SAND2022-15946C

Sandia National Laboratories

Exceptional service in the national interest

LAB TALK: Exploring HSI for High Consequence Facility Security

Adam D. Williams, PhD

Global Nuclear Security & Nonproliferation Group

Elizabeth "Scottie-Beth" Fleming, PhD

Statistics & Human Systems Group

Human System Integration Workshop – HSI2022

Hybrid Event || 16 November 2022

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Workshop Outline

Session Outline

Setting the scene…

- Security for High Consequence Facilities (HCF) → Common Approaches & Challenges
- The role for HSI?

What we've done so far…

- System context layers for multilayer network models for HCF security
- Applied cognitive task analysis (ACTA) for HCF security

What have we learned so far…

- Useful analytic insights for HCF security
- How to identify & overcome challenges to HSI research in HCF security

What's next…

Our Team…

Scottie-Beth Fleming (Co-PI)
- PhD Aerospace Engineering, GaTech
- Human factors, systems engineering, decision-support, metric development, human risk & reliability

Adam Williams (Co-PI)
- PhD Human & Systems Engineering, MIT
- Systems-theoretic analysis, managing complex risk, physical protection system development & analysis, nuclear security R&D

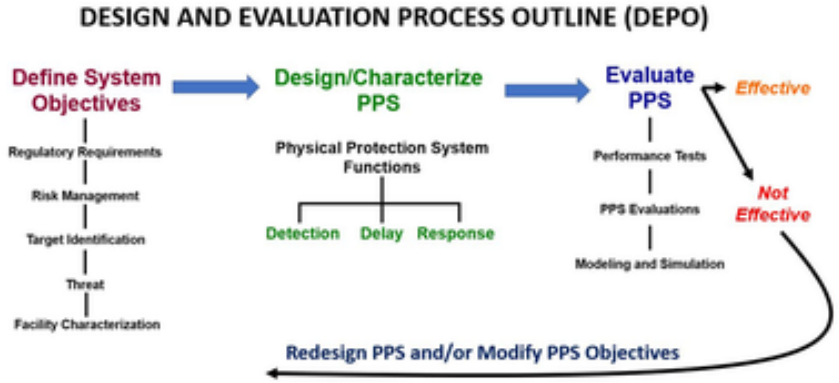
Wesley Odom
- MS Industrial Engineering, Purdue
- PhD-ABD, Engineering Ed, Purdue
- Human factors, situated cognition, knowledge transfer, instrument validation

Cheryl Bolstad
- PhD Psychology, North Carolina State
- Human Factors Fellow, knowledge elicitation, cognitive psychology, situation awareness

Jawad Moussa
- MS Nuclear Engineering, UNM
- PhD-ABD Nuclear Engineering, UNM
- Advanced modeling & simulation, nuclear safeguards, numerical methods

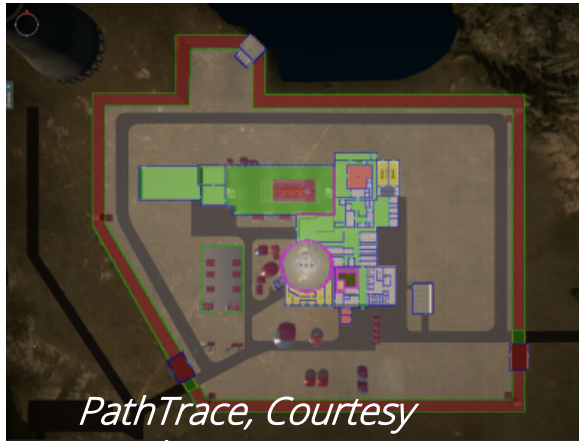
Setting the scene…

Setting the scene…



Current approaches (e.g., DEPO), vaguely incorporate each of these

- ***Ignores*** more complex interactions/interdependencies
- Treats each element in the ***PPS as a simple system*** with scalar state values (e.g., Pd = 95%)
- Interactions in current approaches consist of ***simple stacked probabilities*** (i.e., $P_D = P_S \times P_T \times P_A$)


PathTrace, Courtesy

For example, security is ***NOT ONLY***:

- A microwave sensor alarming when an intruder is in the PIDAS
- A CAS operator assessing movement in an VTR and alerting the response force for deployment
- A firewall stopping malware attacks on sensitive information


Scribe3D, Courtesy Sandia

Setting the scene…

Dynamic trends increase ***complexity*** for high consequence facility (HCF) security

- Complex risk environment-based challenges
- Adversary innovation-based challenges
- Disruptive technologies-based challenges
- Increasing levels of automation in facility operations

2018: Increased digitization of control elements in HCF

2020: Nuclear facilities deployed to increasingly remote locations

2019: Cyber attack Kudamkulam Nuclear Power Plant in India

2011: DHS memo "violent extremists… insider positions"

2019: Yemeni rebels use UAS to attack Saudi Oil facilities

2020: Expected threat from deep-fakes & malicious AI

Setting the scene…

Result → challenge to efficacy of current HCF security paradigms

- Linear causality model
- Static “snapshots in time”
- (At best) overly simplify or (at worst) ignore the role of human actor(s)

Response → Sandia research reframes HCF security

- Interactions matter!
- Multidomain interactions within HCF security (including HSI!)
- High consequence facility (HCF) security → complex system behavior (including HSI!)

Setting the scene…

What does human-system integration look like for HCF security systems?

Setting the scene…

What does human-system integration look like for HCF security systems?

As our team embarked on this research, several questions quickly emerged:

1. If we do not want simple probabilistic description of human, what other models are available? (and appropriate)?

2. If HCF security wants to incorporate ***MORE*** autonomy, what changes in the roles of human actors?

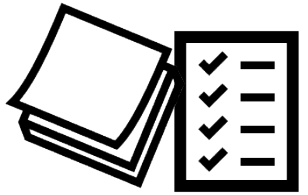
3. For HSI, what role does “trust” play in optimizing the interactions between humans and systems to enhance system performance?

Setting the scene…

What does human-system integration look like for HCF security systems?

1. If we do not want simple probabilistic description of human, what other models are available? (and appropriate)?

System Upfront & (re)design



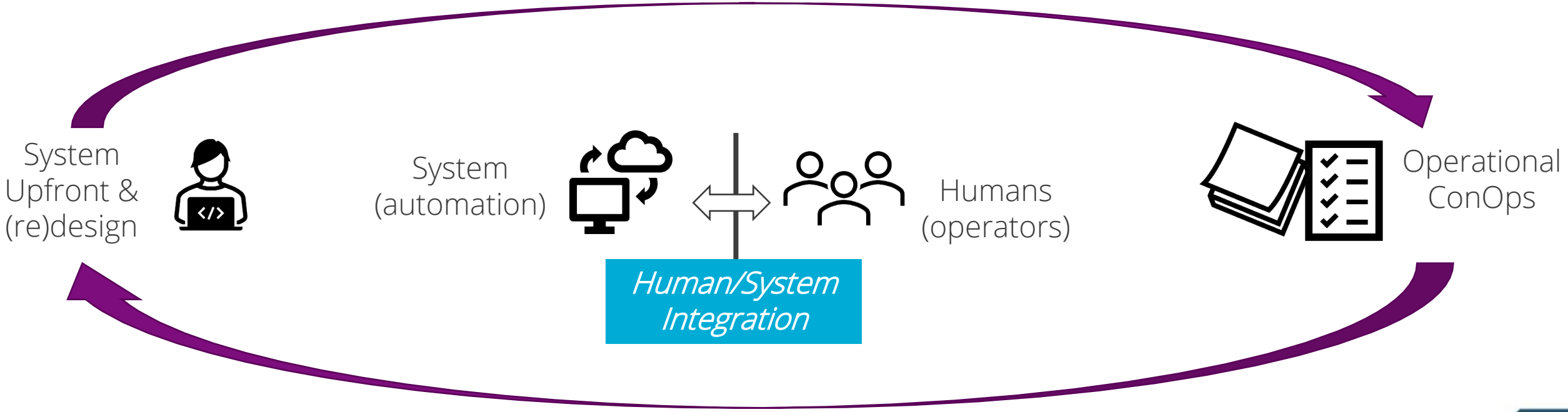
Operational ConOps

Probabilistic human degradation on system performance

Setting the scene…

What does human-system integration look like for HCF security systems?

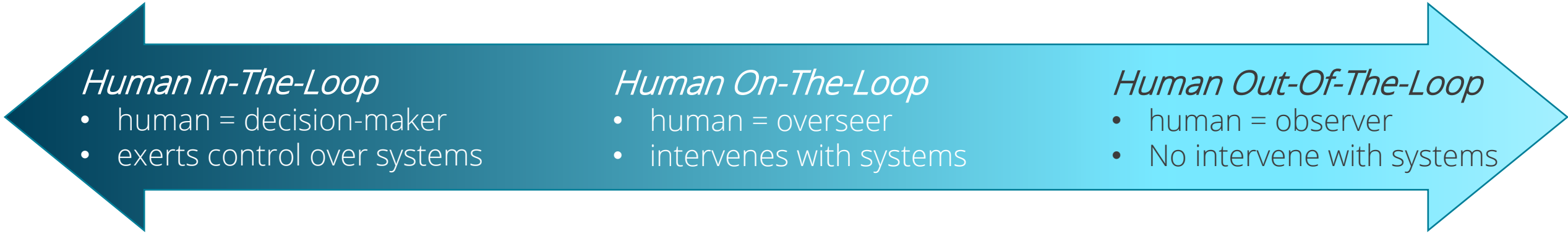
1. If we do not want simple probabilistic description of human, what other models are available? (and appropriate)?



Setting the scene…

What does human-system integration look like for HCF security systems?

2. If HCF security wants to incorporate ***MORE*** autonomy, what changes in the roles of human actors?



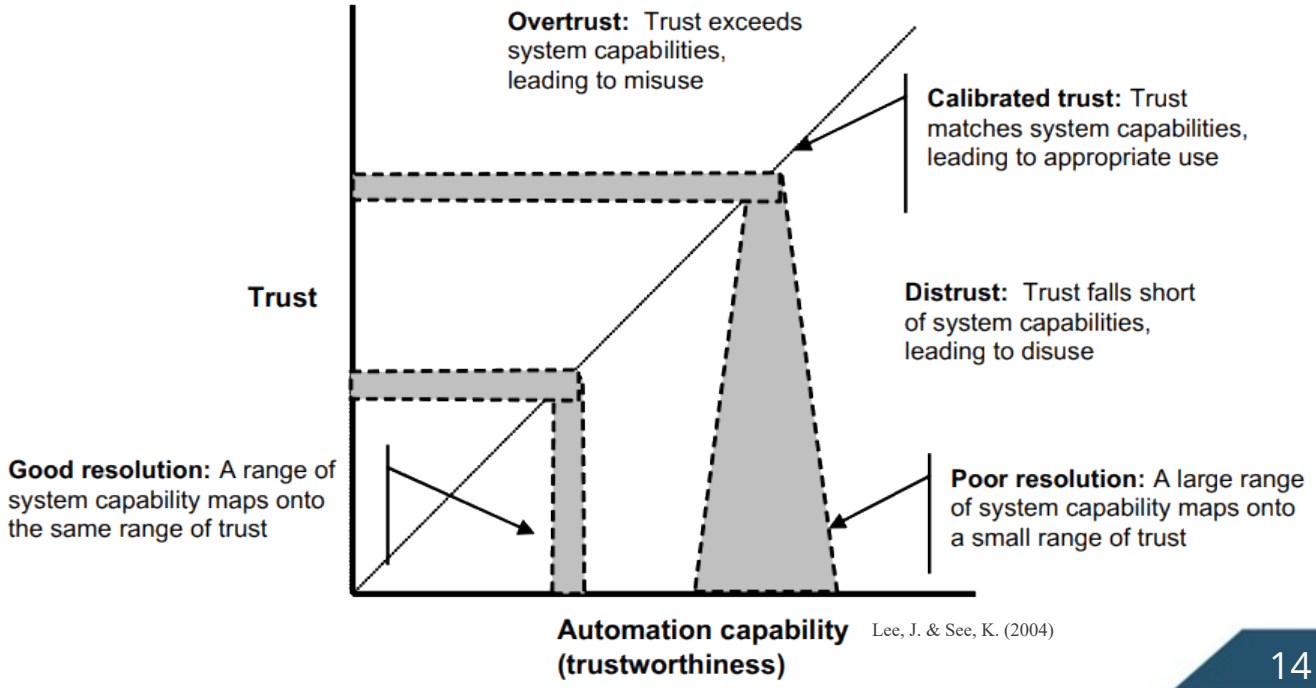
Setting the scene…

What does human-system integration look like for HCF security systems?

3. For HSI, what role does "trust" play in optimizing the interactions between humans and systems to enhance system performance?

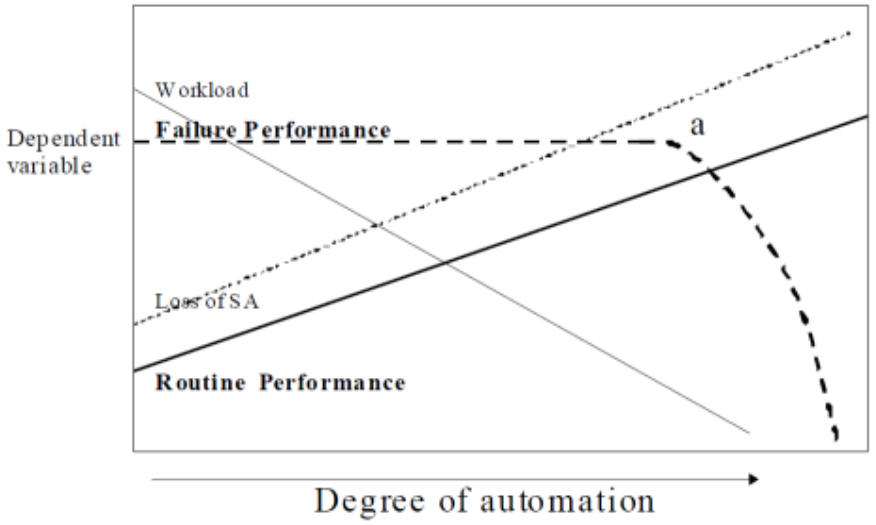
"Inappropriate reliance associated with misuse and disuse depends, in part, on *how well trust matches the true capabilities* of the automation."

(Lee & See 2004, pp 6)

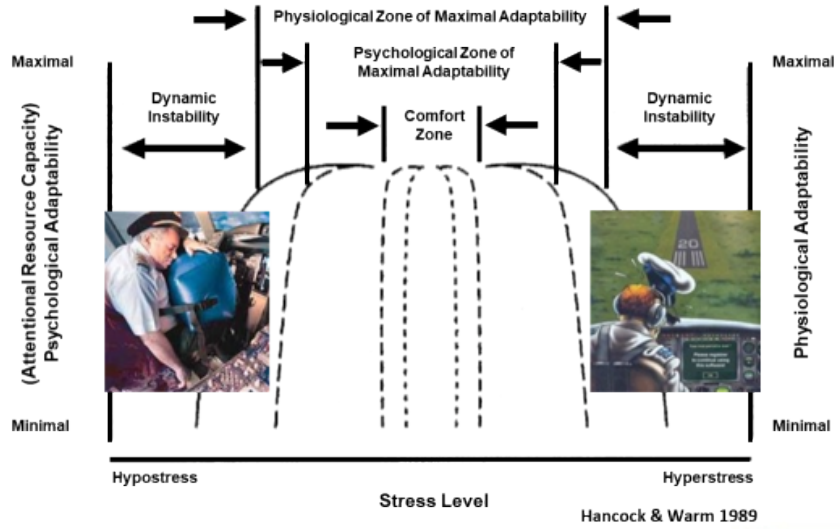


Setting the scene…

- IF HCF security is looking to incorporate more automation and technology to minimize uncertainty due to human interactions…
- THEN there is a need to understand the resultant changes in the roles of humans in HCF security…
- STARTING with a Fitts'-based HABA/MABA framing:
  - IF more procedural or predictable tasks are being given to machines
  - THEN humans may have decreasing situation awareness due to lack of robust information sources
  - AND humans are responsible for increasingly difficult cognitive tasks (particularly during emergent situations)
- HSI provides a perspective to understand the performance trade space between human-driven versus machine-driven approaches



Wickens et al 2010



Hancock & Warm 1989

What we've done so far...

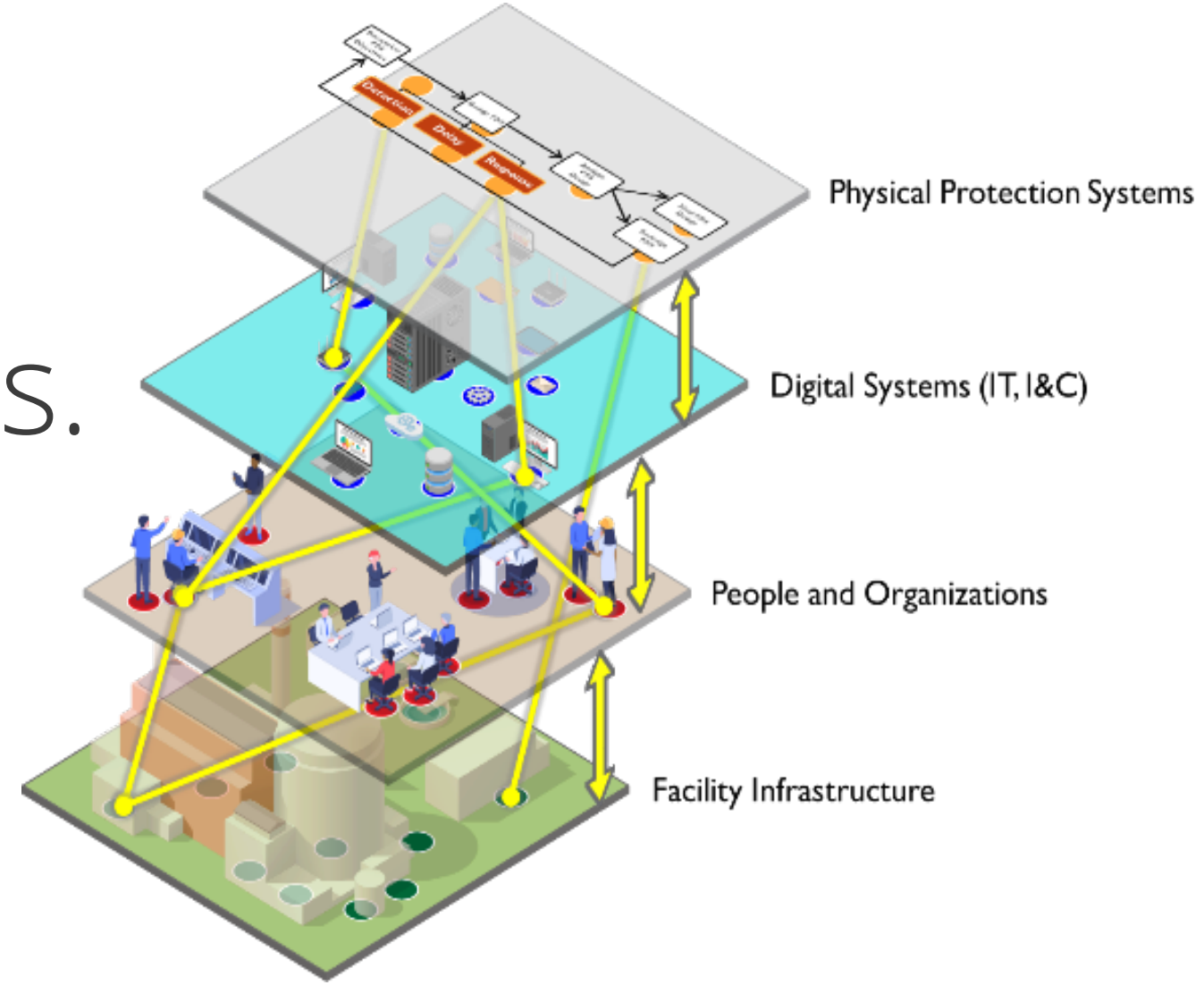
Multilayer Network (MLN) Approach

Disparate, 'individual' security mitigations

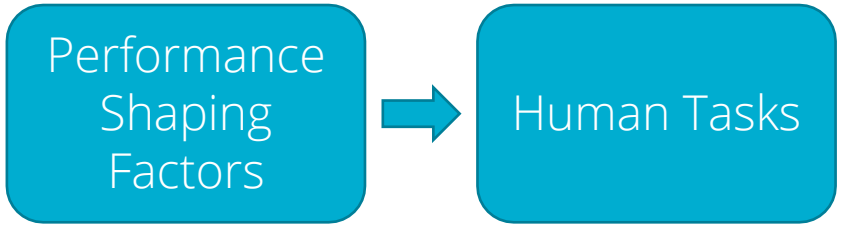
- Cyber security via common vulnerability scoring system
- Physical security via "gates, guards, guns"
- Personnel security via human reliability programs

These are often assumed independent!

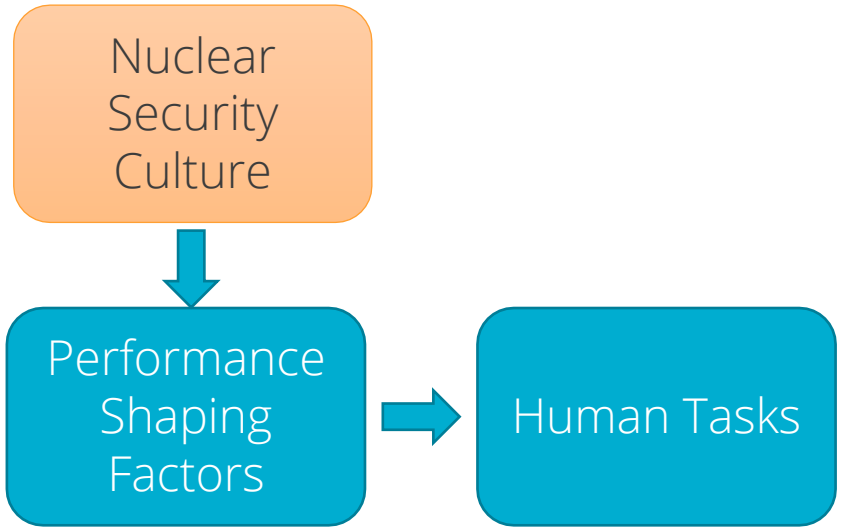
VS.



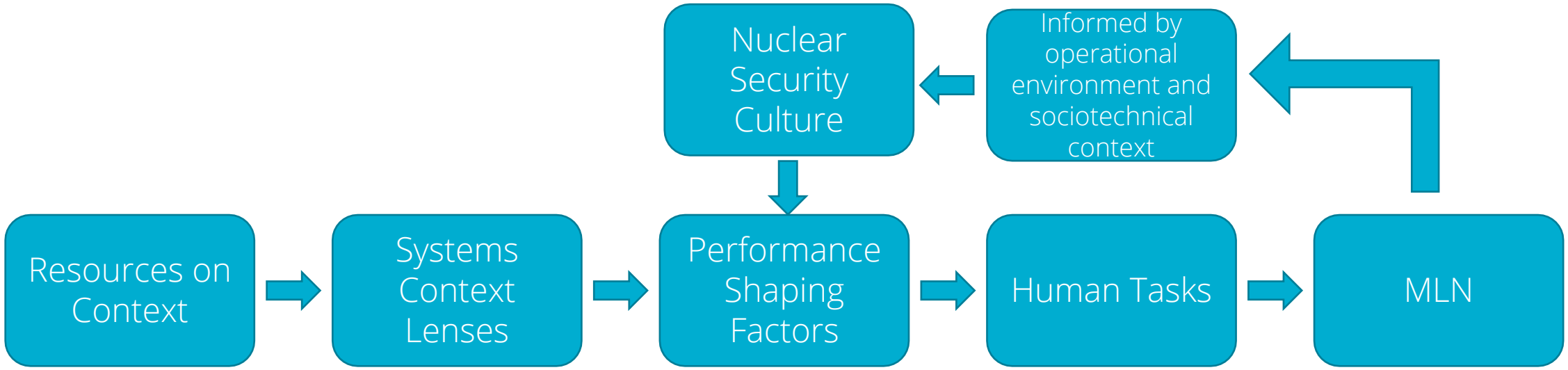
MLN Approach: Integrating Humans



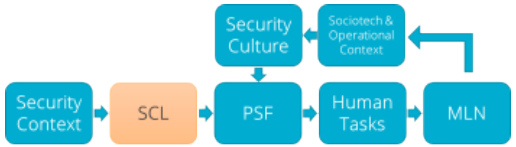
MLN Approach: Integrating Humans



MLN Approach: Integrating Humans



MLN Approach: System Context Lenses



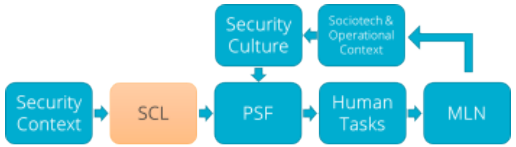
System Context Lens	Example Questions for Designers
System Design	• What is the primary technical goal of the system? • What technologies need to (can, or should) be integrated to meet that goal?

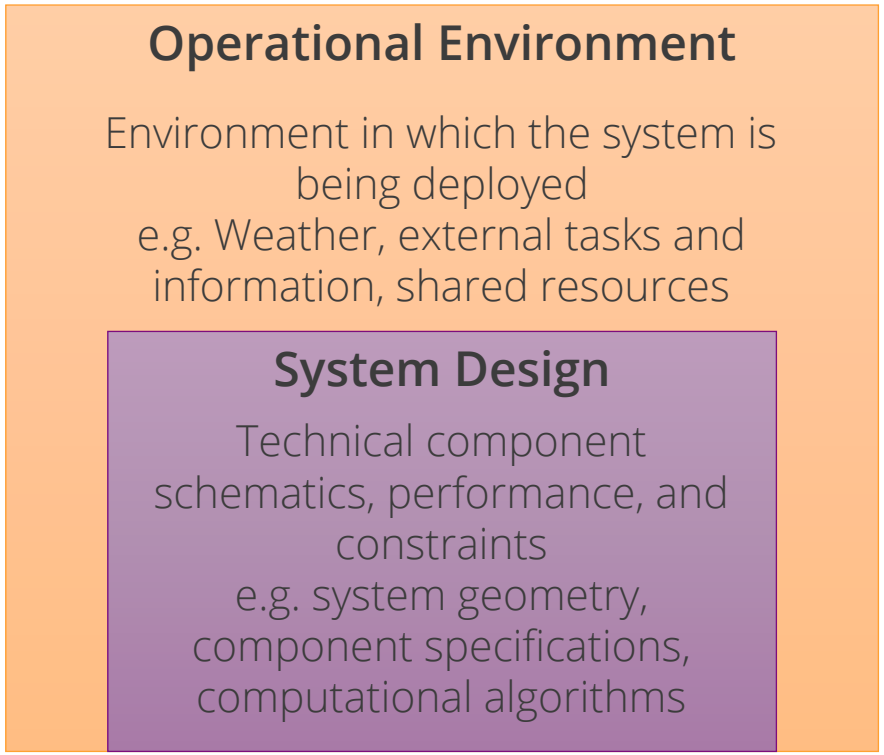
System Design

Technical component schematics, performance, and constraints
e.g. system geometry, component specifications, computational algorithms

Fleming. & Williams (2020)

MLN Approach: System Context Lenses

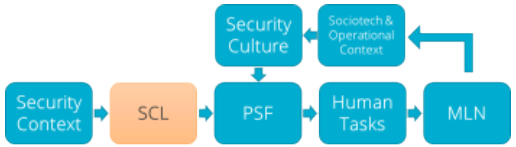


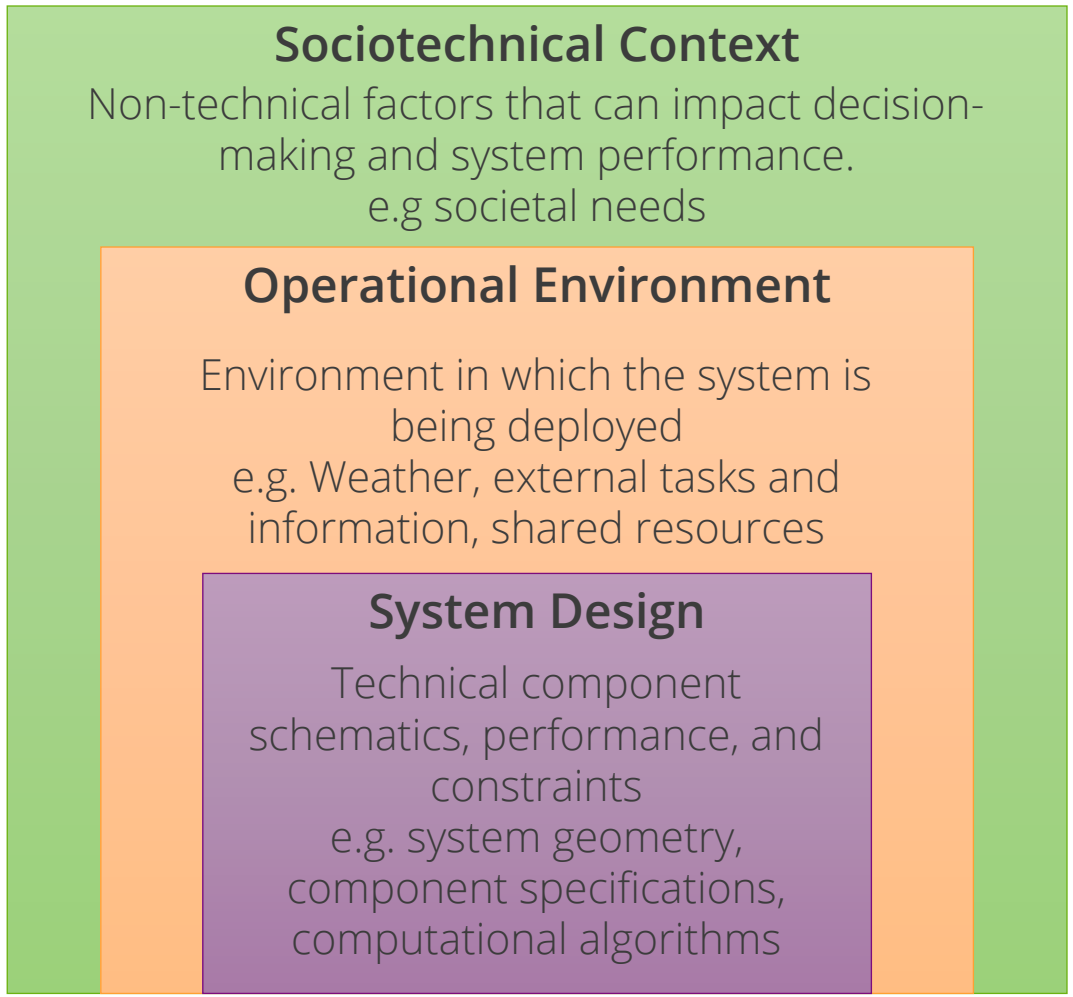


System Context Lens	Example Questions for Designers
System Design	• What is the primary technical goal of the system? • What technologies need to (can, or should) be integrated to meet that goal?
Operational Environment	• How might the system perform differently in this real context? • What external dependencies drive system performance?

Fleming. & Williams (2020)

MLN Approach: System Context Lenses

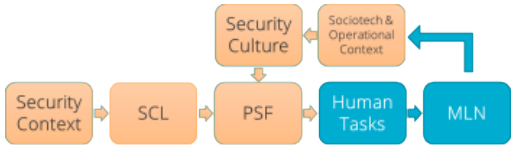


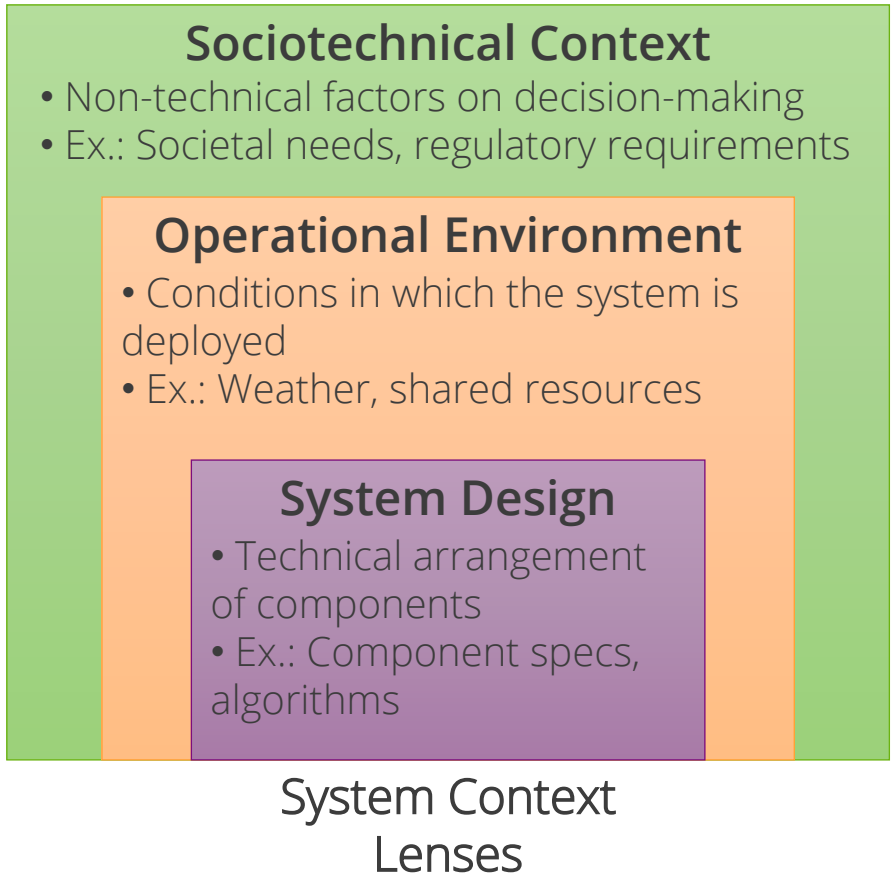


System Context Lens	Example Questions for Designers
System Design	• What is the primary technical goal of the system? • What technologies need to (can, or should) be integrated to meet that goal?
Operational Environment	• How might the system perform differently in this real context? • What external dependencies drive system performance?
Sociotechnical Context	• What are the competitor's capabilities? • How do existing partnerships impact design and development? • What are driving societal impacts and perceptions? • How can this system be/perceived as being misused or harmed?

Fleming. & Williams (2020)

MLN Approach: System Context Lenses



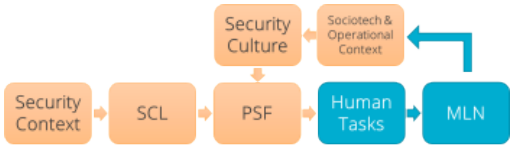


System Context Lenses

System Context Lens	Human Stakeholders	Representative Performance Shaping Factors
System Design	• Response personnel (Commander, Alarm Station Operators, Roving/ Fixed Position Guards) • Facility employees • PSS designers	• Training and Experience • Physical fitness/stress • Work Flows, Procedures, Communications • PSS interface design • Team dynamics/available staffing
Operational Environment	• Facility management • Security guard union • Security contractor	• Organizational Culture • Attitude • Available staffing
Sociotechnical Context	• Government Oversight • Public • Adversaries	• Perceptions • Resources & Regulations • Attitude

Fleming. & Williams (2020)

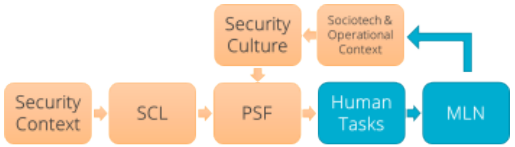
MLN Approach: System Context Lenses, The Y-12 Case



System Context	Human Stakeholders	Human Decision-Making Influences	Representation in MLN Models
System Design	• ARGUS system designers • Security guards • Y-12 employees	• Requirement to mesh "new" design into "old" (existing) system • Higher false alarm rates	• Breaking edges/removing nodes in one layer and not addressing deleterious impacts on other layers • Adding "new" nodes into "old" edges

Williams et al 2020; Schlosser 2015

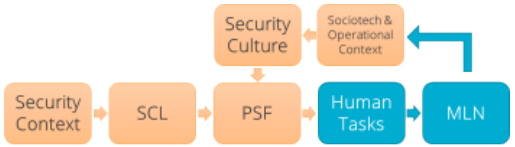
MLN Approach: System Context Lenses, The Y-12 Case



System Context	Human Stakeholders	Human Decision-Making Influences	Representation in MLN Models
System Design	• ARGUS system designers • Security guards • Y-12 employees	• Requirement to mesh "new" design into "old" (existing) system • Higher false alarm rates	• Breaking edges/removing nodes in one layer and not addressing deleterious impacts on other layers • Adding "new" nodes into "old" edges
Operational Environment	• Y-12 management • Security guard union • Security contractor (WSI)	• Security personnel complacency • Ambiguity in executing established security procedures • Drawn-out security union negotiations	• Damaged edge between human layer (operator) & PSS layer (alarm display) results in reduced performance • Conflicting information on edges between human & system layers • Examples of multilayer communicability & additive page rank

Williams et al 2020; Schlosser 2015

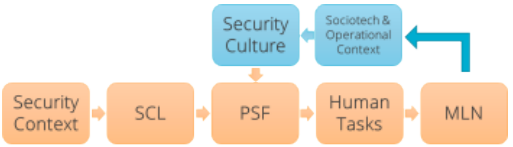
MLN Approach: System Context Lenses, The Y-12 Case

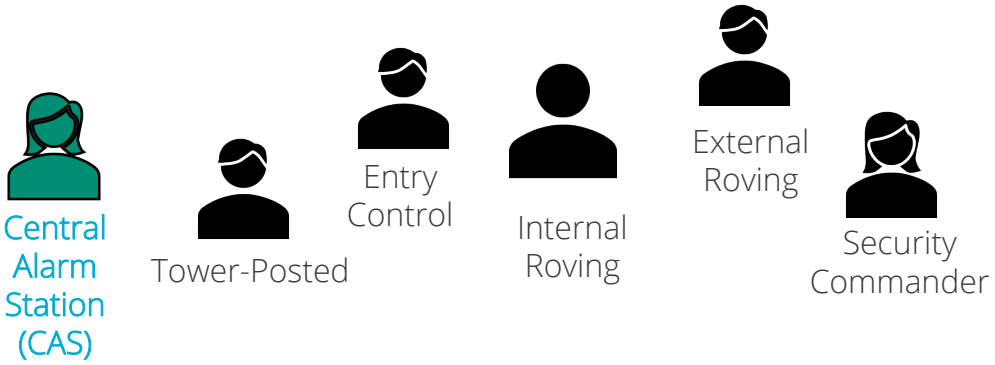


System Context	Human Stakeholders	Human Decision-Making Influences	Representation in MLN Models
System Design	• ARGUS system designers • Security guards • Y-12 employees	• Requirement to mesh "new" design into "old" (existing) system • Higher false alarm rates	• Breaking edges/removing nodes in one layer and not addressing deleterious impacts on other layers • Adding "new" nodes into "old" edges
Operational Environment	• Y-12 management • Security guard union • Security contractor (WSI)	• Security personnel complacency • Ambiguity in executing established security procedures • Drawn-out security union negotiations	• Damaged edge between human layer (operator) & PSS layer (alarm display) results in reduced performance • Conflicting information on edges between human & system layers • Examples of multilayer communicability & additive page rank
Sociotechnical Context	• Oversight (NNSA) • Protestors (Nuns)	• Reduced oversight • Security standardization across facilities • Moral opposition to nuclear activities	• External impacts on intralayer (human/ PSS) & interlayer (operator/regulator) edges • Examples of multilink community detection & versatility

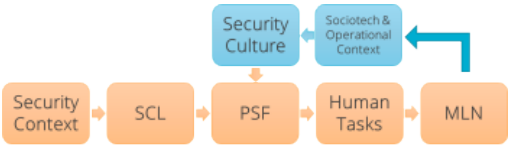
Williams et al 2020; Schlosser 2015

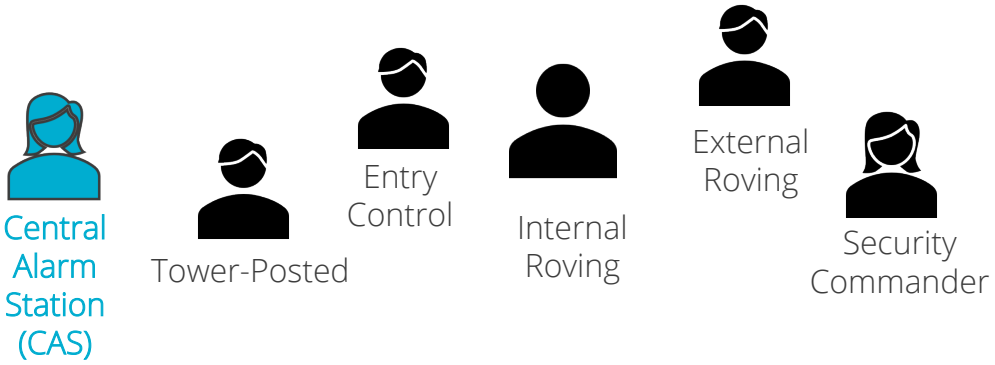
MLN Approach: Security Personnel Task Model

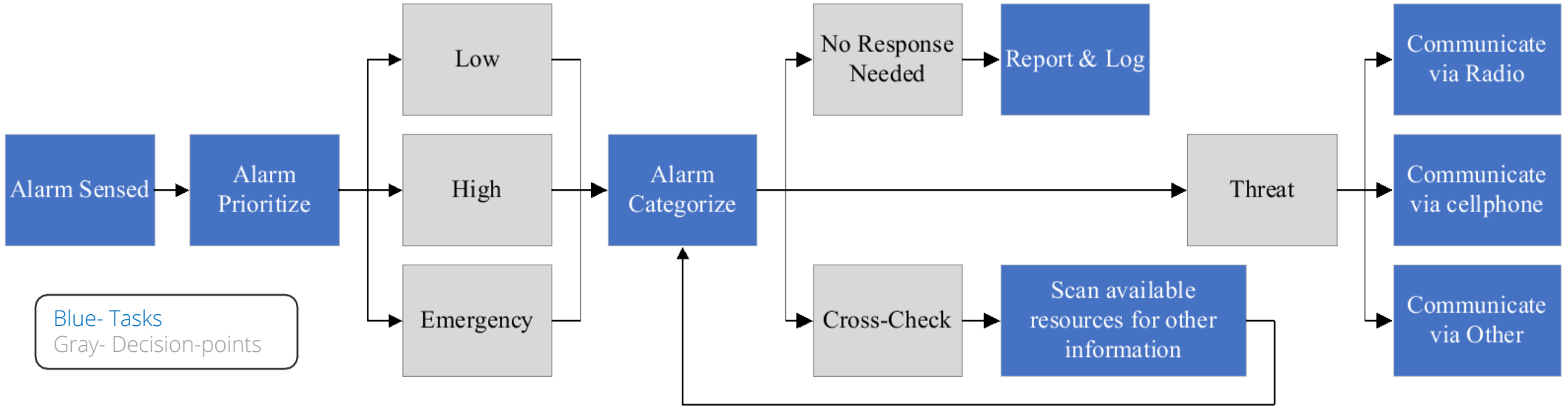




MLN Approach: Security Personnel Task Model

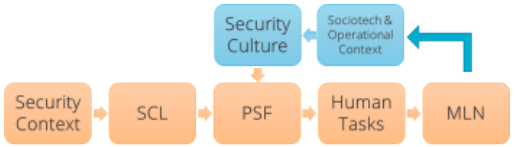


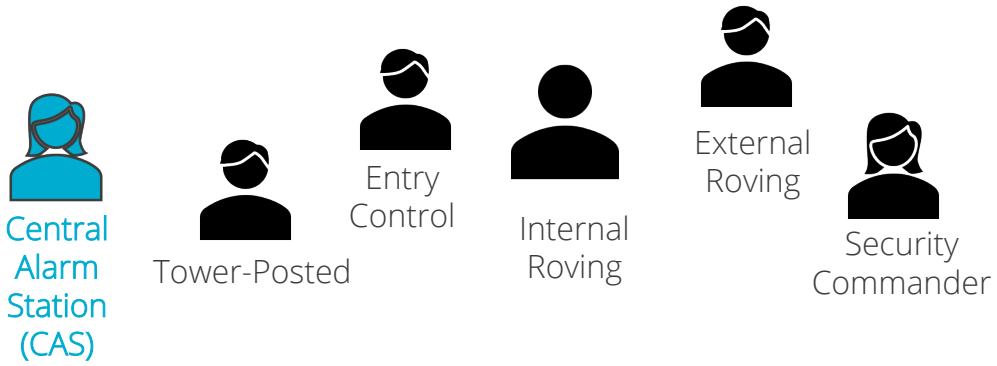




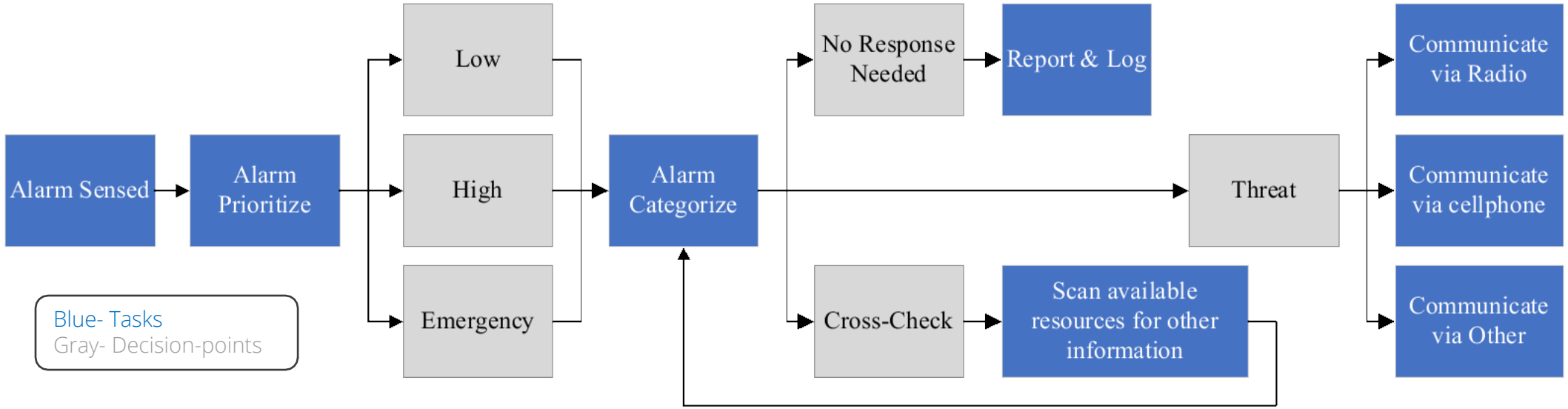
Fleming & Williams, 2021

MLN Approach: Security Personnel Task Model



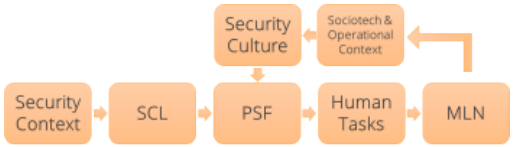


Individual Impact (Defined by Persona)	Job Impact (Defined by Role)	Site Impact (Defined by Site)
Experience	Human-machine Interfaces	Communication & Coordination
Stress	Time Available	Organizational Factors
Fitness for Duty	Procedures	Training
	Environment	



Fleming & Williams, 2021

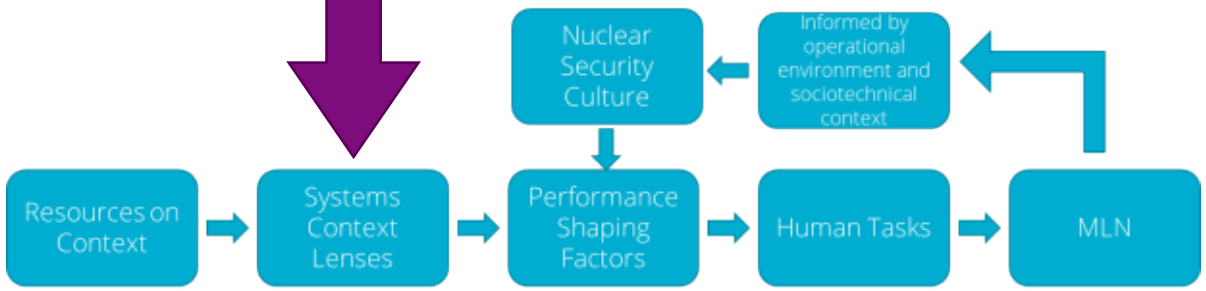
MLN Approach: Supports HSI (?)

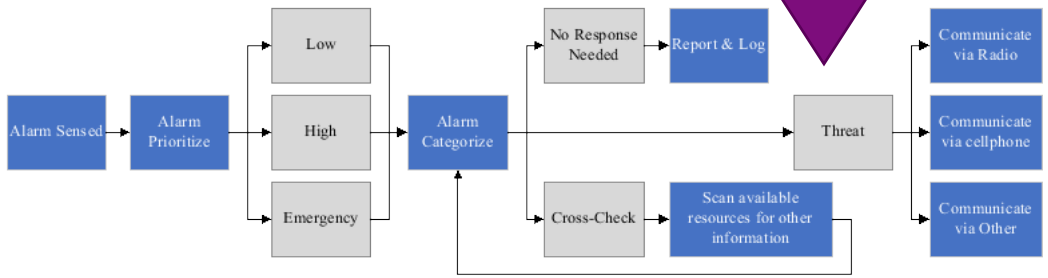


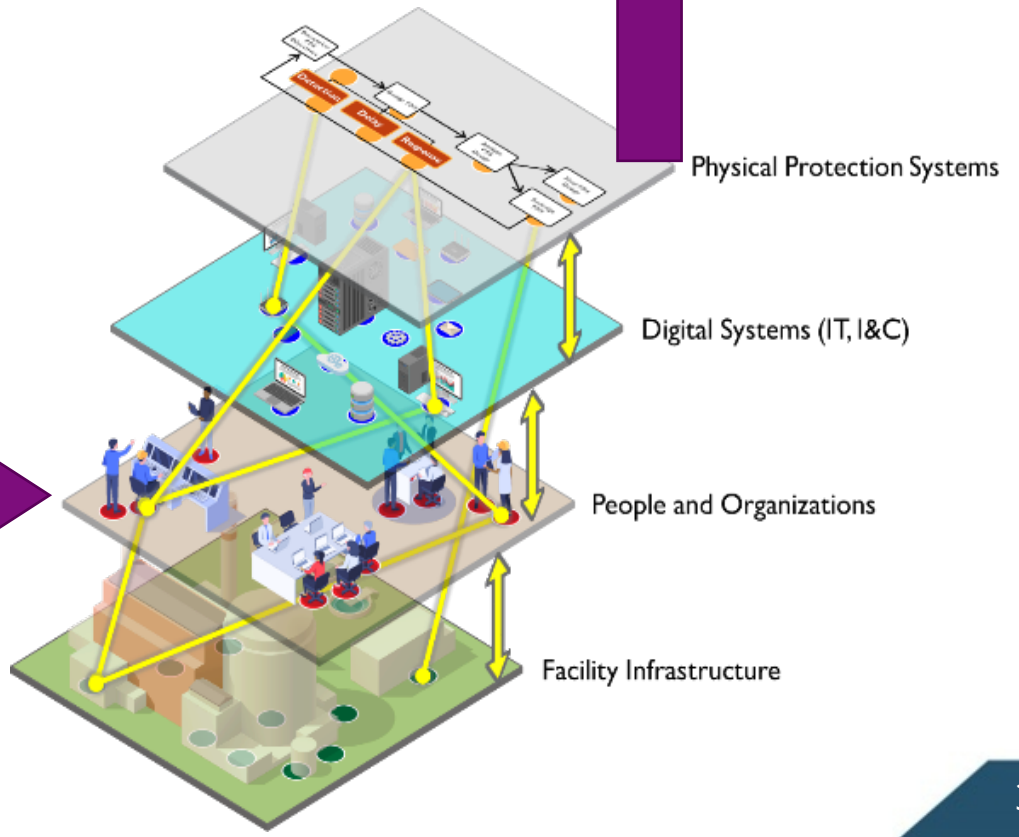
Sociotechnical Context
- Non-technical factors on decision-making
- Ex.: Societal needs, regulatory requirements

Operational Environment
- Conditions in which the system is deployed
- Ex.: Weather, shared resources

System Design
- Technical arrangement of components
- Ex.: Component specs, algorithms

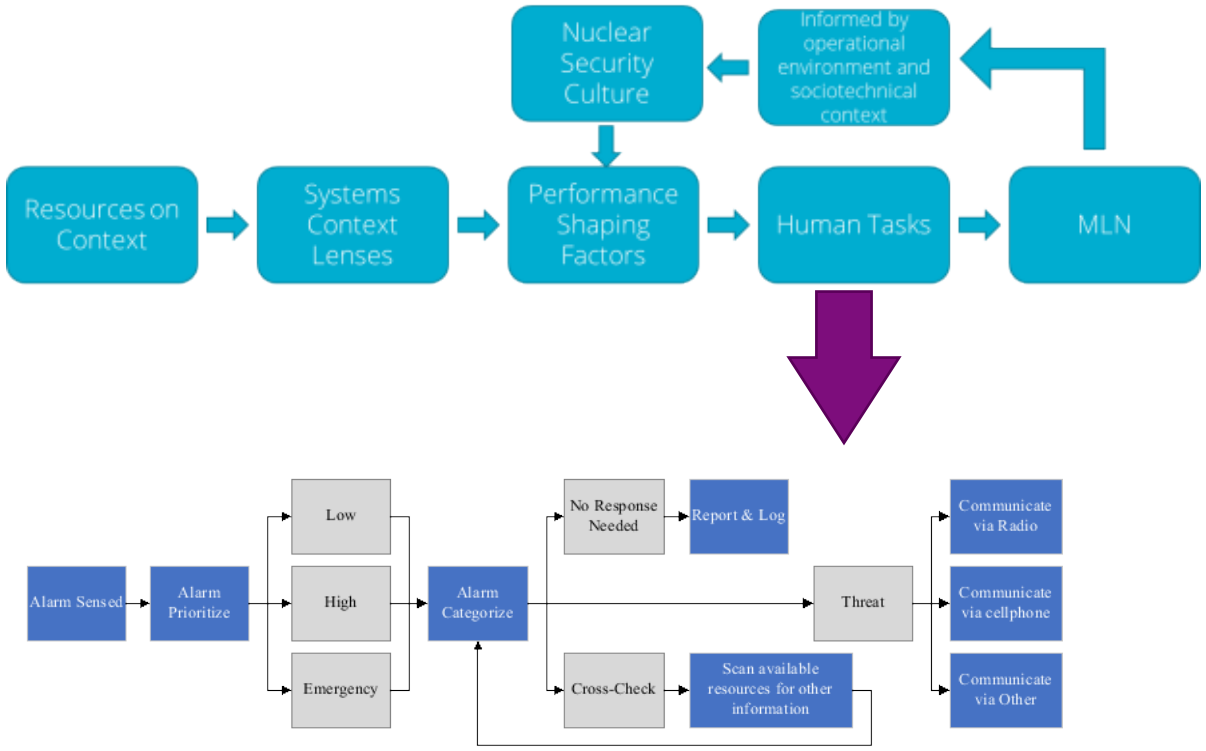






Applied Cognitive Task Analysis (ACTA) Approach

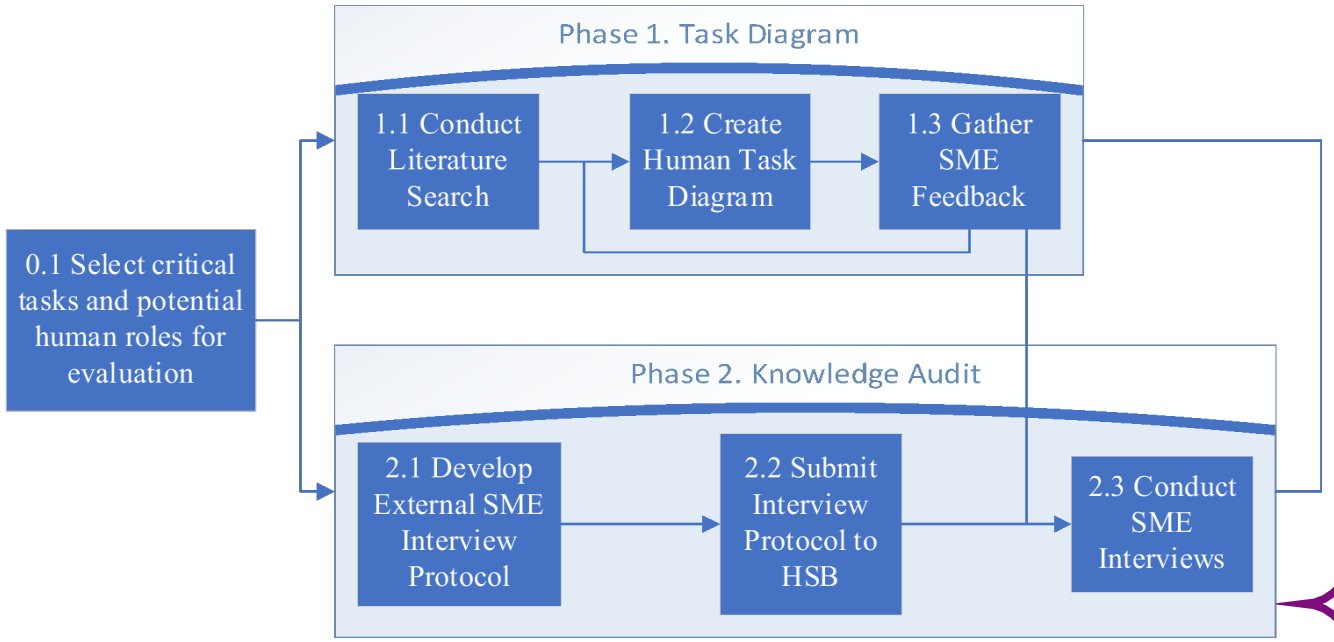
- Scaffold ***observations*** & ***interviews*** via a modified ACTA approach
  - Establish an evidence-based framework for evaluating human/automation tradeoffs
  - Understand the cognitive demands of security personnel (with/without automated assistance)



Participant Type	Sites Included		
	Site 1	Site 2	Site 3
Facility Administrators	X	X	
Facility Employees	X	X	X
Response Force Dispatch	X	X	X
Response Force Leadership	X		X

Question Type	Example
Site Information	Who monitors and responds to security alarms?
Participant Background	What is your experience?
Alarm System Description	Walk me through how you respond to alarms.
False/ Nuisance Alarm Response	How do you determine an alarm is “false” or “nuisance”?
Other	If money were no object, what's would incorporate into your security system?

ACTA Approach: Knowledge Audit + Task Diagram



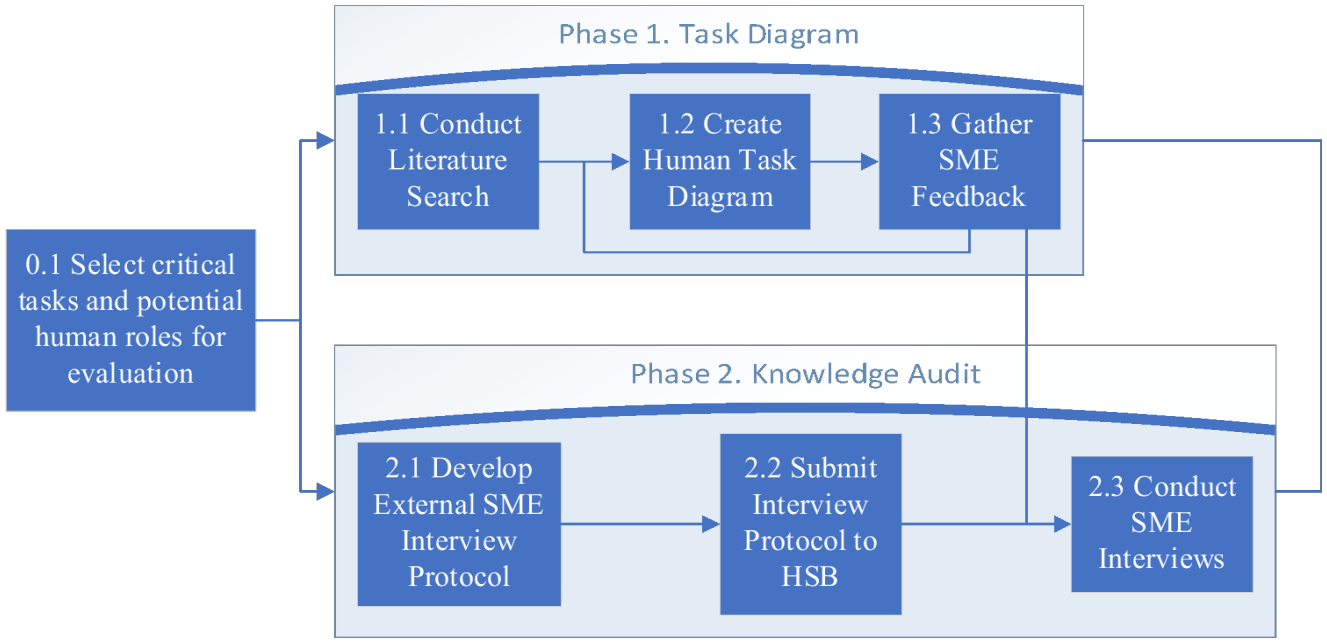
Participant Type	Sites Included		
	Site 1	Site 2	Site 3
Facility Administrators	X	X	
Facility Employees	X	X	X
Response Force Dispatch	X	X	X
Response Force Leadership	X		X

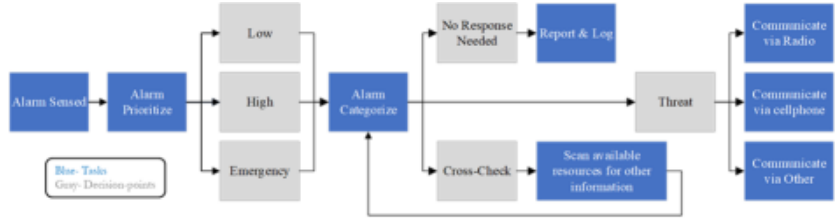
Question Type	Example
Site Information	Who monitors and responds to security alarms?
Participant Background	What is your experience?
Alarm System Description	Walk me through how you respond to alarms.
False/ Nuisance Alarm Response	How do you determine an alarm is “false” or “nuisance”?
Other	If money were no object, what's would incorporate into your security system?

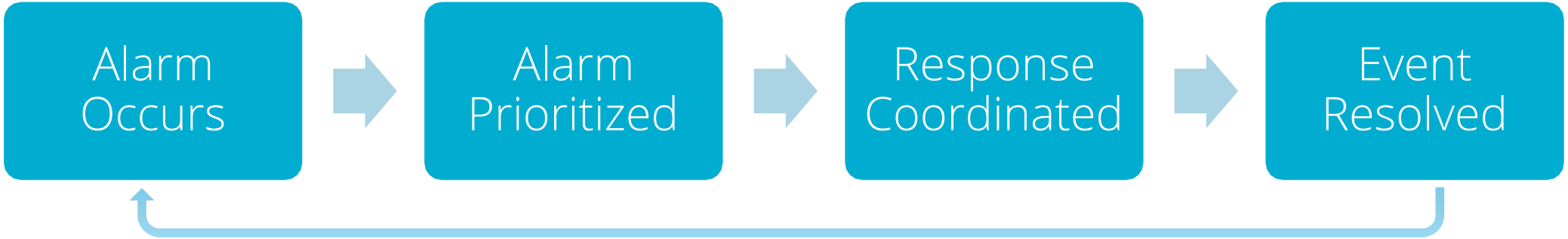
Knowledge audit → multi-dimensional info gathering

Task diagram → comprehensive info synthesis

ACTA Approach: New Task Diagram





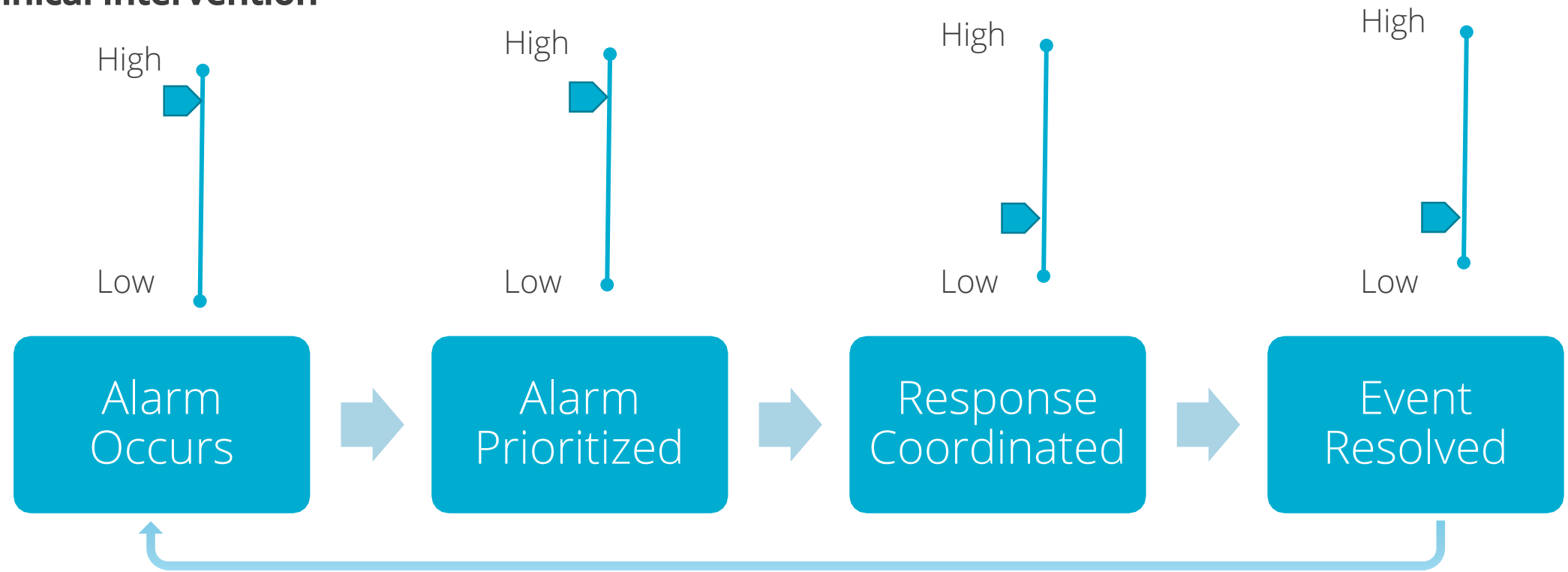


ACTA Approach: New Task Diagram

Alarm Occurs and Prioritized were generally automatic & driven by technical components of the system

Alarm Response and Resolution were generally manual & driven by human decision-making, task completion

Technical Intervention

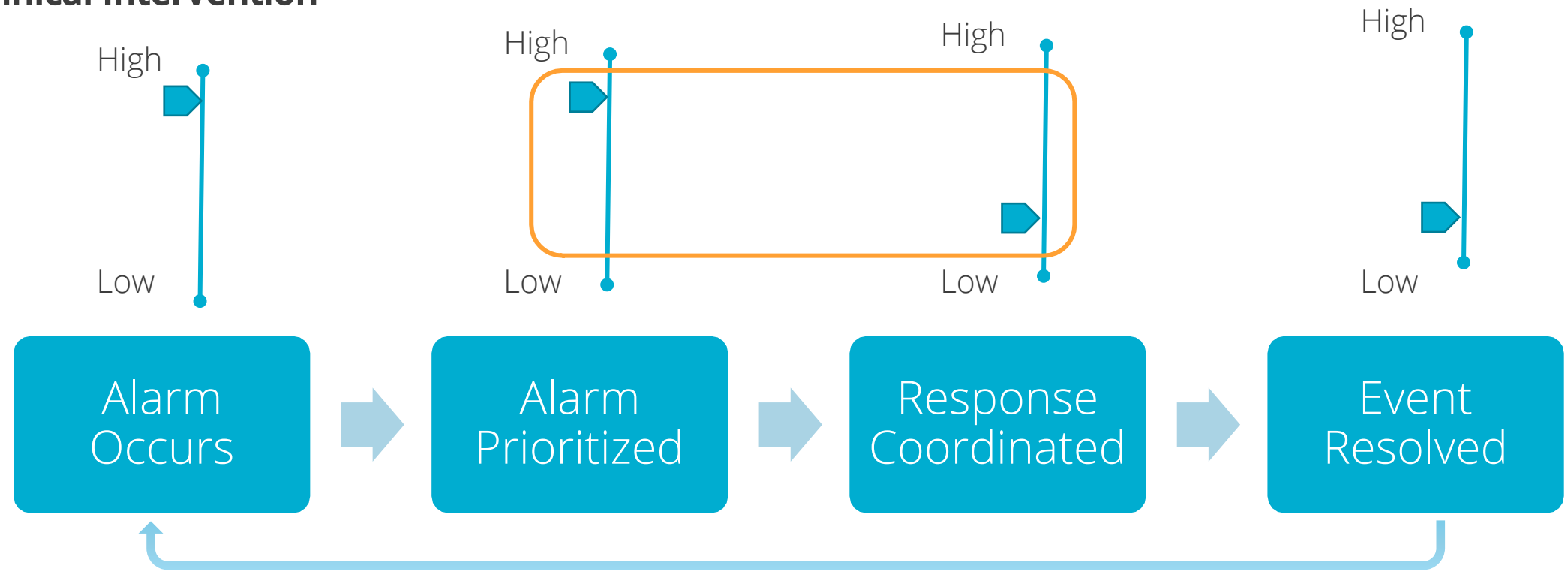


ACTA Approach: New Task Diagram

In most cases, the system automatically assigned alarm priority using a concept of operations

If multitasking, the response urgency could be overridden by the responding forces

Technical Intervention

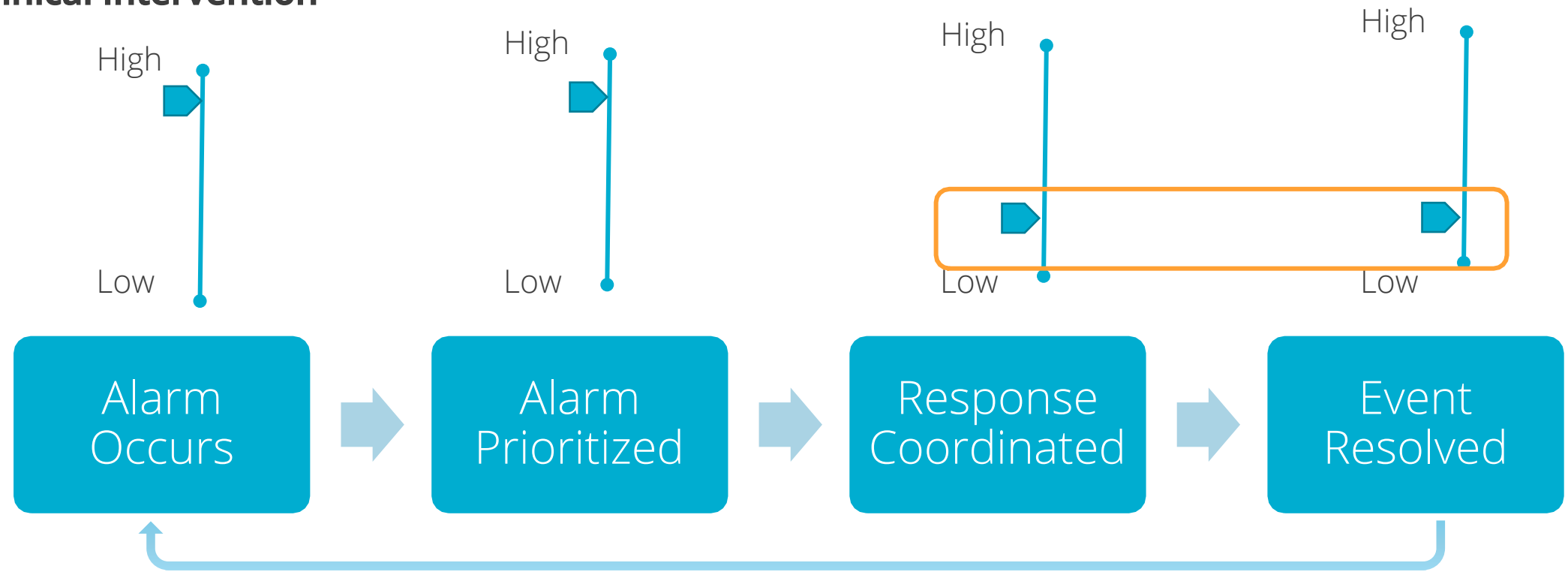


ACTA Approach: New Task Diagram

Response was driven by dispatch <u>situation awareness (SA)</u>

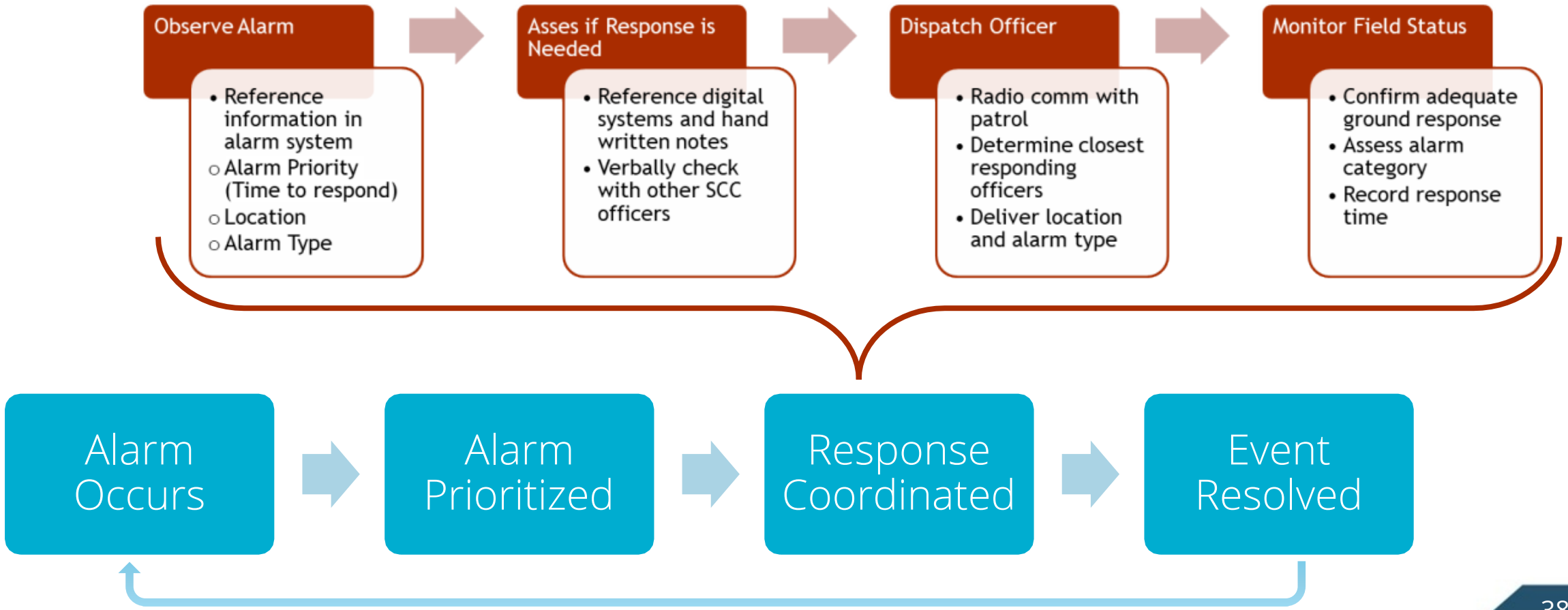
Dispatch updates SA using multiple sources of (internal and external) information

Technical Intervention



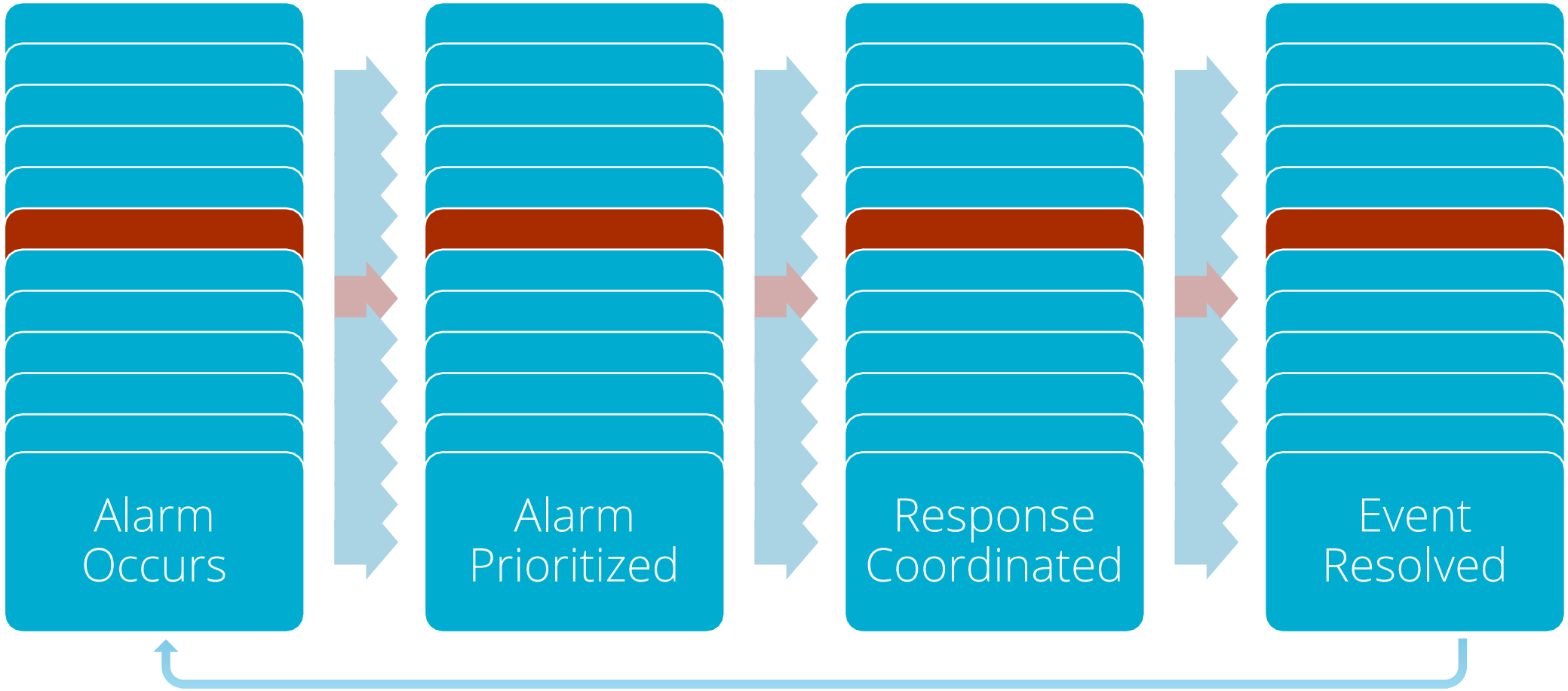
ACTA Approach: New Task Diagram

Iterative rounds of analysis on the knowledge audit → more detailed task diagrams…



ACTA Approach: New Task Diagram

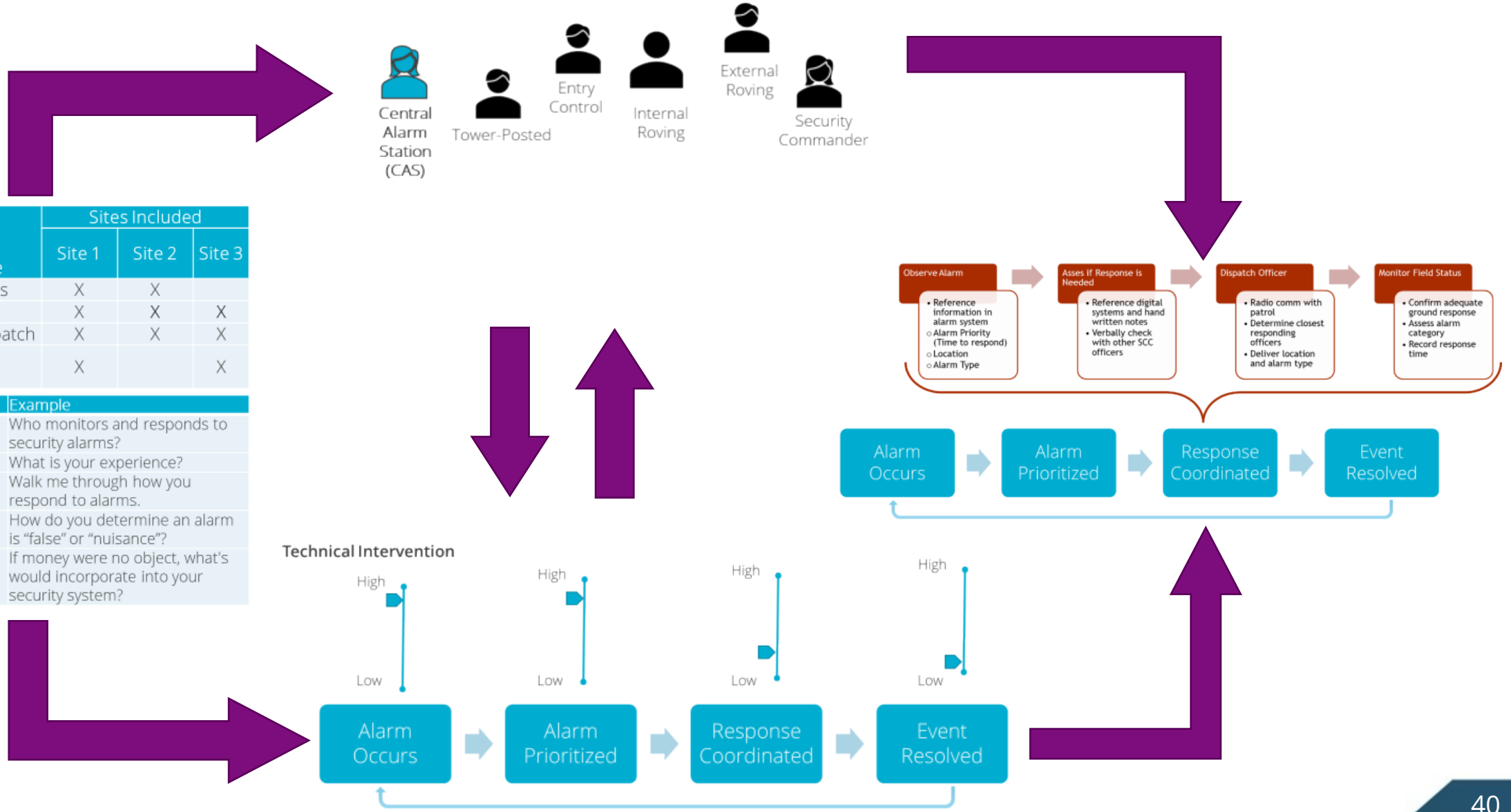
Even simple task diagrams can be yield complex systems outcomes (e.g. alarm run)



ACTA Approach: Supports HSI (?)

Participant Type	Sites Included		
	Site 1	Site 2	Site 3
Facility Administrators	X	X	
Facility Employees	X	X	X
Response Force Dispatch	X	X	X
Response Force Leadership	X		X

Question Type	Example
Site Information	Who monitors and responds to security alarms?
Participant Background	What is your experience?
Alarm System Description	Walk me through how you respond to alarms.
False/ Nuisance Alarm Response	How do you determine an alarm is "false" or "nuisance"?
Other	If money were no object, what's would incorporate into your security system?



What have we learned so far…

Key Empirical Findings

Situation Awareness during alarm response & resolution

- Alarm monitoring systems vary in how they present information about the alarm
- Dispatch information needs don't connect with displayed information
- Dispatch relies on hand-written notes to capture external sources
- Other information may be available via system logs, but not incorporated in security operations (e.g. facility badge logs)
- Alarm resolution outcomes were captured in system external to alarm response

Nuisance alarms are frequent

- Dispatch may override an alarm based on external information or the operational environment

Alarms are only useful if they're enabled

- Facility may be disarmed by a stakeholder, limiting ability of dispatch to monitor security
- Non-security site/facility employees may disable alarms if they conflict with primary goals

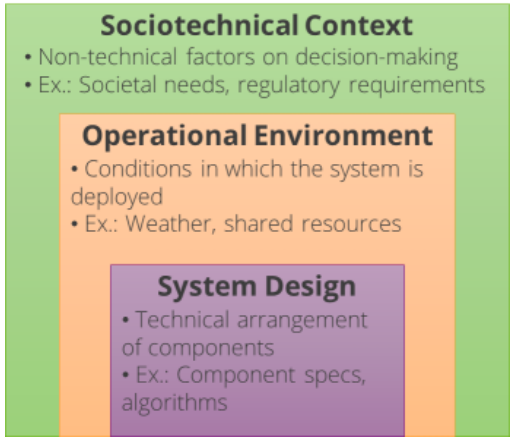
Non-security employees serve a role in security operations

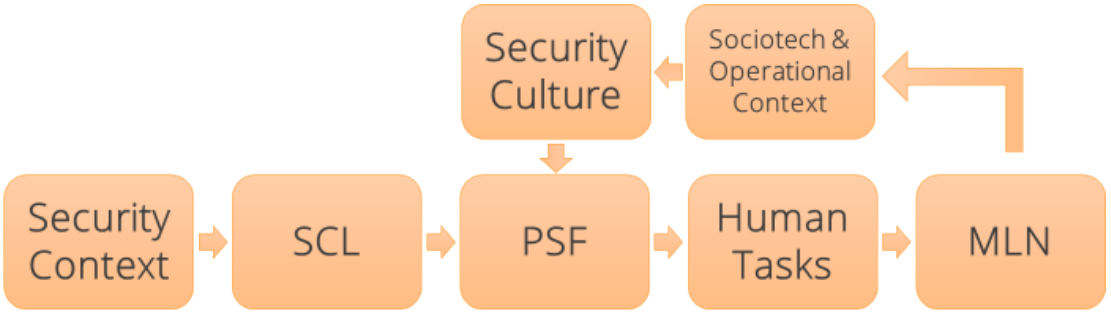
- Facility walk-downs, awareness of unauthorized individuals, awareness of sensitive activities (e.g. refueling)

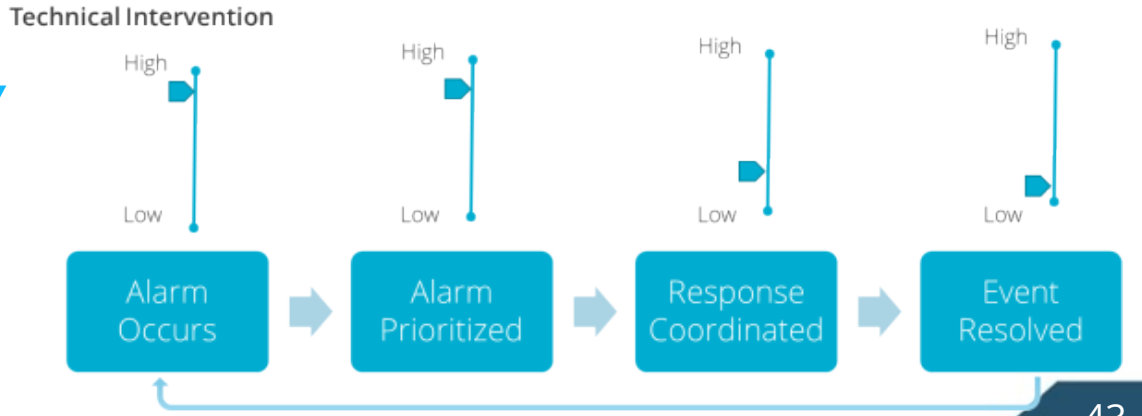
Analytic Insights…

Restating from previous slides:

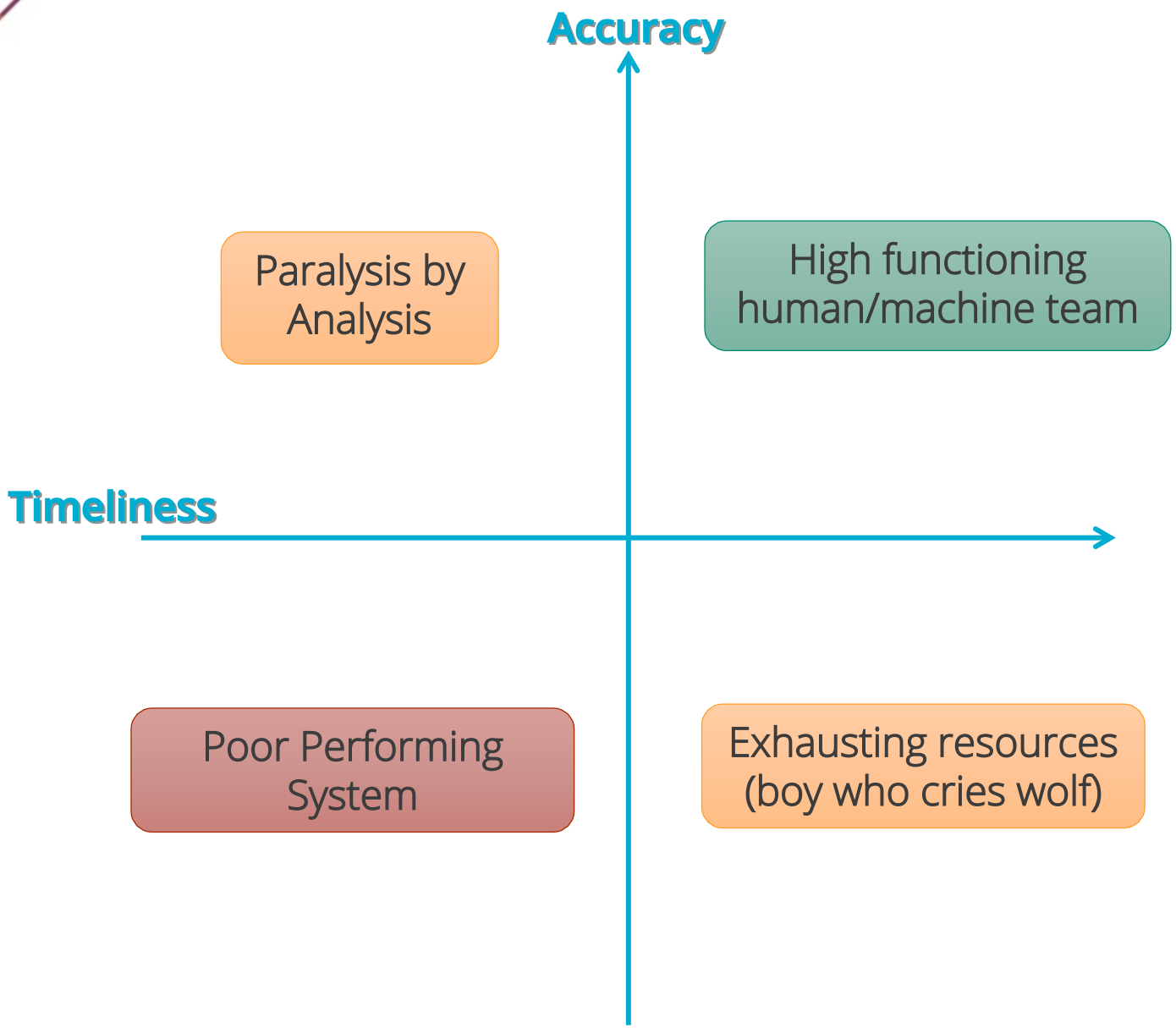
- More ***complex, comprehensive inclusion*** of human actor roles in HCF security
- Dynamic relationships between ***system context lenses***
- Incorporating ***non-linear impacts of human actors*** (via MLN)
- Task diagrams to help evaluate ***levels of autonomy***
- The basis for ***HSI-based design decisions*** for HCF security







Analytic Insights…



Event response timeliness & event detection accuracy are key dimensions

Mapping them together provides additional clarity on:

- Evaluating this element of the overall “detection” capability
- Designing to optimize the timeliness/accuracy trade-off
- Determining the impact of automation in HCF security

Research challenges + lessons learned

- Interest/willingness of facilities
  - **Challenge** → Facility hesitance to allow access to security operations
    - **Lesson learned** → Use professional networks, MOU/NDAs help clarify the boundary of the research, emphasize potential to share lessons that may improve their performance

- Clearances
  - **Challenge** → Some areas, individuals, activities or information fall in areas in which the researcher needs a security clearance
    - **Lesson learned** → Ensure at least one (ideally multiple) research team members have all necessary clearances
    - **Lesson learned** → Having a research team member without a clearance can help "force" the conversation to stay in the 'open source" range

- Timing
  - **Challenge** → Planning observations amidst busy operational schedules
    - **Lesson learned** → Plan well in advanced, be flexible…but be persistent! Also, have contingency site visits prepared

  - **Challenge** → Finding the "right" amount of time to ask to observe operations (research do not want to become a distraction or hindrance to good employees
    - **Lesson learned** → Use traditional data convergence tactics, as well as "read the room"

Research challenges + lessons learned

- Collecting & storing data (re: HCF security practices & performance)
  - **Challenge** → Navigate sensitive/classified data information
    - **Lesson learned** → Only use sensitive information for background/context + ANONYMIZE!!!
  - **Challenge** → Protecting data (another dimension of protecting interviewees/observation hosts)
    - **Lesson learned** → Encrypted digital storage/transmission, anonymize sources, only link source to data point for additional context
- Publishing
  - **Challenge** → find right balance of detail/academic rigor that avoids classification issues
    - **Lesson learned** → ask questions early and often; prepare non-sensitive comparative uses cases
  - **Challenge** → conveying sufficient nuance & intricacy in HSI-related insights
    - **Lessons learned** → (At best) Find a creative way to describe a similar nuance or (at worst) do not publish such key insights

Future Work

Potential Future Work

Experiments on HSI design impacts on evaluations of early-stage automation designs and ConOps integration

Sensitivity analysis to investigate the impact of timeliness and accuracy dimensions on security system consequences

Use interviews and focus groups to identify elements which significantly impact the timeliness and accuracy dimensions

Identify and define specific technology requirements based on function allocation characteristics for HCF security

QUESTIONS