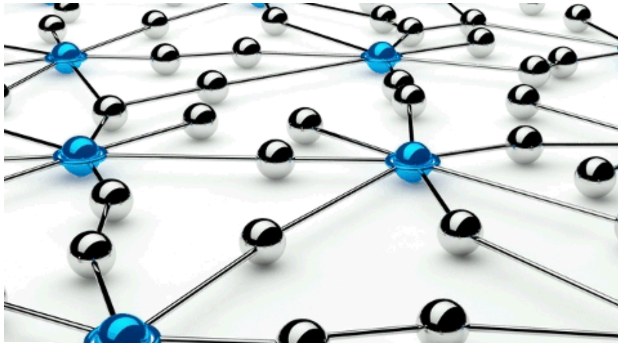
SAND2017-6169C



Modeling Human-Technology Interaction as a Sociotechnical System of Systems

Amanda Wachtel, awachte@sandia.gov

Jessica Turnley, Matt Hoffman, Karina Muñoz-Ramos, John Gauthier, Ann Speed, Robert Kittinger

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-NA-0003525.
SAND2017-#

Background and Purpose

- Many (if not all) Systems of Systems (SoS) are human-centric, but SoS models do not factor in human/HSI effects
  - Humans introduce greatest amount of uncertainty and potential for error (e.g., Y12, Three Mile Island)
  - Human-related uncertainty can lead to higher cost, greater logistics tail, increased vulnerability
- Potential exists for significant gained efficiencies and risk mitigation if human & human-system effects are understood and accounted for in the SoS engineering process
  - E.g., lower troop-to-task ratio, lower error rates, fewer cascading failures
- Research purpose: Develop an SoS modeling framework that includes human behavioral models with enough fidelity to understand interactions with technology, and resulting impacts on organizational performance
  - Enable more realistic assessment of SoS performance and efficiency under different circumstances
  - Understand impact of changes such as augmentation/automation, organizational/doctrinal revisions, improved technologies and interfaces, etc.

The Spectrum of Interest

Human

- Fall asleep during task
- Failure to detect item during unaided visual search
- Human failure leading to loss of equipment capability
- Insider can disable/degrade equipment capabilities

Human-Technology Interaction

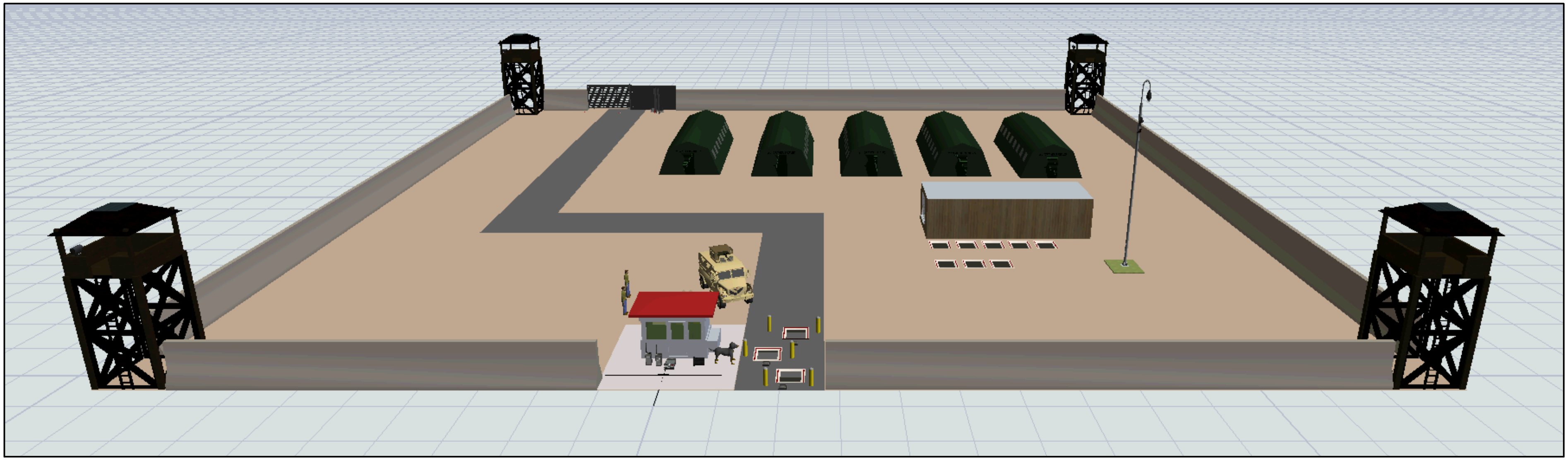
- **False alarm fatigue**
- **Failure to detect item via IR, cameras, etc.**
- **Over-reliance on technology; potential inability to adapt to equipment failure**
- **Equipment can degrade task performance (e.g. by reducing dexterity, endurance etc.)**
- **Technology interface affects cognitive load, usability etc., particularly in special situations (combat, sand storm, etc.)**
- **Semi-automated capabilities requiring human discretion**

Technology

- Equipment failure leading to loss of human effectiveness
- Failure to maintain equipment
- Equipment failure
- False alarms

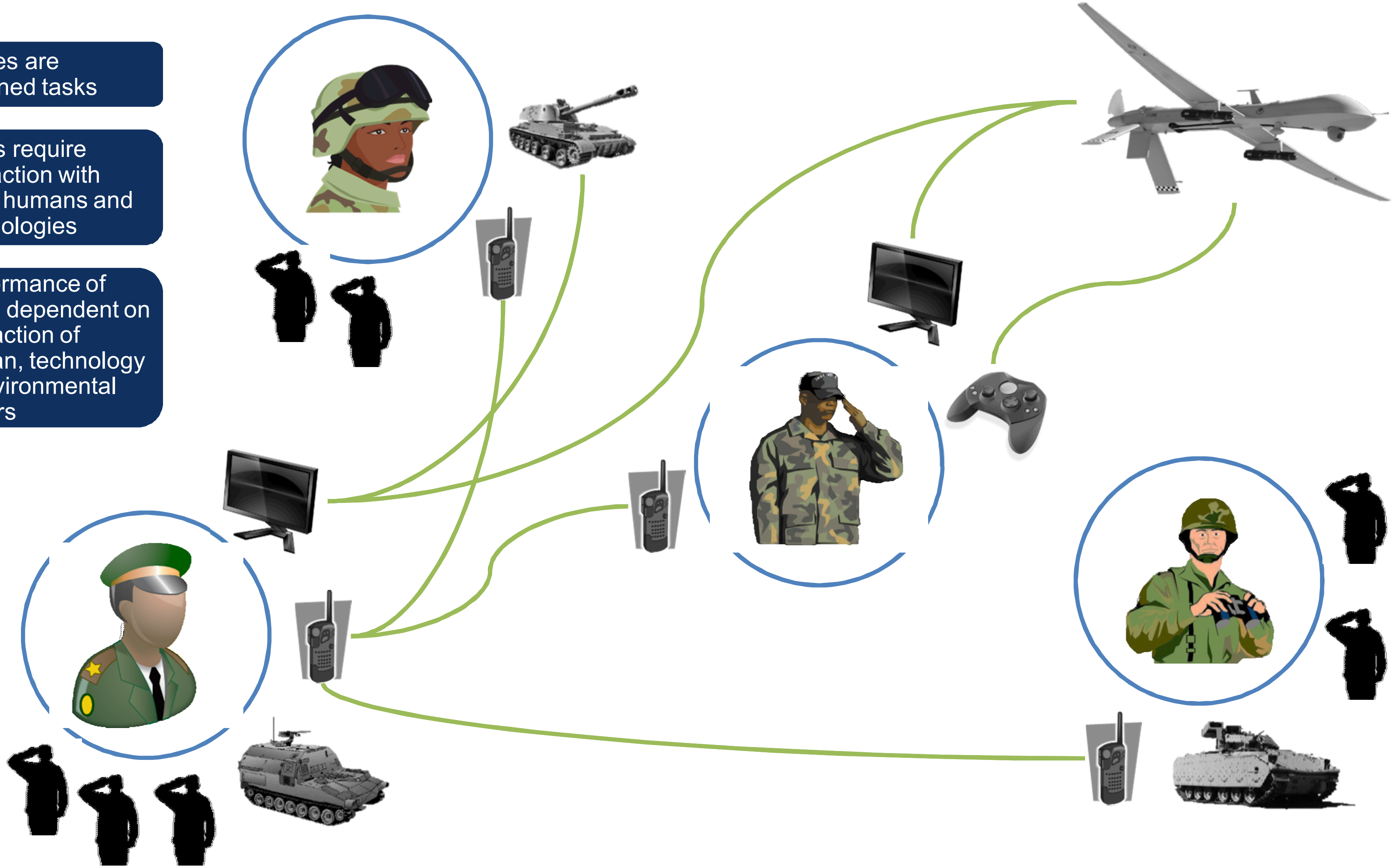
Use Case Model:
Layered Security at Forward Operating Base (FOB)

- Use case allows us to explore and exercise abstract, general ideas in a more concrete scenario
- Baseline model effort looks at small FOB and how human-technology interaction affects ability to complete tasks
  - Tractable but interesting
  - Lots of human & human-system factors
  - Layered security is relevant to multiple national security mission areas
  - Explicitly models interdependence between humans, technology, tasks and communication/response modes



Mental Model of SoS Interactions

- Entities are assigned tasks
- Tasks require interaction with other humans and technologies
- Performance of tasks dependent on interaction of human, technology & environmental factors



Methodology

Problem definition

Define SoS boundaries | Define function(s) | Define range of scenarios

Job/Task Analysis; Business Rule Elicitation

Who, what, where, when, how; task frequency, duration, SOPs

Factor Elicitation

What affects performance/stresses | What conditions/issues are encountered

Parameterize interdependencies and dynamics

Develop SoS model

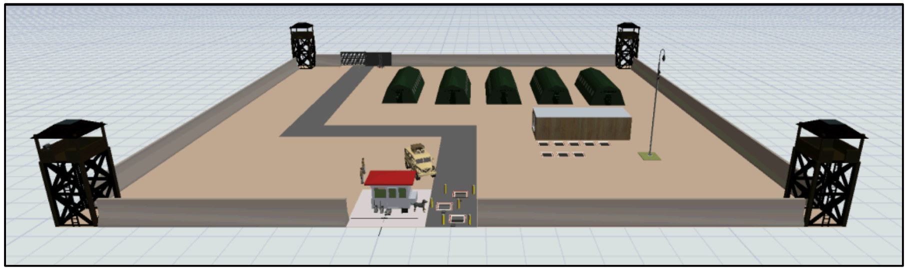
People, roles, technologies, task logic flow, performance multipliers

Perform Analysis

Baseline Vetting | Excursions | Sensitivity/UQ

FOB Layered Security Model Description

- Layered security requires completion of various jobs/tasks at various stations
  - tower guard, gate guard, TOC operator, sergeant, response team
- Task accomplishment requires resources, such as human personnel and technologies
- Duration and performance of task dependent on
  - state of human (e.g., training, exhaustion)
  - type of task (physically vs. cognitively demanding)
  - technology availability/usability
  - environmental conditions, etc.
- Includes interactive effects – e.g. some technologies are harder for human to use in certain environments
- Events/tasks can trigger other events/tasks
- Task failure can have different consequences
  - delay, retry, alternate process, mission failure

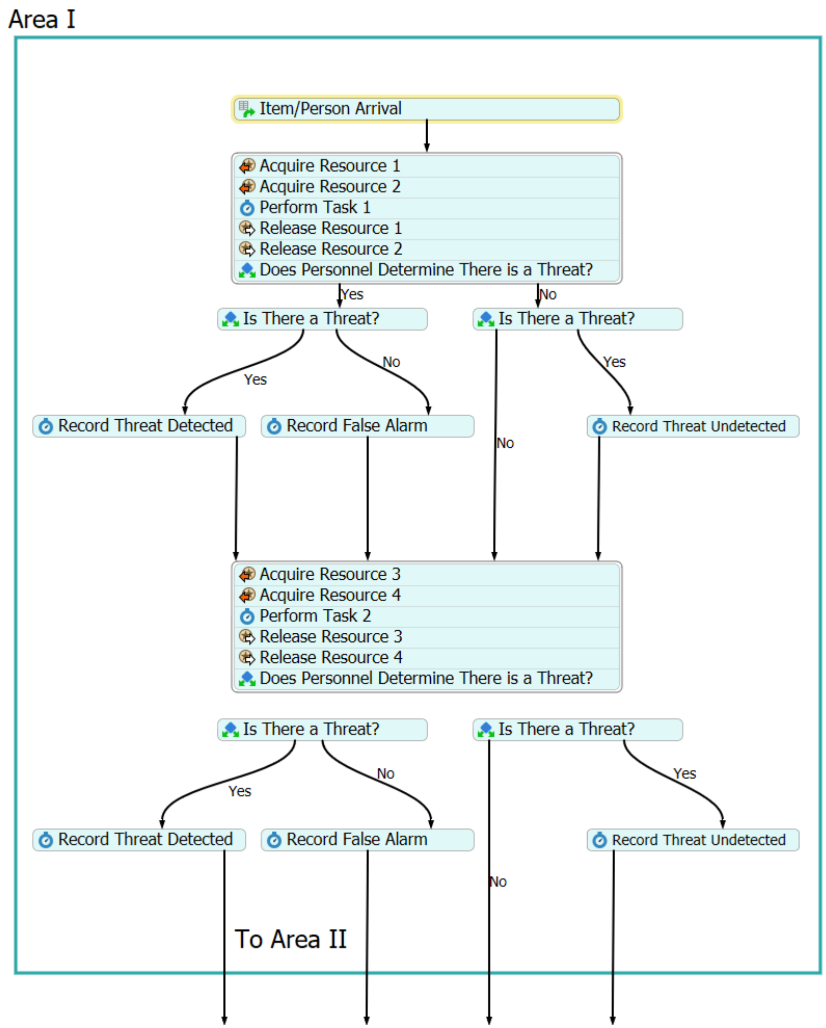


VBIED Scenario Example

- Model randomly assigns IED to some vehicles
- Tasks specified based on location (holding area, entry gate, TOC, etc.)
- Multiple technologies needed for tasks
  - Examples: radios, biometric scanners, security cameras, etc.
  - Failure modes with time to repair specified for each technology
- Probabilities defined for each threat type
  - Logic includes false positives and false negatives
  - Detailed communication modes determine how successfully threat is communicated and whether response is appropriate to threat type

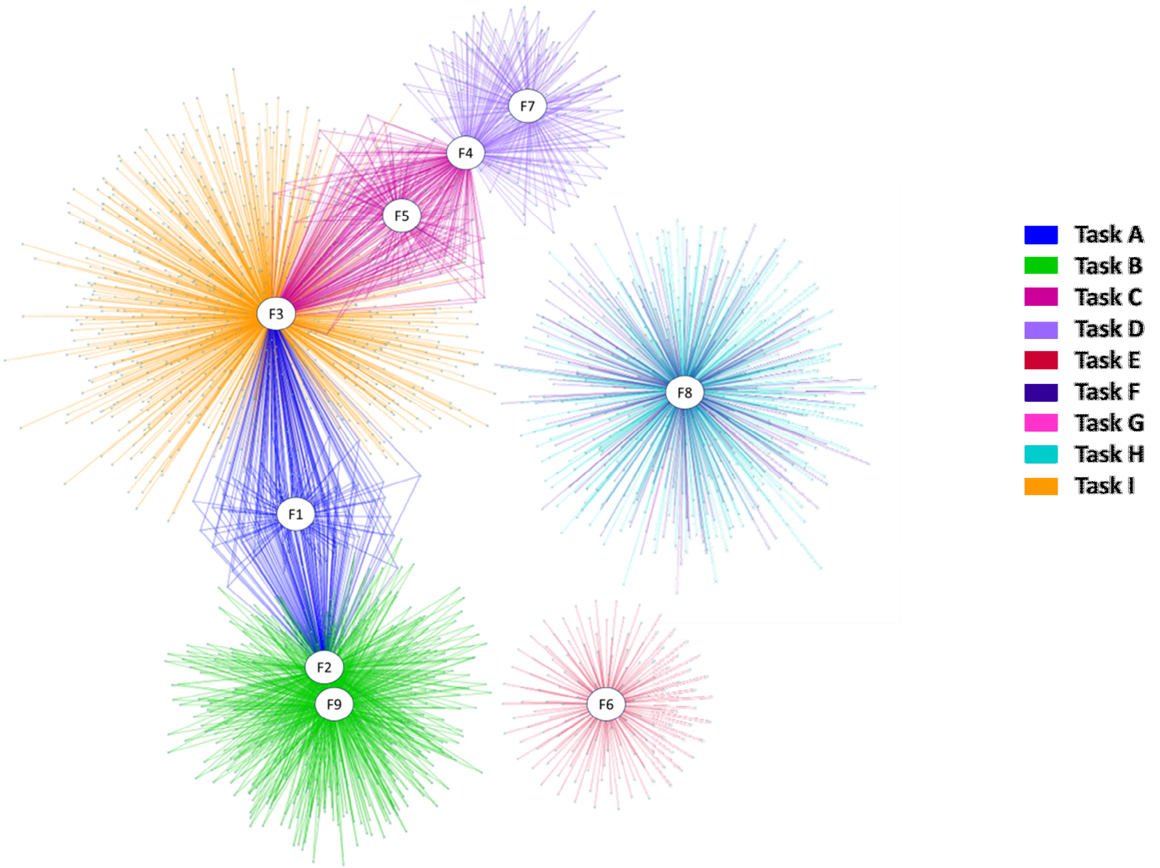
- Ability to complete task based on interactions with required technology and affected by performance-modifying conditions such as weather and fatigue
- Jobs, tasks, and technologies obtained through SME input

Notional Model Logic Example



Task Mapping to Cognitive Factors

- Many performance parameters in model—need way to combine similar parameters
- Focused on human-technology interaction so grouped tasks by cognitive factors used
- Graphic shows task instances for two month simulation and how they map to cognitive factors



Sensitivity (from Detection Theory)

- Extending concepts from detection theory to delay, communication, and response aspects of security
- Extending from single-system metrics to SoS metrics
- Key metrics:
  - P(hit)
  - P(FA)
  - P(miss)
  - d’ = z(P(hit)) – z(P(FA))
- d’ measures the *sensitivity* of a security technology; e.g., how well it distinguishes between true threats and false ones.
- In this domain, d’ could, for example, be an indicator of whether personnel might eventually become susceptible to false alarm fatigue

Detection

- a “hit” occurs when an attacker is detected; a “false alarm” occurs when a detection occurs without an attack (shown below)

Delay

- a “hit” occurs when an attacker is delayed enough for a response; a “false alarm” occurs when a friendly is delayed

Comms

- a “hit” occurs when messages are properly communicated during an attack; a “false alarm” occurs during no attack when messages are misinterpreted to be related to an attack

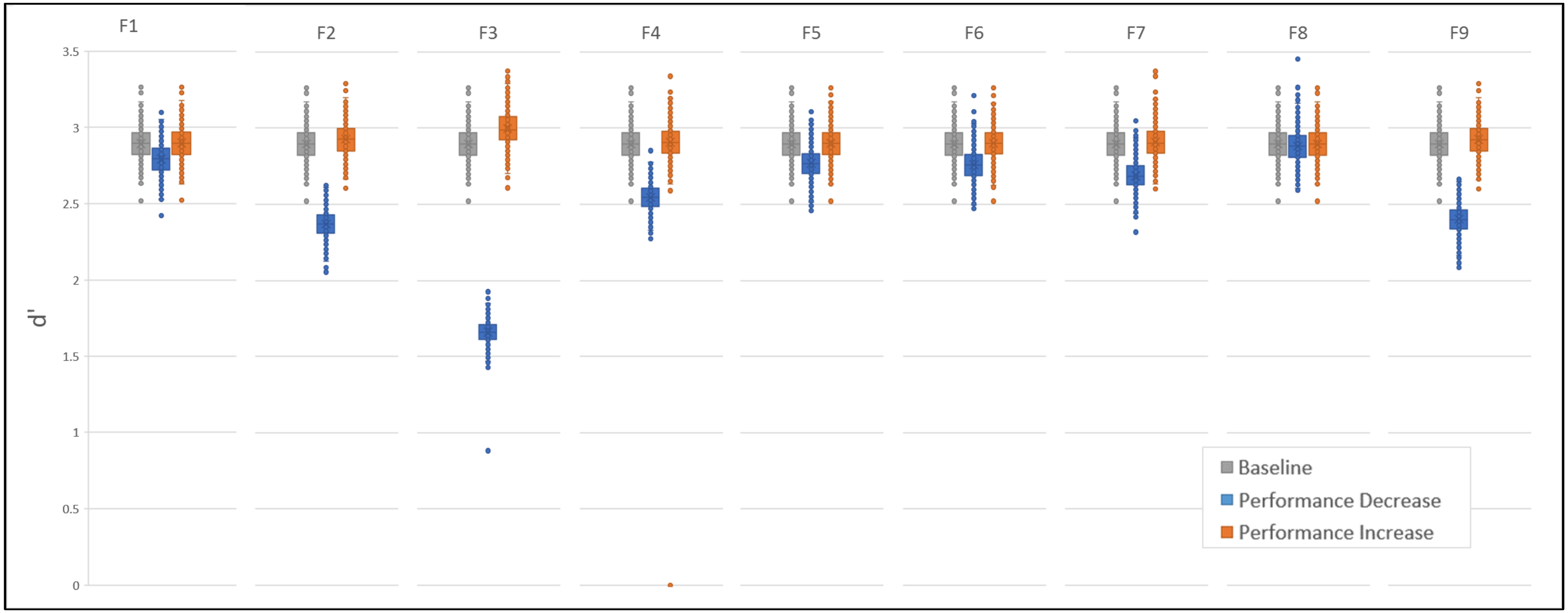
Response

- a “hit” occurs when the response stops an attack; a “false alarm” occurs when a response occurs to no attack

	Response	
Attack	**Detected**	**Undetected**
Yes	**hit**	miss (false neg)
No	**false alarm** (false pos)	correct rejection (true neg)

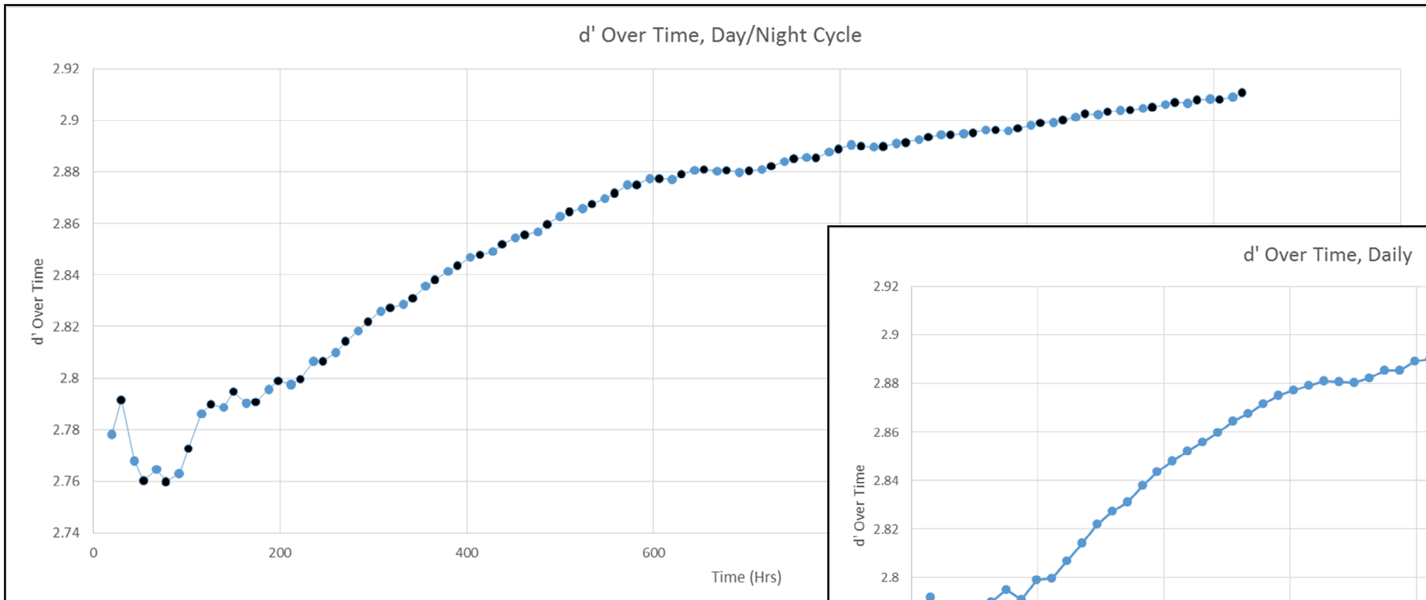
Cognitive Factor Sensitivity Analysis

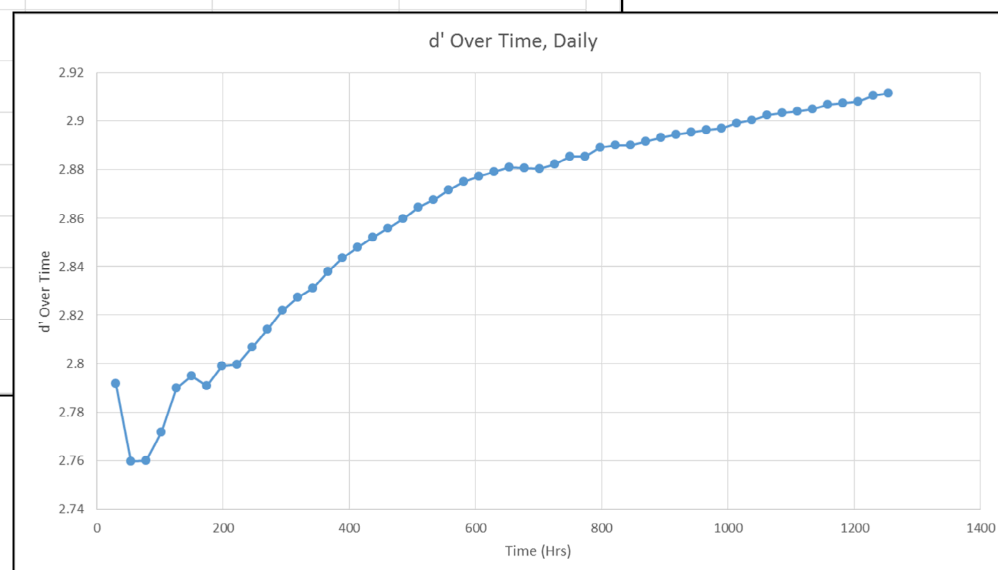
- Grouped tasks based on cognitive factors employed in order to run sensitivity on groupings of parameters
- Changed one factor and its associated tasks at a time, either increasing or decreasing performance by 25%
- Kept other eight factors at baseline values
- Ran 1000 replications of each scenario for a 2-month duration
- Follow-on analysis to look at 2-way interactions



d’ Over Time

- d’ calculated over time for 2-month simulation
- Looked at d’ for day/night cycle and daily
  - Wanted to see impact of tasks whose performance change based on time of day
    - Difference is diminished over time as the learning curve takes effect
- Also have ability to look at overall d’ by area and for the SoS





Significance of Sensitivity Work

- Greatly extends concept of Sensitivity (from Signal Detection Theory*), from a metric for a single detection task, to a metric for the physical security system SoS
  - including all detection, delay, communication and response tasks required to effectively mitigate a given threat
  - now measures how well a security system (including human and technology elements) distinguishes between and reacts to true threats and false ones.
  - can capture two aspects of human involvement – human communications and human interaction with technology
- Shows how certain tasks can have cascading impacts on the performance of the entire SoS
  - Task instances and level of connectivity to other tasks determines strength of impact
  - Even if each task performed relatively well, interactions and dependencies can lead to lower SoS d'
- Reveals which cognitive factors have the largest impact on SoS d'
  - Identifies areas for future research or investment in training, new technologies, etc.
  - Maximizes impact of limited budgets for largest return on investment

*Macmillan, N.A., & Creelman, C.D. (2005). Detection Theory: A User's Guide (2nd Ed.). Lawrence Earlbaum Associates: New York.

Future Work

- Single Factor Excursions
  - Extreme fatigue, night vision goggle usability, sandstorm
  - More complex excursions with interactive effects will also be done
- Validation
  - Can use high-level metrics to verify baseline performance under "normal" conditions
  - SME face validation critical to understand validity of model behavior in less common operating conditions
- Further Applications
  - Methodology expected to be widely applicable to layered security problems
  - Need to explore applicability in other domains
    - Structure of some problems may dictate different types of simulation models and/or opportunities to use agent-based modeling, hybrid dynamical system modeling, etc. in conjunction with discrete event modeling

Questions?

Backup slides

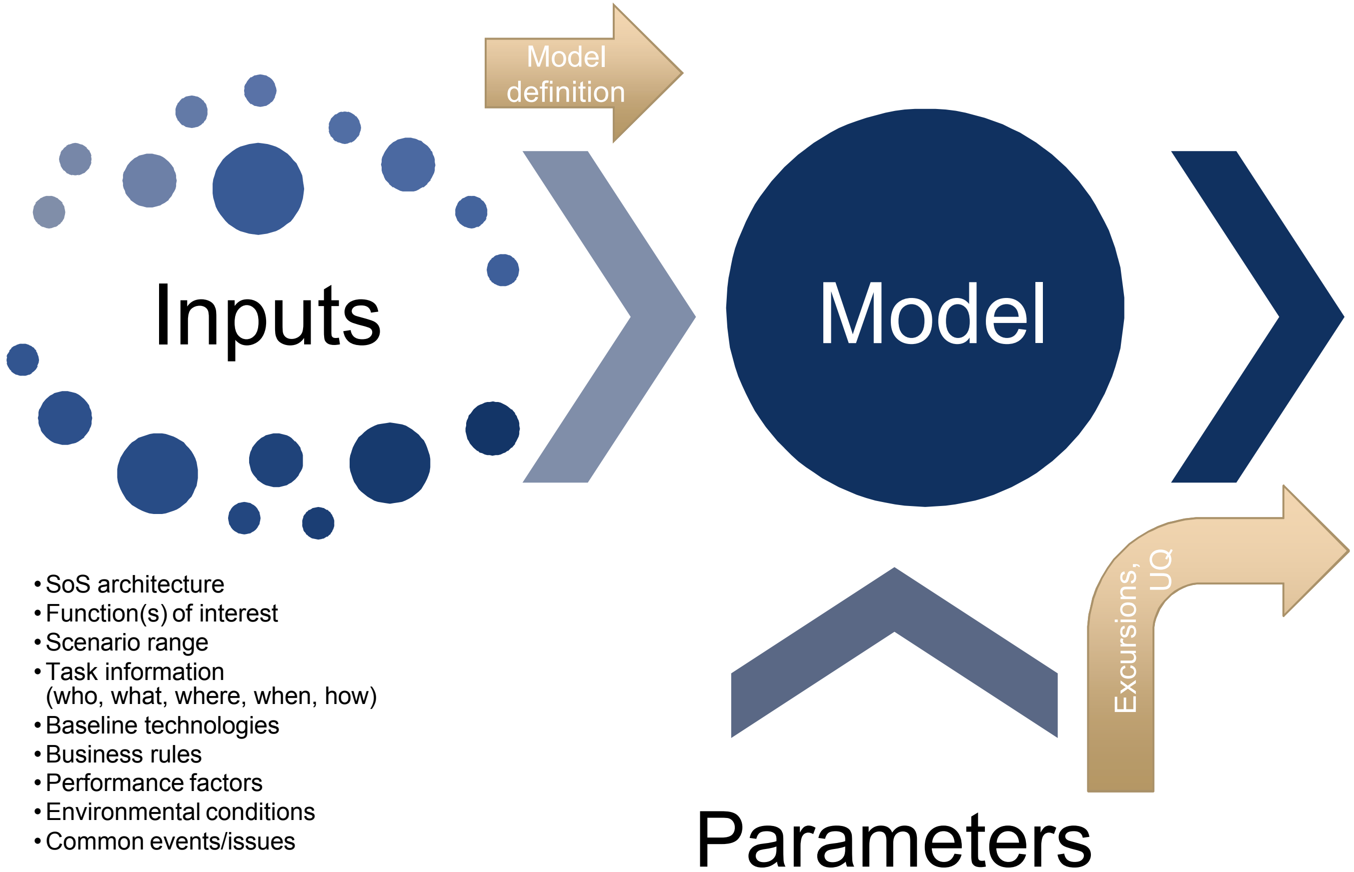
Example Study Questions

- Where are the greatest opportunities to increase human efficiency/ reduce manpower requirements? How do you do this without hurting performance/ adding major risk?
  - Improve technologies and/or interfaces
  - Augmentation or automation
  - Change processes, policies, training, structure
- Where should understanding of operators' skills, cognitive load, etc. play a greater role in the system design process?
- How does effectiveness & robustness change over time and under different conditions?
- What kinds of conditions/perturbations are likely to cause catastrophic failure?
- What are the relationships between layers of the SoS and where does currently assuming independence cause greatest problems?
- Under what conditions do humans have difficulty interacting with technology?
- Where might augmentation or automation be beneficial? Pros/cons? How does shifted human burden affect performance?
- How does use (or presence) of different technology affect human performance of tasks?
  - How does increasing technological sophistication impact human inefficiency and uncertainty? How does this impact overall SoS function?
- Example technology growth areas requiring greater understanding of Human-Technology interactions:
  - Semi/autonomous ISR and combat systems such as Unmanned Aerial Systems
  - Remote Operated Weapon System (ROWS) and automated targeting systems
  - Information and communication technologies
  - Security and Active Protection Systems

Example FOB Human/HSI concerns

- Fall asleep during task
- Failure to detect item during unaided visual search
- Equipment failure leading to loss of human effectiveness
- False alarm fatigue
- Failure to detect item via IR, cameras, etc.
- Over-reliance on technology; potential inability to adapt to equipment failure
- Equipment can degrade task performance (e.g., by reducing dexterity, endurance etc.)
- Technology interface affects cognitive load, usability etc., particularly in special situations (combat, sand storm, etc.)
- Semi-automated capabilities requiring human discretion
- CCTV and Eagle eye require human ability to discern threats, human discretion and successful communication to end point
- CROWS interfaces range from simple/intuitive to highly complex - the latter would be very difficult to use in cognitively demanding situations
- Under significant heat/humidity, weight of armor could degrade human performance
- Under cold/wet conditions, thicker gloves may be required, reducing dexterity
- EOD equipment affects dexterity
- Rifle/pistol may be more difficult to use under cold/wet conditions (thick gloves and/or stiff fingers)
- Effective use of physical barrier requires quick thinking; also freezing conditions etc. may make it more difficult to operate
- Radio failure could lead to human failure (due to loss of situational awareness)
- Under night conditions, failure of flashlight or IR goggles makes task impossible
- Under night conditions, combination of flashlight/mirror more effective (no shadows)
- Long duration, heat/cold can decrease effectiveness of both humans and dogs
- IR goggles cannot be worn for long periods of time; FLIR can be used for many hours but takes both hands and precludes weapon use
- Extreme exhaustion (to the point of hallucination)
- Undiagnosed traumatic brain injury
- Emotional trauma and PTSD

Inputs & Outputs



Inputs

- SoS architecture
- Function(s) of interest
- Scenario range
- Task information
  (who, what, where, when, how)
- Baseline technologies
- Business rules
- Performance factors
- Environmental conditions
- Common events/issues

Parameters

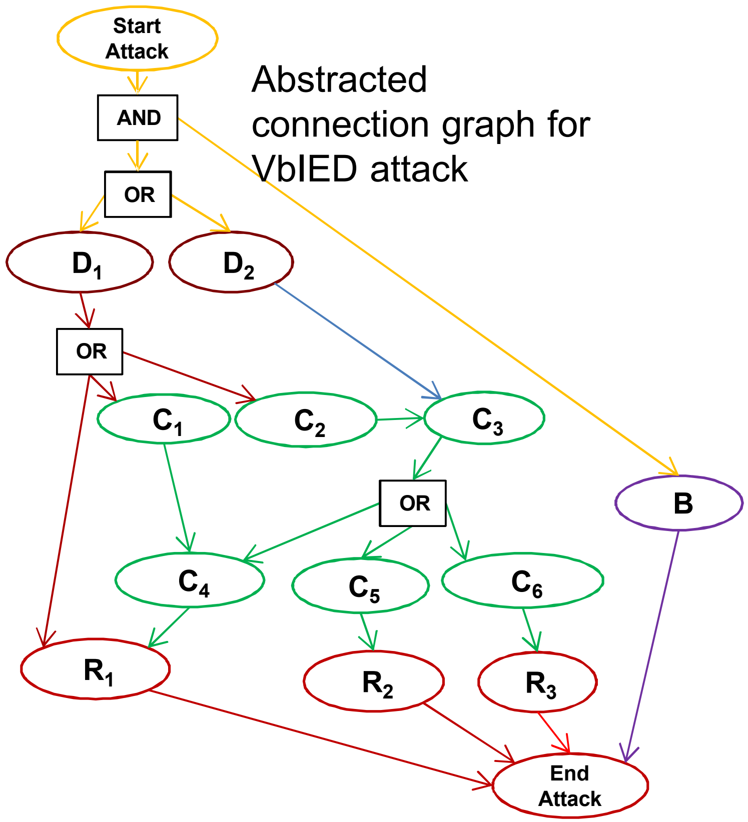
- Design factors
  (incl. technologies, SOPs)
- Uncertainties
- Long-term effects

Results

Metric distributions from Monte Carlo runs

e.g., P(defeat), P(false alarm), P(detect), delay time, response time, …

Calculating P(hit) and P(FA)



Abstracted connection graph for VbIED attack

P^{hit} can be built mechanically:

$$P^{hit} = \{\quad\} * \{P_B\}$$ [AND]

$$\min((\quad),(\quad))$$ [OR]

[OR] $$\min((\quad),(\quad))$$

$$P_{D_2} * P_{C_3} * (\quad)$$ [AND]

[AND] $$P_{C_1} * P_{C_4} * P_{R_1}$$

$$P_{C_2} * P_{C_3} * (\quad)$$ [AND]

$$\min\left(P_{C_4} * P_{R_1}, P_{C_5} * P_{R_2}, P_{C_6} * P_{R_3}\right)$$ [OR]

$$P^{hit} = \left\{\min\left(P_{D_1} * \min\left(P_{R_1}, P_{C_1} * P_{C_4} * P_{R_1}, P_{C_2} * P_{C_3} * \min\left(P_{C_4} * P_{R_1}, P_{C_5} * P_{R_2}, P_{C_6} * P_{R_3}\right)\right), P_{D_2} * P_{C_3} * \min\left(P_{C_4} * P_{R_1}, P_{C_5} * P_{R_2}, P_{C_6} * P_{R_3}\right)\right)\right\} * \{P_B\}$$

Note that a false alarm can occur anywhere in the system and propagate, therefore P^{FA} can be calculated as the ORed probabilities of the false alarms at all of the steps:

$$P^{FA} = 1 - \left(1 - P_{D_1}\right)\left(1 - P_{D_2}\right)\left(1 - P_{C_1}\right) \ldots$$