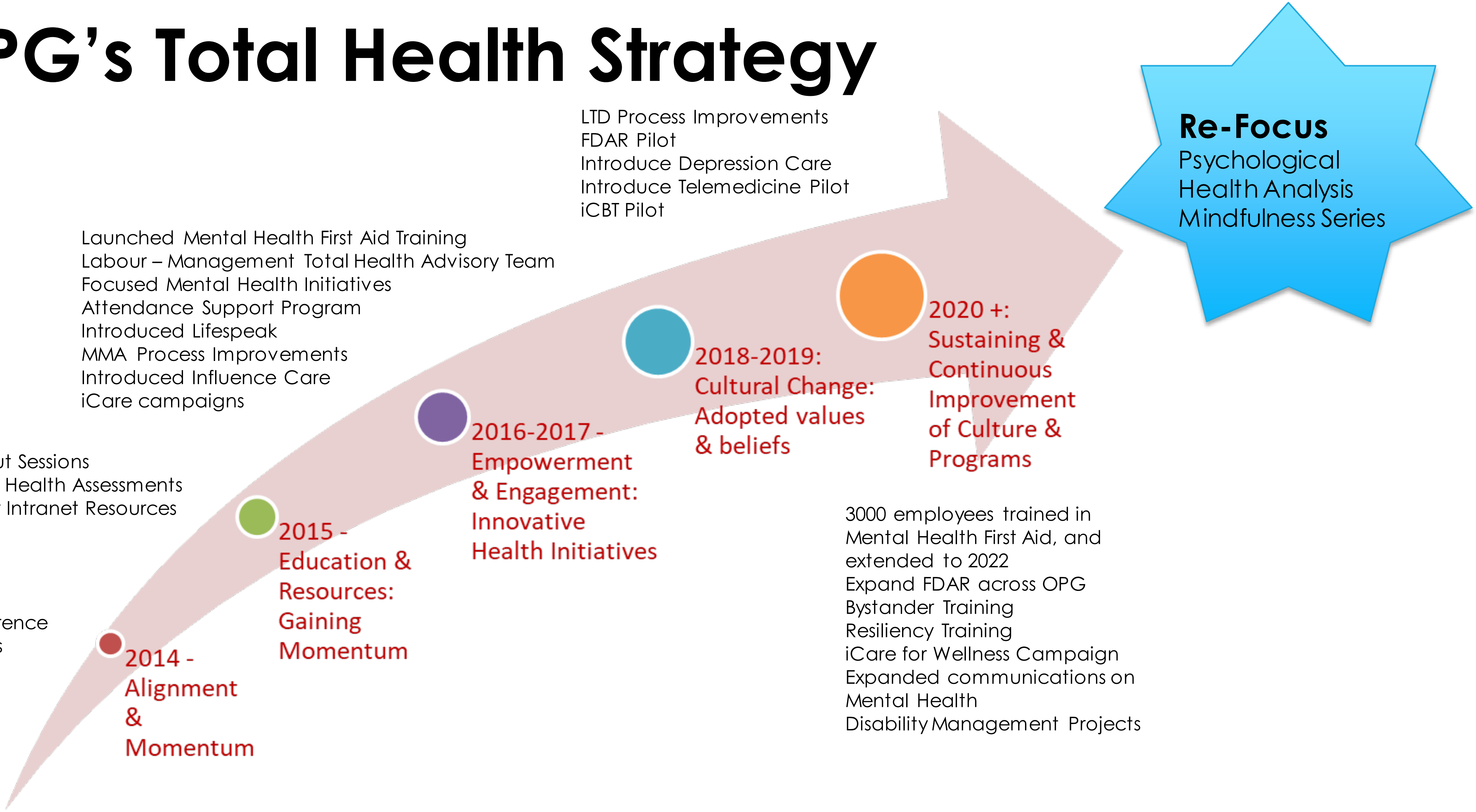
Block 3: Compare CODN per employee to the program spend per employee. The goal is to close this gap.

Increase EBIT
Employee productivity, engagement, and health. Improve, attract, and retain talent.

Build a Effective and Sustainable Organization

Source: Lifeworks THI 2018 (formerly Morneau Shepell)

OPG's Total Health Strategy



Total Health Conference
Alignment Roll Outs

2014 - Alignment & Momentum

EFAP Roll Out Sessions
Online Total Health Assessments
Building Our Intranet Resources

2015 - Education & Resources: Gaining Momentum

Launched Mental Health First Aid Training
Labour – Management Total Health Advisory Team
Focused Mental Health Initiatives
Attendance Support Program
Introduced Lifespeak
MMA Process Improvements
Introduced Influence Care
iCare campaigns

2016-2017 - Empowerment & Engagement: Innovative Health Initiatives

LTD Process Improvements
FDAR Pilot
Introduce Depression Care
Introduce Telemedicine Pilot
iCBT Pilot

2018-2019: Cultural Change: Adopted values & beliefs

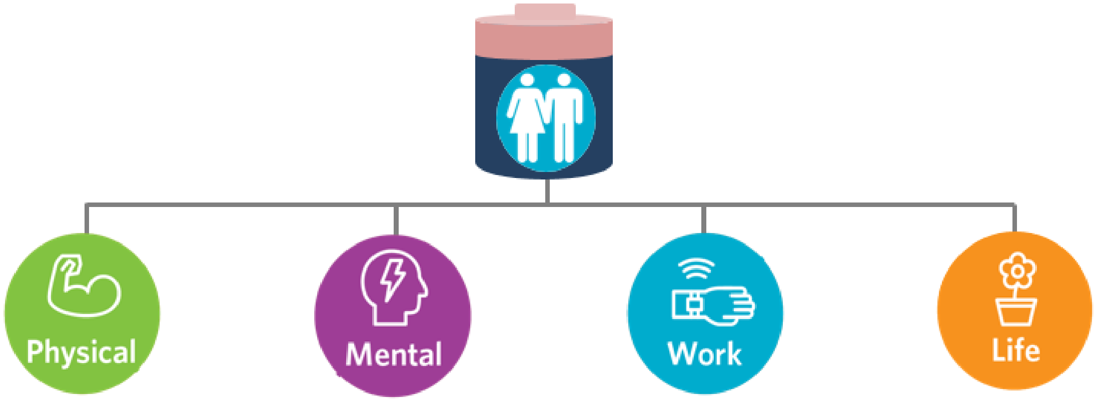
2020 +: Sustaining & Continuous Improvement of Culture & Programs

3000 employees trained in Mental Health First Aid, and extended to 2022
Expand FDAR across OPG
Bystander Training
Resiliency Training
iCare for Wellness Campaign
Expanded communications on Mental Health
Disability Management Projects

Re-Focus
Psychological Health Analysis
Mindfulness Series

How Do You Generate Improvement?

Total Health Programming EXAMPLE



Prevention	- Global challenges - Health club membership	- Coping skills Training - Mindfulness Coaching	- Employee recognition - Orientation	- Mindfulness Coaching - Regular Medical Check-up
Early invention	- EFAP - Flu Program - Virtual Doctor	- EFAP - Stress Management Workshop - iCBT	- EFAP - Career Coaching	- EFAP - Work-Life Resiliency Coaching
Support	- EFAP - Smoking Cessation Resources	- EFAP - Grief Counselling Resources - Trauma Support	- EFAP - Respectful Workplace Support	- EFAP - Legal Advice and Referral Services

OPG's Successes to Date

- Decrease in average closed claim duration across top driver diagnostic catergories (since 2016):
  - ✓ 22% decrease in duration of mental health cases ($2.75M) by 2019, a slight increase in 2020 (but less than national norms)
  - ✓ 70% of our claims are resolved in less than 20 days of absence.
- ▪ 28% decrease in average major medical absence days lost per 1000 employees.
- ▪ 40% reduction in new LTD claims
- ▪ First Day Absence Reporting Program saved just under $1M (878 employees in program) in two years. It is expected the savings would range from $2M to $4.5M per year across OPG. 2020 was an anomaly year with a significant reduction in sick leave.
- ▪ 6% increase in Return to Work (86%)
- ▪ 82% increase in trauma support in 2018 and 2019, slight reduction in 2020 (WFH)
- ▪ 20% increase in counselling services for urgent mental health issues

Key Elements of Success

- For those interested in undertaking a similar strategy, the following factors were instrumental in the successes to date:
  - Leadership commitment and support
  - Internal resources to support the program
  - Union communication and involvement
  - A shift in employee culture
  - A strong partnership with your service provider.

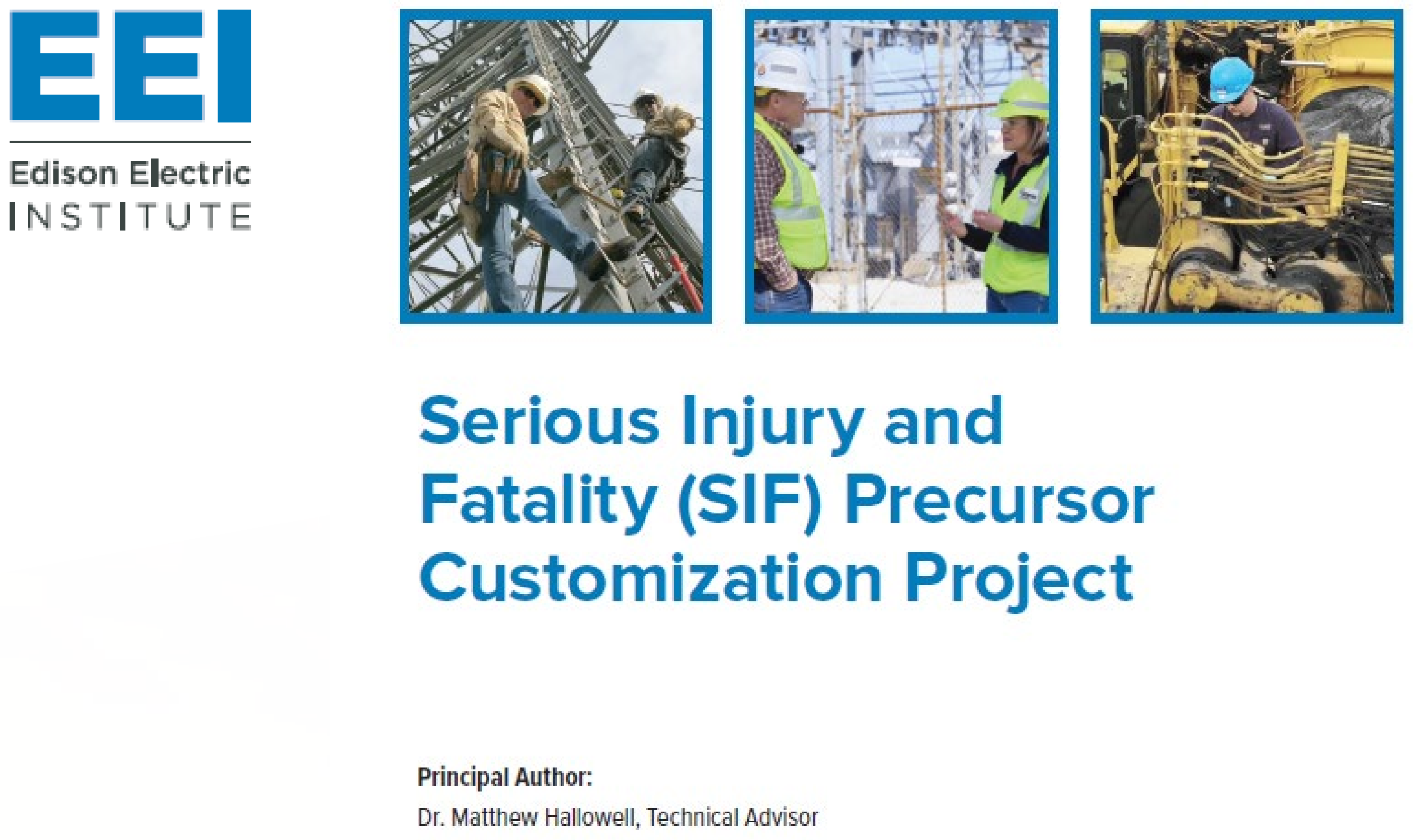
Questions?

Contact info: Tanya.hickey@opg.com

ONTARIO POWER GENERATION

Edison Electric Institute (EEI)
Serious Injury and Fatality (SIF) precursors

Providing proactive, real-time feedback



Edison Electric INSTITUTE

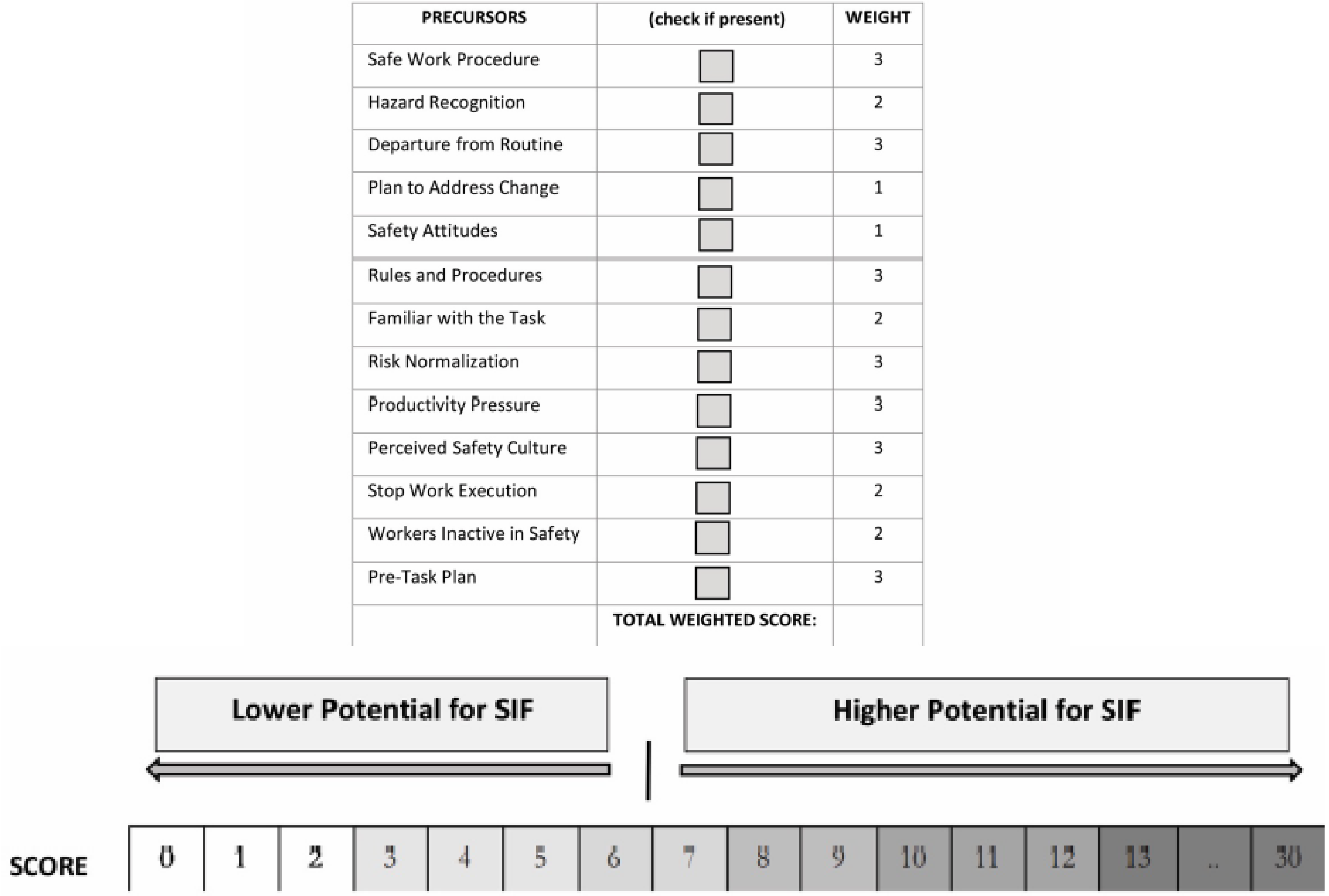
Serious Injury and Fatality (SIF) Precursor Customization Project

Principal Author:
Dr. Matthew Hallowell, Technical Advisor

EEI published the SIF precursors in April 2019

- Recognized that SIFs had plateaued over the last decade
- EEI assembled a team of 21 safety professionals from different industries
- They identified 59 SIF precursors--and narrowed it to 13
- Developed a scorecard with weighted values assigned to each of the 13 SIF Precursors
- The scorecard is used to collectively identify the potential for a SIF before work begins

EEI SIF precursors Analysis Scorecard



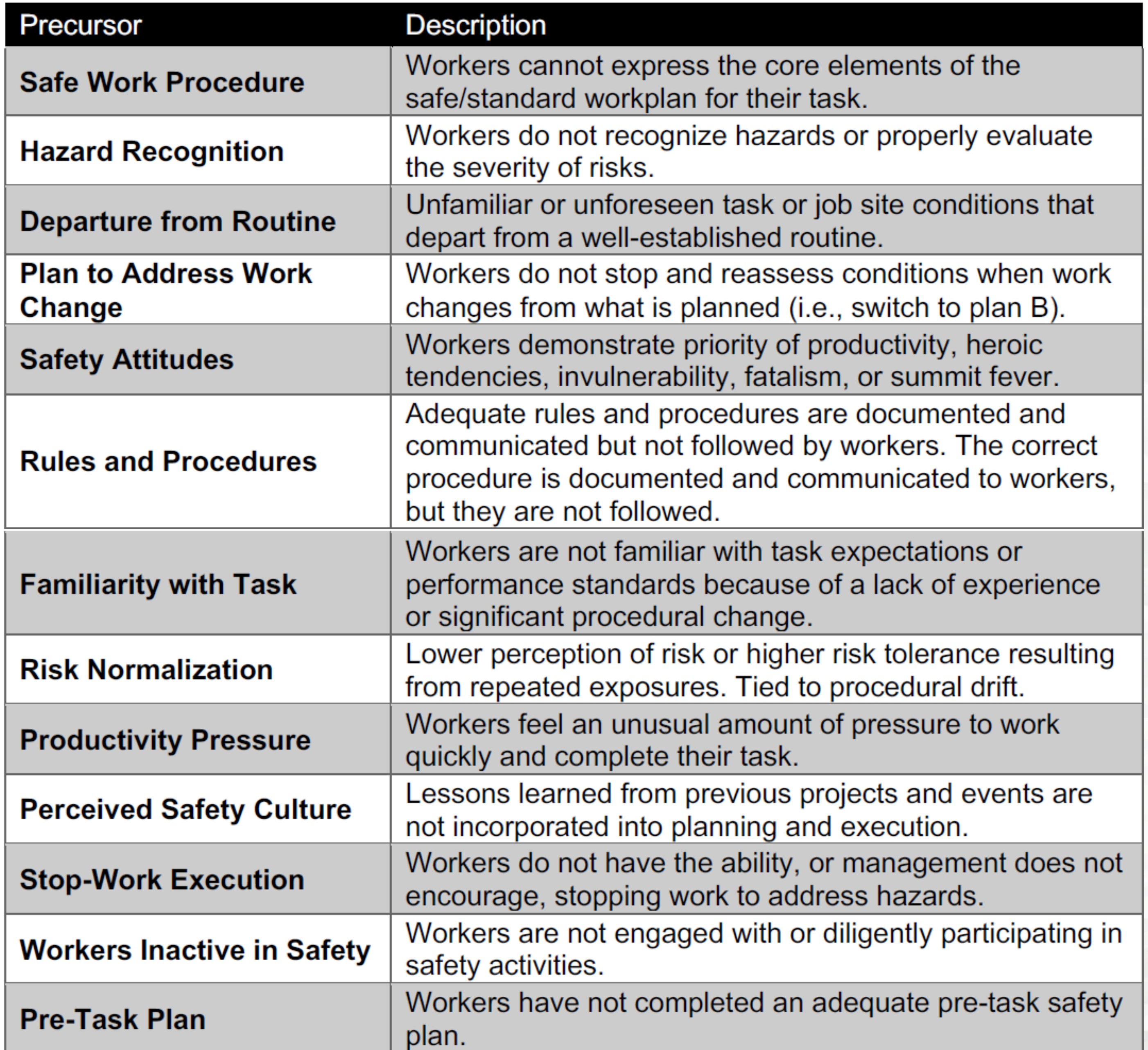
PRECURSORS	(check if present)	WEIGHT
Safe Work Procedure	□	3
Hazard Recognition	□	2
Departure from Routine	□	3
Plan to Address Change	□	1
Safety Attitudes	□	1
Rules and Procedures	□	3
Familiar with the Task	□	2
Risk Normalization	□	3
Productivity Pressure	□	3
Perceived Safety Culture	□	3
Stop Work Execution	□	2
Workers Inactive in Safety	□	2
Pre-Task Plan	□	3
	TOTAL WEIGHTED SCORE:	

Lower Potential for SIF

Higher Potential for SIF

SCORE	0	1	2	3	4	5	6	7	8	9	10	11	12	13	..	30

KnowledgeVine



Precursor	Description
Safe Work Procedure	Workers cannot express the core elements of the safe/standard workplan for their task.
Hazard Recognition	Workers do not recognize hazards or properly evaluate the severity of risks.
Departure from Routine	Unfamiliar or unforeseen task or job site conditions that depart from a well-established routine.
Plan to Address Work Change	Workers do not stop and reassess conditions when work changes from what is planned (i.e., switch to plan B).
Safety Attitudes	Workers demonstrate priority of productivity, heroic tendencies, invulnerability, fatalism, or summit fever.
Rules and Procedures	Adequate rules and procedures are documented and communicated but not followed by workers. The correct procedure is documented and communicated to workers, but they are not followed.
Familiarity with Task	Workers are not familiar with task expectations or performance standards because of a lack of experience or significant procedural change.
Risk Normalization	Lower perception of risk or higher risk tolerance resulting from repeated exposures. Tied to procedural drift.
Productivity Pressure	Workers feel an unusual amount of pressure to work quickly and complete their task.
Perceived Safety Culture	Lessons learned from previous projects and events are not incorporated into planning and execution.
Stop-Work Execution	Workers do not have the ability, or management does not encourage, stopping work to address hazards.
Workers Inactive in Safety	Workers are not engaged with or diligently participating in safety activities.
Pre-Task Plan	Workers have not completed an adequate pre-task safety plan.

- Our analysis is primarily performed during work observations (not only before the work starts) to more accurately identify the behaviors.

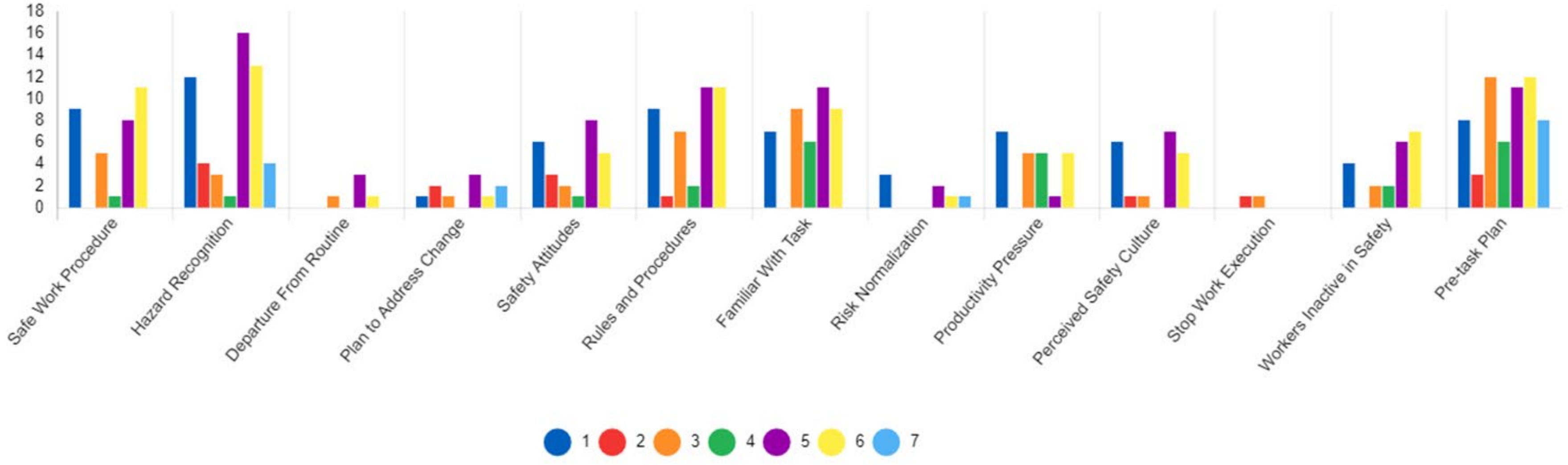
- In this way, KnowledgeVine interacts with the crew in a proactive manner, coaching them in real-time to ensure human performance behaviors are understood and demonstrated.

- Each contractor is distinguished by a particular color code on the dashboard for use by the utility in assessing performance.

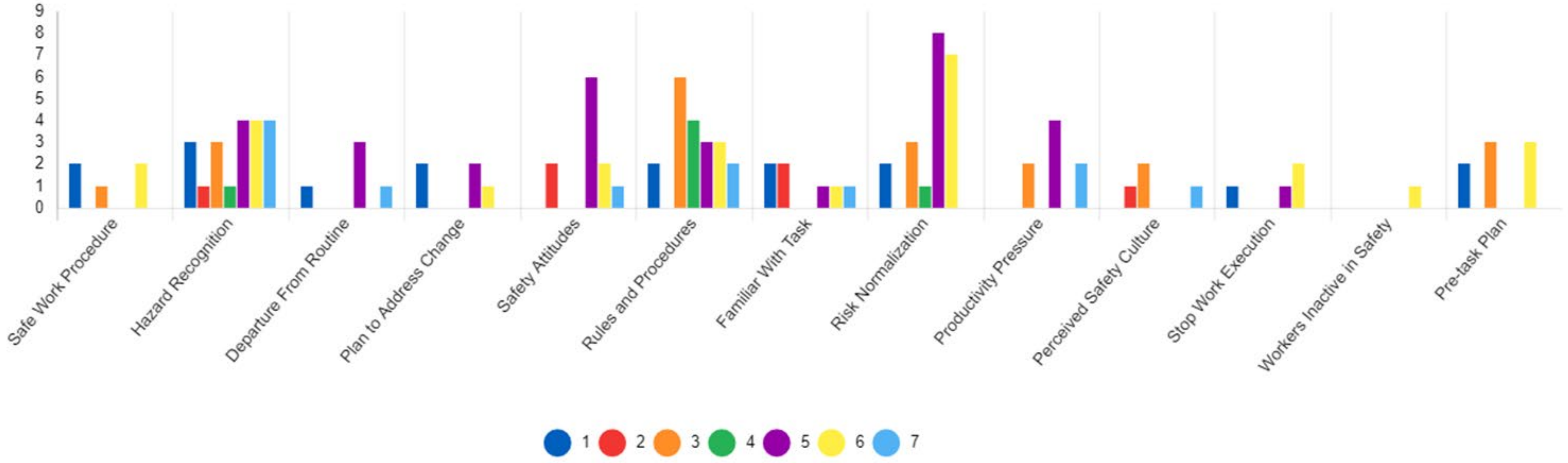
- Each contractor has their own dashboard that displays only their data. This is used during periodic meetings to determine if any actions are warranted.

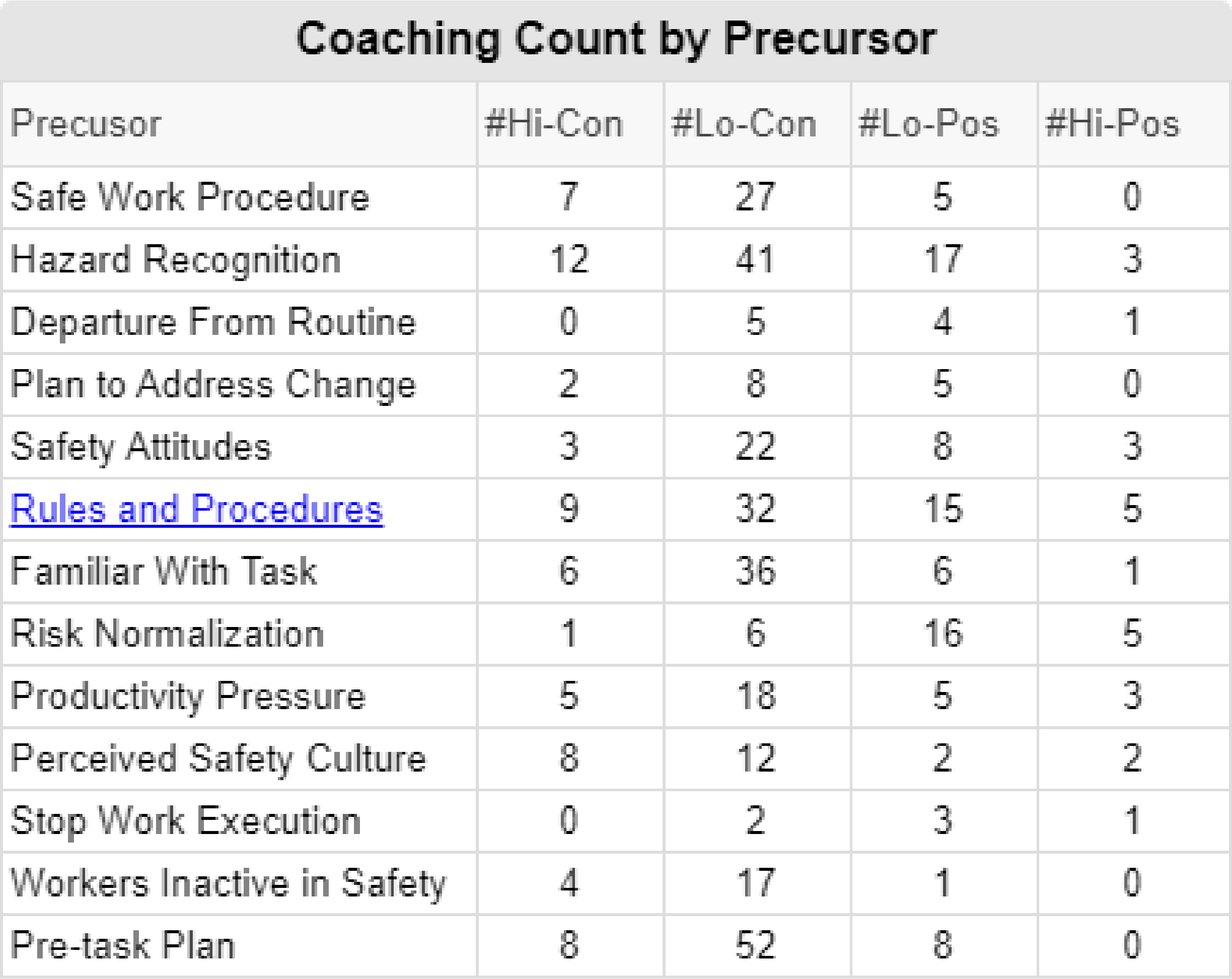
- Our field specialists flag each observation as either *Positive* or *Constructive*, with two levels assigned to each of these categories.

Positive Coaching - EEI Precursors



Constructive Coaching - EEI Precursors





Coaching Count by Precursor

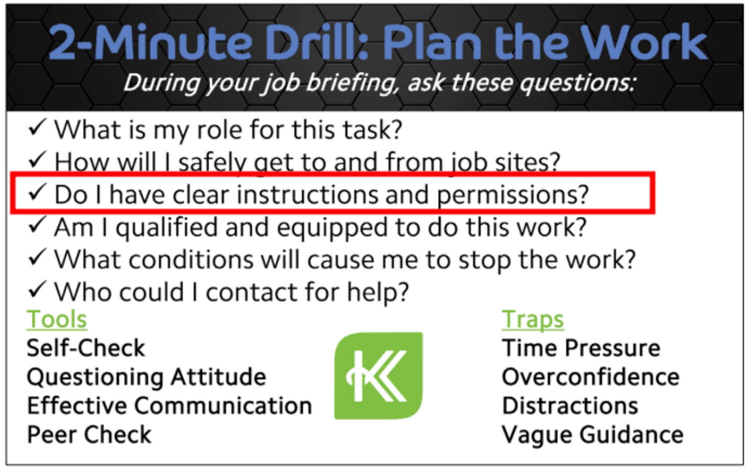
Precusor	#Hi-Con	#Lo-Con	#Lo-Pos	#Hi-Pos
Safe Work Procedure	7	27	5	0
Hazard Recognition	12	41	17	3
Departure From Routine	0	5	4	1
Plan to Address Change	2	8	5	0
Safety Attitudes	3	22	8	3
Rules and Procedures	9	32	15	5
Familiar With Task	6	36	6	1
Risk Normalization	1	6	16	5
Productivity Pressure	5	18	5	3
Perceived Safety Culture	8	12	2	2
Stop Work Execution	0	2	3	1
Workers Inactive in Safety	4	17	1	0
Pre-task Plan	8	52	8	0

Things to consider…

SIF Precursor #6: Rules and Procedures

(Adequate rules and procedures are documented and communicated AND followed by workers.)

- Executive Level-
  - ASK – Have we assessed the processes and procedures we expect employees to use while working? When was the last time we communicated the importance of adherence?
  - DO – Spend some time in the work environment watching employees perform routine tasks. Seek their input on how to make the work instructions better, safer, and more efficient.
- Supervisors and Managers –
  - ASK – Have I read the instructions or procedures that my crew are being asked to follow? Do I understand the process? Do I demonstrate the importance of following the rules through my actions?
  - DO – Engage employees and ask for specifics regarding the work process. Provide demonstrative coaching that ensures employees know you expect them to follow rules and to stop and get clarity when they can't. Act and remove unclear instructions.
- Individuals –
  - ASK – Do I really understand what I am about to do? Is there a rule, checklist, or other instructional guidance that I should be following?
  - DO – Stop when unsure. Get the answer from supervision before attempting to "figure it out." Provide ongoing guidance for process or rule change where it is needed to prevent future mistakes for others.

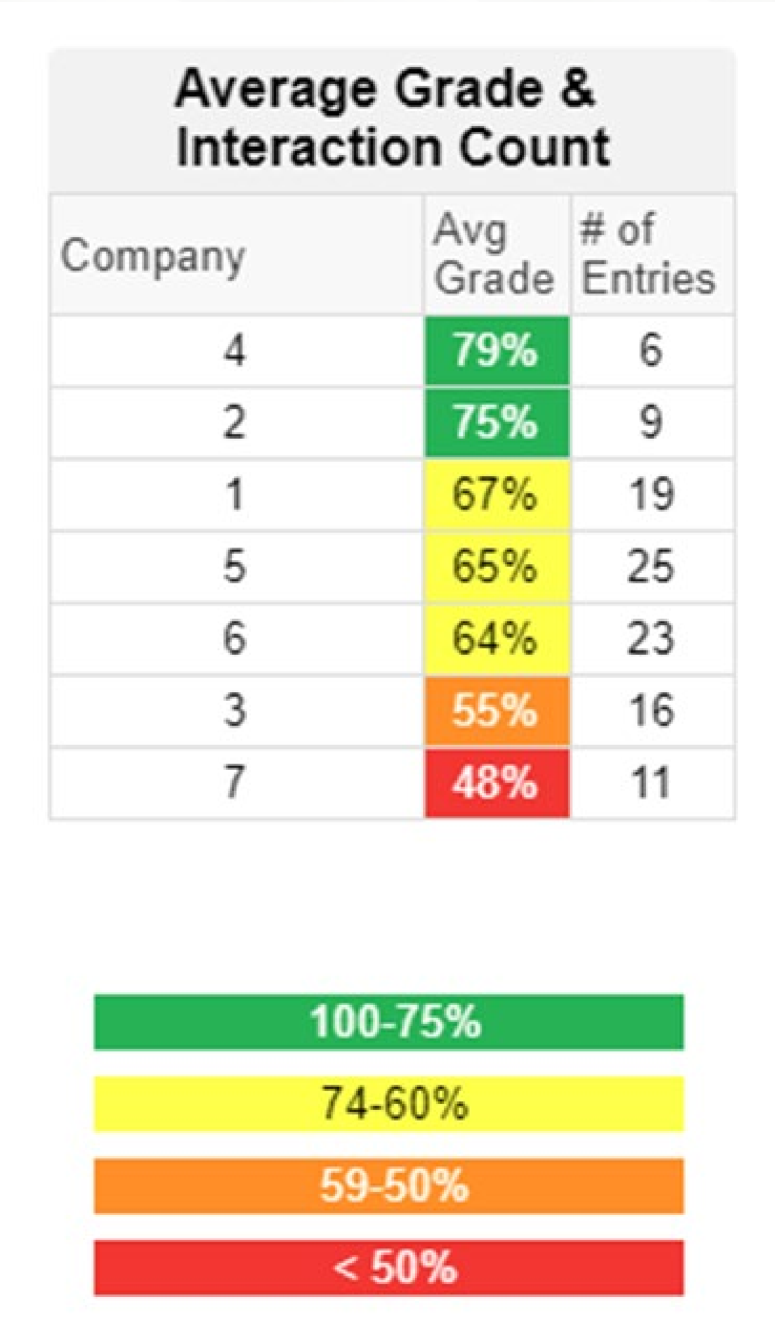


2-Minute Drill: Plan the Work

During your job briefing, ask these questions:

✓ What is my role for this task?
✓ How will I safely get to and from job sites?
✓ Do I have clear instructions and permissions?
✓ Am I qualified and equipped to do this work?
✓ What conditions will cause me to stop the work?
✓ Who could I contact for help?

Tools	Traps
Self-Check	Time Pressure
Questioning Attitude	Overconfidence
Effective Communication	Distractions
Peer Check	Vague Guidance



Average Grade & Interaction Count

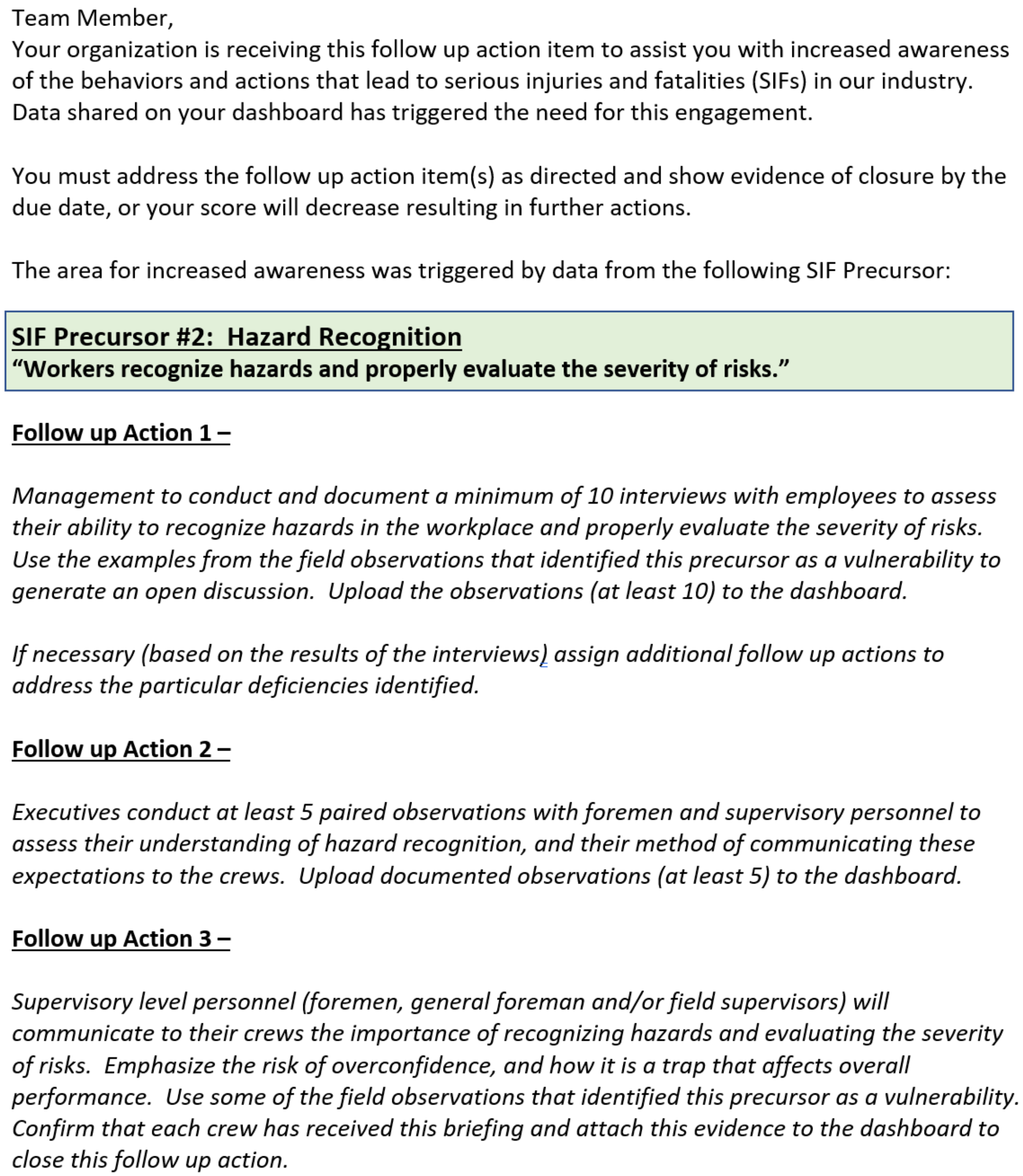
Company	Avg Grade	# of Entries
4	79%	6
2	75%	9
1	67%	19
5	65%	25
6	64%	23
3	55%	16
7	48%	11

🟩 100-75%

🟨 74-60%

🟧 59-50%

🟥 < 50%



Team Member,
Your organization is receiving this follow up action item to assist you with increased awareness of the behaviors and actions that lead to serious injuries and fatalities (SIFs) in our industry. Data shared on your dashboard has triggered the need for this engagement.

You must address the follow up action item(s) as directed and show evidence of closure by the due date, or your score will decrease resulting in further actions.

The area for increased awareness was triggered by data from the following SIF Precursor:

<u>SIF Precursor #2: Hazard Recognition</u>
"Workers recognize hazards and properly evaluate the severity of risks."

<u>Follow up Action 1 –</u>

Management to conduct and document a minimum of 10 interviews with employees to assess their ability to recognize hazards in the workplace and properly evaluate the severity of risks. Use the examples from the field observations that identified this precursor as a vulnerability to generate an open discussion. Upload the observations (at least 10) to the dashboard.

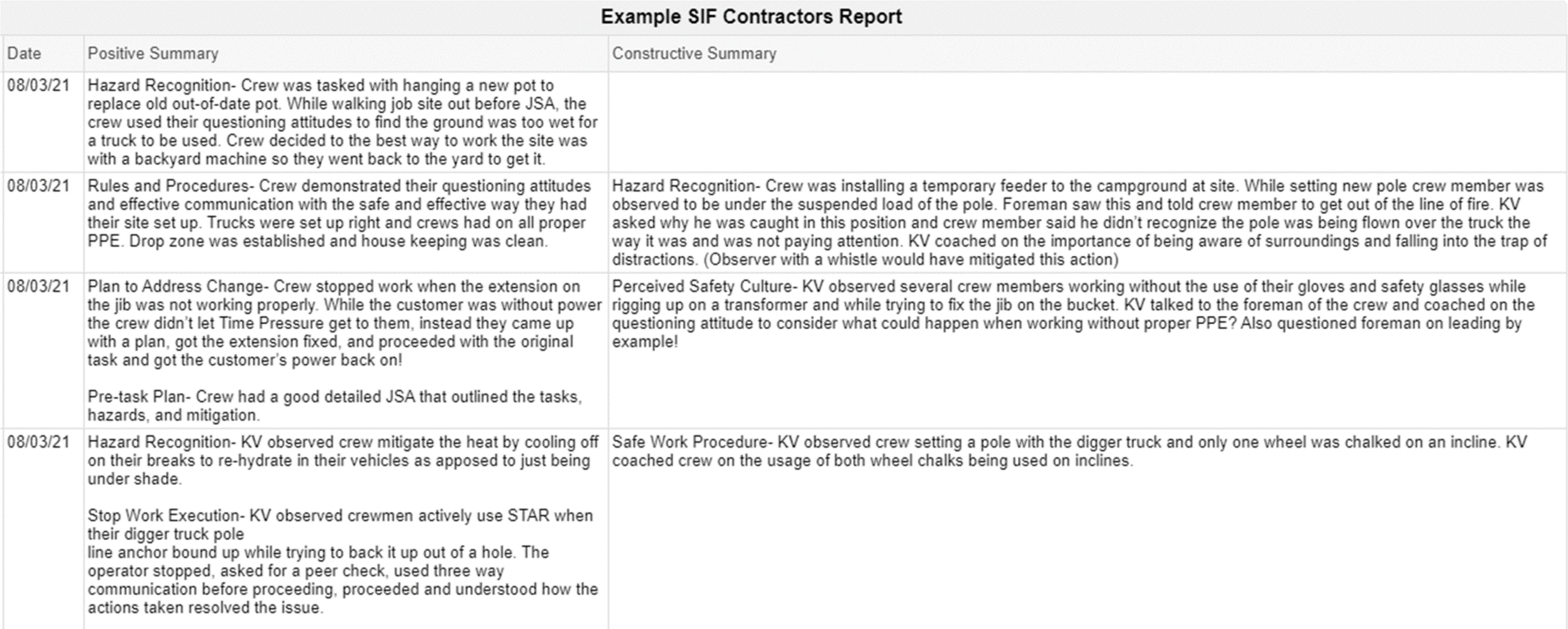
If necessary (based on the results of the interviews) assign additional follow up actions to address the particular deficiencies identified.

<u>Follow up Action 2 –</u>

Executives conduct at least 5 paired observations with foremen and supervisory personnel to assess their understanding of hazard recognition, and their method of communicating these expectations to the crews. Upload documented observations (at least 5) to the dashboard.

<u>Follow up Action 3 –</u>

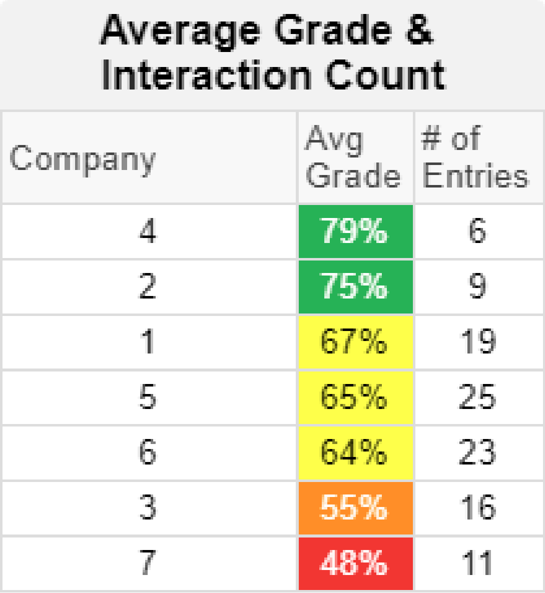
Supervisory level personnel (foremen, general foreman and/or field supervisors) will communicate to their crews the importance of recognizing hazards and evaluating the severity of risks. Emphasize the risk of overconfidence, and how it is a trap that affects overall performance. Use some of the field observations that identified this precursor as a vulnerability. Confirm that each crew has received this briefing and attach this evidence to the dashboard to close this follow up action.



Example SIF Contractors Report

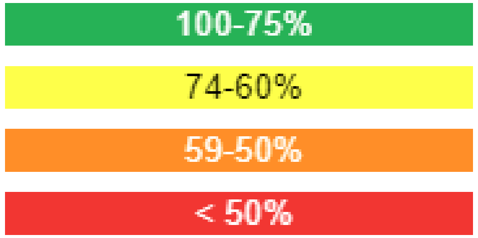
Date	Positive Summary	Constructive Summary
08/03/21	Hazard Recognition- Crew was tasked with hanging a new pot to replace old out-of-date pot. While walking job site out before JSA, the crew used their questioning attitudes to find the ground was too wet for a truck to be used. Crew decided to the best way to work the site was with a backyard machine so they went back to the yard to get it.	
08/03/21	Rules and Procedures- Crew demonstrated their questioning attitudes and effective communication with the safe and effective way they had their site set up. Trucks were set up right and crews had on all proper PPE. Drop zone was established and house keeping was clean.	Hazard Recognition- Crew was installing a temporary feeder to the campground at site. While setting new pole crew member was observed to be under the suspended load of the pole. Foreman saw this and told crew member to get out of the line of fire. KV asked why he was caught in this position and crew member said he didn't recognize the pole was being flown over the truck the way it was and was not paying attention. KV coached on the importance of being aware of surroundings and falling into the trap of distractions. (Observer with a whistle would have mitigated this action)
08/03/21	Plan to Address Change- Crew stopped work when the extension on the jib was not working properly. While the customer was without power the crew didn't let Time Pressure get to them, instead they came up with a plan, got the extension fixed, and proceeded with the original task and got the customer's power back on! Pre-task Plan- Crew had a good detailed JSA that outlined the tasks, hazards, and mitigation.	Perceived Safety Culture- KV observed several crew members working without the use of their gloves and safety glasses while rigging up on a transformer and while trying to fix the jib on the bucket. KV talked to the foreman of the crew and coached on the questioning attitude to consider what could happen when working without proper PPE? Also questioned foreman on leading by example!
08/03/21	Hazard Recognition- KV observed crew mitigate the heat by cooling off on their breaks to re-hydrate in their vehicles as apposed to just being under shade. Stop Work Execution- KV observed crewmen actively use STAR when their digger truck pole line anchor bound up while trying to back it up out of a hole. The operator stopped, asked for a peer check, used three way communication before proceeding, proceeded and understood how the actions taken resolved the issue.	Safe Work Procedure- KV observed crew setting a pole with the digger truck and only one wheel was chalked on an incline. KV coached crew on the usage of both wheel chalks being used on inclines.

The overall grade provides perspective on our observations, and focuses the corrective actions



Average Grade & Interaction Count

Company	Avg Grade	# of Entries
4	79%	6
2	75%	9
1	67%	19
5	65%	25
6	64%	23
3	55%	16
7	48%	11

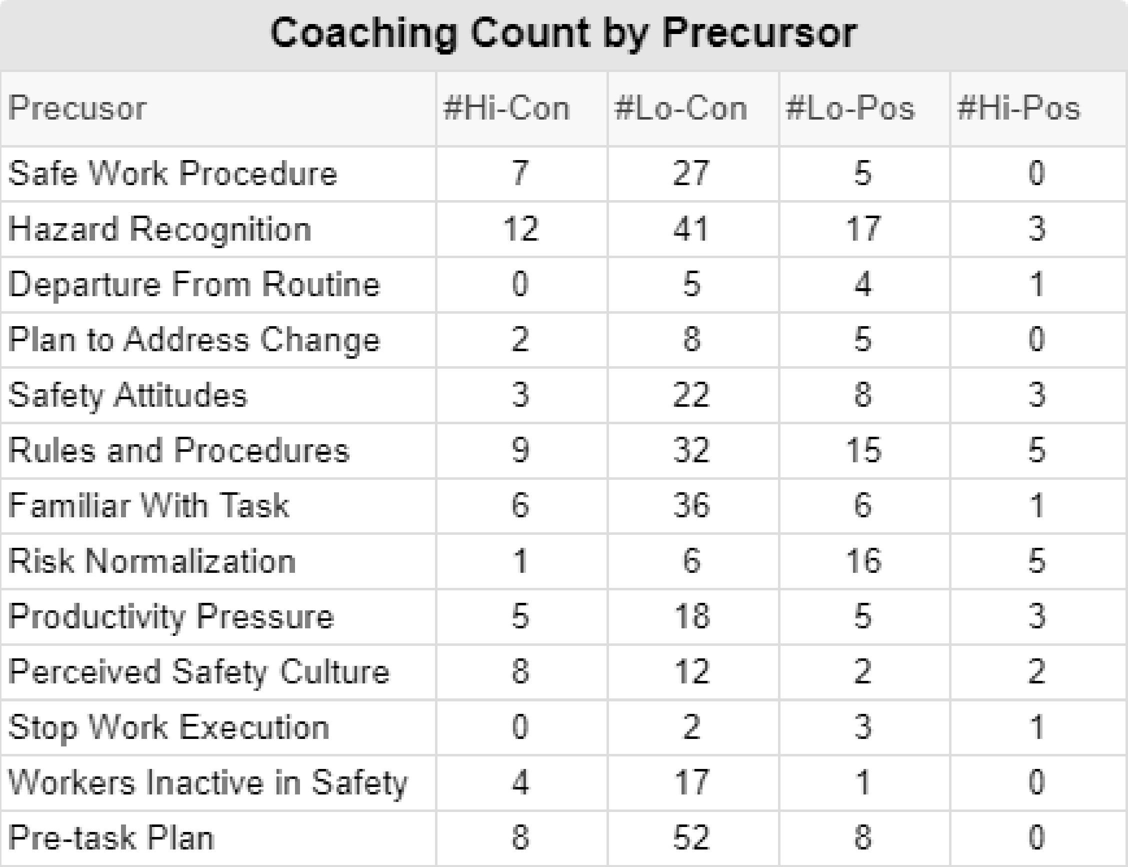


100-75%

74-60%

59-50%

< 50%

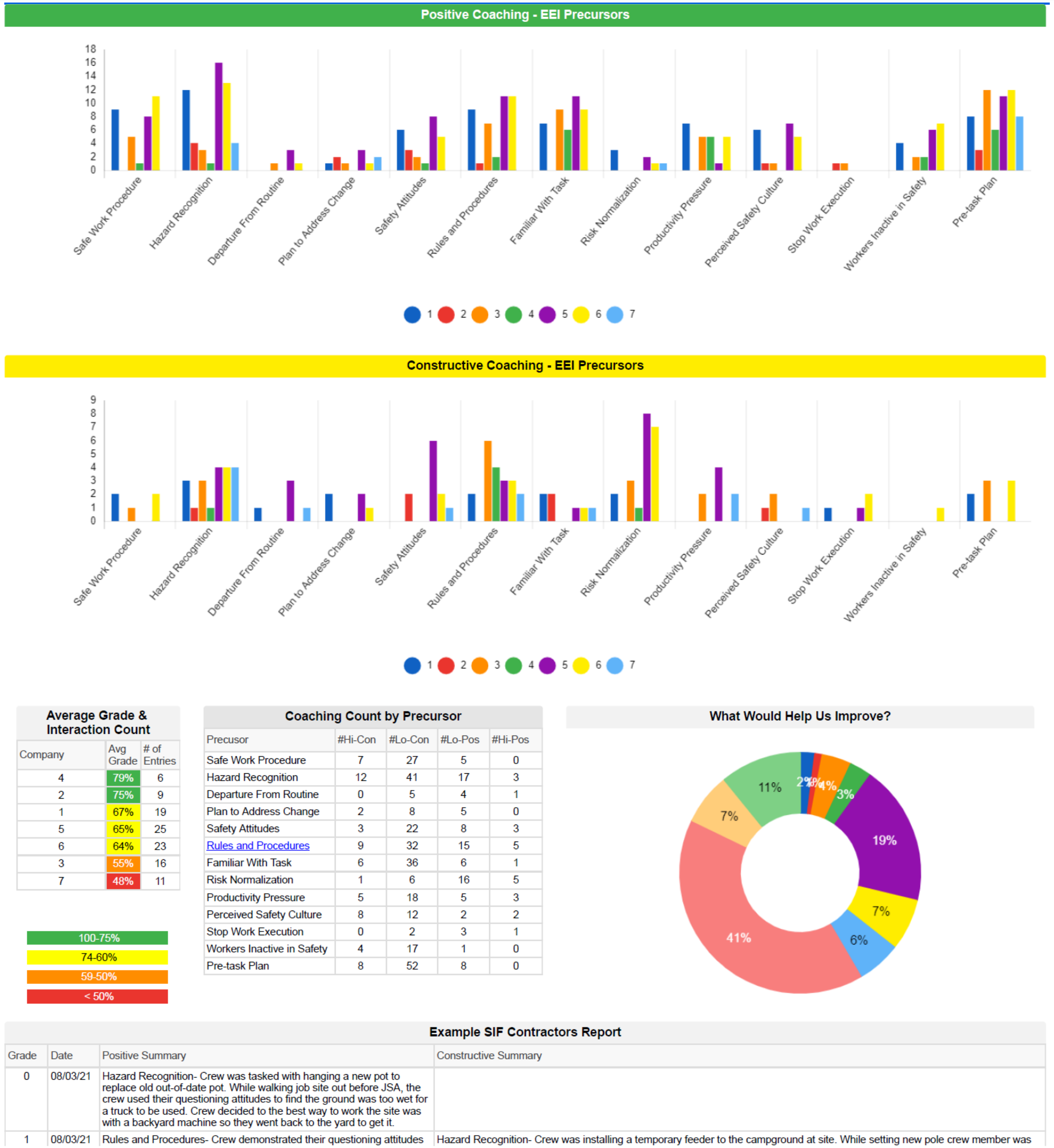


Coaching Count by Precursor

Precusor	#Hi-Con	#Lo-Con	#Lo-Pos	#Hi-Pos
Safe Work Procedure	7	27	5	0
Hazard Recognition	12	41	17	3
Departure From Routine	0	5	4	1
Plan to Address Change	2	8	5	0
Safety Attitudes	3	22	8	3
Rules and Procedures	9	32	15	5
Familiar With Task	6	36	6	1
Risk Normalization	1	6	16	5
Productivity Pressure	5	18	5	3
Perceived Safety Culture	8	12	2	2
Stop Work Execution	0	2	3	1
Workers Inactive in Safety	4	17	1	0
Pre-task Plan	8	52	8	0

Click on any of the 13 precursors to see a recommended set of actions for Executives, Leaders and Employees

Two levels of Constructive and Positive observations: HI is more significant and LO is routine. Used to determine the overall grade



Positive Coaching - EEI Precursors

Constructive Coaching - EEI Precursors

Average Grade & Interaction Count

Company	Avg Grade	# of Entries
4	79%	6
2	75%	9
1	67%	19
5	65%	25
6	64%	23
3	55%	16
7	48%	11

🟩 100-75%
🟨 74-60%
🟧 59-50%
🟥 < 50%

Coaching Count by Precursor

Precusor	#Hi-Con	#Lo-Con	#Lo-Pos	#Hi-Pos
Safe Work Procedure	7	27	5	0
Hazard Recognition	12	41	17	3
Departure From Routine	0	5	4	1
Plan to Address Change	2	8	5	0
Safety Attitudes	3	22	8	3
Rules and Procedures	9	32	15	5
Familiar With Task	6	36	6	1
Risk Normalization	1	6	16	5
Productivity Pressure	5	18	5	3
Perceived Safety Culture	8	12	2	2
Stop Work Execution	0	2	3	1
Workers Inactive in Safety	4	17	1	0
Pre-task Plan	8	52	8	0

What Would Help Us Improve?

Example SIF Contractors Report

Grade	Date	Positive Summary	Constructive Summary
0	08/03/21	Hazard Recognition- Crew was tasked with hanging a new pot to replace old out-of-date pot. While walking job site out before JSA, the crew used their questioning attitudes to find the ground was too wet for a truck to be used. Crew decided to the best way to work the site was with a backyard machine so they went back to the yard to get it.	
1	08/03/21	Rules and Procedures- Crew demonstrated their questioning attitudes	Hazard Recognition- Crew was installing a temporary feeder to the campground at site. While setting new pole crew member was

KnowledgeVine

Todd Brumfield

VP Operations

225-259-1239

www.knowledgevine.com

U.S. DEPARTMENT OF
ENERGY

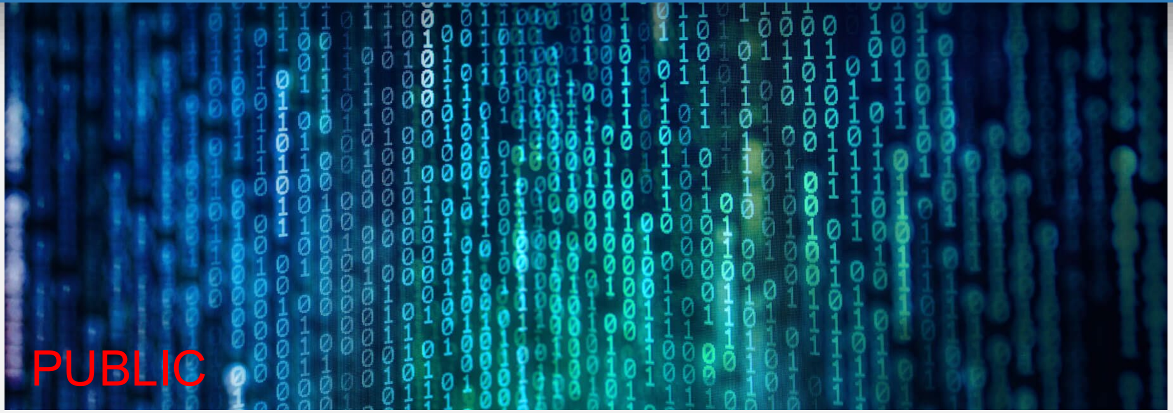
OFFICE OF
Cybersecurity, Energy Security,
and Emergency Response

CyOTE

Cybersecurity for the
Operational Technology
Environment

HP in Cybersecurity: CyOTE™

ReliabilityFirst Human Performance Workshop – August 12, 2021 – Sam Chanoski, Idaho National Laboratory



PUBLIC

CyOTE Purpose and Goals

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

What Need is CyOTE Targeting?

Today's energy sector IT and OT systems are **complex and interconnected**.

Sophisticated adversaries have the knowledge to target OT environments that result in **physical disruptions** to energy flows or damaged equipment.

Industry visibility, monitoring, and analysis capabilities in the OT space are still relatively new and immature—leaving asset owners and operators (AOOs) struggling to **determine** whether **anomalous operational events** potentially have a malicious cyber cause.

We need to **change the paradigm** for security and begin thinking of security as a holistic analysis of business operations to **identify anomalies** from unalterable data sources and investigate further from those sources.

What is the Problem CyOTE is Trying to Address?

Most AOOs lack the capability to analyze data from their OT networks effectively and consistently identify attacks, much less in real time – in significant contrast to their IT networks.

Even those who have some capabilities still want and need to improve their level of OT understanding.

Improving understanding of OT data enables AOOs to make better risk-informed decisions to secure their OT environments.

Challenges

Regulations limit the information that can be shared.

Geographic dispersion of assets in the field.

Communications channels may be limited.

No common lexicon for data fields and threat information.

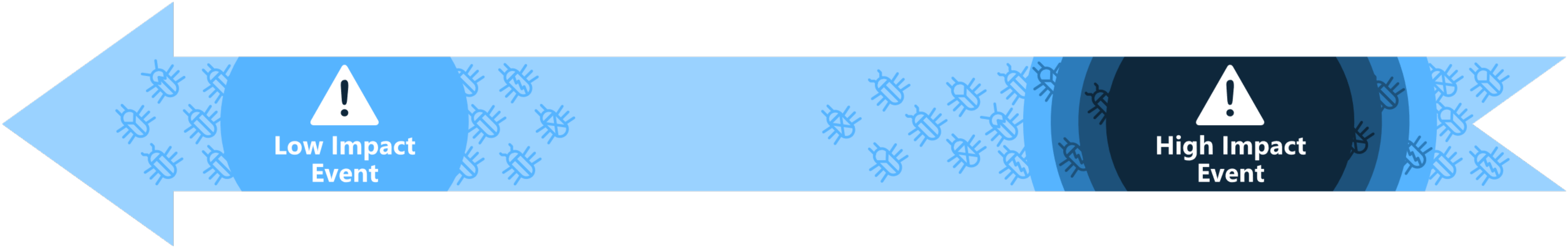
Understanding anomalies in operations.

CyOTE Vision

Develop a threat identification capability for energy sector asset owners and operators to independently identify indicators of attack within their operational technology (OT) networks.

Solution

CyOTE aims to move the energy sector AOO's threat detection capability **earlier into an attack campaign**. The better understanding an asset owner has into their OT environment, the less obvious anomalies they may be able to confidently identify as either an attack technique or a non-malicious operational failure. This shifts the AOO's threat detection capability **earlier into an attack campaign** to **identify attacks with ever-decreasing impacts**.



Leveraging HOP Principles

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Central Concept

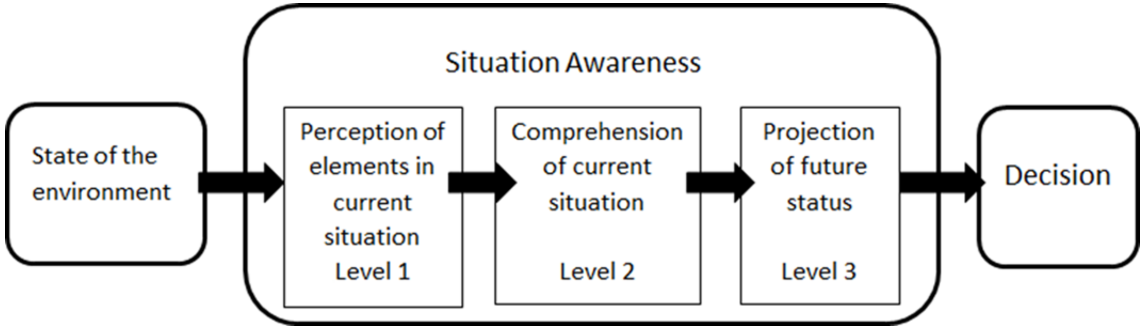
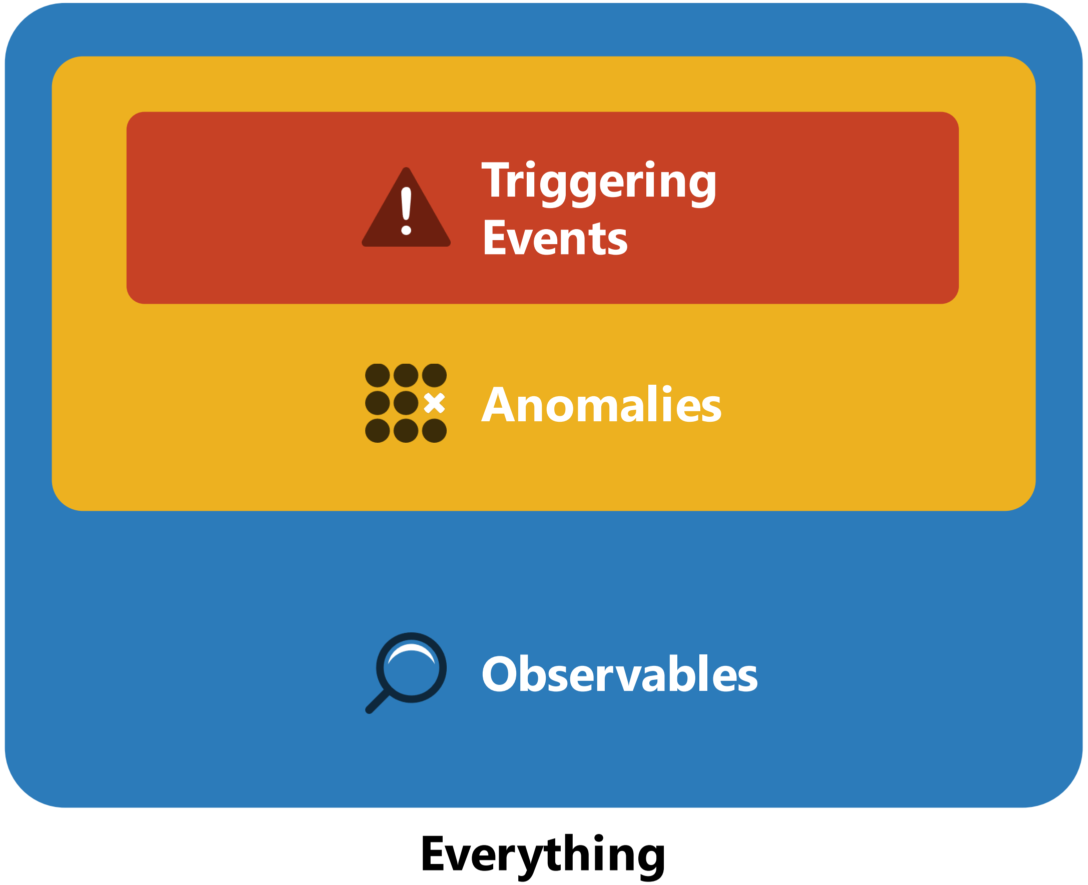

Situation Awareness
State of the environment
Perception of elements in current situation
Level 1
Comprehension of current situation
Level 2
Projection of future status
Level 3
Decision

Image: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SA_for_System_Operators.pdf

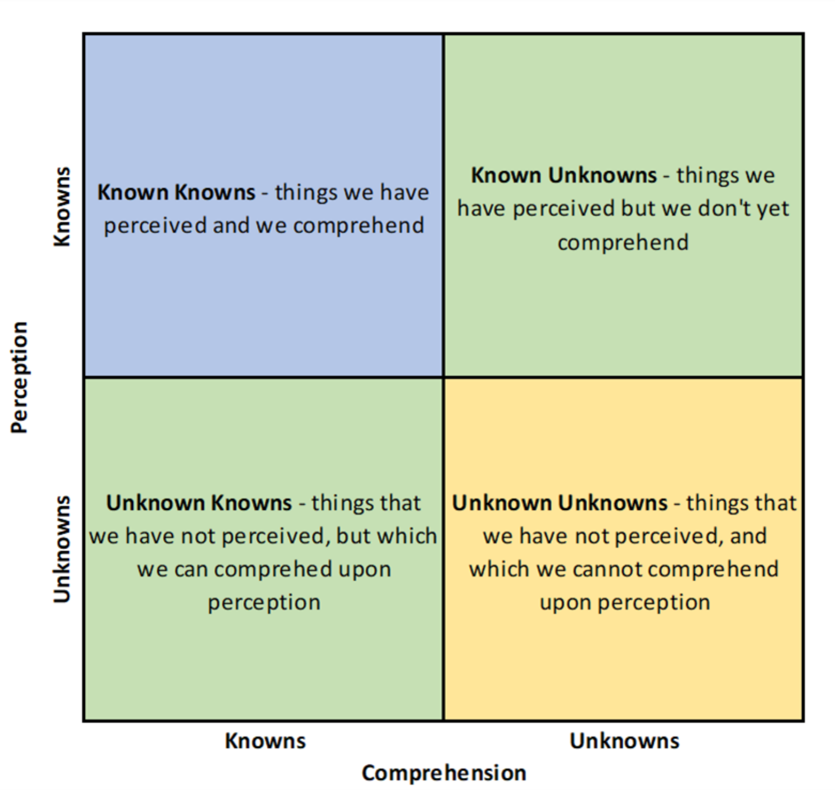
- Adapted from Endsley’s 1995 Model of Situation Awareness
- Perception: individual human ability to detect an observable
- Comprehension: organizational human ability to understand an observable

Nested Mental Model of Occurrences



- **Observable:** an occurrence that can be perceived
- **Anomaly:** an observable different from what is expected or “normal”
- **Triggering event:** an anomaly that merits investigation

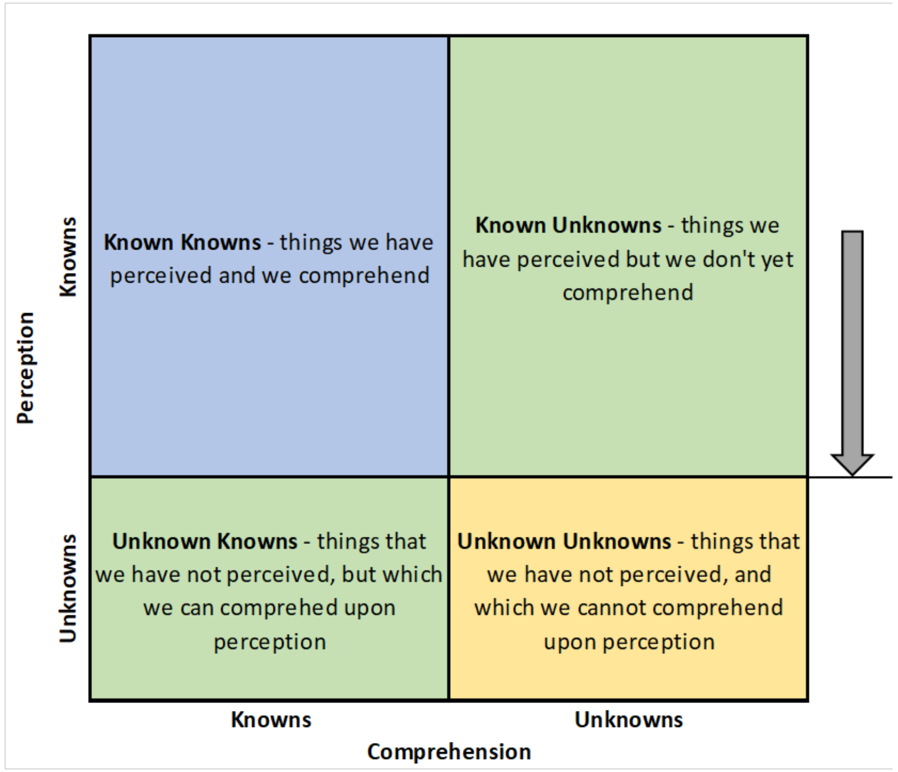
Knowns and Unknowns



		Knowns	Unknowns
Perception	Knowns	**Known Knowns** - things we have perceived and we comprehend	**Known Unknowns** - things we have perceived but we don't yet comprehend
	Unknowns	**Unknown Knowns** - things that we have not perceived, but which we can comprehed upon perception	**Unknown Unknowns** - things that we have not perceived, and which we cannot comprehend upon perception
		Comprehension	

- The world is divided into Knowns and Unknowns
- Division applies to perception and to comprehension

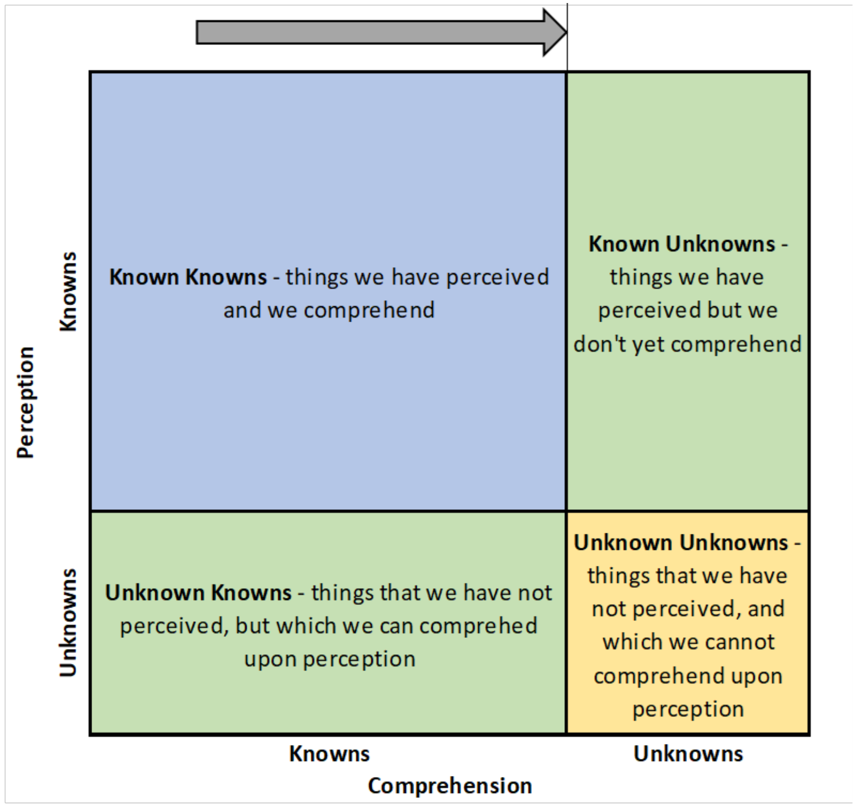
Improving Perception



Perception		Comprehension: Knowns	Comprehension: Unknowns
	Knowns	**Known Knowns** - things we have perceived and we comprehend	**Known Unknowns** - things we have perceived but we don't yet comprehend
	Unknowns	**Unknown Knowns** - things that we have not perceived, but which we can comprehed upon perception	**Unknown Unknowns** - things that we have not perceived, and which we cannot comprehend upon perception

- Improving our perception shrinks the Unknown world
- Conscious visibility
- Still need to understand the newly perceived observables

Improving Comprehension



Perception		Knowns	Unknowns
	Knowns	**Known Knowns** - things we have perceived and we comprehend	**Known Unknowns** - things we have perceived but we don't yet comprehend
	Unknowns	**Unknown Knowns** - things that we have not perceived, but which we can comprehed upon perception	**Unknown Unknowns** - things that we have not perceived, and which we cannot comprehend upon perception

Comprehension

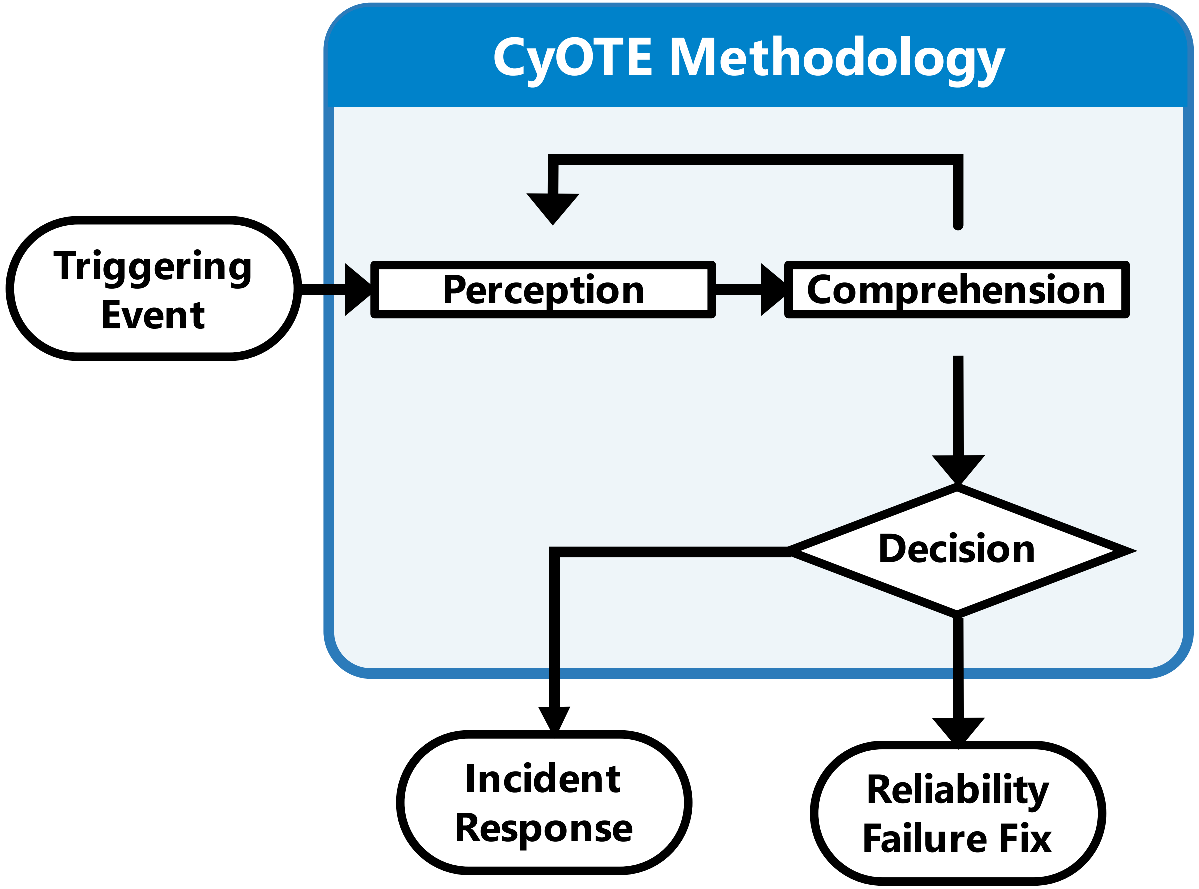
- Improving our comprehension further shrinks the unknown world
- Better idea of what not-yet-perceived observables look like (Fact Sheets and Recipes)

Organizational Capabilities

- Relationships between departments
- Energy monitoring capabilities and practices
- Capability to respond to and resolve reliability failures
- Capability to respond to and resolve cybersecurity incidents*
- Understanding of organizational risk appetite*
- Capability for organizational learning and continuous improvement
- OT instrumented visibility*

* Relates to a Cybersecurity Capability Maturity Model (C2M2) domain

CyOTE Methodology Overview



- How to understand the information you have, not get more data
- Applies concepts of perception and comprehension to a world of Knowns and Unknowns
- MITRE ATT&CK® Framework for ICS is a central part of our common lexicon
- Endpoint is making a risk-informed decision to conduct incident response or to treat as a reliability failure
- Over time, detect fainter signals sooner

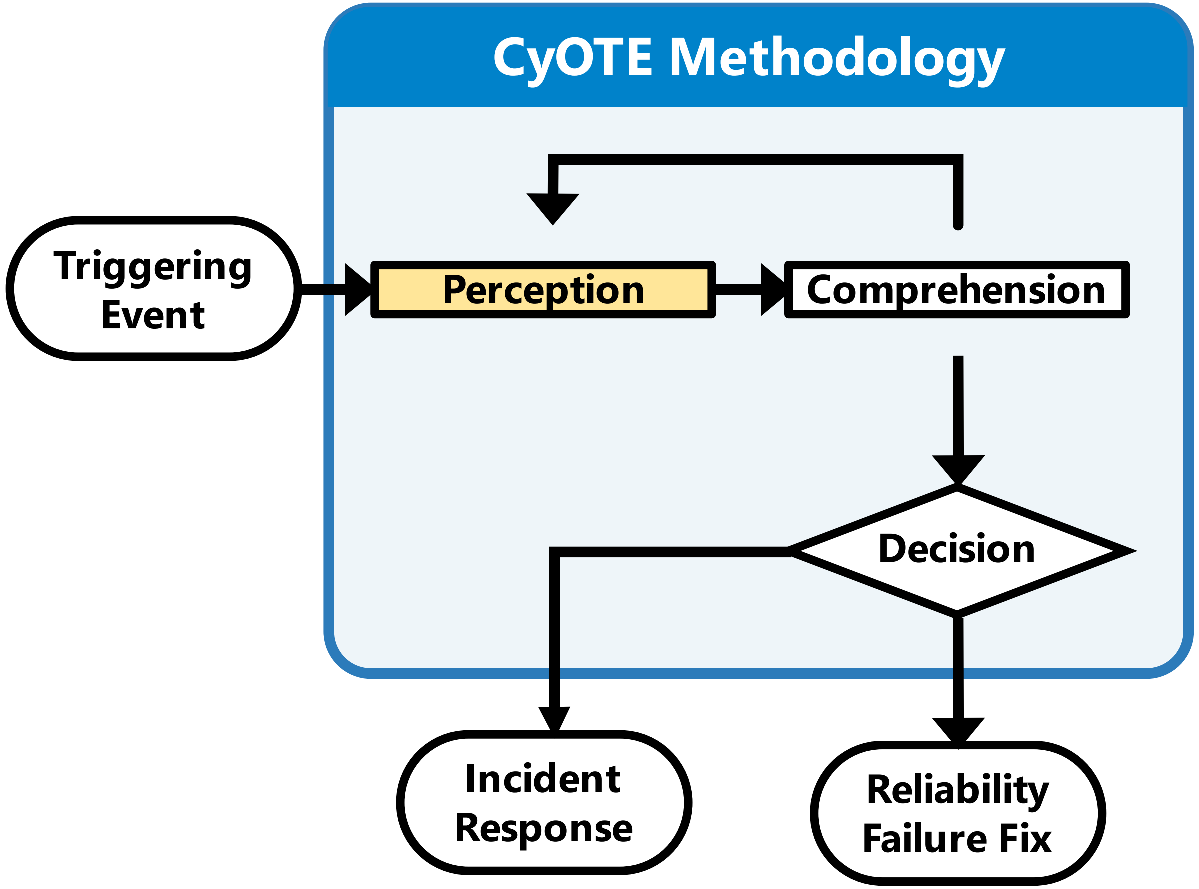
Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise 🟩🟦🟧	✓ Change Program State 🟩🟦🟧	Hooking	Exploitation for Evasion	✓ Control Device Identificatio n 🟩🟦	✓ Default Credentials 🟦	Automated Collection 🟩	Commonly Used Port	Activate Firmware Update Mode 🟩	✓ Brute Force I/O 🟦🟧	Damage to Property 🟩🟦🟧
Drive-by Compromise	Command-Line Interface	✓ Module Firmware 🟧	✓ Indicator Removal on Host 🟩🟦🟧	✓ I/O Module Discovery	Exploitation of Remote Services 🟩🟦	✓ Data from Information Repositories 🟩🟦🟧	✓ Connection Proxy 🟦	Alarm Suppression 🟧	✓ Change Program State 🟩🟦🟧	Denial of Control 🟩🟦🟧
Engineering Workstation Compromise 🟩🟦🟧	Execution through API 🟩	✓ Program Download 🟩🟦🟧	Masquerading 🟧	Network Connection Enumeration	External Remote Services 🟦	✓ Detect Operating Mode 🟩🟦	Standard Application Layer Protocol 🟩🟦	Block Command Message 🟩🟧	Masquerading 🟧	Denial of View 🟩🟦🟧
Exploit Public-Facing Application 🟦	Graphical User Interface 🟩	Project File Infection 🟩🟦	Rogue Master Device 🟦🟧	Network Service Scanning	Program Organization Units 🟩🟦	Detect Program State 🟩🟦		✓ Block Reporting Message 🟩🟧	✓ Modify Control Logic 🟩🟧	Loss of Availability 🟩🟦🟧
External Remote Services 🟦	Man-in-the-middle	System Firmware 🟧	Rootkit 🟩🟦	Network Sniffing	✓ Remote File Copy 🟩🟦	I/O Image		Block Serial COM 🟧	✓ Modify Parameter 🟩🟧	Loss of Control 🟩🟦🟧
Internet Accessible Devices 🟦	Program Organization Units 🟩🟦	Valid Accounts 🟩🟦	✓ Spoof Reporting Message 🟩🟧	Remote System Discovery 🟩🟦	Valid Accounts 🟩🟦	Location Identification		✓ Data Destruction 🟩🟦	✓ Module Firmware 🟧	Loss of Productivity and Revenue
Replication Through Removable Media 🟩	Project File Infection 🟩🟦		✓ Utilize/Change Operating Mode 🟩🟦🟧	Serial Connection Enumeration		Monitor Process State 🟩🟦		✓ Denial of Service 🟩🟦🟧	✓ Program Download 🟩🟦🟧	Loss of Safety 🟩🟧
Spearphishing Attachment	Scripting					✓ Point & Tag Identification 🟩🟦		✓ Device Restart/ Shutdown 🟧	Rogue Master Device 🟦🟧	Loss of View 🟩🟦🟧
Supply Chain Compromise 🟩🟦	User Execution 🟩🟦					✓ Program Upload 🟩🟦		Manipulate I/O Image 🟦	✓ Service Stop 🟩🟦🟧	Manipulation of Control 🟩🟦🟧
Wireless Compromise 🟦						Role Identification 🟦		✓ Modify Alarm Settings 🟩🟦🟧	✓ Spoof Reporting Message 🟩🟦🟧	Manipulation of View 🟦🟧
						Screen Capture 🟩		✓ Modify Control Logic 🟩🟧	✓ Unauthorized Command Message 🟩🟧	Theft of Operational Information 🟩🟦
								✓ Program Download 🟩🟦🟧		
								Rootkit 🟩🟦		
								System Firmware 🟧		
								✓ Utilize/Change Operating Mode 🟩🟦🟧		

Legend

Tactics | Techniques | Use Cases: HMI 🟩 Remote Login 🟦 Alarm Logs 🟧 | ✓ Fact Sheet

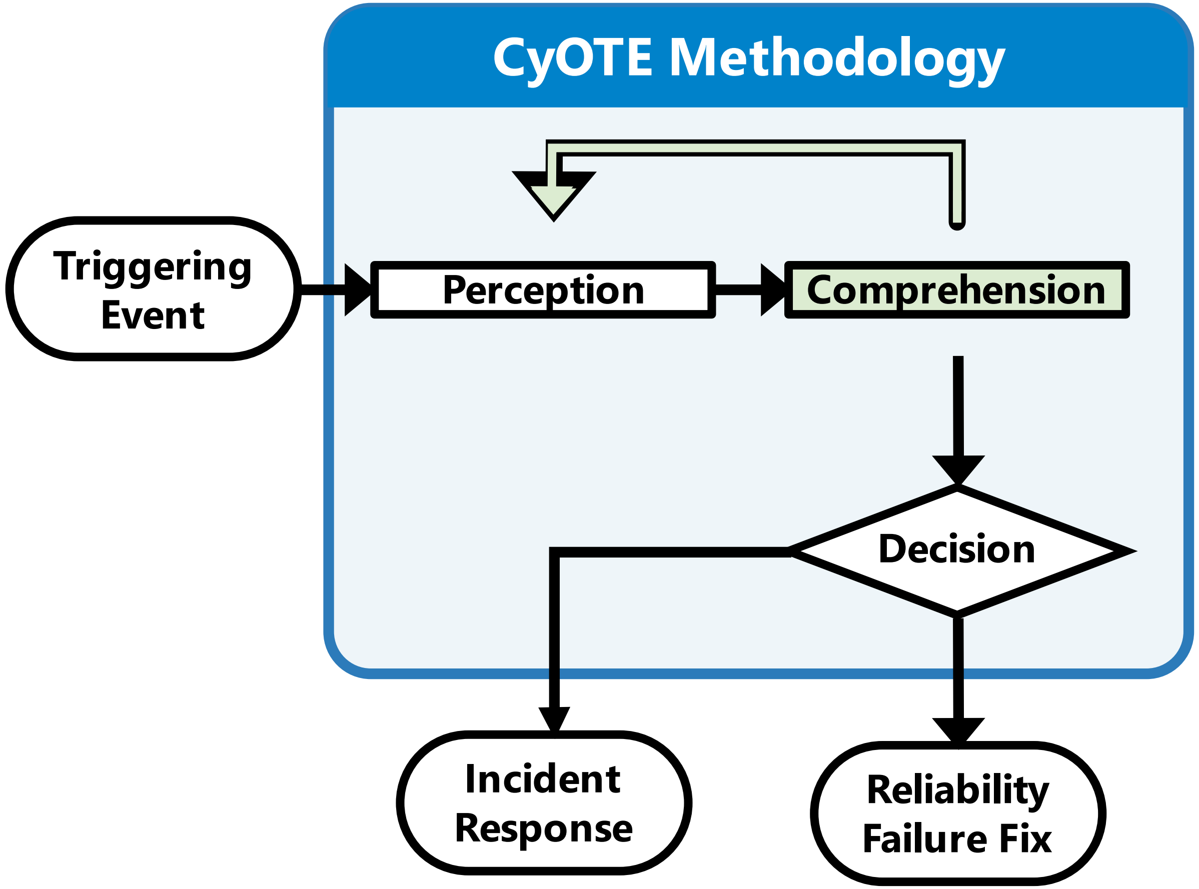
MITRE ATT&CK for ICS Matrix (October 2020)

Employment: Perception



- Define **your** triggering events
- Alarms, human pattern matching, business process exceptions
- Who else needs to know, i.e. transition from individual to organizational awareness

Employment: Comprehension

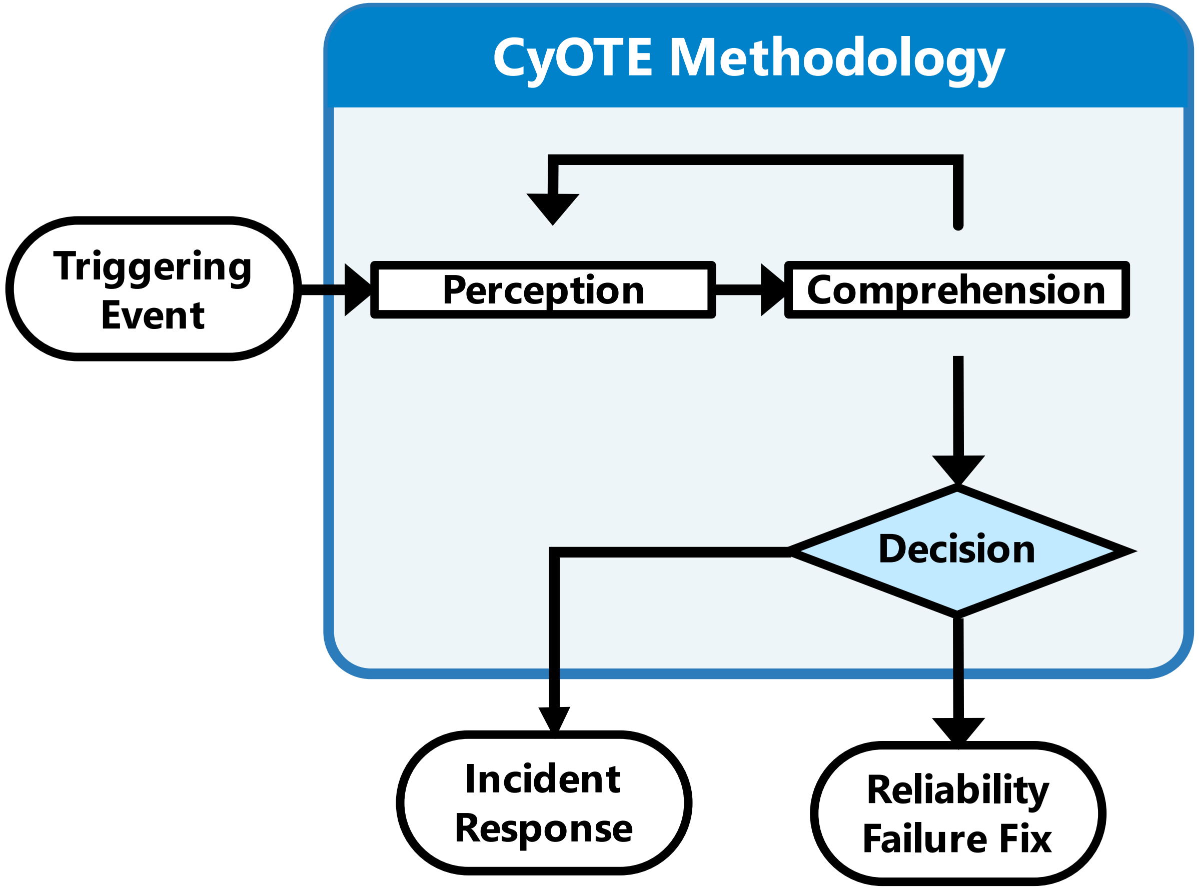


- Identify and locate sources of information
- Build context: are related observables expected or not, present or not?
- How much does this resemble a known technique?
- Knowledge management and documentation
- Recursive pivots to explore related observables

Collaboration

Organizational comprehension requires significant cooperation between disparate roles and responsibilities across an AOO's organization that may not regularly work together, including some roles that do not have traditional security responsibilities.

Employment: Decision



- Risk-informed, binary business decision on how to resolve the situation
- Scientific method analogy
  - H_0: Reliability failure
  - H_1: Incident
  - Confidence level based on risk appetite

Learning through Case Studies

- The CyOTE team is creating Case Studies using both historical OT attack scenarios and scenarios identified with AOO partners to demonstrate where AOOs could **apply the CyOTE methodology to identify effects of malicious cyber activity** and correlate the effects to techniques.
- These Case Studies provide the opportunity to **better demonstrate how the CyOTE methodology could create broader understanding of OT environments and help** identify attack campaigns with ever-decreasing impacts.

Final Thoughts

- We need to **change the paradigm** for security and begin thinking of security as a holistic analysis of business operations to identify anomalies from unmaskable data sources and conduct further investigation of any associated data.
- Correlating **operational anomalies**/observables to techniques and linking them to other anomalies provides the ability to detect attack campaigns with ever-decreasing impacts.
- Read the **full CyOTE methodology paper** at https://inl.gov/wp-content/uploads/2021/07/CyOTE-Methodology-20210625-final.pdf
- **You can help** by employing the CyOTE methodology in your organization:
  - look for anomalies in your environments,
  - identify anomalies that would trigger further investigations,
  - correlate available data sources,
  - associate additional anomalies, and
  - determine if you are in the early stages of an attack campaign.

QUESTIONS and DISCUSSION

CyOTE.Program@hq.doe.gov

Sam Chanoski

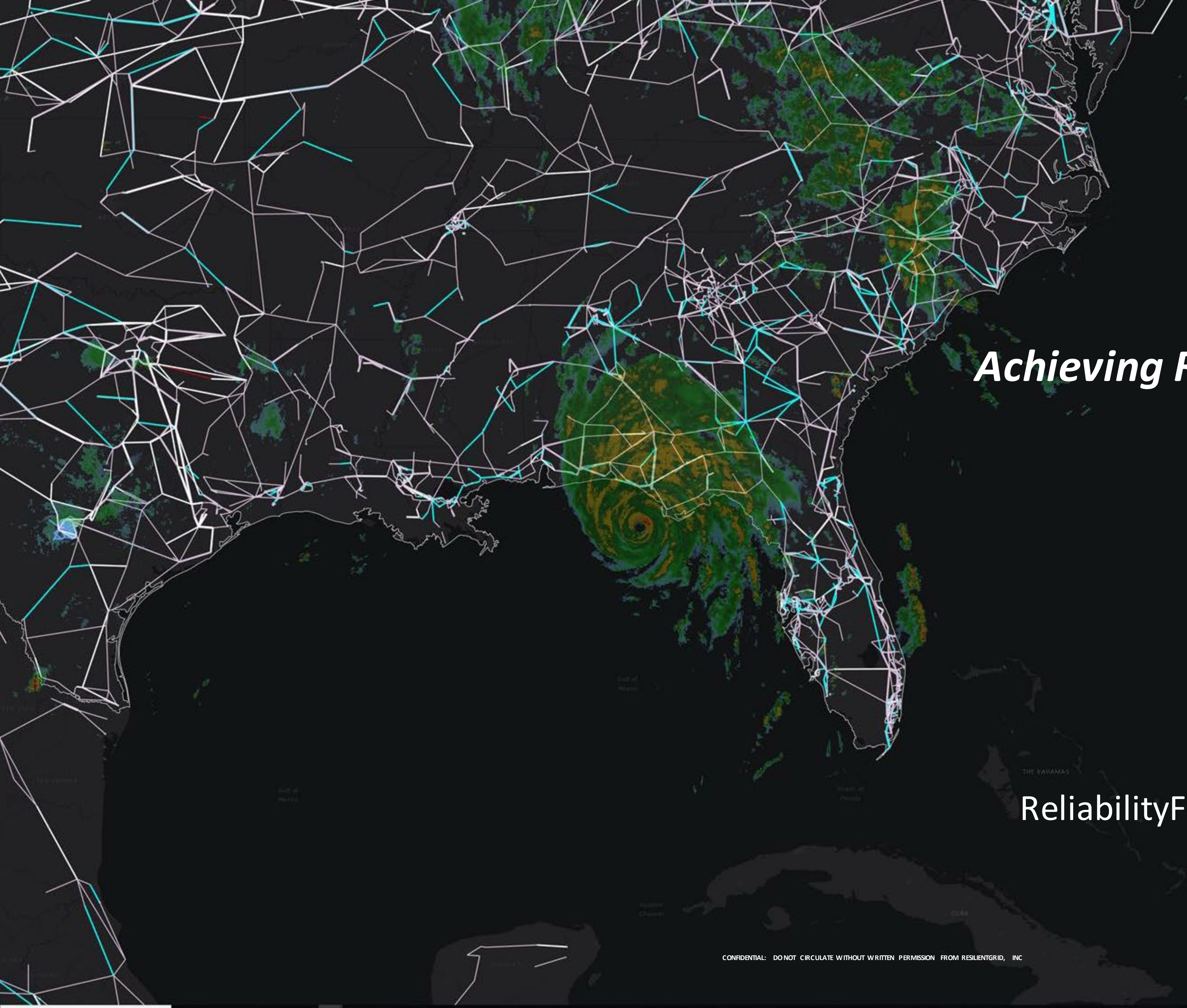
Technical Relationship Manager | Cybercore Integration Center

samuel.chanoski@inl.gov

Idaho National Laboratory | Atlanta, GA

ResilientGrid

Go Beyond the One Line™



Achieving Real-Time Operational Success With Network Modeling: “One-Lines for the Front Line”

Mike Legatt, ResilientGrid

ReliabilityFirst Human Performance Conference

August 12, 2021

Overview

- Human Performance concepts focus heavily on real-time operations: control room and the field
- However, real-time operations depends on high-accuracy and high-fidelity data from upstream sources, including network modeling
- Therefore, looking at network modeling activities from a human performance lens not only helps network modeling, but also all the reliability and market functions that depend on modeling.
- This presentation covers several stories across multiple entities around human performance issues noted in network modeling. All components are anonymized

Core Philosophies:

“All organizations are perfectly aligned to get the results they get.”

Arthur W. Jones

The same core principles

- Situational Awareness
- Adaptive Capacity
- Mental Models
- Resiliency
- Reinforcement and Punishment
- Human Information Processing Limitations
- Domains of function
- “Out of the Loop Syndrome”
- Latent Risk
- Complexity vs. Complicatedness

Challenge #1: Over-work, stress, distraction

- “Do more with less”
- Growth in network modeling as core system of record
- Serving multiple new systems simultaneously: EMS, market, outage management, logging
- Interfacing with member entities
- Data confidentiality and CEII concerns

Challenge #2: Over-reliance on tooling

- Fredrick W. Taylor: transfer of expertise from the front line to managers to tooling
- Multiple modeling errors may lead to the appearance of “all good”:
  - Multiple model parameters incorrect in a change request
  - Powerflow convergence no unanticipated contingencies
  - Potential introduction of latent risks

Challenge #3: One-Line copy/paste errors

- EMS one-line displays focus on displaying elements and lines, not representing accurate topologies and connectivity
- Breaker/label example:
  - Copy/paste
  - Change SCADA point for label
  - Phone rings with urgent interruption
  - SCADA breaker state pointing to old point but one-line “looks good”

Challenge #4: One-Line mismatches

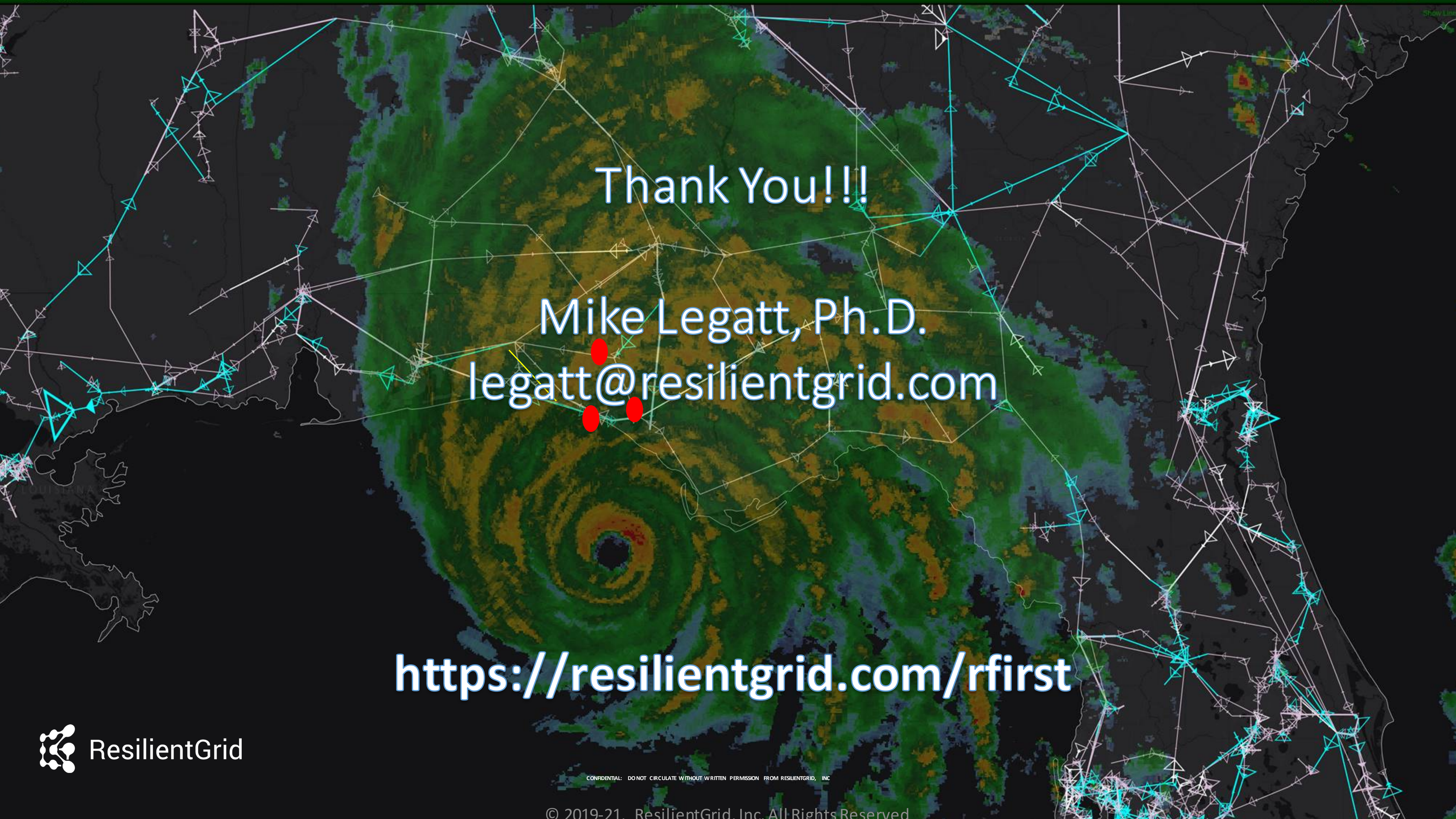
- One-Line displays can be different amongst many groups.
- For example a transmission operator:
  - SCADA One-Line display
  - Study / SE one-line display
  - CAD drawings
  - Operating guides and procedures with embedded images
  - One-lines (and a network model) as represented by the RC
- Naming convention issues
- Different layouts
- Latent risks, especially in high-pressure situations

Challenge #5: Continuous improvement friction

- Activation energy high for model improvements. For example:
  - One-line changes noted by operator or field worker
  - Documentation of the problem usually occurs, documentation of requested solution less frequent
  - Entering the modeling pipeline may lead to significant (up to 6 month) delay, unless emergency updates occur.
  - Problems can be “thrown over the fence”, so the updated one-line doesn’t match what was needed

Challenge #6: Increasing reliance on modeling

- Network models are becoming increasingly important for reliable operations
- Not just powerflows, but for example:
  - Human safety concerns
  - Topological processing (e.g., radiality)
  - Blackstart simulations and estimations
  - Project workflow tracking and forecasting



Thank You!!!

Mike Legatt, Ph.D.
legatt@resilientgrid.com

https://resilientgrid.com/rfirst

ResilientGrid

CONFIDENTIAL: DO NOT CIRCULATE WITHOUT WRITTEN PERMISSION FROM RESILIENTGRID, INC