10TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM
THE FUTURE OF C2

Paper #66

Synergetic Human-System Integration for Reliable and Efficient C2 Operations

Qiuming Zhu, Jeffery Hicks, Plamen Petrov, David Andersen, Eric Lindahl, and Alex Stoyen

21st Century Systems, Inc.,
6825 Pine Street
Omaha, NE 68106

http://www.21csi.com

ABSTRACT

The synergetic integrations of humans with autonomous systems (software agents), active and passive sensors, and data fusion engines in a cohesive loop of information gathering, analysis, management, and decision making are crucial to future military command and control (C2) capabilities. 21st Century Systems, Inc.® (21CSI) has researched and developed a concept for Surveillance System Human-Computer Integration (SSHCI) and a suite of software components for an SSHCI-based Anti-Terrorism/Force Protection (ATFP) C2 application. Our approach is based on the belief that the most reliable and efficient C2 system results from a synergetic integration of humans and computers in a mutual, complementary, and human-in-the-loop configuration. This principle guided us in the development of Sentinel Net, an ATFP decision aid that incorporates multiple sets of agent-based functional modules, 2D/3D visualizations, and human-agent interaction interfaces. Sentinel Net addresses a number of technological aspects of SSHCI and provides a demonstrable means for efficient situation awareness in AFTP operations.

I. INTRODUCTION

With the advent of the 21 Century, the U.S. armed forces are equipped with much improved technologies including powerful sensory capabilities covering space, air, ground, and underwater, as well as advanced command and control systems for automated information gathering, analysis, management, and decision support. Thermal imagers and radars are extending the sentry's eyes and allowing them to "see the unseen." Superb computing facilities allow evaluation of hundreds to thousands of complicated action plans and alternatives, and provide a "down to the point" assessment of their possible outcomes. The technological advances help war-fighters separate the known from the unknowns, and raise situation awareness from the data and information levels to the knowledge levels. The automated systems reduce the burden on personnel by cutting down the number of physical units and mind efforts that have to be deployed to provide awareness. Equally important, it makes time available for personnel to train for taking actions on more complicated situations, as it becomes the essential element in correctly reacting to asymmetric threats and combat. The human-system integration also provides a clear way to share information. A boat can be vectored to intercept a contact, but a clear picture of the target eliminates time-consuming confusion and miscommunication. With the modern technology, a person can report an intruder via a variety ways, and with some additional technology, the reports can be simplified into a picture sent from the sentries, whether automated sensors or actual humans, to the C2 center. Moreover, information from multiple sources can be seamlessly fused to provide a single uncluttered and more confirmatory picture of the situation.

That is to say, *the synergetic integration of autonomous computer systems, active and passive sensors, and humans in a cohesive loop of information gathering, analysis, distilling, fusion, and sharing is crucial to future military C2 capabilities including both decision making and mission execution*.

However, as told by practices and experiences, sometimes poorly chosen technology solutions for information exchange between human and automated systems are more detrimental than the lack of information. For example, a poorly defined flow of a large amount of information overloads the decision maker because it focuses them on filtering the useful information from "chaff" rather than on responses. Thus our view of human factors in a C2 environment is toward the maximization of the overall system's capability (both human and computer), not the replacement of human with highly automated systems (except in the hazardous and human-not-reachable environment, where automated systems are supposed to reduce the human presences for completing the necessary tasks). That is, the relationship between

humans and computer systems in C2 operations should be mutually complementary, rather than a reliance of one to the other. Overall, the principle on what the automated systems should do is to extend and enhance the human's capabilities, in other words, to free human hands from tedious tasks and assist humans to do what they can do the best[1].

This principle guided us in the development of Sentinel Net, an ATFP decision aid system that consists of multiple sets of agent-based functional modules. Sentinel Net addresses different aspects of human-system integration, and incorporates different levels of human judgment and decision making capabilities [HS02]. The system contains both a set of back-end agents and a set of front-end agents. The back-end agents of Sentinel Net function in a sensor-human-system networked collaboration environment to perform multi-source intelligence integration, multi-formatted hybrid data analysis, and multi-model belief reasoning. The front-end agents of Sentinel Net operate on 2D/3D visualization, human-system interface, and interactive decision support. The human-system interaction platform provides High Resolution Situational Awareness for C2 and ATFP operations. Figure 1 is a conceptual illustration of the Sentinel Net system.

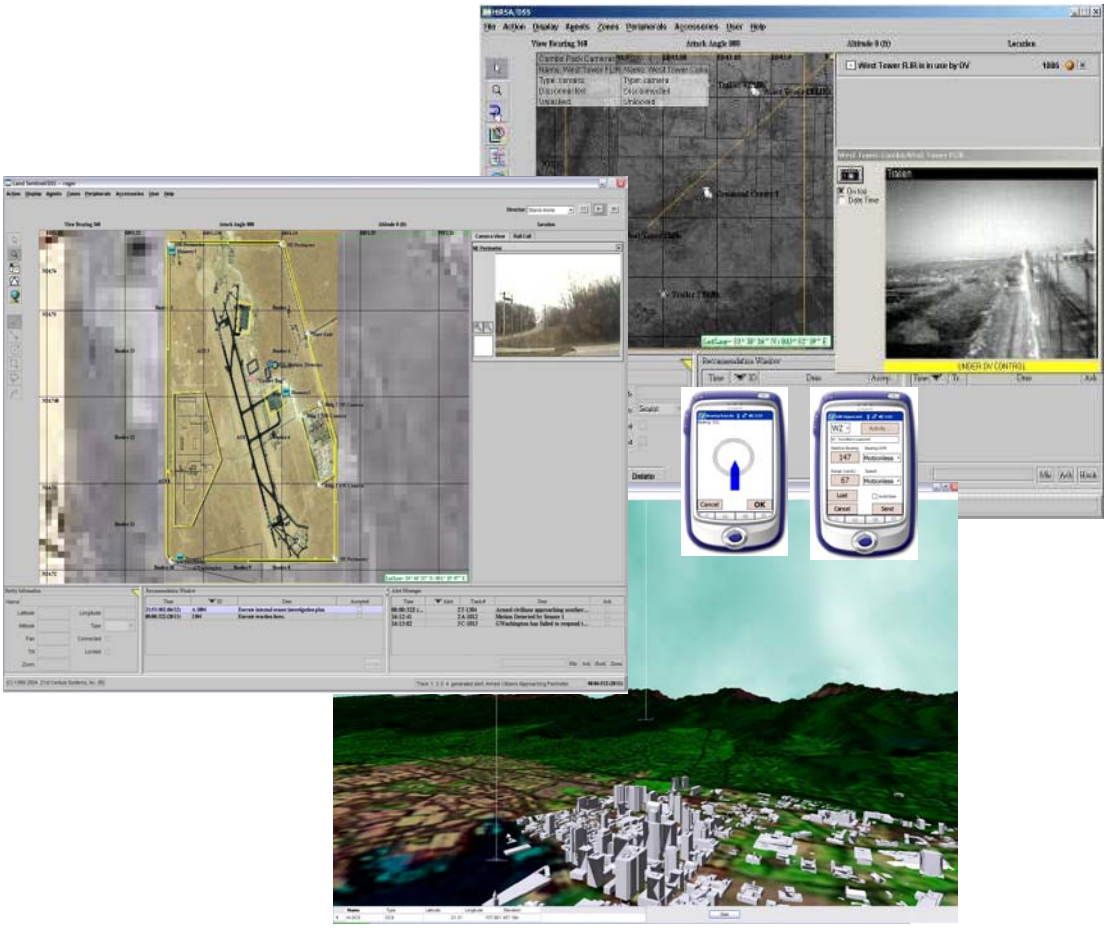

Figure 1. Sentinel Net configuration in demonstrating SSHCI concept

[1] As humans and machines (automated systems in general and computers particularly) possess distinctive and mutually complementary sets of traits in nature, it is essential to let each do what they can do the best, and let the outcome of combined efforts be the multipliers of their capabilities.

Major techniques in the Sentinel Net development include a tailored semantic knowledge representation model and a smart-media communication scheme, a simple, versatile, extendable, and rapid human-computer interaction mechanism. Personnel functioning as sentries are issued a holstered pocket PC that has wireless connectivity – either direct to other PC or via a repeater – using a dynamical data structure (DDS) and signal package (SP) scheme. Human sentries use the DDS to communicate their observations on the surrounding environment over a wireless network, such as entering these observations on a PDA device. Upon notice of activity, the personnel pull out the PC and select record fields in the signal package (SP) and transmit it. The SP, routed by the Sentinel Net Activity Assessment Processor (SNAAP), provides the "templates" for distributed situational awareness among the FP sentries. All others (Sensors, Sentries, Center C2 systems) in the network can access the DDS and individual SP, where all FP personnel share a common picture of the FP operation. The central tracker in SNAAP keeps a log of all SPs and transactions for reliable and extensive monitoring operations.

While Sentinel Net is originally designed as a shipboard ATFP system, it can be tied generally into many larger C2 systems such as the FORCEnet. The Sentinel Net system leverages existing capabilities of information acquisition, analysis, knowledge derivation, management, and reasoning under uncertainty for decision support. The development is to merge intelligent agent software technology (the system) with roving patrols and watch-standers, which implements a typical level of the SSHCI. Personnel involved in Sentinel Net can include watch-standers, boat operators, marine guards and local authorities, or collocated naval forces. For example, the notional sentries exchange information regarding potential security breaches surrounding a U.S. Navy ship berthed in a foreign port. For operators below deck, a repeater is used to ensure solid communications outside and inside the ship. By tapping a multitude of disparate pieces of information to report unusual – possibly terrorist – activity in a distributed environment, Sentinel Net provides a platform for implementing the SSHCI concept and enabling shared situational awareness.

The organization of this paper is as follows. Section II discusses the concepts and principles of the SSHCI and the functional components of its implementation in the Sentinel Net. Section III described system architecture and implementation details of the Sentinel Net with an illustration of the various technological aspects of the SSHCI concept. Section IV contains concluding remarks.

II. CONCEPTS AND FUNCTIONAL COMPONENTS

II.1 Major Concepts

In this section, we first present the major SSHCI concept that emerged from the general domain of human-computer (automated system) integration to the specific domain of ATFP application. We will then present the key functional components of our HCI construct where the SSHCI concept forms the theoretical foundation for the development of the Sentinel Net system.

II.1.1 ***Complementary Human-System Functions***

It is a general understanding that for an effective C2 operation, sensors, geospatial databases, force locators, and automated reasoning systems in commanding centers should be operating on a common network. This network must include decision support tools for environmental prediction, event reporting, pre-mission planning and post-mission analysis, impact and consequence management, etc. We believe that a key factor to a successful and maximally empowered operation of this networked system is the seamless connect (collaborations and interoperations) between human and the automatically functioning components, where humans and the functional components of the automated system play complementary roles, each to function in their maximum strength.

Look at a typical scenario of modern warfare: new sensors are evolving for the detection of CBNRE (Chemical, Biological, Nuclear, Radiological, and Explosive) threats; systems are developed for intrusion detection; and Information Assurance Operations in the cyber-world of PCs, software and network (wire, fiber, and wireless). While these sensors and system are very capable, a network of "thinking sensors" is still needed to detect that which falls outside those sensors' capabilities. What we need is to bring humans and computer systems together. The joint force is to collaborate on a commonly networked communication paradigm incorporated with intelligent agent technology using a multitude of disparate pieces of information. Detected activity that is anomalous and that is suspicious is then tracked and graded by the system.

The required capability of correlating and integrating the disparate information from heterogeneous sources of FP sensors and watch-standers that come with varying degrees of certainty and reliability in real-time is an impediment issue in crucial Navy force protection situations [SZ96, KA97, RJ00]. The surveillance system concept (SSC) behind the Sentinel Net is to link all personnel and sensors that can provide necessary information useful toward ATFP judgment and decisions. The main interaction comes when watch-standers, guards, sentries, and similar personnel who have been issued a link to the network are interlinked to one another as well as to a central commander (master computer running intelligent decision support software). The automated system is not a replacement for humans, it merely acts as a force multiplier for a well-trained, knowledgeable operator. The system must balance between not overloading the decision makers with extraneous information and inadvertently excluding critical information from them.

II.1.2 ***Humans in the Loop Systems***

Two terms that are often used throughout the C2 domain are Common Operation Picture (COP) and Shared Tactical Picture (STP). The COP is an overall situational awareness tool for decision makers. It includes the STP, current intelligence and threat data, and integrated planning and decision aids. In the ATFP domain, humans are provided with a variety of displays to support the commanders and operators in all phases of terrorist deterrence, detection, and defense. Increased data connectivity and easy-to-use networked communication facilities enable the watch-standers to interact and collaborate with the automated sensors and computer systems, achieving a higher level of understanding and collectively determining if a detected activity is unusual. The action officer that is responsible to react to these anomalous activities is in the loop (using the central tracker) and can bring in higher echelon reports from commanding centers and local distributed spots.

The scenario of human-in-the-loop operations with COP and STP can be illustrated with an "open loop" and a "closed loop" instantiation of the Sentinel Net implementation. In the open loop scenario, human operators or commanders make decisions on reacting to the events according to collected sensory data and other environmental information displayed in the COP and STP. In the closed loop scenario, while human operators and commanders react to the environmental situations as in the open loop, they also actively seek for and extend with control and management of the sensory devices and means of verifying current information and acquiring new information in the COP and STP. That is, the SSHCI concept maintains a two-way information flow with the overall command and control (C2) system; that is, (1) the flow from sensors and sentries to the C2 center and event tracker and (2) the flow from C2 centers to the sensors and sentries.

II.1.3 ***Knowledge Augmentations***

It was said that "Shared information does not automatically, if ever, lead to shared understanding," [Kau05]. For the purpose of tactical C2 operations, there is a significant difference between information exchange and knowledge exchange. Information exchange alone is useful but requires knowledgeable operators at all points to correctly process and react to that information. Successful force protection begins with ability to share critical knowledge in a timely manner with a network of forces. The very

nature of asymmetric warfare requires rapid response to threats from all dimensions in a coordinated, systematic response. The ability to transfer knowledge reduces the amount of processing and information required at each stage of the information pathways.

The possession of a knowledge integration capability is significant to Sentinel Net both notionally and operationally. This capability also enables FP officials to gain a greater situational awareness of the environment, to assess and to decide on solutions to the threats of urgency, and, in turn, to seize the initiative faster than the opponents.

II.1.4 ***Integrative System of Systems***

The diversity and complexity of the operation environment of modern warfare determines that military surveillance system has to be equipped with superior capabilities to deal with a configuration of system of systems where a large set of system components interaction with each other to serve as a corporative construct for any specific application. That is, a SSHCI system should be able to operate as a secure stand-alone system as well as an integrated component in an existing security and key-management system.

The merging of many different descriptions of the same point-of-contact into a single point-of-contact is a central task for situational awareness systems. Sentinel Net utilizes agent technology to create a data fusing agent that uses semantic distance, temporal, and hybrid information to create speculative fusing in a dialog with the Sentinel Net agent in order to minimize the negative effects of either a wrong or missed data. Sentinel Net's data fusing agent leverages the error recovery information from the source using its built-in knowledge base, and is able to learn in both supervised and unsupervised modes. Sentinel Net's maximal utilization of its knowledge representation is crucial to success of Sentinel Net's data fusing capability and represents a significant advance in the area of data fusion.

II.2 Key Functional Components

II.2.1 Knowledge Representation (KR)

A robust and flexible KR is essential to being able to capture the highest resolution and clearest picture of the environmental situations in the SSHCI space.

Representation framework

The Sentinel Net KR provides a common data dictionary and belief network used, as much as possible, by all Sentinel Net software agents. It provides a common framework for encoding the meaning of force protection plans into threat-response matrices and the encoding and matching of events from sentries and sensors. Sentinel Net's variable complexity leverages the KR for arbitrary precision of information while providing an encoding scheme.

The Sentinel Net KR provides support for low-level sensor classification, and higher level semantic and synonym-set representation. A crucial correlative bridge is provided between the high-level force protection plans and advisories and the lower-level encoding and recognition of the events that comprise the Sentinel Net situational space. As well, the Sentinel Net belief projection framework provides a basis for calculating confidentiality and integrity for secure communications. Since counter-example representation is important for specifying and recognizing asymmetric concepts and to deal with the so-called "antonym problem," the Sentinel Net KR utilizes a triple belief statement comprising of belief, disbelief, and uncertainty to tackle the problem [AMS96]. This scheme allows the Sentinel Net KR to represent incomplete examples or counter-examples more precisely.

For maximum flexibility, the Sentinel Net KR has a system configurable semantic and inference mechanism where the problem space of the deployed environment guides the implementation of these functions.

Semantic Distance

For different problem spaces, different semantic distance and belief functions should be used. One problem domain of concern to force protection is the cognitive metrics of sentry input. The nature of eye-witness testimony and cognitive metrics govern the mechanisms of gathering the most relevant and accurate descriptions in the shortest amount of time, yet optimizing the probability that the Sentinel Net agents can detect threats contained in that testimony. Developing semantic distance functions for the discovery of sentry malapropisms and other cognitive errors is critical to providing optimal force protection. Sentry malapropisms are the accidental entry of a wrong activity description because in that sentry's mind that description has a higher but inappropriate correlation.

The Sentinel Net KR allows for crucial semantic distance functions to be utilized for data fusion and rules matching. The semantic distance functions measure the distance from one concept to another. Belief space operators introduce uncertainty and provide formal methods of verifying consensus and discounting for chains of authorities. Belief statements also provide an avenue for Sentinel Net to learn via the introduction of new derived belief statements. This allows for like descriptions of a threat to have lower distance values, even if the sentries who entered the descriptions used different words [BH01].

II.2.2 Knowledge Communication

A communication scheme based on a dynamical data structure (DDS) is employed in Sentinel Net. The DDS serve as a smart media and encode information about threats and possible terror attacks that need to be observed or monitored. Each DDS records one type of threat or attack.

Organization

The Sentinel Net DDS is organized in groups according to geospatial zones or threat types. There are multiple DDSs for each zone or split-zones or threats. Inter-connections can be established among the DDSs of same group or different groups to encode different threat patterns and causal relations in different zone identities. The DDS can be set-up, added, deleted, or modified through the network communications remotely or on ship locally. The structure is flexible to make changes and to adapt to different situations – on the network (remote) and/or on the ship's central tracker (or the naval facility, as the case may be). The DDS is also easy to manage and operate. No special knowledge is needed to learn to operate the DDS (and the system) – military personnel can manage the system with little or no special training (as long as the person knows how to connect to network and to generate some kind of text input using a software like a word processor).

Operations

The Sentinel Net operation is data-driven. Once a DDS transaction event takes place, a human-system collaboration process starts in the Sentinel Net process. Collaboration is between users (humans) and the computer system (agents) operating the DDS, and between humans and the SSC central tracker. The SSC central tracker is also agent-based. Agents will attempt to use the quickest method to try to converge on a decision whether activity is usual or anomalous. There are a number of ways for judging whether an event is anomalous enough to track and to determine its magnitude of anomaly. Two algorithms for reasoning and execution management are considered: One algorithm is based on pattern matching and the other is based on probabilistic evaluations.

II.2.3 Knowledge Engine

This entire process of SSHCI in Sentinel Net involves data acquisition, analysis, comparison, cross-examination, filtering, extraction, and reasoning to detect the anomalies.

Data Acquisition

Data acquisition in Sentinel Net can be addressed (push/pull) from the multiple, heterogeneous resources. Data can be fed, or acquired by the system, in multiple channels ranging from sources of intelligence resources, surveillance sensors, and the HUMINT originated from the pocket PCs of the on-ship observers in charge of each zone. The data acquisition engine of the system can be constructed in two ways: either as a centralized controller or a distributed controller. Functions of the engine include queuing, prioritization, mapping, evaluation, and directions of linking. That is, the sensory and watch-stander observations from the multiple sources are gathered in a buffer/queue, prioritized, and then sent to the inference agent. The threat/attack detection inference engine associates the real-time data with the knowledge stored in the system to identify a possible terror attack(s) and trigger an alarm/reaction. The inference engine performs a sequence of operations such as look-up with respect to the events reported, and invokes activities specified by the pre-set models (e.g., look up other events according to the current situation).

Inference Engine

Inference engine is a necessary component for any system of information integration and decision support [Ma97, RP97, LCV02]. Sentinel Net has a built in inference engine that utilizes the KR for reasoning and evidence integration. The inference engine resides in the SNAAP and allows for common use cases and force protection plan inheritance from other like protection plans. It facilitates force protection personnel to build a force protection knowledge base that can quickly specify a more complex force protection plan with higher resolution. A higher resolution force protection matrix with a large knowledge base can be more anticipatory to threats, and have a wider array of recommended threat responses.

The inference engine of Sentinel Net is designed to perform, in a sequence of, two pattern matching operations for alignment, correlation, association, and integration of multiple reports from different sentries and automated sensory devices with disparate information of observed objective situations. As a result of this engine, Sentinel Net is able to provide a more efficient threat/solution matrix and increase the force protection efficacy overall.

Characterization

Main characteristics of the knowledge engine of the Sentinel Net system include:

- Easy to operate: For system set up, the users only need to know how to enter text into DDSs (will have templates) and one only needs to push a button to trigger the system.
- Easy to modify: Operations can be done either off-line or on-line.
- Easy to expand: Sentinel Net renders a nice separation from the system control engine. Knowledge and Inference rules are not hard-coded in software.
- Easy to enhance and comprehend: A natural language interface provides the ability for user to participate in the system building activities by creating the DDS, communicating the contents, and fusing the data in the inference engine.

III. TECHNIQUES AND IMPLEMENTATIONS

III.1 Sentinel Net Software Architecture

The Sentinel Net system implements an open architecture for Human-System Interface and information integration. The system is equipped with a high-resolution GIS user interface. It receives information from a number of sensors distributed on a wired and wireless information network to produce situational awareness concentrated visualization for the area of operations that is critical for effective force

protection. Sensor control, tasking, and arbitration capabilities are provided to the users via a natural, intuitive 2D/3D graphics interface. The high-resolution human-computer interface allows commanding center personnel to clearly see the integrated tactical picture using available GIS terrain data or synthetic 3D urban terrain views built from available mapping tools such as LIDAR in a fly-through view. Operators can create security zones, place sentries and locate sensors on the visualization, use agents to monitor the zones and correlate sentry and sensor surveillance reports. Information provided from the sentries will also be depicted graphically.

The system architecture consists of four major functional blocks:

(1) Network environment – The linked DDSs, the set-up, activation, access, and utilization of the system will all be done through message communication in the network.
(2) System control agent assembly – The system control agents coordinate the creation, modification, access, and activation of the sentry entities. There are different types of agents, each responds to a specific task, such as access control, event inference, parameter adaptation, etc.
(3) Agent communication – Agents in the system communicate using smart DDS organized in stacks according to zone categorization. The DDSs can be created, organized, accessed, and modified through operations that can be performed either remotely (via network) or locally.
(4) Event Buffer /Queue – The event buffer is organized as a data queue. The buffer receives event report and other surveillance information from multiple sensors, observers in every zone, and other information sources. There is an event control agent in the system agent assembly that is in charge of setting the event processing priorities and preliminary filtering for the events entering the queue.

Figure 2 shows a diagram of the Sentinel Net architecture for an implementation of SSCHI concept.

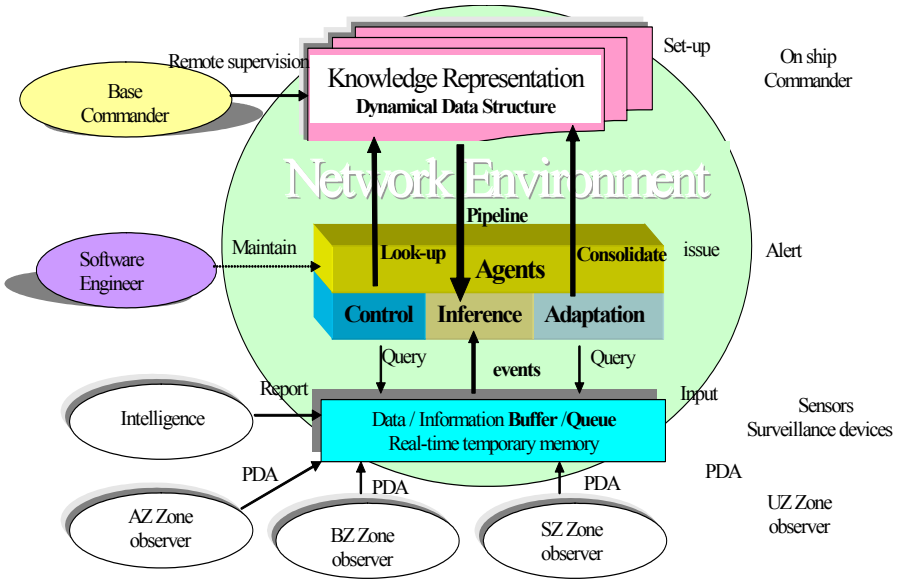

Figure 2. Sentinel Net architecture of Surveillance System Concept

III.2 Agent technology ensuring human-system communication effectiveness

In Sentinel Net, software agent development efforts incorporate increasingly sophisticated threat detection and decision support algorithms with a diverse set of automatic sensory devices and functionalities to provide ATFP personnel an integrated set of course of action (COA) recommendations. Taking full advantage of intelligent agent characteristics and capabilities [ASP00,BR97, GPS00], the resulting system

is featured with an efficient client-server communication paradigm that is both secure and robust, while minimizing available bandwidth usage.

Information fed to Sentinel Net may be video data, radar tracks, voice communications, operational guides or a multitude of other feeds. It is the knowledge embedded in the agents of Sentinel Net that possess the ability to transform the data into comprehensive information. For example, a radar track outlining position, course and speed of contact is transformed into threat relevant knowledge. The kinematics information plus identifying information (friendly or hostile) clearly defines action related to that information (if hostile evade or engage), and the understanding and ability to execute the required actions.

One of our principles in Sentinel Net development is to provide an open system concept that allows interchangeable hardware. As technology for hand-held devices (e.g., PDA - Personal Digital Assistant) and wireless communications continually improving, it is desirable to include the technology in Sentinel Net for improving SSHCI capability and enhancing human-machine communication effectiveness. The US Navy PDA policy issued in December 2003 stipulates the approval authorization for PDA use in military networks. Several commercial vendors offer such PDAs, and special shock- and water-proof cases are available for standard PDAs as an alternative. We anticipate a considerable amount of research will be devoted to develop a suitable solution that will meet the requirements for a robust device capable of withstanding harsh conditions and repeated hard use. While standard PDAs were used, additional devices including optical, infrared, ultrasonic, motion, and other physics-based sensors can be deployed. Automatic operation and wireless network connections of these devices with the other components of the Sentinel Net are employed.

Sentinel Net has a flexible security layer and is able to operate as a secure stand-alone system as well as an integrated agent component in an existing security and key-management systems. Security is addressed and appropriate schema designed to provide adequate end-to-end system communication security. Department of Defense evolving secure communications standards for wireless connectivity requires VPN tunneling for all 802.11b communications. Thus, as a baseline, a VPN-type of system is studied and implemented using commercially available encryption protocols to provide layered system security.

III.3 Distributed processes supporting diverse ATFP operations

In ATFP operations, threats are often identified by people who spot the anomaly in the normal pattern of events. Very simply, something just doesn't feel right and they respond with a higher state of awareness to identify the trigger. It is a far different requirement from detecting an incoming cruise missile over the horizon or an unseen submarine at the edge of the torpedo danger range. The force protection officer must be closely connected to the other people on his team so they can rapidly communicate this "hunch," much as a SPY-1 radar communicates the presence of an airborne threat electronically to the ship. In the transit stage, the ship has no real electronic triggers. The sensors serve to give the person a full range of information, it is up to the person to apply knowledge and find the elements that don't fit.

Sentinel Net integrates automated sensors and human sentries equipped with wireless PDAs distributed on topside of ships, signal processing and intelligence analysis severs and C2 officers at control rooms, and decision-support software running in front of the ships' force protection commanders via the ship's combat C2 system, or standalone as required. Remote sensor (radar, optical, motion, IR, acoustic) detection information is incorporated into the system to gather unusual and suspicious activity reports. The system addresses four major naval force protection scenarios in the FP effort:

(1) Ship entering port,
(2) Ship is pier side or at anchor in port,

(3) Threat approaching from port, underwater, and the sea; and
(4) Threat detection and reaction.

For example, a single ship is preparing to enter a port with no additional support overseas. Prior to entering port, the ship finalizes her force protection plan, reviews threat data, and compares the planned approach with the potential threats in the area using integrated charting displays. The security forces are briefed on the plan, review the rules of engagement, and prepare for operations. As the ship nears the port, she gradually shuts down the traditional combat systems and sensors. Simultaneously she turns on her shipboard protection system that includes electro-optical sensors, surface search radar, cameras, lights and non-lethal defense systems. Close in main weapon systems and various small arms stations around the ship may be manned depending on the Force Protection condition. The security forces communicate using secure radios or wireless devices and the force protection officer maintains the battle-space, similar to how the command officer currently fights.

As the ship anchors or moors pier-side, the security forces maintain the watch as the ship is shut down. The Shipboard Defense System (SDS) remains fully functional. Boats or unmanned vehicles (if available), the watch officer, and senior team leads share a common tactical picture of the area. Swimmer detection sensors monitor the underwater environment; radar, EO and other sensors monitor the surface and air. Any unusual activity can be quickly reported, analyzed and, if required, sent out to regional commanders. They can update it, expand information, and compare it with expectations built through experience. Manning can be kept to the minimum required for effective response, and people are freed from the mind numbing job of surveillance.

In order to provide characterization of the area around the ship or naval facility, Sentinel Net defines defensible zones around the area such as a ship during docking and while berthed at pier side. Each zone is categorized by a security level (see Figure 3) such as:

(1) Exclusion (Red) zone - a ship's stay out area
(2) Medium security zone (light gray) - vessels at minimum speed on a non-threatening course
(3) Surveillance zone (dark gray) area under surveillance - Size and shape of a surveillance zone may change due to time of day, weather, etc.These zones are further categorized by medium type in which activity might take place. The four types are:
(1) WZ: Water surface in harbor
(2) BZ: Berth area land surface
(3) UZ: Under water in dock area
(4) AZ: Airspace around protected area.

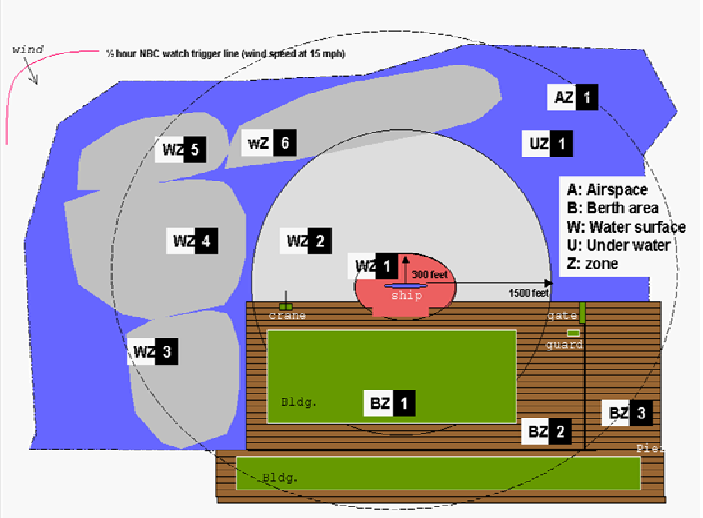

Figure 3 Zoning Illustration for a Berthed Ship

Outside the immediate area of security zones are harbor and port area activity reporting by collocated forces and local authorities. Reports of interest may include movement of group of people or vehicles to a critical infrastructure access points such as a fence or a gate, or perhaps a sudden dispersal. Critical infrastructures are bridges that cross a waterway, data and power lines serving the harbor, pier warehouses, water supplies, and fueling.

The potential for a wide variety of activity is certainly possible for any zone. However, some activity types are more prone to suspicion than others. Anomalous activities can be characterized by vessels. For example, recreational or commercial vessels that are fishing in locations not typically used for fishing, unattended vessels, unusual filming activity or diving operations, unusual number of people on board, or lights flashing between boats and shore at night. For facilities and waterway structures, anomalous activities include fishing in locations not typically used for fishing/hunting, unattended vehicles in unusual locations, filming, drawing or note taking of traffic and movements, divers entering water near facility or bridge, missing fencing, lighting, facility detection devices reporting intrusions, or lack of status reports. Other types of activity include people wearing unusual clothing as if for spraying, aircraft misting or spraying in area or large number of insects or unusual type of insects.

Sentinel Net decision support elements allow FP forces the means to share knowledge of multiple security zones guarded by distributed sentries, thereby sharing a common situational awareness toward increased mutual support and decreased threat response time. The signal package (SP) of smart-media system enables user-defined reports from among a large number of possibilities and ensures that the reports accurately reflect the sentry's observation(s) within a specific force protection zone. The Sentinel Net PDA client simulated the use of a GPS-type device by allowing the PDA user to select their current location from a prepared list. Each location had normalized relative bearing and range from bow of own-ship using the standard SP transaction. As a result, implementing GPS in a refined Sentinel Net PDA client will require no changes on the Sentinel Net server. Figure 4 (below) shows a screen capture depicting a notional scenario with security zones surrounding a berthed vessel and shore facilities.

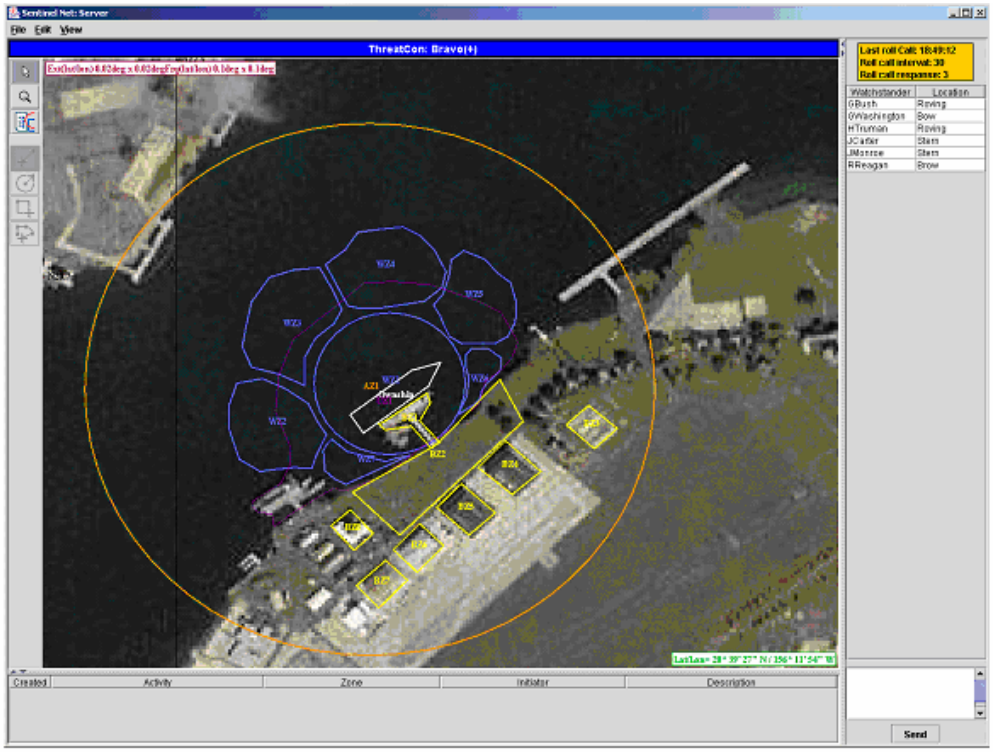

Figure 4. Simulation scenario.

As shown in Figure 4, the Sentinel Net server provided icons indicating current location of sentries, sensors, SP incidences, and WCA (Warning, Caution, and Alert). This visual feedback is crucial for FP officer to discern patterns of attack and develop a course of action. Using data-driven inference engine to perform data fusion, the SNAAP of the Sentinel Net system provided output as recommendations to the FP server using human-assist agents (in this case in a simplified form) to aid the FP "Command Center"

in making timely, accurate decisions in response to perceived threats as reported by the "human" sentries, in combination with information from automated sensory outputs.

Current Sentinel Net architecture lends itself well to additional sensor integration. Examples of such sensors are swimmer detection systems, IR detection devices, passive motion sensors and land-based acoustic sensors. We anticipate learning more aspects on how human and systems (sensors and inference engines) can interact most effectively and efficiently with respect to the availabilities of more advanced sensory and automated systems.

IV. CONCLUSION

The capability to defend our armed forces is dependent not only on technology alone, but also an investment in training and technology to expand the operational field of efficiency and effectiveness in interaction and communication with the automated systems. The very nature of warfare spells out that superior knowledge leads to superior tactics and overwhelming victory in spite of overwhelming technical superiority of the enemy. Synergistic integration of human operators and automated computer systems can more accurately emulate C2 processes in processing vast amounts of information and helping speedy decisions. We believe Sentinel Net represents a crucial technology for providing our forces with effective tools for reporting unusual or hostile activities in real time. Functioning as an integrated network of humans and "intelligent" sensors, this capability cannot be fully realized with current "dumb" or passive sensors and systems.

In addition to physical threats, modern day terror also includes threats to computers and network services. Port facilities that report attacks are monitored not only for the attack itself, but the possibility of a synchronized attack where the terrorist intent to disrupt the network to reduce communications and follow with physical attack to increase the level of terror and chaos. The types of cyber warfare include the compromise of classified information; destruction of computer databases, denial of services (DoS) and codes or manipulation of computer, cable, satellite, or telecommunications services. The concepts of SSHCI laid in this development of ATFP operation can also be applied to a variety of these kinds of scenarios including the war in cyberspace. For example, in the network security protection case, the sensors and sentries will be automated intrusion detection agents and network activity monitors (watch-standers), and the inference engine collaborating with human operators closely can identify any potential attack pre-actively.

Sentinel Net's situational awareness, threat detection, and intelligent decision support capabilities make it a unique and useful tool for either stand alone applications in a controlled Force Protection environment, or as a component in a larger system such as airport security, Coast Guard port and harbor security, state and local law enforcement, event security, and myriad other applications. The ability of Sentinel Net to integrate various system components from a configuration of system of systems will provide an excellent upgrade path for existing security systems towards realization of a high-level integrated decision support system that can be seamlessly merged into existing force protection security systems. As homeland defense evolves standards and practices for integrated first responders and centralized reporting, intelligent situational awareness becomes crucial for sifting through the massive flood of information to find real threats. Sentinel Net, in this environment, can become a bridge, or transformational technology, between existing security systems and the evolving modern integrated defense network. The research team at 21CSI intends to take full advantage of the large market potential for Sentinel Net to maximize spin-off applications from the R&D effort.

References

[AMS96] C. Amaro, T. J. Marlowe, A. D. Stoyenko, "An Approach to Constructing Complex Evolving Systems Using Composition of Knowledge Domains," *21st IFAC/IFIP Workshop on Real-Time Programming,* November 1996.

[ASP00] T. Arai, K. Sycara, and T. Payne (2000), "Experience-based reinforcement learning to acquire effective behavior in a multi-agent domain," *Proceedings of the 6th Pacific Rim International Conference on Artificial Intelligence*, pp. 125-135.

[BH01] A. Budanitsky, G. Hirst, "Semantic Distance in WordNet: An Experimental, Application-oriented Evaluation of Five Measures"*, Workshop on WordNet and Other Lexical Resources, in the North American Chapter of the Association for Computational Linguistics* (NAACL-2000, Pittsburgh, PA, June 2001. http://citeseer.nj.nec.com/budanitsky01semantic.html

[BR97] J. Bradshaw (ed.) (1997), *Software Agents*, AAAI Press, USA.

[GPS00] J. Giampapa, M. Paoluc, K. Sycara (2000), "Agent Interoperation across Multi Agent System Boundaries," *Proceedings of Agents 2000*, Barcelona, Spain, June 3-7, 2000.

[HS02] Hewish, M. and Scott, R.; "Navies Expand Their Air Defenses"; Jane's International Defence Review, November 2002, pp 41-43.

[KA97] C. Knoblock and J. Ambite (1997), "Agents for information gathering," *Chap. 16 in Software Agents* (J. M. Bradshaw, ed.), pp. 347-373.

[Kau05] Alfred Kaufman, "How the Doctrine of Network-Centric Warfare Allows Technology to Dictate Military Strategy," *Armed Forces Journal*, February 2005, pp. 20-22.

[LCV02] E. Lefevre, O. Colot, and P. Vannoorenberghe, "Belief function combination and conflict management," *Information Fusion*, Volume 3, Issue 2, Pages 149-162, 2002.

[Ma97] F. Martinerie, "Data Fusion and Tracking Using HMMs in a Distributed Sensor Network," *IEEE Trans. Aerospace & Electronic Systems*, Vol. 33, No.1, pp. 11-28, 1997.

[RJ00] J. Rickel, and W. L. Johnson, "Task-oriented Collaboration with Embodied Agents in Virtual World," In J. Cassell, J. Sullivan, and S. Prevost, editors, *Embodied Conversational Agents*, pp. 95-122, MIT Press, 2000.

[RP97] B. Rodriguez and W. Poehlman (1997), "A system for distributed inferencing," *Proceedings 1996 Rochester Forth Conference Open Systems*, p. 118.

[SZ96] K. Sycara and D. Zeng (1996), "Multi-Agent Integration of Information Gathering and Decision Support," *Proceedings of the 12th European Conference on Artificial Intelligence*, 1996.