Use of Pattern Recognition in Detection of Improvised Explosive Devices

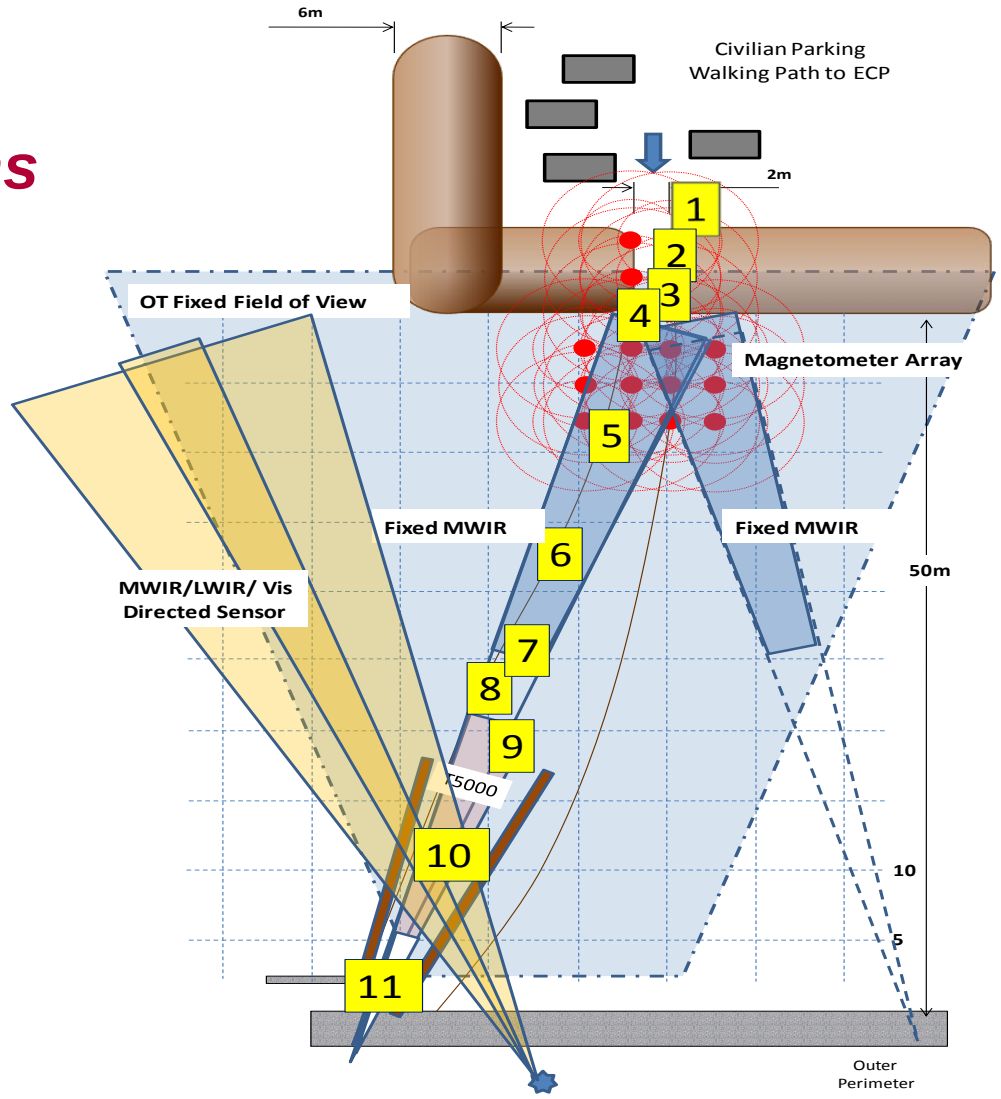
Jorge Buenfil, PhD candidate
US Army Armament Research, Development and Engineering Center (ARDEC)

20160427

Distribution A: Approved for Public Release: Distribution is unlimited.

Mobility Patterns

Mobility/movement patterns and their implication in the CIED problem.



Distribution A: Approved for Public Release: Distribution is unlimited.

Mobility

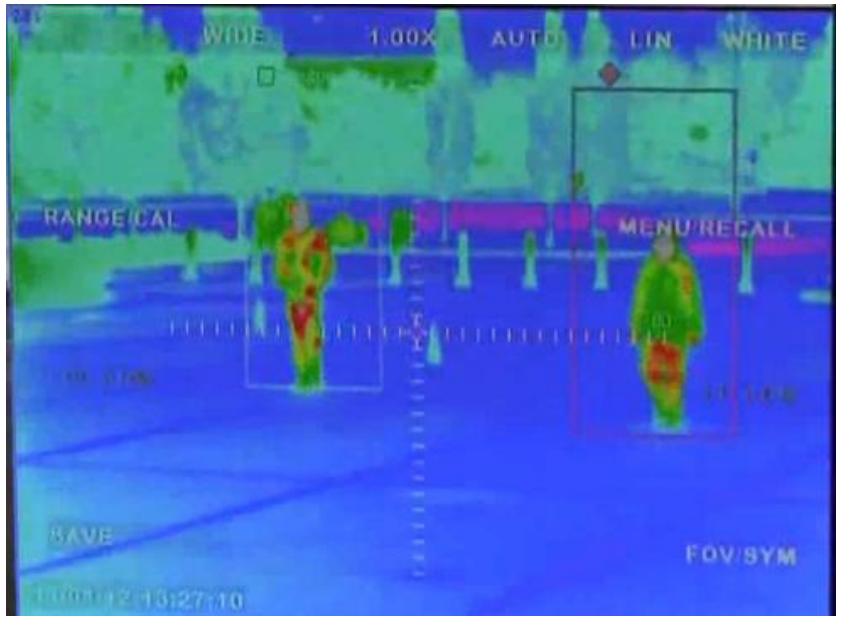
- Let an AUS be a particular area under surveillance that contains no Improvised Explosive Devices (IEDs) at time zero (t_0) and which might be penetrated by an agent carrying an IED at time k (t_k). Then $E = AUS_{t_0} \rightarrow AUS_{t_k}$ is an event of the form $e \in \{null, IED\}$ which results in either no IED introduced in the AUS or an IED introduced in the AUS. The event e consists of a potential carrier (human, animal or machine) crossing the threshold of the AUS with or without an IED.
- Therefore, mobility patterns are of great importance for detection of IEDs.
- Regarding the aspect of mobility randomness, in the CIED domain mobility randomness is not desirable. Mechanisms and policies are usually set in place to prevent random mobility by groups or individuals to control their flow.

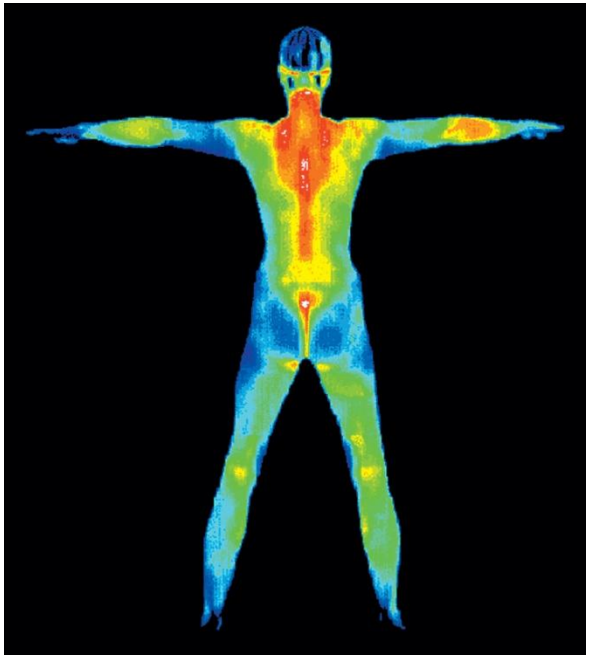
Mobility Patterns Considered

- Individual:
  1. Follow pathway (expected)
  2. Loiter
  3. Turn around
  4. Run[1]
- Group:
  1. Clustering
  2. Occlusions

1. Zeng, W., C. Wang, and F. Yang, *Silhouette-based gait recognition via deterministic learning.* Pattern Recognition, 2014. **47**(11): p. 3568-3584.

Methods of pattern recognition and their strengths, weaknesses, and constraints with respect to anomaly detection.





Distribution A: Approved for Public Release: Distribution is unlimited.

Anomaly vs. Pattern Recognition

–Anomaly Detection:

- Statistical deviation from a norm
- Looks for evidence of interruptions in energy flows
- Computationally simple *[2]*
- Usually direct observation

–Pattern Recognition:

- Hypothesizes the class of objects perceived by the sensors by matching to learned models *[3]*
- Feature vectors
- Good for indirect observation

2. Yinon, J., Counterterrorist detection techniques of explosives. 2007, Oxford: Elsevier.

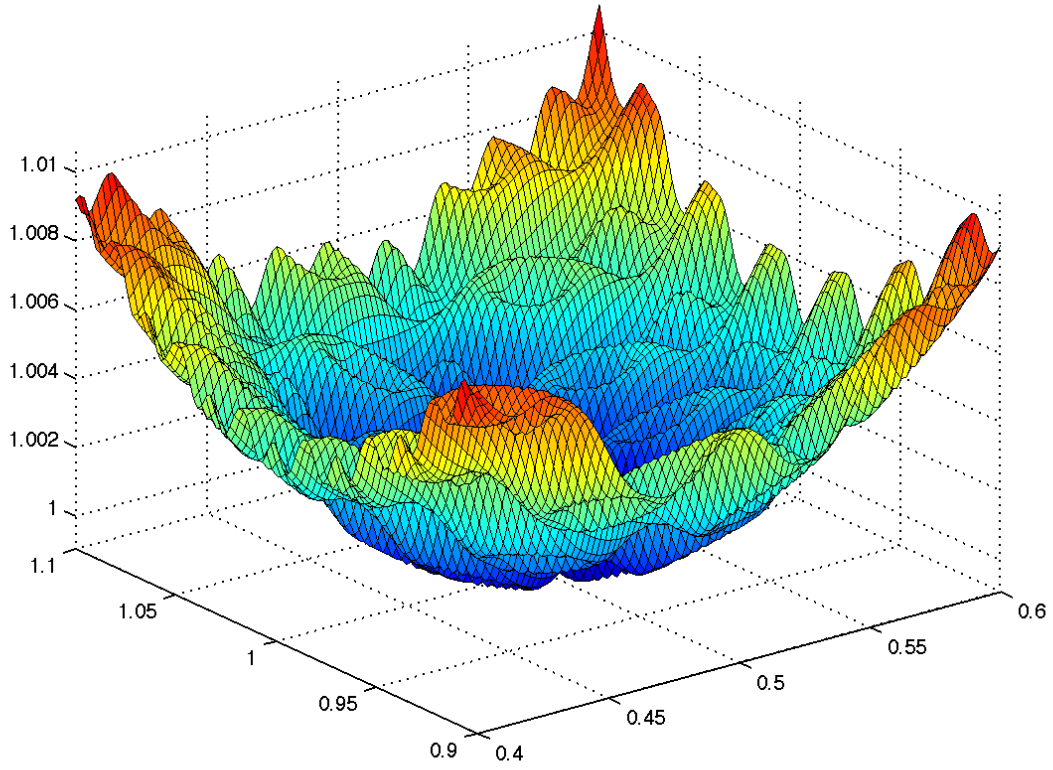
3. Duda, R.O., P.E. Hart, and D.G. Stork, Pattern Classification. 2, revised ed. 2004: Wiley.

Pattern Recognition Methods

1. Statistical
   - Easy to compute
   - Well developed method
2. Syntactic
   - Easy to understand
   - Compact rules
3. Analysis by Synthesis
   - Exploit knowledge of the solution domain *[4] [5]*
4. Artificial Neural Networks
   - Formal Analysis
   - Availability of libraries *[6]*
   - Non-linear functions *[7]*
5. Perceptron
   - Ideal for DSPs
   - Multiple layers *[8] [9]*

4. Stevens, K.N., *"Segments features and analysis-by-synthesis", in Language By Ear And By Eye*. 1972.
5. Mannell, R. *Speech Perception. Background and Some Classic Theories*. 2015.
6. Hochreiter, S. and K. Obermayer. *Optimal gradient-based learning using importance weights*. in *Neural Networks, 2005. IJCNN '05. Proceedings. 2005 IEEE International Joint Conference on*. 2005. IEEE.
7. Kriesel, D. *A Brief Introduction to Neural Networks*. 2007.
8. Gallant, S.I., *Perceptron-Based Learning Algorithms.* Neural Networks, IEEE Transactions on, 1990. **1**(2): p. 179-191.
9. Minsky, M. and S. Papert, *Perceptrons: An Introduction to Computational Geometry*. 1969: MIT Press.

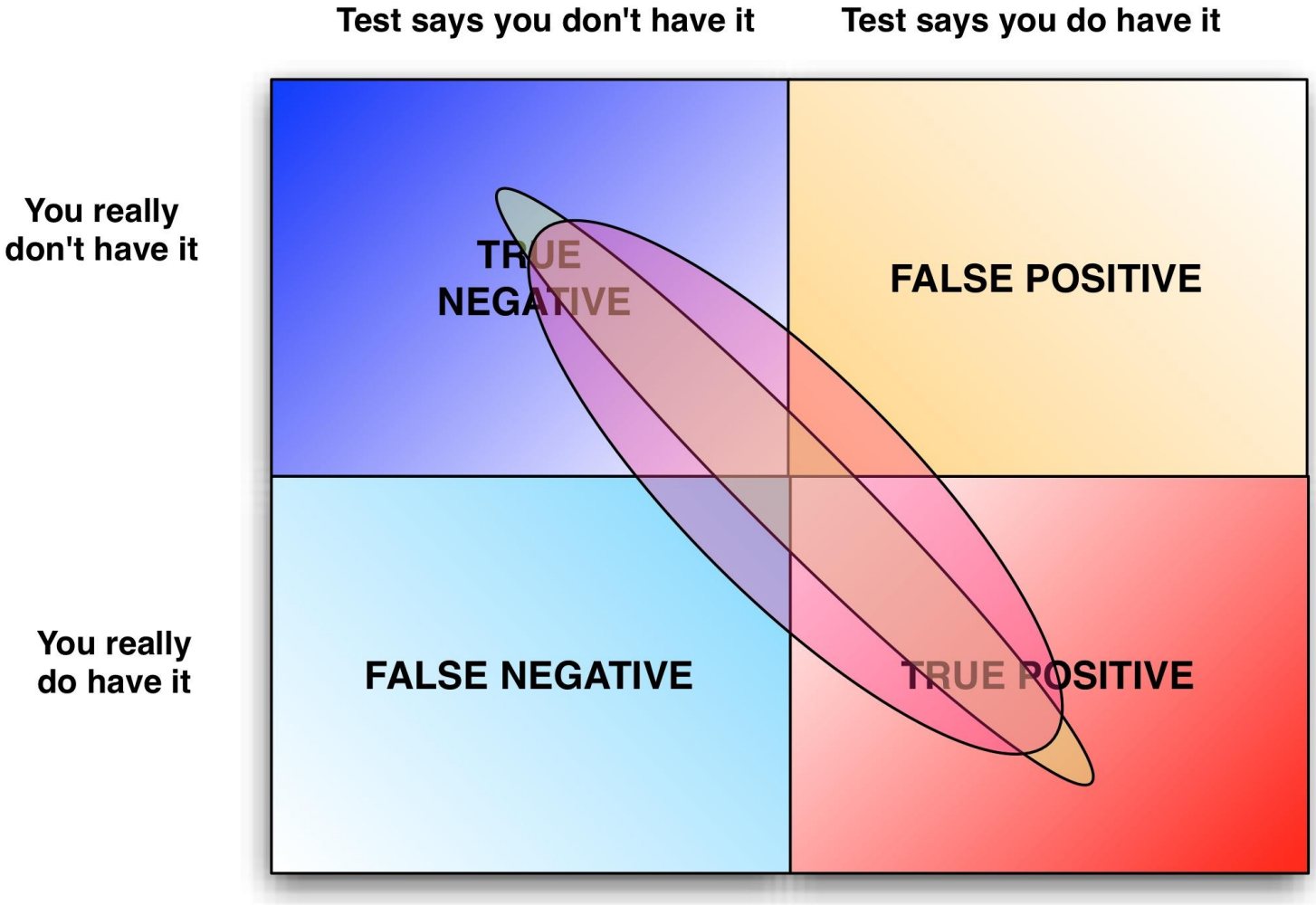
Parameters to judge the "goodness" of the system



System Parameters

1. Adaptability
2. Manpower Reduction
3. Cost Reduction
4. Design for Robustness
5. Open architecture

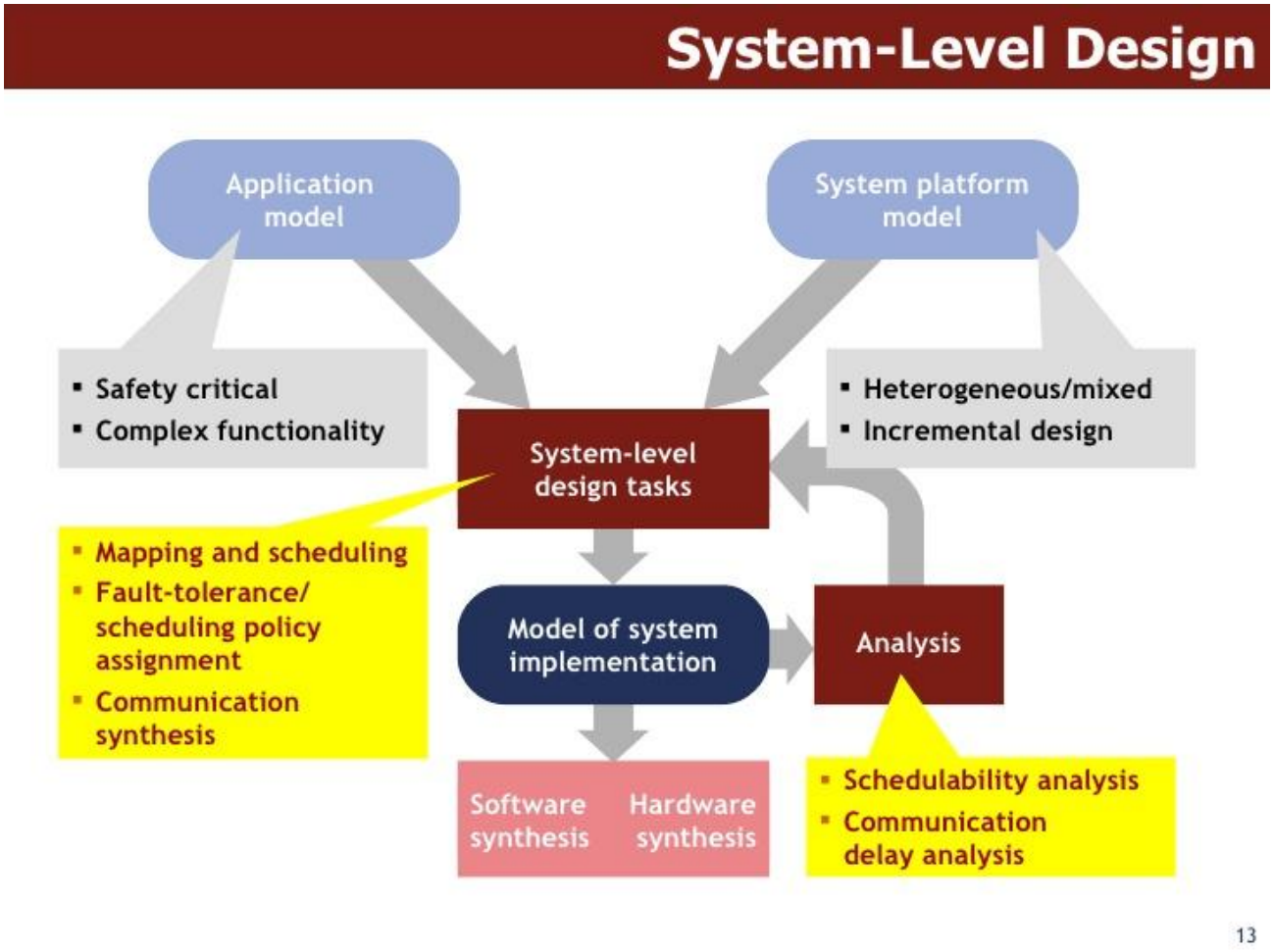
Beyond quality and false negatives



Beyond Quality and False Negatives

- **Quality** and **low rate of false negatives** are variables of the system in operation, as opposed to the parameters of the system at architecture and design time.
- **High reliability** measured in terms of mean time between failures (*MBTF*) and mean time to repair (*MTTR*).
- **Plays well with others**: lack of interference with normal operations of this includes physical obstruction of normal operations of other systems (physical and electronic.)

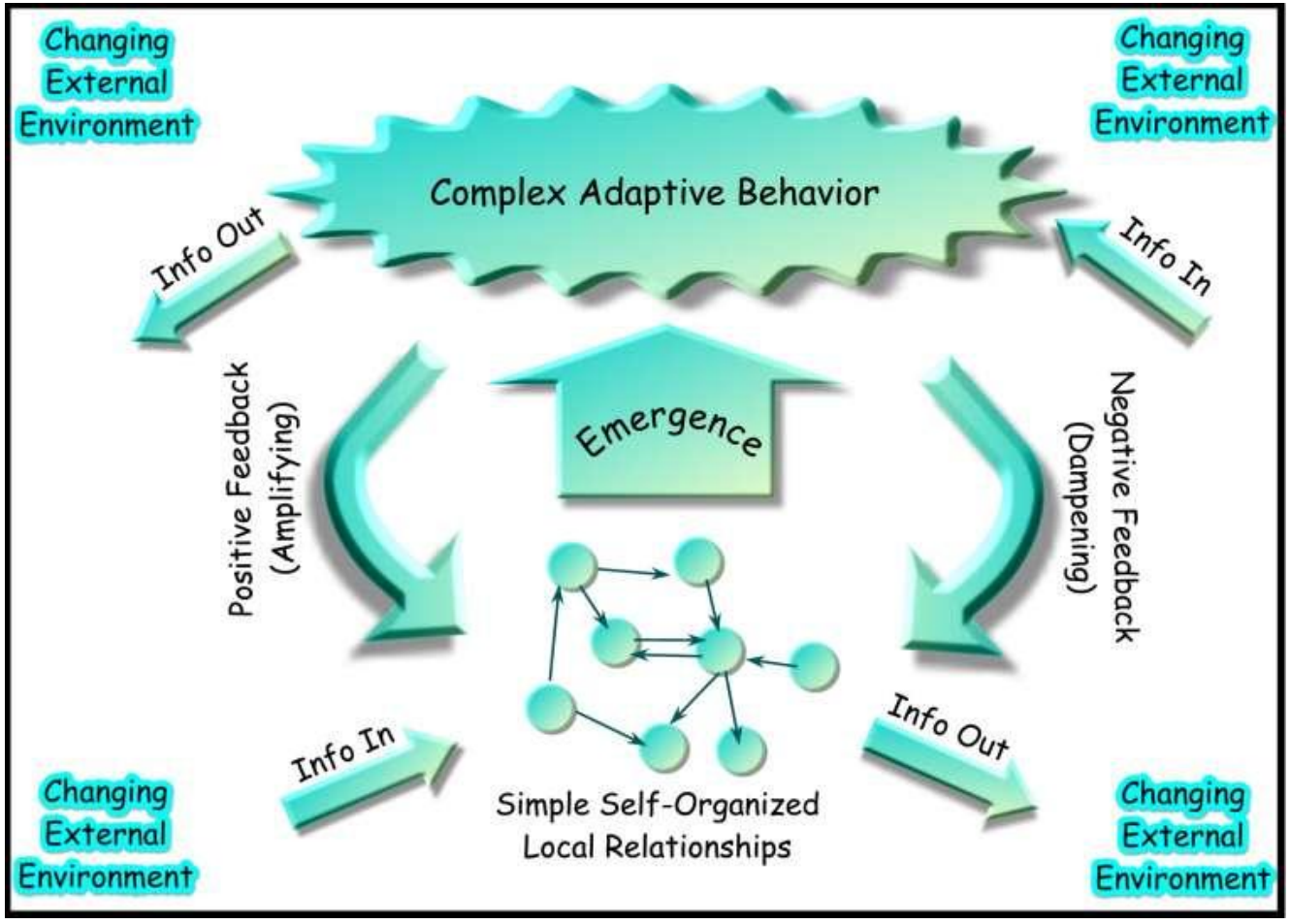
System Optimization



Architectural Pillars

1. Modularity
2. Scalability
3. Simplicity
4. Openness
5. Common Standards

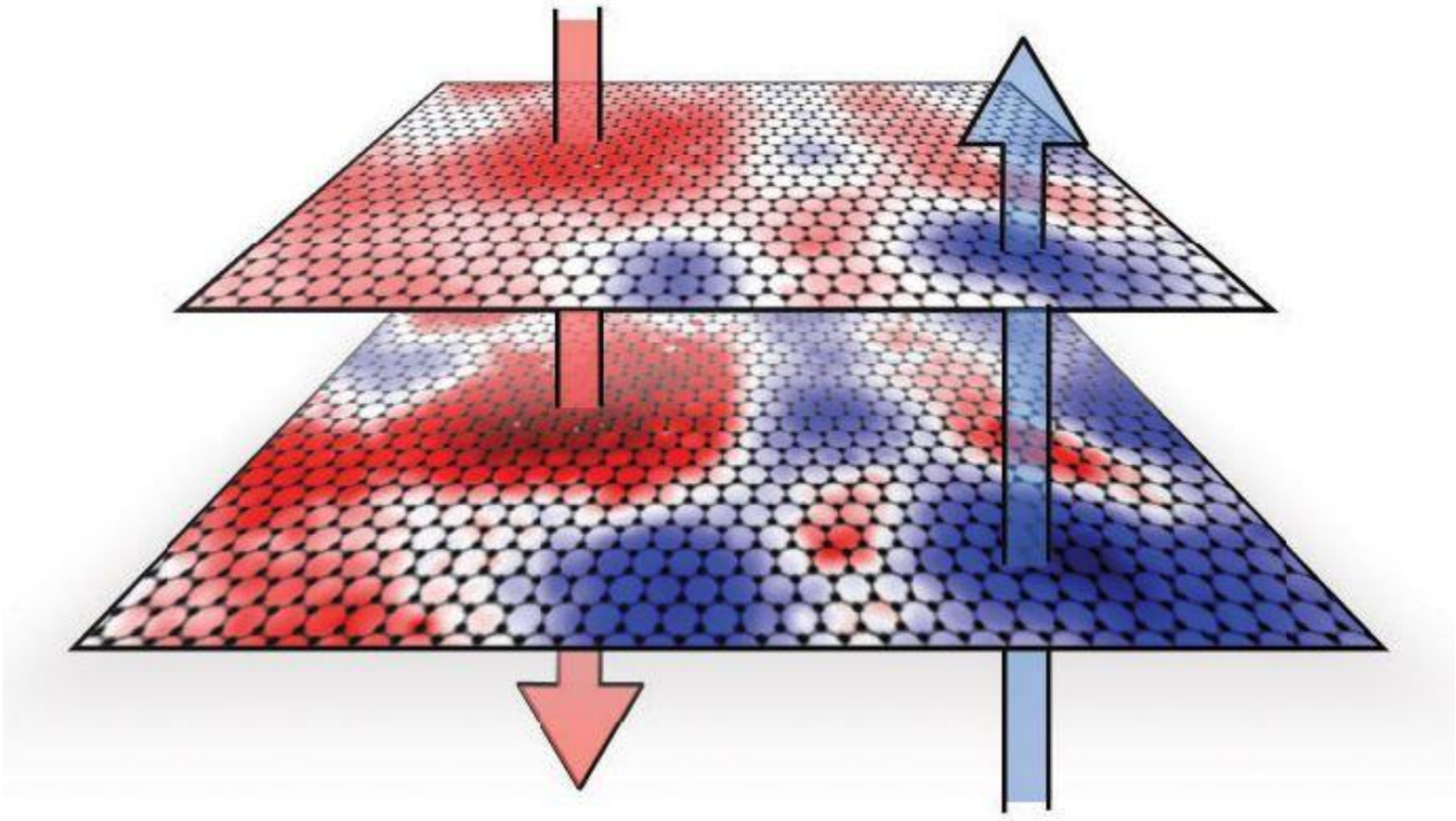
Capabilities and limitations of the techniques discussed



System Capabilities and Limitations

1. Adaptability
2. Manpower reduction
3. Cost Reduction
4. Design for Robustness
5. Open architecture

Layering the techniques to address the utility function



Layering of Techniques

The system architecture combines all those techniques into a coherent framework that meets the conditions necessary to support the utility function.

Using an open architecture, based on widely accepted standards, I propose to have a 3-layer approach.

1. **Framework**: The first layer is the basic framework architecture where elements that compute the results (threat assessment values for individuals, groups and the whole AoI) are identified and encapsulated; I call this part the Inference Engine (IE).
2. **Logical Architecture**: The second layer of the architecture is the logical model of the system. Logical because it exists in the realm of ideas and math, not in the physical sense of an actual system.
3. **Physical Architecture:** The third layer of the architecture is a physical instantiation of the second layer. At this level system functionality is allocated to software, hardware or a mix of them.

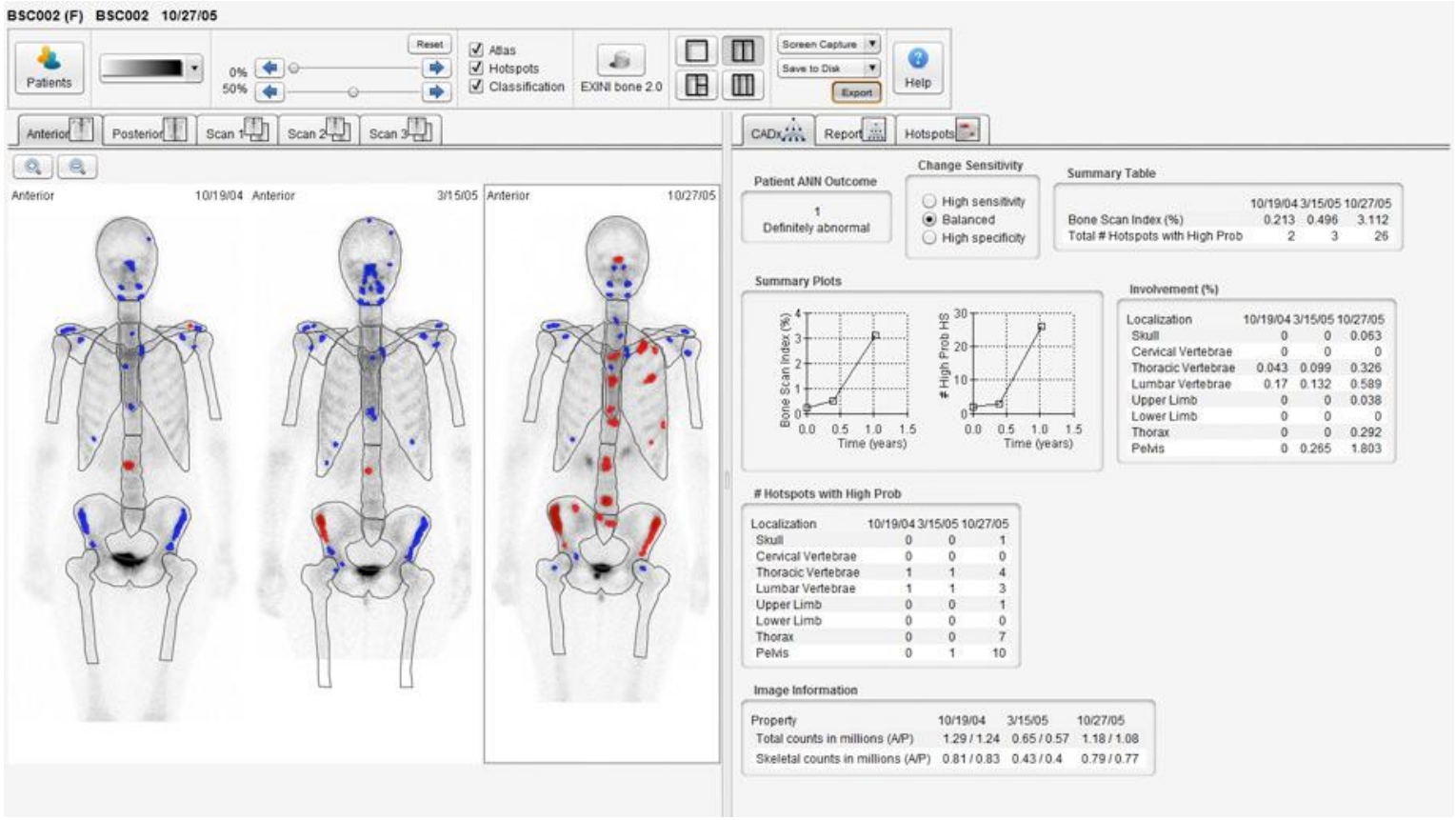
Gaming the system.

Distribution A: Approved for Public Release: Distribution is unlimited.

Anti-spoofing

- Attackers would not be able to use the adaptability of the system to their advantage is because the system is not fully automatic.
- the human-in-the-loop as a sensor is responsible for inspecting the AoI.
- The human operator in conjunction with security personnel on the ground coordinate random checks and questioning people and pat downs.
- the system dynamics portion of the Threat Assessment function would gradually elevate the sensitivity of the whole system by noticing via feedback loops an increase in suspicious readings, even when those readings do not cross the threshold of a system alert

Measuring approach for quantifying the detection process.



System Metrics

- Let A_x be a discrete assessment of threat made by an individual sensor x in the range *[0.0, 1.0]*.
- Let W_x be a weight assigned to sensor x in the range *[0.0, 1.0]*.
- Each individual sensor reading is weighted by a factor that represents the relative confidence assigned to that individual sensor regarding its potential determination that an IED is present in the AoI.
- Let TA_x denote the weighted Threat Assessment of sensor x on a person p
- Then for each person in the AoI their Threat Assessment Level TAL_p which includes adjustment factors given by pattern analysis if applicable is given by:

$$TAL_p = Max(TAx_1, \dots, TAx_n)$$

- The DFV at $time_k$ is the highest Threat Assessment Level (TAL) of the AoI.

$$DFV = Max(TAL_{p_1}, \dots, TAL_{p_n})$$

- The DFV must satisfy the following two conditions:

$$DFV \geq 0 \text{ and } DFV \leq 1$$

- The area-wide detection is quantified by a value, called Threat Assessment Value (TAV) which represents the probability of the presence of an IED in the Area of Interest (AoI).
- A value of 0.0 would represent absolute confidence that there is no IED in the AoI at the moment of the estimation. A value of 1.0 would represent absolute certainty that there is at least an IED in the AoI. The values in between correspond to different estimated probabilities that an IED is present given the detection of indicators of threat without being able to ascertain absolute certainty one way or another.

System Metrics 2

- The DFV is modified by a feedback loop from a system dynamics engine that provides temporary effects on the current estimation based on prior estimations according to Bayes Rule. For example, If DFV at $time_{k-1}$ was elevated beyond a set threshold that indicates what is the statistical DFV given current conditions of number of people in the AoI, time of day, weather conditions, Day of the week, etc. A positive factor is applied to the DFV at $time_k$ to elevate the threat level accordingly. This is done because of the assumption that higher than usual DFVs, but still below the alert-level, could mean that multiple individuals with moderately elevated threat levels may collaborate and assemble an IED from parts each one carried into the AoI. The system dynamics model applies a decay rate to this factor of accumulated threat indication, in order to dissipate the extra indication of risk of threat and avoid a self-reinforcing loop that would produces a false alarm otherwise.
- Finally, the TAV is the result of multiplying the DFV for the AoI by the systems dynamics model weight factor at time t_k.
- **Precision**
  - Relevant IED Detection (tp/(tp + fp))
- **Recall**
  - Fraction of IEDs found (tp/(tp + fn))
- Naïve Bayes Classifier

What exactly is the detection system measuring?

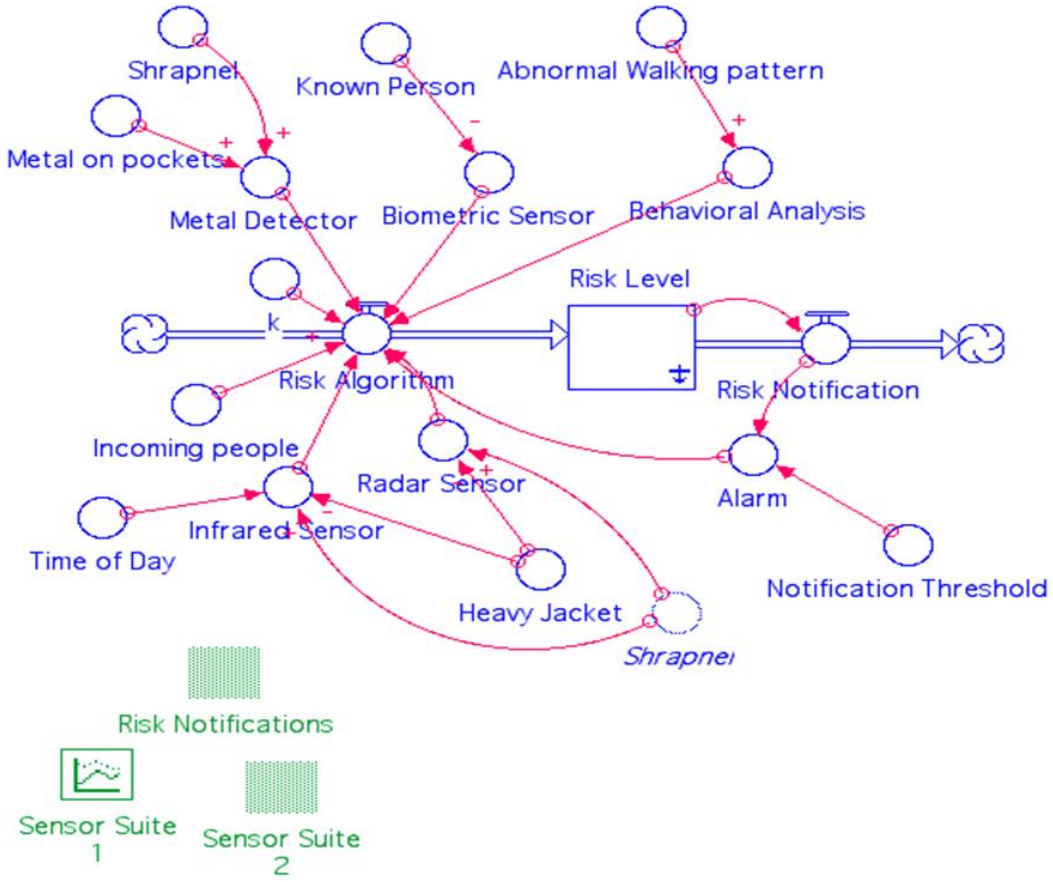
What the System Measures

- The system measures abnormal conditions with regards to normal scans of the human body under magnetic, infrared, microwave sensors, as well as behavioral deviations from the normal gait and biometric information.
- The detection system attempts to indirectly detect improvised explosive devices by applying pattern matching methods on the potential carriers of the IEDs.

Relationship of outcome metric with the ones collected from different internal approaches such as pattern identification, image processing, non visual inputs, etc.

Data Fusion

- Naïve Bayesian Classifier in conjunction with a dynamic system with reinforcing feedback loops.



Superiority of the multi-entry approach.

Multi-tiered/multi-entry approach

- To show true superiority of the multi-tiered/multi-entry approach the proposed system needs to demonstrate improvements over an existing non-tiered solution
- Not only in terms of quality of predictions of IED presence and low false negatives, but also in terms of Adaptability, Manpower reduction, Cost reduction, Design for Robustness, and Openness of the architecture
- The best approach is to use past data of another system the US Army has in place or has investigated with intent of development. This I would consider the ultimate test.

Validation plan

Validation Plan

The validation plan for this system is also a multi-tiered approach:

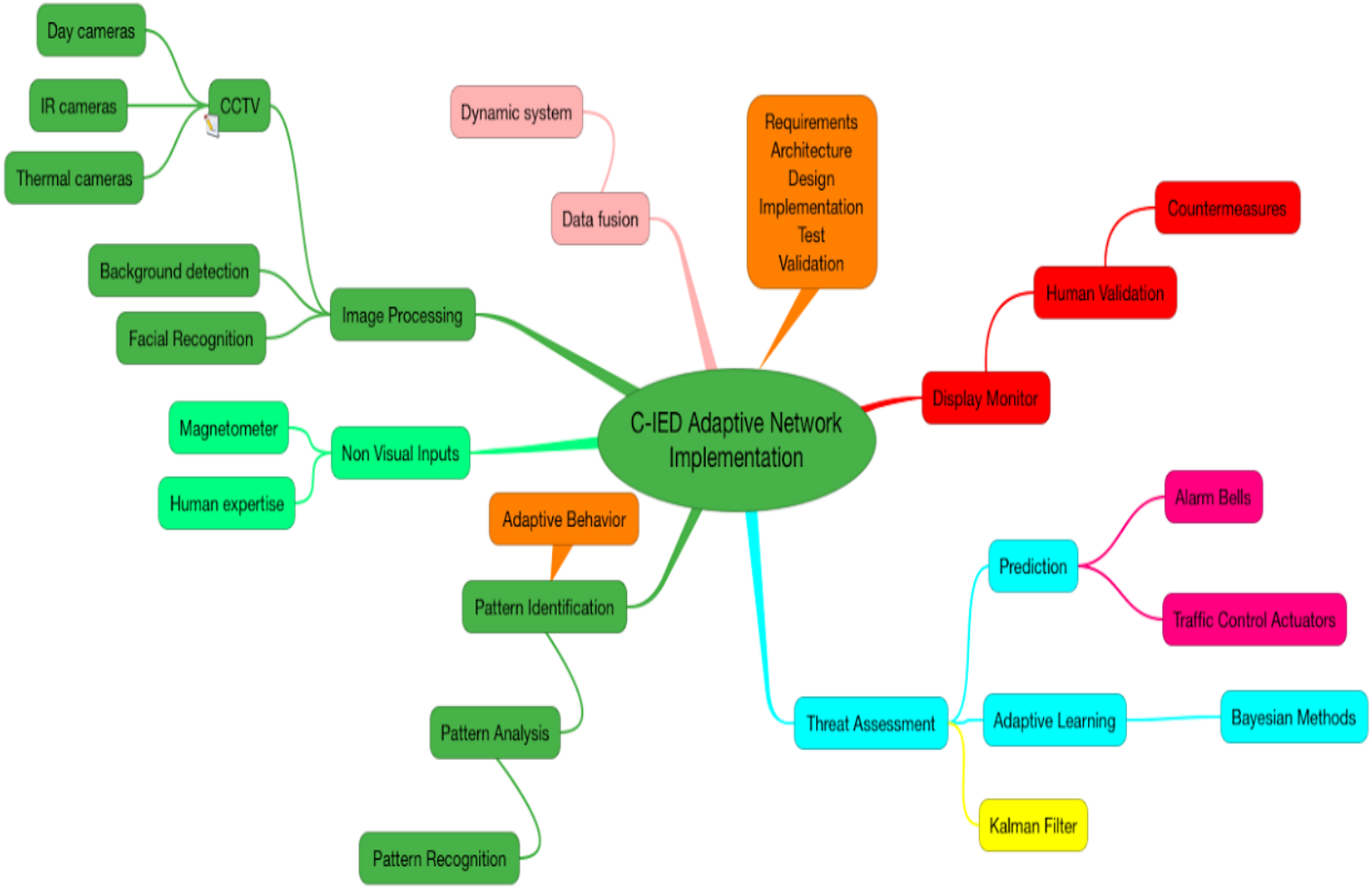
- The first level of validation is to validate the logic of the CIED system. For this I plan to analyze the algorithms and formulas mathematically.
- The second level of validation is to run the CIED application as a computer simulation, where instead of having actual sensors providing the data I will use Montecarlo techniques on probability density functions that approximate the sensing capabilities of the actual sensors planned to be used for the prototype system.
- The third level of validation is experimental. An actual prototype system is planned to include some of the most important sensor types. The software will run on Raspberry Pi microcomputers for signal preprocessing and the data fusion and inference engine will be hosted on a suitable computer that will act as the C2 system. The plan is to have a scaled down version of the actual system being proposed as proof of concept.

Validation Plan 2

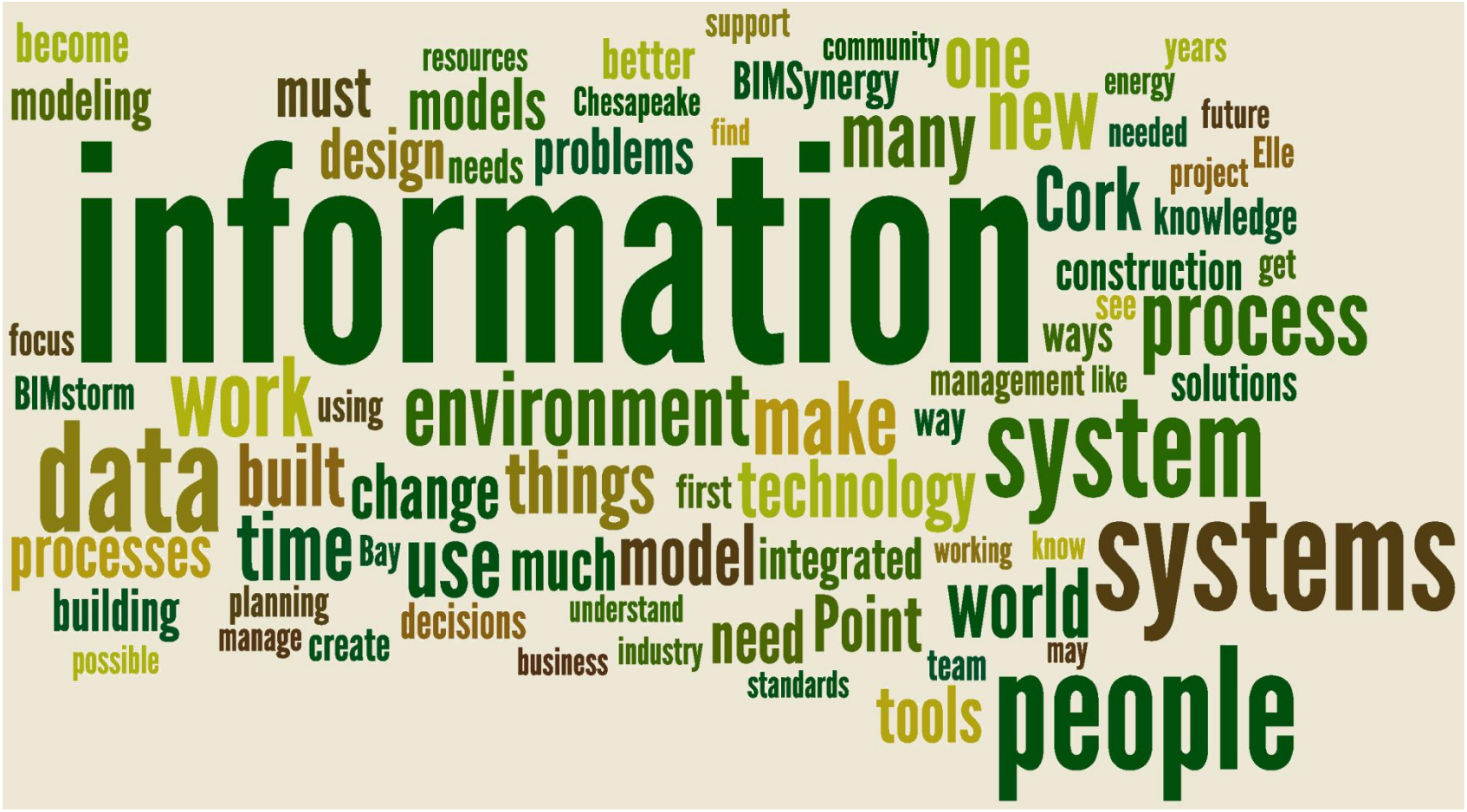
- With regard to the availability of real data, yes it is correct that the data is classified.
- I have access to the data to use for comparisons.
- One possibility to handle the aspect of availability of the data to my academic committee is to "sanitize" the actual data
- Alternatively, some members of my committee have the appropriate security clearance to look at the real data without any modifications and verify my findings.

BACKUP MATERIALS

System Design



Example table for each of the methods.



Summary of Techniques

	Adaptability	Manpower Reduction	Cost Reduction	Robustness	Openness
Day Cameras	The cameras by themselves do not possess adaptability, they always work the same.	Human operators use the day cameras to observe suspicious behavior hightlighted by the system and to direct countermeasures where appropriate. The system uses these cameras to fuse the normal view with additional information on to the operator screen.	Day cameras for CCTV are abundant in offerings and vary in cost from $18 for a camera module for a Raspberry Pi,	The system requires multiple day cameras in order to cover the whole AoI. Should any or all Day Cameras become unavailable, the system would continue working but in degraded mode, informing the human operator of this condition.	The system architecture allows for use of practically any COTS or GOTS camera by providing a standard interface plus the ability to create customized interfaces using a framework.
IR Cameras	The cameras by themselves do not possess adaptability, they always work the same.	IR Cameras are used for low light and to see through haze and fog. The images are blended with visible light to enhance the content of images for human operators to more rapidly.	Anywhere from $25 for a basic camera for the Raspberry Pi computer to high-end $40K long range imaging cameras.	The system requires multiple IR cameras in order to cover the whole AoI. Should any or all IR Cameras become unavailable, the system would continue working but in degraded mode, informing the human operator of this condition.	The system architecture allows for use of practically any COTS or GOTS camera by providing a standard interface plus the ability to create customized interfaces using a framework.
Thermal sensors	The sensors by themselves do not possess adaptability, they always work the same.	Thermal sensors provide a way to indirectly detect explosive devices borne on a person's body by observing the heat emissions captured by the thermal sensors.	About $100 for a basic model to around $40K for military-grade equipment.	The system requires at least a couple of Thermal sensors. Similarly to the Day and IR cameras, should one or all Thermal sensors fail the system will continue operations in degraded mode and will notify the human operator.	The system architecture allows for use of practically any COTS or GOTS thermal sensor by providing a standard interface plus the ability to create customized interfaces using a framework.
Background Extraction	Background Extraction is inherently adaptable because the algorithms do not use a static image of the area to use as background. Instead they do some image processing to determine which aspects of the scene are immutable and subtracts them from the scene to proceed to hightlight contours of the foreground objects (people).	The impact on manpower is that the human operators can focus on the actual agents that move through the AoI, which will be highlighted with an edge contour in color, thus reducing the amount of effort and time needed to comprehend what is happening. Also, by observing any modifications to the background, it is possible to detect objects left behind, or buried, which could be IEDs.	There are software routines running on the images from day cameras. Free open source libraries available. Another optionis to use Digital Signal Processors (DSP) optimized for this function, such as the Texas Instruments TMS320C64/64x+, which costs less than $40.	If the system loses its background extraction capabilities, the human operator would be notified and the system will continue operations in degraded mode, where automatic detection of packages left behind will not be available, but the human operator will be asked to take over that function.	This is an area where the system is open in software. The background extraction algorithms are a service provided to the core software of the system control module and it would require the integration of a new background extraction service as a publisher (in the Publisher/ Subscriber design pattern). As long as the new module abides by the standards the system uses and the protocols to use the service, no disruption should occur to the rest of the SoS.
Facial Recognition	Facial Recogntion, even though it can adjust for angles, lighting of the picture and some other minor changes, is not usually considered an adaptable system because it only recognizes faces that are already contained in database. It cannot recognize somebody new basing the recognition on fragmentary features from other people, for example.	The ability to identify people using facial recognition and match them against a black list is a significant reduction in manpower need since a person who is included in the black list will be highlighted and detained. On the other hand, if using a white list, if a person is found there, their risk assessment will be able to be lowered so that system resources focus on other people who are not known.	There are software routines available as open source libraries to process visual images such as Open Source Computer Vision Library (OpenCV), and the DLib C++ Library.	Just like with Background Extraction, the system will go into degraded mode of operation if the Facial Recognition module fails.	Similarly to the way the Background Extraction service works, the Facial Recognition is a service provide by a specialized substystem (hardware, software or hybrid) that could be easily replaced by adding a new service provider who will publish the service and abide by the designated protocols for invocation and transmission of the results.
Gait Analysis	Just like Facial Recognition, Gait Analysis is not considered adaptable since it only recognizes a limited number of patterns and the number does not automatically increase by learning.	Automatic identification of suspicious gait patterns will free the human operator from this aspect of surveillance since the system will automatically flag persons walking as if carrying more weight than their proportions would indicate or male gaits for female dressed people.	Algorithms available from Wei Zeng (see reference section). There are also companies, such as GSI (http://globalseci.com/?page_id=44) that offer technologies for gait recognition.	Same as with Background Extraction and Facial Recognition, the system will continue working, but in degraded mode, if the Gait Analysis fails to work at some point.	Another example of a service provide to the SoS that can be replaced as indicated in the case of Facial Recognition and Background extraction.
Magnetometers	The magnetometers are probably the least adaptable part of the system since this device does one and only one thing, detect metal in a specified amount or larger.	Magnetometers are usually the first line of defense in an AoI. If triggered, that's an immediate alert, if not an alarm, and the system will immediately highlight the person who triggered the sensors and request human assistance.	Simple hand held models start at $160.00 and sophisticated units can cost up to $4.5K	Like other sensors such as cameras, the magnetometers can fail and yet the system will continue operations in degraded mode with enhanced human participation to compensate for the loss of the sensor.	The system architecture allows for use of practically any COTS or GOTS magnetometer by providing a standard interface plus the ability to create customized interfaces using a framework.
Human Expertise	Definitely the most adaptable part of the system. Humans are capable of modifying their behavior according to circumtances even in the presence of new stimuli never seen before.	Human expertise cannot be replaced completely for several reasons, the main one being that for military applications it is illegal to have machines automatically take actions that may result in death or severe injuries to people. So, this is one aspect that results in a direct increase in manpower needs.	Human expert labor is generally expensive (around $120/hr for government civilians), however for US Army personnel, cost is not really the problem but availability of personnel. Not having the personnel to run a system is perhaps the most costly part.	This is probably the worst case scenario. If the human expertise becomes unavailable, they system will continue operations in a severely degraded mode, since it would only be able to react to automatic alarm events which cause the system to stop traffic and manipulate actuators to control flow. The assumption of the operation of they system is that even if all human operators were unavailable, the system wil be able to escalate the notification of severe degradation up the chain of command until somebody acknowledges and restores human expertise for the system.	The CIED SoS sees the human as a sensor. The human operator can also be replaced as long as the new operator is familiar with the ways of interacting with the system (protocols) and meets the criteria for skills in the operation of the system, which is provided by training.
Pattern Recognition	There is some degree of adaptability in Pattern Recogniton modules based on statistical methods, which take into consideratin previous evidence to compute a current prediction of which pattern is a best match for the new features discovered.	Automatic pattern recognition saves manpower needs by preprocessing the vast majority of the traffic in the AoI, which overwhelmingly is not a threat, thus saving human operators a lot of work. There is one aspect that results in demands for manpower: that is the training of the system to assist with its learning for adaptability to potential new threats.	Pattern recognition techniques and algorithms are freely available to use. The cost is really the cost of developing the software that is tailored for the applications needed by the CIED system.	Should the system lose the ability to perform pattern recognition it would be severely degraded but will continue to provide assistance to the human operator by presenting visual data in a way that facilitates the comprehension of the operator regarding the situation in the AoI. Simple sensors such as magnetometers could still detect unusual amounts of metal, and the human operator would still be able to observe the thermal signatures of people on his/her monitor to make judgements about the presence of an IED threat.	Another example of a service provide to the SoS that can be replaced as indicated in the case of Facial Recognition and Background extraction.
Adaptive Learning	Adaptive learning is the mechanism by which the system gains its adaptability characteristics, other than using Human Expertise.	This support function of the system lowers the demands on manpower by keeping a high level of skill at finding IEDs, even when the IEDs change over time and the techniques to conceal them.	Adaptive learning techniques and algorithms are freely available to use. The cost is really the cost of developing the software that is tailored for the applications needed by the CIED system.	If the system loses the ability of performing adaptive learning functions temporarily, there would be practically no ill effects in the operation of the system. If the loss of the adaptive learning capability takes several weeks or is permanent, then the system will continue to operate the same as the last time it was trained and reinforced in the detection of IEDs, but it will not be able to continue to flag new potential threats, nor refine its behavior.	Adaptive learning is the hardest subsystem in terms of openness. The reason for this is that its methodologies and behaviors are built into the core of the main system controller module. Replacing it would entail modifying the main system controller, and swapping or enhancing the code already there. This by no means impossible, but it requires deep knowledge of the CIED SoS architecture, design, coding standards and dependencies of associated software elements.

Kalman Filter

- The final threat assessment is computed by applying a customized *Kalman filter* which estimates the *a posteriori* threat assessment as a linear combination of an *a priori* threat assessment and a weighted difference between a current threat assessment value and a threat assessment prediction on the next threat assessment value.

$$\hat{x}_k = \hat{x}_k^- + K(z_k - H\hat{x}_k^-)$$

- $\hat{x}_k$ is the *a posteriori* threat assessment.
- $\hat{x}_k^-$ is the *a priori* threat assessment.
- $(z_k - H\hat{x}_k^-)$ is the residual, the discrepancy between the predicted threat value $H\hat{x}_k^-$
- and the current threat value z_k
- K is an *n* x *m* matrix that represents the gain or blending factor that minimizes the *a posteriori* error covariance.