Heartbeat e9-1-1

Steven James McGee
CEO Simple Always Wins Concepts LLC
stevenjmcgee@sawconcepts.com

Abstract: One of the DHS's top three goals is (enabling) "A national common operating picture for critical infrastructure". A congressional directive states "nothing less than network centric homeland security akin to network centric warfare". Heartbeat e9-1-1 addresses the interoperability challenge where unique Federal / military situational awareness (SA) systems and Telco networks supporting First Responder e9-1-1 systems agree on common, settings of three common denominators: (1) TCP/IP heartbeat protocol (2) heartbeat (XML) messages that convey network configuration data (e.g, router MIBs / multicast group subscriptions) (3) Common Alert Protocol child schemas and / or data islands. When the DOD's system integrators and the world's e9-1-1 Telco network providers agree on these three common denominators / building blocks, direct collaboration based on consistent timing of events and common symbology will be achieved.

1 Introduction: Heartbeat e9-1-1: Method to enable a Homeland Security Heartbeat

The Department of Homeland Security forwarded this paper's methodology to enable Heartbeat e9-1-1 to the federal government's Technical Support Working Group – TSWG who tabled this idea on 11 January 2006. The TSWG is comprised of board members from the major anti-terrorism agencies (e.g., FBI, CIA, NSA, DHS, DIA and DOD).

Federal / military situational awareness (SA) systems & Telco / cable networks supporting First Responder e9-1-1 systems use the common denominators: the TCP/IP heartbeat protocol, heartbeat (XML) messages that convey network configuration data (e.g, router MIBs / multicast group subscriptions), & XML schemas -- DIFFERENTLY.

What if the military's Network Centric Warfare (NCW) operational procedures that hinge on the heartbeat protocol & heartbeat network management messages & CAP child schemas are applied thru the world's Telco network Public Safety Answering Points (PSAPs) supporting the (inter) national e9-1-1 system as leased thru key federal contracts (NETWORX, Alliant, IWN, EAGLE, Encore II, DHS First Source...)?

Heartbeat e9-1-1 addresses the interoperability challenge where unique & proprietary Federal / military situational awareness (SA) systems // Telco networks supporting First Responder e9-1-1 systems agree on common, consistent settings of the three common building blocks.

The user base of Heartbeat e9-1-1 are customers / stake holders of major federal contract vehicles with Situational Awareness & Telco Contract Deliverable Requirement Lists & eventually as cited in the article titled "DHS revamps Emergency Alert System - DEAS": "every cell phone owner who has not opted out of the Heartbeat e9-1-1 subscription service currently offered to Blackberry device owners" as quoted by Government Executive Magazine.

1.1 Heartbeat e9-1-1: Three Common Building Blocks

1.1.1 TCP/IP Heartbeat Protocol

Heartbeat protocol: "The Heartbeat protocol signals the presence of a node and its state. The Heartbeat message is a periodic message of the node to one or several other nodes. It indicates that the sending node is still working properly." A DHS state interoperability funding document dated May 2006 on page 32: a goal to "Improve capacity to include EMS responder status management and vehicle location as an extension of the HEARTBEAT computer aided dispatch system".

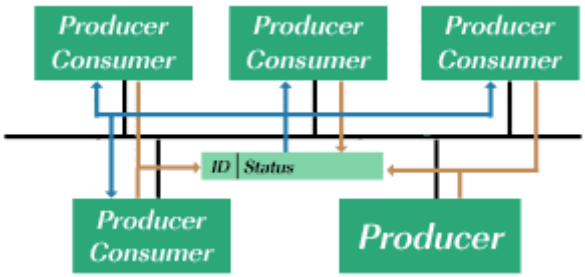


Figure 1: Heartbeat protocol role in motion-oriented machine control networks

The above figure is from the CANopen web site. "CANopen is a CAN-based higher layer protocol. It was developed as a standardized embedded network with highly flexible configuration capabilities. CANopen was designed for motion-oriented machine control networks. It is used in many fields, such as medical equipment, off-road vehicles, maritime electronics, public transportation, building automation, etc."

1.1.2 Heartbeat XML network (re) configuration schemas

The heartbeat protocol as a low level data harvester gathers network configuration data (e.g., current IP lease, multicast group participation, state information such as moment greater than 50 meters, at halt, off line, or straggler…) that is gathered and forwarded by any newer, more efficient products or systems. Once multicast subscription group (s) state data is consolidated, data is consolidated by the tactical equivalent of the corporate system administrator or the S-6 in military parlance. The Tactical Internet Management System or TIMS is used to configure router management information bases (MIBS) and associated multicast entries describing the grouping of organizations (units) for missions (Unit Task Order). The S-6 / tactical system administrator then broadcasts the updated network configuration data in the form of (K00.99 Variable Message Format) heartbeat messages to higher, lower and adjacent organizations refreshing router/switch unicast / multicast subscriptions. On the military side of this procedural method, situational awareness data subscriptions are updated and units tether and untether to network nodes as they maneuver. A similar process occurs on the commercial side of this methodology as cell phone / smart phone / wireless laptop users tether and untether to cell tower nodes – differently i.e., different heartbeat protocol data collection-distribution rates and different heartbeat XML message schema structures). Heartbeat e9-1-1 involves the commercialization of network centric warfare message structures / documents / schemas into Emergency E9-1-1 cell phones and smart phones E9-1-1 Public Safety Answering Points – PSAPs emulation.

This concept involves commercialization of military proprietary tools such as the Tactical Internet Management System (TIMS) that produces the UTO – Unit Task Order. The UTO is a message template that military situational awareness applications FBCB2 and Blue Force Tracking) apply. The Unit Task Order is a hierarchical depiction of unit structure showing how units are organized for operations similar to corporate wiring diagrams. UTO distribution is enabled by the use of TCP/IP's heartbeat mechanisms in terms of the heartbeat protocol's send to, get

from and timer / data harvest trigger. Gathering network (re) configuration data used to update tactical / corporate organization / first responder's multicast subscription information based on unit / organizational mission posture change is key Heartbeat e9-1-1 methodology. The commercial equivalent of the military proprietary UTO Tool composes heartbeat protocol gathered network (re) configuration data as a XML EDXL-DE formatted schema with military DDMS data as embedded islands or child schemas. Commercial equivalent UTO tools will exchange these network reconfiguration messages with military counterpart organizations. Tool functionality includes the feature to update corresponding Multi-Cast Group (MCG) subscription data and Management Information Base (MIB). The UTO is part of the military TIMS (Tactical Internet Management System). The TIMS supports several complex tactical systems (e.g., FBCB2 / Blue Force Tracking / Land Warrior). These main situational awareness propagation systems apply workflow logic stored in APIs that are instantiated by scripts, defined by filters as implemented and broadcast by unicast / multicast IP groups supported by router/switches.

1.1.3 Common Alert Protocol CAP Child / Data Islands

XML repositories, NIEM, JXDM, DDMS, OpenGIS OGC, EDXL-DE formatted sets reference the: National Information Exchange Model - NIEM, Global Justice XML Data Model (Global JXDM), DoD Discovery Metadata Standard (DDMS), Open Geospatial Consortium – OGC. These repositories will provide XML tag repositories for the viewers / applications / browsers to formulate Common Alert Protocol – CAP schemas with Emergency Data Exchange Language Distribution Element (EDXL-DE) formatted messages with child schemas and / or DDMS formatted data islands to bridge emergency response threads between .mil, .gov, .com, .org domains. The Heartbeat K00.99 network configuration message initiates a sequence whereby other data dissemination messages are spawned stimulating operational, intelligence, logistics etc data cascades on the military side of the Heartbeat e9-1-1 equation.

A commercial equivalent heartbeat message is needed to instantiate emergency message data cascades on the commercial, organizational side of the equation. The Common Alert Protocol - CAP goal to provide "a standard method to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally and nationally for input into a wide variety of dissemination systems" must be designed in a manner that is backwards compatible with current FBCB2 / Blue Force Tracking equipped units and forward compatible with Future Combat Systems equipped units that both employ the heartbeat protocol and heartbeat XML network configuration messages for forwards / backwards compatibility. Expanding on the application of a Common Alert Protocol designed with child domain schemas / embedded with military DDMS tags to emulate the military notion of "stragglers" to suit commercial / Homeland Security domains by tracking organizations, units or high profile users. RFID tracked packages that stray from posted itineraries or routines are labeled as "stragglers". Stragglers on a Blue Force Tracking screen are shown as dimmed or grayed out icons as "stale" since they failed to report within established time limits.

Restructuring the Common Alert Protocol (CAP) by adding nested XML schema elements as data islands or derivative child domain CAP schemas are developed; the intent behind structured military messaging as driven by the TCP/IP heartbeat network reconfiguration process will be combined with a unified CAP structure or child structures to achieve a universal military / commercial, JIM (Joint Interagency, Multinational) domain "Heartbeat e9-1-1" service given North American Aerospace Defense Command – NORAD data is processed by the Public Safety Answering Points but not directly exchanged with the military fast movers (fighters) or air defense units. A recent Armed Forces Communications and Electronics Association's Signal Magazine article quoted a 30 second web page refresh rate accordingly – too slow for targeting and tracking purposes. The Common Alert Protocol child schema / messages Emergency Data Exchange Language Distribution Element EDXL-DE formatted standard may also include DoD Discovery Metadata Standard – DDMS elements as data islands in child schema or as data islands within the main CAP schema designed to trigger data exchange cascades / harvesting to / from disparate stakeholder domains (e.g., .mil, .gov, .edu, .com, .biz, .net, .org.). Aggregated state data elements derived from structured military messaging FFIRNs and FUDNs converted into equivalent XML tags in CAP XML (child) schemas will be parsed by commercial forms engines with intrinsic message parsers enabling the ability to resolve to the individual platform level (e.g, vehicle, plane, train) describing situational conditions symbolically e.g., "stale", "straggler", and under duress platforms of interest / commercial subscribers vice a general geographic area of interest as is the state of the current Common Alert Protocol – CAP OASIS standard that is separate and distinct from military equivalent standards.

The Common Alert Protocol – CAP equivalent of the Army's Unit Task Order - UTO heartbeat (field order) message described by the below table describes the key parameters that enable FBCB2-BFT and their commercial equivalent platforms to receive/transmit current active situational awareness data -- who, what, where, when, how often at a later time if platforms of interest (e.g., GPS equipped handheld, laptop or smart phones) conditions e.g., out of radio range, turned off, or down for maintenance or in a duress condition at the time of the initial or follow on heartbeat timed data collection interval (e.g., stale, straggler).

2. DETAILED DESCRIPTION OF HEARTBEAT e9-1-1

2.1 Topic: use of the TCP/IP Heartbeat protocol / Heartbeat (XML) message (OASIS Common Alert Protocol – CAP) schema(s) to implement a Homeland Security/Network Centric Warfare digital heartbeat.

2.2 Issue statement: Military situational awareness (SA) systems and Telco networks apply two common denominators: the TCP/IP heartbeat protocol and heartbeat (XML) messages --**DIFFERENTLY**. What if the DOD and the world's Telco networks agreed on common procedures based on these building blocks? Heartbeat e9-1-1 involves reapplying Network Centric Warfare (NCW) procedures commercially leveraging the world's network providers (Telco's) that provide up to 80% of a unit's leased network connectivity. The goal is to improve interoperability & operational synergy via direct message/data exchanges reapplying war tested operational procedures that update router/switch multicast group subscriptions linking DOD Situational Awareness systems/networks & Telco Public Safety Answering Points – PSAPs that apply regulations stipulating the use of the heartbeat protocol & heartbeat schemas.

2.3 Assumption: PSAP's processing NORAD aircraft tracks and DOD SA systems processing aircraft tracks do not directly exchange messages / XML schema's with each other Given that up to 80% of a unit's communications can be commercially leased, this implies that only 20% of a force's network centric warfare supporting assets (router/switches) are employing network centric warfare practices and that if these military assets were not available, soldiers would not be able to fight as they have trained nor would they be able to discuss an event "apples to apples, oranges to oranges" with First Responder counterparts given different OPTEMPO data collection / screen refresh rates and symbol sets.

2.4 Supporting Facts:

2.4.1 The widely adopted Emergency Management Network (EMnet) "Generates (Nadat) **HEARTBEAT** messages to maintain lost connections ... EMnet/EAS **messages** are delivered to broad casters within seconds using the secure satellite delivery system".

2.4.2 The C4ISR/Sim Technical Reference Model Sourcebook published by MITRE and VMASC with assistance from Northrop Grumman et al, page 13 describes the role of the heartbeat in context with C4ISR systems: 2.3.1.4.1 System Health/Heartbeat/Status: Definition: Information necessary to initiate and sustain a connection to a C4ISR system. Examples: "Ping" message to enable a system to transmit data. Heartbeat message to indicate the presence of a system; Keep Alive signals, Health & functional status messages... Physical Models: Models that replicate the physical characteristics of a system or entity, for example, range & bearing calculations, aerodynamics, and **aircraft systems simulations**. Relating this to like military systems such as Battlefield Airborne Communications Node (BACN), BACN is an Internet protocol-based airborne communications relay and information server that links radios and intelligence, surveillance, and reconnaissance systems for DOD networks. Flying at extremely high altitude, BACN extends the range of line-of-sight radios, relaying information to airborne and surface-based units, and, via satellite, to distant command centers".

2.4.3 "Network-centric warfare and other technological and economic developments are producing a burgeoning demand for commercially operated satellite communications. The Department of Defense's use of commercial satellites has grown from next to nothing a decade ago to heavy reliance now, with 80 percent of the satellite capacity used by the military in Operation Iraqi Freedom coming through commercial operators." See article in Military Information Technology.com:

3.0 GRAPHICAL DESCRIPTIONS:

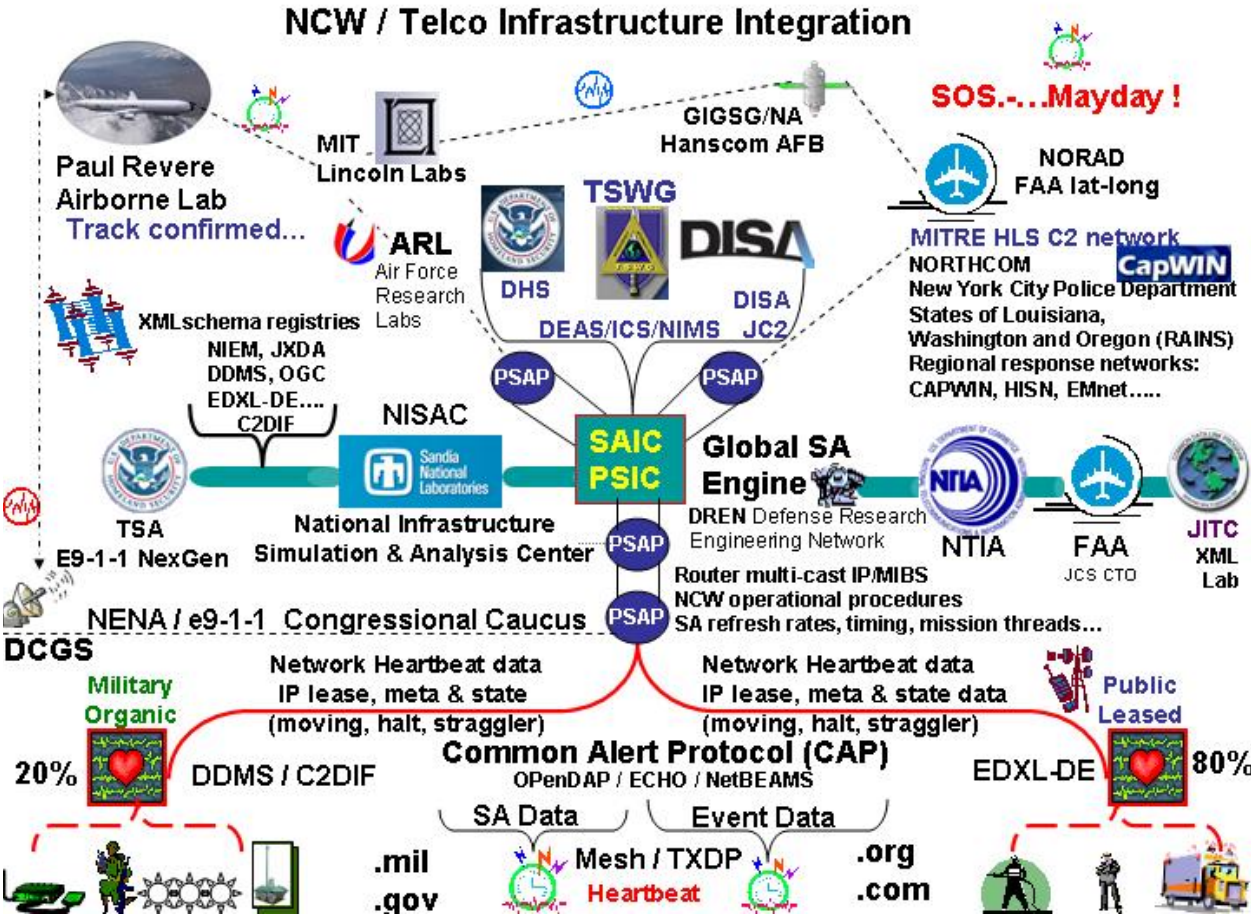


Figure 2: Simulation Scenario for Heartbeat e9-1-1

3.1 Simulation Scenario. The graphic above is a possible scenario to simulate the concept of fully commercializing the procedures of network centric warfare through the (inter) national infrastructure. Given the DHS is funding an infrastructure testing facility for NISAC – National Infrastructure Simulation and Analysis Center, the NISAC would be and probably is the infrastructure testing focal point.

3.2 Focal points of this example simulation scenario are SAIC's Public Safety Integration Center where the largest system integrators and the major telecommunication firms demonstrate their capabilities providing the infrastructure for n complex Homeland Defense / Security systems. DISA's DREN: Defense Research and Engineering Network is a research and development network provided leased from commercial telecommunication providers (i.e., MCI) applying state of the art equipment from infrastructure providers (Juniper Networks). The DREN has 120+ research and development organizations linked over a high speed, high performance computing infrastructure.

3.3 Incorporate TCP/IP heartbeat protocol timed network heartbeat harvested data formatted in Emergency Data Exchange Language (EDXL-DE) with DOD Discovery Metadata Specification (DDMS) XML tags standardized and derived from the various C2 and simulation (e.g Battle Management Language BML) and commercial standards as data islands in the CAP (child) schemas is the task at hand as pictured above..

3.4 Simulate the direct exchange of these XML structures between NCW systems & sensor net SA producers with Telco Public Safety Answering Points (PSAPs) for processing and onward delivery to SA consumers (high value targets / corporate stakeholders). Use the Common Alert Protocol via domain specific child schemas and / or by embedding DDMS or other tags as data islands in the CAP to cause data cascades / harvesting via military mission threads and the commercial equivalent business workflow logic is the depicted scenario's goal.

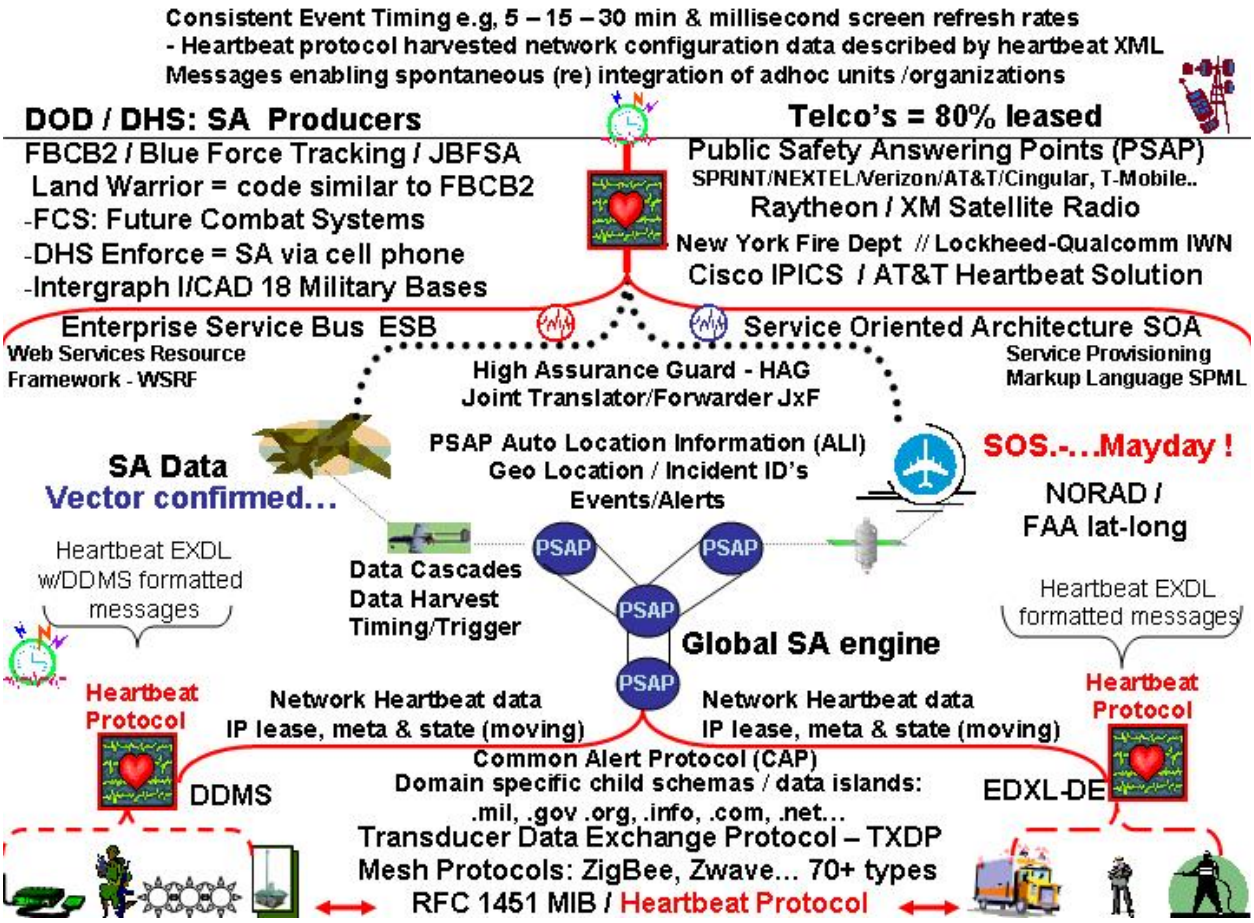


Figure 3: Direct Exchange of DOD & Telco Common Denominators: Heartbeat Protocol Harvested Network Configuration Data & Heartbeat Messages

3.5 The above picture describes the Heartbeat e9-1-1 concept where the TCP/IP Heartbeat is applied as the basis of a Homeland Security Heartbeat / Heartbeat e9-1-1 service in context with SAIC's Public Safety Integration Center (PSIC) during a live demonstration / simulation such as JEFX where the heartbeat protocol has been added to provide publisher and subscriber awareness. Direct message / XML schema exchanges between .mil and .com SA aircraft systems will improve interoperability and response times mitigating the reoccurrence of another 9/11 event by directly linking e9-1-1 and .mil systems. A demonstration in SAIC's PSIC involving a heartbeat protocol initiated failover of a military system that relies on military terrestrial / satellite communications to a commercial system that is also employing network centric warfare heartbeat protocol / heartbeat message set type procedures will demonstrate applying network centric warfare procedures applied to a unit / organization's entire communications portfolio instead of only the organic military assets thus increasing the power of network centricity while allowing soldiers to function as they have trained with their civilian First Responder counterparts in terms of OPTEMPO synchronized EAC screen refresh rates and similar symbolic views. (Simulation / Demo's scenario / goal), Hanscom AFB's Airborne Network Centric Warfare program / Electronic Service Center - ESC may be

willing to assist team SAIC (ARINC, Boeing, Northrop,…) since it has reviewed the scenario described (attachment) and has stated in July that it needed funding for the simulation to be moved up in priority (SAW Concepts interpretation of the MITRE representative's response). Hanscom AFB's ESC is conducting a Airborne Network Centric Warfare data relay exercise during JEFX that will do much to establish preconditions on the military side of the equation. The real time messaging middleware chosen for the Joint SAIC – Boeing Future Combat Systems program applies the heartbeat protocol as does TENA middleware protocol developed and required by the Department of Defense by SAIC / Object Sciences Corporation (acquired). The Joint Translator Forwarder JxF converts proprietary tactical data link messages (TADL) from proprietary to open system, non proprietary formats enables linking systems that track military aircraft and the public sector e9-1-1 NORAD track processing Public Safety Access Points (PSAPS) via direct data / message exchanges. This will improve 30 second web screen refresh rates that are too slow for targeting and fast mover tracking.

3.6 Network Centric Warfare / Public Safety Answering Point Integration Framework.

The graphic below describes how the heartbeat protocol and heartbeat XML messages as commonly designed by the various committees and organizations developing homeland defense / homeland security strategies could enable the sharing of data / workflows between the citizens of our homeland and first responders as consumers of situational awareness information gathered by our military(s). The heartbeat protocol and heartbeat XML messages as common denominators provide focus for interoperability and cross agency, organization, & stakeholder collaboration. The nearly universal heartbeat protocol as a low level data harvester, publish – subscribe & timing mechanism (2nd Claim Area) harvests & places network configuration data in files, queues, & object stores. Structured military messaging military unique field unit identifiers & field unit reference numbers (e.g., the time honored "FFIRNs and FUDs") once converted to equivalent XML tags in Common Alert Protocol CAP) child schemas / embedded data islands format (1st Claim Area), will allow nearly any commercial forms engine with an XML parser to parse / process them for delivery by any more advanced sensor / data transport mechanism (e.g., Microsoft's Groove or Biztalk or ZigBee, TXDP, OPenDAP, ECHO, NETBEAMS… etc) providing forward and backwards interoperability & standardization for both the military and commercial systems. Common operational tempo, symbology refresh to Emergency Action Screens will be possible across n complex systems.

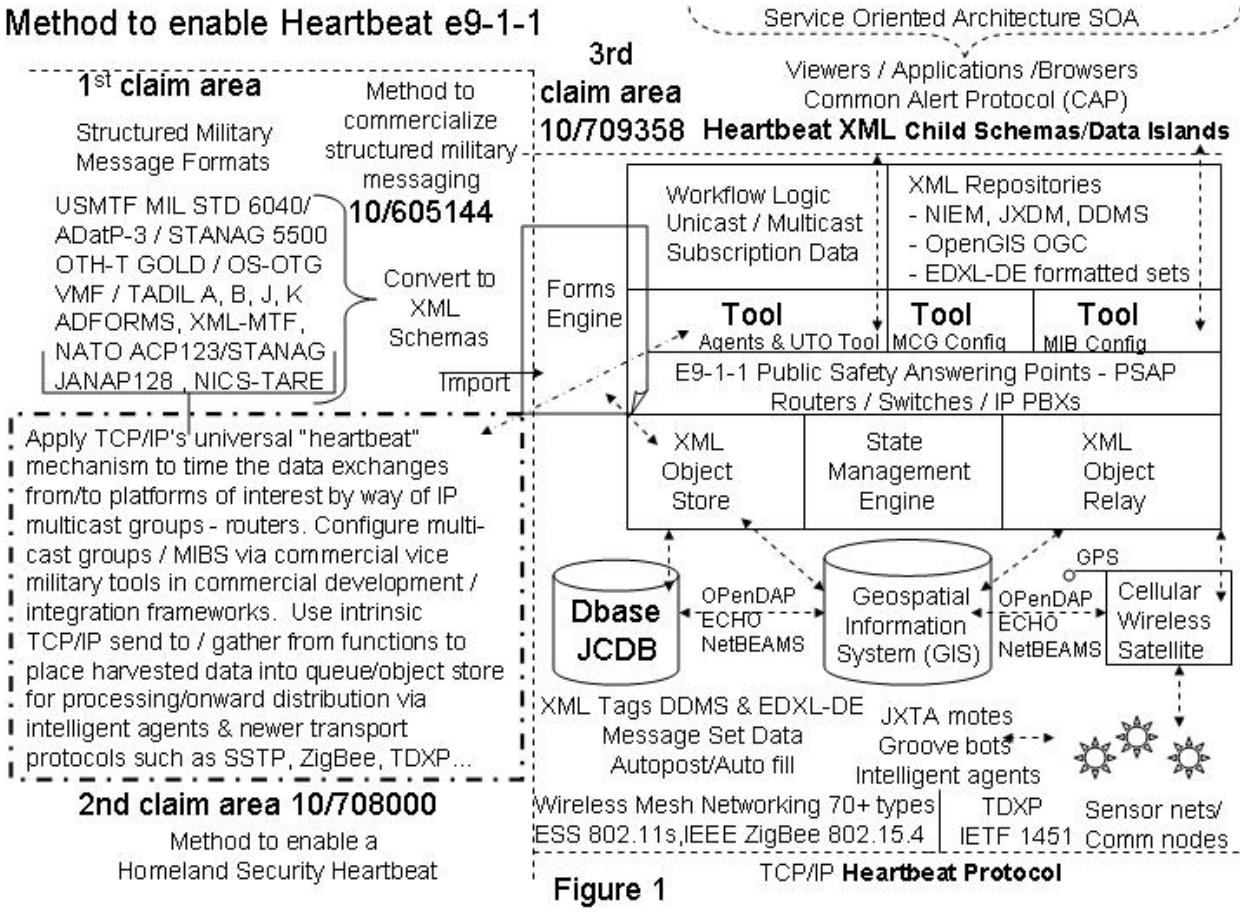


Figure 1

The heartbeat protocol and heartbeat XML messages as part of DISA's Network Centric Enterprise Services Technical Plan, Telco regulations, and bell weather IT firms, is a simple but effective means to improve interoperability. At the enterprise level, Service Oriented Architectures or SOAs implement a system wide heartbeat enabling failover, health status checks and reconfiguration of network assets applying network configuration data carried in Heartbeat XML messages.

4.0 Key cross over system integration opportunities

4.1 Common ARTS Air Traffic Control Systems

Automated Radar Terminal Systems (ARTS) manage air-traffic control at U.S. airport locations such as New York, Dallas/Fort Worth, Chicago, Southern California, and Atlanta. The Common ARTS program sought to develop a common software baseline at the Nation's Terminal Radar Approach Controls (TRACONs) and incorporate more COTS products. Thousands of tracks are supported, and so are hundreds of displays. Because Common ARTS is a safety critical application, a standby system is always ready to take control if any subsystem ever ceases to broadcast its **heartbeat** on the network. Programs are written in C language and run under the **LynxOS** RTOS.

4.1.1 Comparing the Air Traffic Control system with the Army's air to ground solution, "ICI's Improved Data Modem (IDM) is a communications and targeting system that can interface between the different communications formats in use by the U.S. Army and the U.S. Air Force. **A LynxOS** RTOS resides inside the IDM. Future plans called for incorporating in the IDM an embedded subset of the Army's Force XXI Battle Command, Brigade and Below (FBCB2) system software. Having the same operating system using the same formats will facilitate direct message / data exchanges between civilian and military responders.

4.1.2 Solution: With the DOD's use of the Heartbeat with the DOD's application of the heartbeat protocol & heartbeat messages; AFCEA's SIGNAL Magazine article "Defense Knowledge Management Hinges On Compatibility" By Robert K. Ackerman May 2005. "Using Web services technology and a laptop computer, these researchers separated the FBCB2 application from Blue Force Tracking data according to an established schema. An extensible markup language (XML) wrapper exposed the discovery metadata to a portal for updating every 30 seconds". The Heartbeat protocol and messages are part of Defense Information System Agencies Network Centric Enterprise Services (NCES) Technology Development Strategy Version Two dated 26 May 2004. The heartbeat protocol as part of DISA's Network Centric Enterprise Services Technical Plan, Telco regulations, and bell-weather IT firms public safety strategies, is a simple but effective means to improve interoperability leveraging the power of net centric warfare.

4.1.3 Analysis: Describing the above paragraphs from this same source document, the DOD's program that contributed greatly to the development of the network centric warfare concept: Force XXI Battle Command Brigade and Below (FBCB2) and its SATCOM variation Blue Force Tracking, soldier worn system Land Warrior and Joint variation JBFSA also rely on the heartbeat protocol and are moving towards implementing an entirely (binary) XML message payload vice the current hybrid military proprietary tactical data link (TADL) / XML header message / web server approach that provides 30 second refresh rates. In contrast, fast mover updates at the National Training Center in the Mohave Desert are required to be in the millisecond range that requires a constant stream of telemetry vice periodic web refreshes. From this same document describing air traffic control systems, ARINC cites the FBCB2 program and how its code was ported to the same OS (Heartbeat e9-1-1 is OS independent).

4.1.4 The point being made is that Air Traffic control systems and the DOD are already on the same page using common denominators or building blocks – with the caveat that OPTEMPO rates and schema structures are employed differently. The DOD's SA producing systems and the assets that they would work with and protect are poised to share data directly vice indirectly via data replication strategies or any number of middleware strategies. It is important to state here that DISA's Service Oriented Architecture (SOA) product (Amberpoint) employs an end to end heartbeat protocol, heartbeat XML message based system health monitor of the NCES runtime environment that it is offering to all other agencies. From foxhole to enterprise, the heartbeat protocol and heartbeat message schema exchange between DOD/military and commercial First Responder domains is clearly worth simulating to examine the potential increase of the power of network centricity and direct collaboration in response to mitigate the next (inter) national event.

4.2 Raytheon & XM Satellite Radio / Raytheon Global Communication Navigation Surveillance/Air Traffic Management services

4.2.1 Raytheon / XM Satellite Radio's approach is described by this magazine clipping "NYC Firefighters plan a military approach to command and control" ... By viewing information displayed as an electronic map, fire department commanders will be able to move firefighters, equipment and emergency medical teams around in much the same way military commanders shift troops and equipment around a battlefield".

4.2.2 Raytheon's Global CNS/ATM services areas of net centric operations, surveillance, navigation, communications, automation, and command and control (C2); border, transportation and critical infrastructure security cross fertilized with Raytheon's XM services as envisioned for (NYC) fire departments.

4.3 Super Bowl: During the super bowl, an approach to fuse sensor data was demonstrated by the 51st Michigan National Guard involving the Transducer Data Exchange Protocol (TDXP). TDXP uses IETF 1451 as a lower level transport that utilize Management Information Bases (MIBS) that make use of the heartbeat protocol for periodic state data updates. More modern protocols are being devised as well as current products / complex systems yet they still rely on the heartbeat protocol / heartbeat messages. Further, the maker of the cited product (Distributed Instruments) states that "TXDP was designed and built for a Service Oriented Architecture (SOA)" supporting direct interoperability between layer one and two (mobile, chaotic environments) with enterprise level SOA(s).

4.4 The Home Heartbeat as the "World's First Home Awareness System" by Eaton as a prime example of the technology backed by the ZigBee Alliance of 100 companies employing the ZigBee mesh networking protocol that makes use of the underlying heartbeat protocol that is a logical bridge to exchange situational awareness data with

the terrorist information producing systems that also make use of the heartbeat protocol. In addition to receiving alerts that a situation like washers overflowing or the garage door is left open when the occupants are scheduled away (an open invitation to terrorist activity), the owners and appropriate first responders can be alerted and situational awareness maps updated. Neighborhoods can be alerted in mass is say an airplane like the one that was downed in rural Pennsylvania is headed for a more populated area.

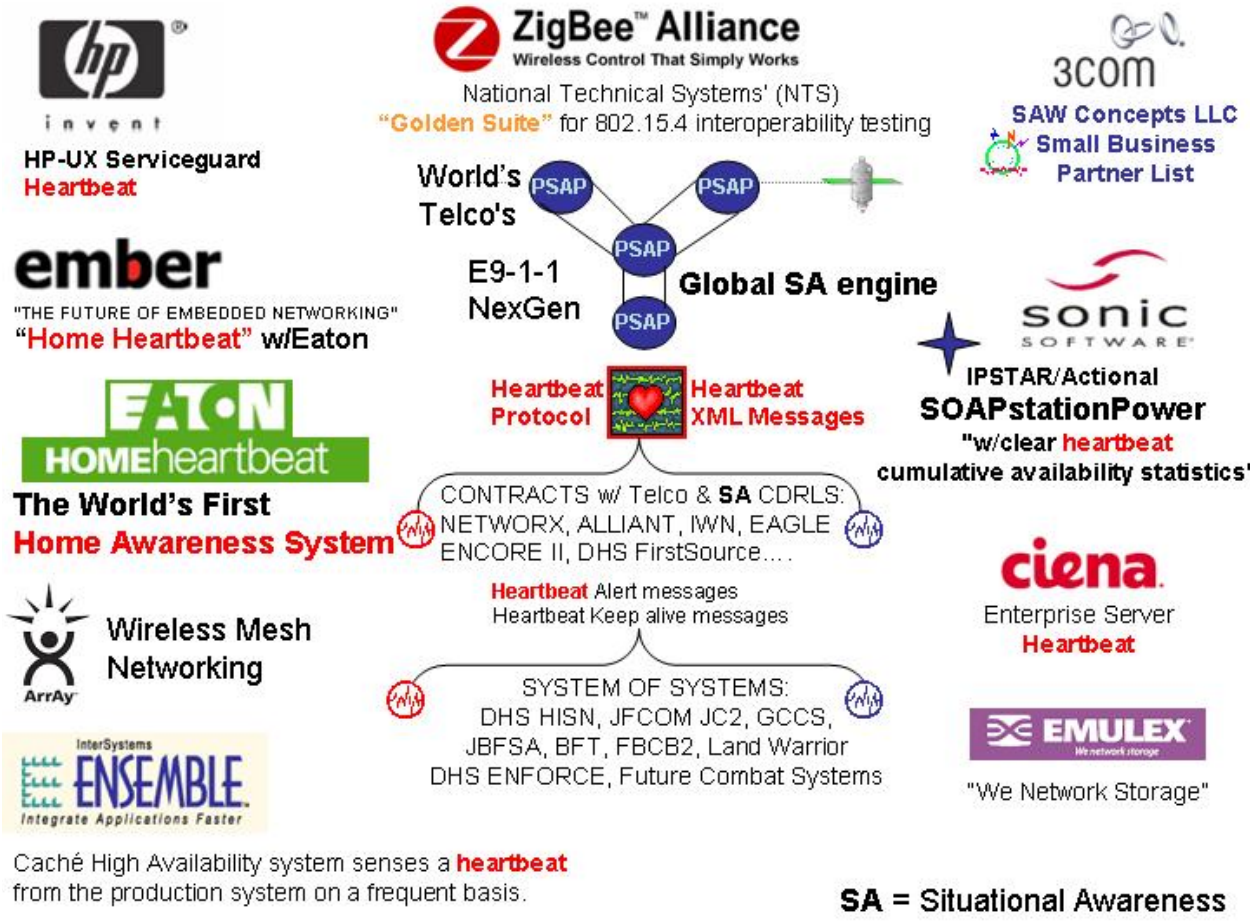


Figure 5: The ZigBee Alliance as commercial tech for the Homeland Security Heartbeat

The ZigBee Alliance / Telco E9-1-1 Public Safety Answering Points (NEXGEN) as interoperability standards bodies could work with military standards bodies such as the Joint Interoperability Test Center (JITC) both east and west to agree on Common Alert child schema's / data islands as required by both core federal / DOD contracts to achieve interoperability, symbolic commonality & operationally timed synergistic refresh rates thus providing a simple, efficient basis to enable the National Common Operating Picture (NCOP).

4.5 Motorola's Integrated Digital Enhanced Network (iDEN™): iDEN is a wireless communication architecture that applies "heartbeat" messages to send network status to maintain high system availability and other mission critical tasks that involve heartbeat XML messages sent internally. Motorola's architecture and industry leadership then is applied across the major carrier's networks Integrated Digital Enhanced Network (iDEN) wireless support for voice, data, short messages (SMS) and dispatch radio (two-way radio) in one phone. Channels can be divided six times to transmit any mix of voice, data, dispatch or text message. Used by various carriers around the globe, Nextel Communications provides nationwide coverage in the U.S.

4.6 AT&T has developed a movement detection process that it calls the "Heartbeat Solution." To implement this solution, AT&T has designed its VoIP telephone adapters to enable it to detect when an adapter has been disconnected and then reconnected. Once the Heartbeat Solution detects a reconnection, "the AT&T network will temporarily suspend the customer's service and will post a message at the customer's web portal directing the customer to confirm the existing registered location address or register a new location address." http://www.fcc.gov/ogc/briefs/05-1248-110805.pdf. Comparing the AT&T Heartbeat

4.7 General Motor's OnStar as originally named "Project Beacon" in 1994 as a global fleet broadcast system.

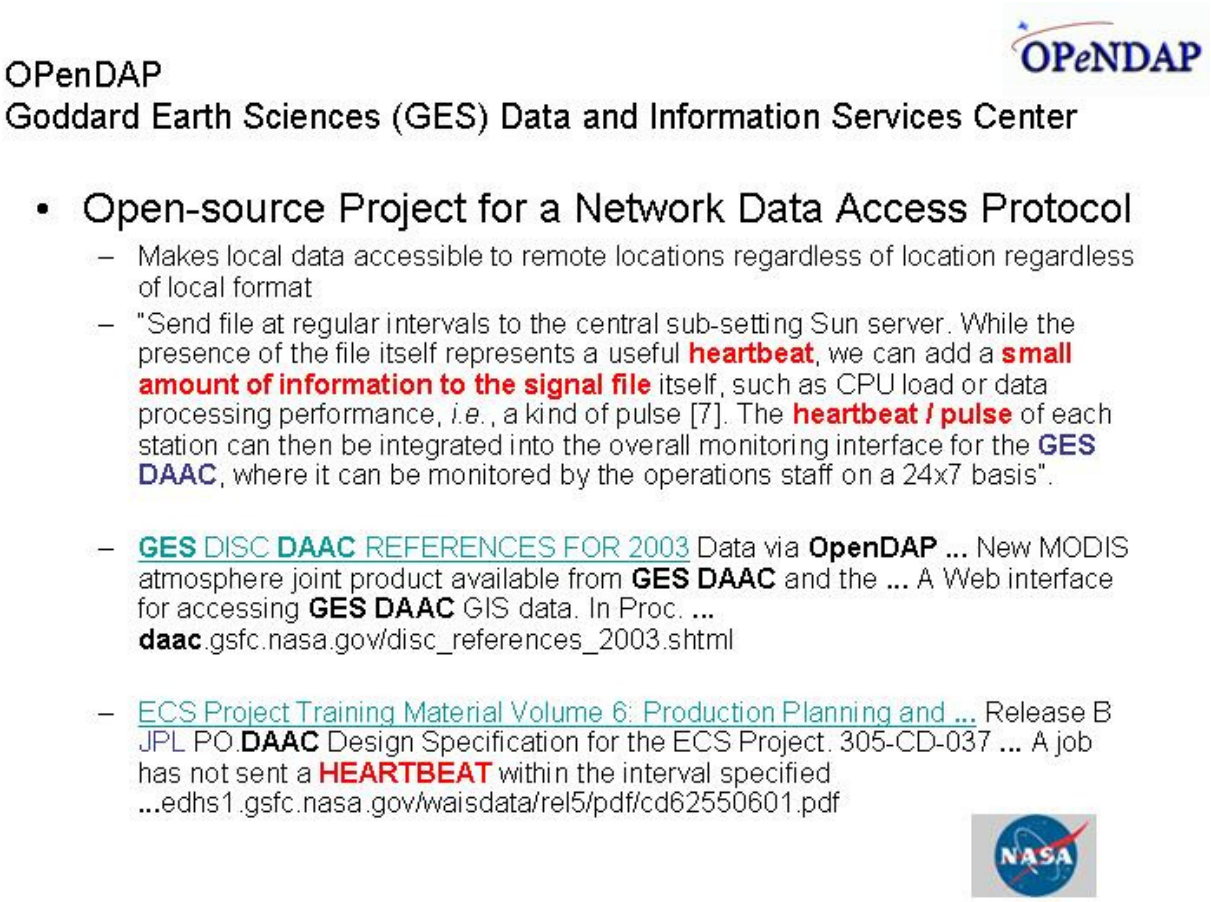
4.8 Cisco Systems IPICS Communications Interoperability and Safety Systems is "based on proven IP standards" "the Cisco IPICS server is monitored using a "heartbeat".. "IPICS software uses XML messaging schemas to identify types of communications devices managed by the system."

4.9 Juniper Networks DISA's DREN: Defense Research and Engineering Network is a research and development network provided leased from commercial telecommunication providers (i.e., MCI) applying state of the art equipment from infrastructure providers (Juniper Networks network configuration tool). The DREN has 120+ research and development organizations linked over a high speed, high performance computing infrastructure.

5.0 SUMMARY / RECOMMENDATION: Reapply Network Centric Warfare (NCW) procedures commercially leveraging the world's main network providers (Telco's) that provide up to 80% of a military unit's connectivity. Simulate from SAIC's PSIC, a Homeland Security Heartbeat / (inter) National Common Operational Picture (NCOP) to demonstrate system failover, improved interoperability & operational synergy by direct message exchanges & use of battle tested procedures to update router/switch multicast group subscriptions between DOD SA systems/networks and Telco Public Safety Answering Points or PSAPs & selected key events, programs e.g., JEFX06, Capital Wireless Integrated Network CAPWIN.

6.0 REFERENCE GRAPHIC: Heartbeat Protocol support NASA / JPL's OPenDAP

---------- NASA JPL OPenDAP / Heartbeat ----------



7.0 MILITARY ACRONYM TO COMMERCIAL EQUIVALENT

Military // Homeland Defense .mil	**Homeland Security, .com .org .gov**
Well-known multicast groups	Subscription service providers for .com, .org, .net etc by domains maintaining customer / subscriber / employee multicast groups
Doctrinal multicast groups	Multicast groups by domain segment or by formal agreement (e.g., transportation, security, users by type, service, agency etc)
Moving unit, gaining unit of action, platform tethering, untether ing to radio nodes / satellite on the move equipment	Platform or user / handoff subscriber node e.g., cell tower to tower. Satellite radio subscriber.
Command relationship (OPCON, attach), Unit of Action, Unit of Employment affiliations	Heartbeat 911 subscriber service, primary provider, affiliate provider, if roaming, affiliating, disaffiliating from cell towers
Effective Date/Time/Group (DTG) Block	Date / Time adjusted for Daylight Savings, world time zones
Synchronization Delta Time Block	Time when moving or traveling group executes network changes that change data distribution routes in supporting routers
UTR (U = Unit, T = Task, R = reorganization) command is broadcast to the entire net / subnet for execution	UTR = Unit Task Reorganization modified = Heartbeat XML network (re) configuration message sent containing data changing router Management Information Bases (MIBS) that change participation in multicast groups subscriptions reflecting organization structure. Enables military to join first responder nets and vice verse on an adhoc basis. Accounts for device mobility.
Affected platforms belonging to Moving Unit execute as per the Effective DTG.	Service providers router multi-cast groups change given organizational changes, user movements, pre-set time intervals
All others not affected execute at Synchronization Delta Time	Agreed upon time frame e.g., 5 seconds - 15 - 99 minutes for heartbeat protocol to harvest / refresh multicast subscriptions
The Heart Beat process incorporates the UTR command into the periodic Heartbeat message. This becomes the method by which “stragglers” or “stale” platforms re-affiliate / maintain network configuration synchronization	“Stragglers” i.e., Radio Frequency Identification Designation RFID tagged package(s), travelers, prisoners… not shipped / departed from a checkpoint or pattern is erratic. Deviation from schedule exceeding established parameters. Stale – no reports received for set periodic reporting period.
Task organization of the tactical internet Planning on when and what to change is critical to tactical maneuver / hasty reorg	Changing major network configurations based upon major events (Olympics), or anticipating major movements of subscribers (natural, manmade disasters), major corporate meeting

Table 1: Military unique awareness system attributes compared with commercial counterpart domains