Visualization Design for Immediate High-Level Situational Assessment

Robert F. Erbacher
Computational and Information Sciences Directorate,
U.S. Army Research Laboratory, Adelphi, MD, USA
Robert.F.Erbacher.civ@mail.mil

ABSTRACT
We present the design of a visualization technique based on the results of a human in the loop process, which relied on network managers and network analysts. This visualization design was directly targeted at supporting tasks identified by the domain experts. This was the need for the ability to provide rapid and immediate assessment of the state of the network and associated hosts. This visualization technique, the Cyber Command Gauge Cluster (CCGC), allows analysts to review the state of the network and locate potentially problematic anomalies, drill down into those anomalies, and prioritize the anomalies for detailed analysis and remediation. By providing a summary representation combined with independent representations of critical parameters, the technique is unique in its ability to aid decision makers in making rapid assessments and prioritization of identified anomalies. While the prototype focuses on network analysis, the technique is devised to provide generalized support for situational awareness in any domain. The generalized parameter mapping allows the technique to be applicable to any level of decision making, from the front-line network analyst to the CIO.

Categories and Subject Descriptors

General Terms

Keywords
Situational Awareness, Decision Makers, Cyber Security.

1. INTRODUCTION
The network managers’ goal, as a main line decision maker, is to prioritize network events and anomalies based on their likelihood of maliciousness and their potential ramifications. To handle the ever-increasing numbers of attacks, network analysts and managers have processes and analysis stratagems for dealing with typical cyber anomalies. Their first level of analysis is at a highly abstract, situational awareness level, derived from our recent cognitive task analysis with network managers and network analysts [8][9]. In essence, the network analysts and network managers identified the need for visualization techniques that allow a manager to immediately identify the state of the network.

For situational awareness, we used Endsley’s model [5]. This model intrinsically consists of three levels: perception, comprehension and projection. Perception is providing a representation of the current state of a situation. Comprehension relates to a higher-level understanding of all available data. Comprehension requires a far greater level of correlation and data integration than is incorporated into the perception level. Finally, the projection level looks at projecting the event into the future to determine its impact and progression. The goal with situational awareness is to rapidly answer:
- What is happening?
- Why is it happening?
- What will happen next?
- What can I do about it?

The goal of this research is to improve the decision making process such that better actions are taken. D’Amico et al. [3] identify the need to develop different visualization techniques designed for the desired level of situational awareness. Jajodia et al. [13] lay out the research issues and challenges specifically in applying situational awareness to cyber security. These two works exemplify much of our research process resulting in a technique that will allow analysts to make better decisions and better prioritizations than is currently being done.

With the goal of improving the decision making process in mind, we document a high-level situational awareness visualization technique designed for decision makers, detail how the design and
implementation came about, provide a case study on the applicability of the technique, and summarize the feedback from actual network analysts and managers from Pacific Northwest National Laboratory (PNNL).

2. PREVIOUS WORK
There are currently too many visualization techniques designed for cyber security to enumerate here. The VizSec [21] workshop alone has been geared towards publishing a dozen such techniques a year. These techniques cover the gamut of approaches, techniques, and goals. The typical goals of visualization for cyber security will focus on data analysis, event identification, event analysis, and situational awareness. These techniques can be designed for either the network analyst at a low level or for the decision maker, a higher level view. Our goal in this work is to present a high-level situational awareness technique designed for the decision makers; though the configurability of the system allows it to be used in a wide array of tasks and users.

Focusing on visualization for situational awareness of cyber security has received the least amount of attention in this domain. The best-known tool being VisAlert [11], which is designed to provide correlation of events within a topology and provide high-level analysis of events. Its ability to correlate events ensures it is effectively suited for identification of the sophisticated persistent threat. Its configurability and high-level view allows it to be of use to both the network analyst and the decision maker.

A second environment is NVisionIP [14], which provides numerous techniques for the identification of network characteristics. It is focused on providing situational awareness for the analyst and not the decision maker. VisFlowConnect [20] provides a specialized link relationship visualization technique to provide a more narrow-scope network awareness capability to analysts. PanaMet [18] while providing separate passive monitoring capabilities uses a simple network connectivity graph to display network topology and topology changes. Best et al. [4] provide real-time visualization for situational awareness geared towards monitoring network traffic by support staff.

What becomes clear quite readily from the existing previous work is that the majority of the work focuses on situational awareness for the network analyst and not for the decision maker. Overall, very little of the visualization effort itself has been focused on situational awareness; rather, the majority of the research has focused on identification and analysis techniques. While VisAlert does consider situational awareness for the decision maker it still focuses on an analysis (correlation) perspective and not the high-level rapid assessment we focus on for decision making.

3. VISUALIZATION DESIGN FOR DECISION MAKERS
The visualization design process involved several steps. This process was focused on keeping the user in the loop and integrated extensive input from network analysts and managers; the complete details of this user process is documented in our cognitive task analysis [8][9]. First, was an initial brainstorming meeting with analysts, network managers, security researchers, and visualization researchers at PNNL. This resulted in an initial series of questions such as the time frame we needed to consider for this level of analysis. Such questions were primarily answered from existing Cognitive Task Analysis (CTAs), especially Anita D’Amico’s from Secure Decisions [2] and Stefano Foresti’s from the University of Utah [12]. Second, was an initial set of individual interviews with network analysts and managers. Third, was the examination of previous work. These knowledge-gathering steps provided the initial background needed to conduct a more detailed interview/brainstorming meeting with analysts and network managers. The resulting discussion session led to the development of a new task flow diagram [8][9] for our target network analysts and managers.

Based on the task flow diagram we created several visualization mockups. In order to meet the full needs of this task flow diagram, the mockups targeted the needs of both the assessment and response phases of the developed task flow model. While we have identified how characteristics for other phases could be incorporated, we did not actively pursue aspects from those phases as they were deemed to be out of scope of the current project. Of note is that after the design of these mockups we performed a set of evaluations with analysts and visualization experts to acquire their feedback and aid in refinement of the visualizations. These interviews also aided in identification of which visualizations would be targeted for implementation. Here we focus on the design of a visualization technique specifically geared towards decision-making; many of the other mockups focused on the analysis task.

The design of the mockups, conceptual designs, essentially followed the process exemplified by Figure 1. The cognitive task analysis exemplified the incorporation of the domain experts and their impact on phases 1, 2, and 5 of the process. Phases 1 and 2 revolved around acquiring the understanding necessary to design effective visualization techniques. Phase 3 was the main effort in designing initial concept diagrams for the visualization techniques. Phase 4 employed a review of the cognitive aspects of the visualization techniques and phase 5 employed a domain expert review of the visualization techniques. Clearly, the process

![Figure 1. The iterative process followed in the design of the visualization techniques.](image-url)
was iterative based on feedback. Finally, prototype implementation is exemplified by phase 6.

The focus of the techniques on decision makers combined with the goal of representing an array of nodes and parameters through clusters of such gauges resulted in the name decision maker command gauge cluster (DMGCC). More specifically, for cyber security scenarios we term the display the cyber command gauge cluster (CCGC). The unique name actually has an important etymology. Information visualizations have several mechanisms for representing parameters of a node in a dataset:

- **Pixel** [16] – A single pixel can be used to represent multiple parameters by mapping the different parameters to the hue, lightness, and saturation values of the pixel.
- **Icon** [10] – An icon is designed to represent multiple values and displayed en-masse, forming a texture. An icon can be thought of as a generalization of a pixel. By making use of a box of pixels, many parameters can be represented simultaneously. An icon is not meant to be interpreted individually.
- **Glyph** [10] – A glyph is similar to an icon with the difference that they are meant to be interpreted individually. This does not necessitate that they be more complex than icons.
- **Gauge** [22] – A gauge can be thought of as a very complex glyph. This is exemplified by the incorporation of many components that need to be interpreted individually. A gauge can be considered a visualization display in its own right. Typically, a single gauge will be the entirety of one visualization display.
- **Gauge Cluster** – We arrived at the “gauge cluster” term to represent the duality of the fact that our gauges are actually a cluster of elements (a cluster of gauges) and the fact that the visualization incorporates a number of gauge clusters.

### 3.1 Concept 1

This design, Figure 2, is geared towards providing a clear summary of the network status. In particular, in our actual implementation we focused this design on the representation of impact and vulnerability assessment, a similar goal as identified by Nusinov et al. [15]. Similarly, activity of interest scores [17] can be used. Wang et al. [19] examine the extraction of other factors for network security situational awareness. In this design, the large dial provides the overall status of the system, network, or mission; while the prototype focused on systems, the design can easily be generalized. The smaller dials provide more detail identifying how individual components of the system are being impacted. In terms of systems, we generally look at the impact on the system’s disks, memory, network, and CPU usage. For a mission, these dials could represent the analyst, the analyst’s systems, the analyst’s network connectivity to the outside world, redundancy, etc. Again, in the long term the design can be completely generalized for any summary display needs.

The design itself uses dial-like metaphors that are well known and easily interpreted by analysts and the general user. The dial itself is reinforced with color to make interpretation of value far more rapid. In this initial design, the dials were designed to go counterclockwise.

Looking back at the situational awareness model, it is this type of design concept that will provide the desired immediate comprehension of the state of the network. Clearly, the design allows for less analysis but that can be resolved with additional visualization designs.

### 3.2 Concept 2

This design, Figure 3, is a refinement of concept 1 based on feedback from analysts and visualization experts. First, the dials were redesigned to go in a clockwise fashion. Second, history information was added by providing rings within each of the dials. The outer ring provides the most current value. The filling of the rings also reinforces where the zero axis is, an issue identified with concept 1.

### 3.3 Mockup Implementations

The implementation resulting from the original mockups is shown in Figures 4-6. Key components of the implementation include:

The number of gauge clusters is configurable. Figure 4 shows nine while figures 5 and 6 show six. The gauge clusters are designed to form a square as closely as possible; N=number of gauge clusters.

$$
\begin{align*}
\text{Cols} &= \left\lfloor \sqrt{N} \right\rfloor \\
\text{Rows} &= \left\lfloor \sqrt{N} \right\rfloor \\
\theta &= \begin{cases} 
   i \times 36^\circ + 33.33^\circ & S \leq 10 \\
   i \times 360^\circ + 33.33^\circ & S > 10
\end{cases}
\end{align*}
$$

Positioning and size of the sub-gauges relative to the center are determined by (S=number of sub-gauges, \(i\)=index of the sub-gauge, \(d\)=diameter of sub-gauge, \(r\)=radius of arc inscribed by sub-gauges):
The percentage contribution of each sub-node is configurable (M=main gauge value, S=number of sub-gauges, s_i=sub-gauge value, w_i=sub-gauge weight).

\[ M = \sum_{i=1}^{S} s_i \times w_i \]

The parameter mappings are also completely configurable. This includes what parameter gets mapped to the main node color, the main node angle, and the sub-gauge angle/color.

The number of time periods represented by the rings in the main gauge, i.e., the number of rings, is configurable (R=radius of the main gauge, p=number of time periods, t=thickness of each ring).

\[ t = \frac{2\pi \times R}{p} \]

The duration of a time period is configurable. This impacts the duration of time represented by rings in the main node and the duration of time encompassed by the represented values. The time periods can be fixed or geometric (T=accumulated thickness, a=initial value, r=ratio):

\[ T = t \times p, \quad \text{fixed} \]
\[ T = \sum_{i=0}^{p} (t_i = ar^i), \quad \text{geometric} \]

All angles follow the standard trigonometric organization. The history rings are always fully mapped so as not to lose history information when current activity is not of concern.

\[ y_0 = \sin(0), x_0 = \cos(0), y_1 = \sin(\theta), x_1 = \cos(\theta) \]

In the complete environment, selecting a node will bring up a detailed visualization representing the encompassed activity. This is currently related to visualizing and analyzing alerts. Ultimately, the context and focus visualization will be directly tied to the task being performed with the cyber command gauge cluster.

The implementation supports network security and network health parameters, including:

- Impact assessment score
- Network impact
- Memory impact
- Disk impact
- CPU impact
- Vulnerability assessment score
- Source IP
- Destination IP
- Source Port
- Destination Port
- Packet type
- Alert classification
- Alert priority
- Date & time
- Payload length

Support for a broader array of parameters and application to other domains is designed in but not implemented generically.

Figures 4-6 exemplify the scenario in which the angle and color of each of the nodes is redundantly mapped to the same parameter, overall system impact, for the main node. For the sub-nodes, we assume that both the angle and color are redundantly mapped due to the size of the node. Clearly, alternative-mapping strategies can be used to represent additional parameters.

This redundant mapping results in a low expected impact being bright green but also having no angle. In essence, this reduces the visual impact of the node in this scenario; effectively removing it from the network analyst’s or network manager’s consideration.

Past history clearly stands out identifying when high impact events have been occurring. The historical information allows impact history to be reviewed even when a period of live activity may have been missed. The history information also shows when high impact(s) have occurred over multiple time periods, indicative of sustained activity. Similarly, intermittent high impact events are also clearly identifiable.

Figure 4. This is the prototype implementation of concept design 2. Originally termed the impact assessment console, we more recently named it the Cyber Command Gauge Cluster to be more representative of its full applicability. Any parameter may in essence be mapped to the gauges and the weighting of the sub-gauges as represented in the main gauge can be specified. Nine gauge clusters are shown with most activity nominal except for one short period in the bottom right gauge cluster.

Figure 5. A second example showing six gauge clusters. This example in particular shows far more anomalous activity among all of the represented nodes. Such a display should raise concern among decision makers. Of note is the long and repeated periods of concern in the bottom left gauge cluster.
When a node is representing multiple related components in aggregation, it is important to use the correct aggregation formula. For instance, using the average of the aggregated components is quite typical. However, in the security paradigm the most appropriate aggregation formula is simply to revert to the worst common denominator, i.e., the most significant attack. This is critical since a formula such as using an average of the aggregated components can very easily intentionally or accidentally obfuscate critical attacks.

The time scale. The display should show the relative contribution of each subcomponent; specifically showing the weighting of each sub-gauge in the display.

4.3 Color
Have the ability to choose different fill colors. Have someone doing research in the area pick the colors. This may not necessarily be configurable by the analyst since they may choose less desirable color combinations.

Color itself may not be a good indicator. For instance, the navy uses red lights a lot that affects the user’s view of the visualization and may affect the interpretation of the visualization. In fact, there may be too much color in the filled version resulting in the color becoming over powering.

The use of color can possibly be strengthened by fading out the fill colors in the center of the gauge, i.e., for older data. As with time periods discussed earlier, this can be either fixed or geometric in nature.

4.4 Display Structure
The comments related to the display covered a range of display element suggestions that may at times be individual or culturally derived. The percentage representation is good but consider placing the 0-degree angle at the bottom rather than following the trigonometric model. This will result in a wide arc falling to the bottom. Additionally, the scale for each of the gauges is difficult to determine; i.e., where is 0? This is resolved when the arcs are filled in but not in initial scenarios. The top four gauges are good but it might be better limiting them to 180 or 270 degrees rather than using the full 360 degrees, this would allow these gauges to mesh more intrinsically with the main gauge.

In terms of the representation of time, there were specific suggestions. For instance, make the most recent time frame thicker and the older time frames thinner, i.e., akin to an exponential scale (R=radius of the main gauge, p=number of time periods, t=thickness of each ring). Additionally, have the most recent data at the edges, creating a tunnel of the data; the history concept is good but the default presentation might not be clear.

Finally, consider reinforcing the occurrence of bad conditions using thicker time frame presentations.

4.5 Configurability
The gauge clusters should be highly configurable, allowing the weights used in calculating the averages to be configurable. Analyst must be able to specify what they want as thresholds; this includes things such as the cutoff for bright red alerts, the minimum values to display, etc. Finally, Allow the analyst to control, or specify the mapping; to the thickness and color of the gauge and sub-gauge borders, size, and intensity.

4.6 Scalability
The analyst needs to be able to update and modify definitions. For example, a cluster of gauges needs to be able to represent a single system, a network of systems, a network of networks, etc. In essence, the user must be able to zoom in and out of a specific network scale. We must identify the ability for the gauge clusters to display nodes en-masse, i.e., for a large number of hosts or networks; the gauge clusters do not appear to be compact or significantly scalable.

4.7 Summary
The focus of the analyst comments on how to improve the visualization shows that they primarily liked the general concept.
There was consistency on many of the basic modifications desired.

5. CASE STUDY

Table 1 exemplifies several tasks a network analyst or manager might perform and a potential configuration of the visualization for that task. The tasks listed and their explanations are:

- **Network Status** – provides immediate assessment of the health and usage levels of standard network components. Focused on the overall health of the entire network at a high level. The routers focus on critical routers such as border routers.

- **Network Status Zoom** – provides an immediate assessment of the health and usage levels of standard network components. Focused on a subset of the entire network. This is essentially a zoom in from the top-level network status display; the same representation can be used for multiple levels of zoom-in. The routers nodes focus on routers between subnets, etc.

- **Detailed Attack Analysis** – the goal is to provide representations of critical parameters associated with the analysis of an event or otherwise identified attack. The representation should allow the analyst to more readily identify the nature of the attack.

- **Host Review** – this mode represents details of a host or group of hosts, essentially summarizing the health, performance, and utilization of the host(s).

- **Attack Review** – attack review can be used in conjunction with detailed attack analysis. Where detailed attack analysis is focuses on providing the analyst with the key components of a current attack, the focus of attack review is providing the analyst with a historical review of the appearance of that attack. This aids in providing historical knowledge of how frequently the attack is being seen. An attack that is being seen frequently, especially recently, or at distinct intervals should receive further attention.

- **Network Activity Distribution** – network activity distribution aids the analyst in identifying the types of packets being seen on the network such that deviations from the norm can be easily seen.

- **Top Talkers** – top talkers represents the hosts involved in the most network communication. This can be further subdivided into the top internal nodes, the top external nodes, the top inbound connections, and the top outbound connections.

- **Server Status** – server status is similar to host review but specifically focusing on servers.

- **Service Status** – identify the status of individual services network wide. For instance, verify redundancy and utilization of specific services. This essentially amounts to readiness. The network manager typically needs to determine if a service is capable of meeting the needs of the network community.

- **Event Prioritization** – provide a summary display of current events. Provide situational awareness details to aid rapid prioritization of the events and show the status of the events for remediation.

6. FUTURE WORK

The visualization implementation is still in a fairly prototype state. The goal is to add the robustness implicit in a deployable capability. This robustness requires extensive features beyond just the integrity of the code base, including:

- Selecting an older time-period should show the values of the sub-gauges at that period of time to aid analysis.
- Incorporate the ability to specify fill color values; e.g., the use of pastels may be less off putting to some users.
- Add command console capabilities to allow for the long-term management of events. This would include report tracking to ensure that remediation has occurred.
- Support for a larger number of simultaneously monitored nodes with aggregation. As mentioned aggregation should be representative of the worst-case scenario.
- Complete quantitative user evaluation of the visualization technique needs to be performed.
- Incorporate support for mobile devices. The design of the Cyber Command Gauge Cluster is uniquely situated to allow support on mobile devices. This will allow decision makers to review the network status on the move.
- Substantial capabilities for the selection and probing of the display to aid the decision maker in understanding what they are seeing is critical.

7. CONCLUSIONS

We created effective next generation situational awareness visualization techniques for the representation of cyber data of concern to decision makers. This includes traditional parameters representative of network health such as CPU utilization and network bandwidth utilization but also meta-data such as vulnerability and impact assessment scores. These visualizations were designed following a human in the loop process. We consulted with actual network analysts and network managers as well as other visualization experts during each phase of the design. The developed visualization techniques go a long way towards improving the cyber decision-making challenges being seen in today’s network environments.

Analyst interviews identified the basic requirements, critical parameters, and characteristics needed for the next generation of cyber situational awareness visualizations for decision makers. These analyst interviews directly resulted in the generation of the visualization design that was the focus of this research. This visualization design meets one of the principal needs identified by the analysts, namely, the summary representations of cyber status for immediate short-term analysis. An additional advantage of the summary representation is its direct solution to the scalability issues inherent in cyber situational awareness.

The immediate assessment situational awareness visualization technique we proposed here essentially matches the perception level in Endsley’s model, namely providing for perception of events. The sub-gauges provide a limited capability for level 2 of Endsley’s model, namely comprehension. Additionally, we provide examples of how level 3 in Endsley’s model, namely projection, can be supported in the new visualization designs. This is primarily incorporated through the representation of vulnerability and impact assessment values [7].

While the presented mockups and prototype were designed for cyber situational awareness for decision makers, they are in fact designed to be completely generalizable. The main issue will be with the implementation and the need to support generalizable data in the long term.
<table>
<thead>
<tr>
<th>Task/Goal</th>
<th>Main Node Color</th>
<th>Main Node Angle</th>
<th>Sub-Node 1</th>
<th>Sub-Node 2</th>
<th>Sub-Node 3</th>
<th>Sub-Node 4</th>
<th>Sub-Node 5</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Status</td>
<td>Network bandwidth usage</td>
<td>Percentage of expected capacity available</td>
<td>Router one network bandwidth usage</td>
<td>Router one network bandwidth usage</td>
<td>Router two network bandwidth usage</td>
<td>Router two network bandwidth usage</td>
<td>Overall impact assessment</td>
<td>This display would be used for rapid assessment of network health and broad identification of areas of congestion or problems.</td>
</tr>
<tr>
<td>Network Status Zoom</td>
<td>Network bandwidth usage</td>
<td>Percentage of expected capacity available</td>
<td>Router one network bandwidth usage</td>
<td>Router one network bandwidth usage</td>
<td>Router two network bandwidth usage</td>
<td>Router two network bandwidth usage</td>
<td>Overall impact assessment</td>
<td>Apply focus and context techniques and zoom into sub-areas of a network to narrow down problem locations and types.</td>
</tr>
<tr>
<td>Detailed Event Analysis</td>
<td>Event severity</td>
<td>Impact assessment</td>
<td>Event classification</td>
<td>Source IP</td>
<td>Destination port</td>
<td>Number of hosts with connected vulnerability</td>
<td></td>
<td>Provide key parameters on a reported event for initial evaluation and aid assessment as to remediation needs.</td>
</tr>
<tr>
<td>Host Review</td>
<td>CPU utilization</td>
<td>Memory utilization</td>
<td>Disk utilization</td>
<td>Network utilization</td>
<td>Video utilization</td>
<td>Vulnerability assessment</td>
<td></td>
<td>Review host health and status. Aggregation with focus and context is critical.</td>
</tr>
<tr>
<td>Attack Review</td>
<td>Attack occurrence</td>
<td>Attack Frequency</td>
<td>Attack Priority</td>
<td>Attack Impact</td>
<td>Attack Vulnerability occurrence</td>
<td></td>
<td></td>
<td>Examine the history of an attack to ensure a world view and acquire insight into its characteristics.</td>
</tr>
<tr>
<td>Network Activity Distribution</td>
<td>% network utilization</td>
<td>% network utilization</td>
<td>% TCP</td>
<td>% UDP</td>
<td>% SNMP</td>
<td>% HTTP</td>
<td>% Encrypted</td>
<td>The distribution of the network traffic itself can identify anomalies. Aggregation with focus and context is critical.</td>
</tr>
<tr>
<td>Top Talkers</td>
<td>Internal host one volume</td>
<td>Internal host two volume</td>
<td>Internal host three volume</td>
<td>External host one volume</td>
<td>External host two volume</td>
<td>External host three volume</td>
<td></td>
<td>Identify the most active networks, sub-networks, and hosts.</td>
</tr>
<tr>
<td>Server Status</td>
<td>Server one uptime</td>
<td>Server one network utilization</td>
<td>Server one memory utilization</td>
<td>Server one disk utilization</td>
<td>Server one time since last login</td>
<td>Server one number of running instances</td>
<td></td>
<td>Focus the host review on only servers. Review server health and status. Minimize or avoid aggregation due to the critically of the designated systems.</td>
</tr>
<tr>
<td>Service Status</td>
<td>Service utilization</td>
<td>Number of service instances</td>
<td>Service readiness</td>
<td>Service capacity</td>
<td>Service availability</td>
<td></td>
<td></td>
<td>Focus on the availability of services specifically. Consider accessibility and vulnerability of a service to disruption.</td>
</tr>
<tr>
<td>Event Prioritization</td>
<td>Event one predicted impact</td>
<td>Event one vulnerability occurrence</td>
<td>Event two predicted impact</td>
<td>Event three predicted impact</td>
<td>Event four predicted impact</td>
<td>Event five predicted impact</td>
<td></td>
<td>Assist the decision maker in identifying the order in which events should be remediated.</td>
</tr>
</tbody>
</table>
8. ACKNOWLEDGEMENTS
This work was supported by AFRL [grant number #FA8750-07-C-0163] at Utah State University before being completed at the Army Research Laboratory. The project supported a number of students in significant roles and many more in minor roles. The students with major roles included: Anusha Davuluri, Srinidhi Kakani, Sarah Moody, Steena Montiero, Rian Shelley, Chris Harris, Anupama Biswas, RB Whitaker, Stephen Miller.

9. REFERENCES
12. Stefano Foresti and Jim Agutter, “Cognitive Task Analysis Report,” University of Utah, CROMDL. Funded by ARDA and DOD.