Network Centric Warfare Requirements - A Live Collective Training Perspective

Paul Dumanoir
U.S. Army PEO STRI
Orlando, Florida
paul.dumanoir@us.army.mil

Rich Keller
Morgan Research
Orlando, Florida
rkeller@ideorlando.org

Wayne Koenig
U.S. ATSC
FT. Eustis, VA
wayne.koenig@us.army.mil

ABSTRACT

Meeting Network Ready Key Performance Parameter (NR KPP) requirements for DoD systems is the key to enabling effective Network Centric Warfare (NCW). The power of NCW is derived from the effective linking geographically or hierarchically dispersed knowledgeable entities that enable them to share information and collaborate to develop shared awareness, and to achieve a degree of self-synchronization. The net result is increased combat power that can be generated by a network-centric force. Net Ready KPP is about performance parameters for exploiting information to maximize combat power by bringing more of our available information and war fighting assets to bear both effectively and efficiently, and developing collaborative working environments for commanders and soldiers to make it easier to develop common perceptions of the situation and achieve (self-) coordinated responses to situations. For training systems, Net Ready KPP applications should focus on monitoring the Soldier networks to evaluate shared awareness, self synchronization, collaboration, and NCW. This paper describes perspectives and concepts of how the Net Ready KPP should be addressed for Live Training systems by enabling the training system to manipulate the “combat” situation to evaluate Soldiers and their systems. The paper describes different types of Global Information Grid (GIG) interoperability required to support “Live” training and simulation as well as Live-Virtual-Constructive (LVC) training events. The paper also discusses interoperability concepts from a System of System (SoS) perspective.

ABOUT THE AUTHORS

Paul Dumanoir is the chief engineer for Live Training Transformation (LT2) responsible for product line engineering of Live training range systems at U.S. Army PEO STRI. He has 19 years experience working in DoD simulation and training programs as project director and systems/software engineer. He is current interests include component-based product-line engineering, embedded training, and mission rehearsal applications. He earned his B.S. in Electrical Engineering from the University of South Alabama in 1987 and his M.S. in Computer Systems from the University of Central Florida in 1991.

Rich Keller is a Systems Engineer for the design and fielding of test and training instrumentation systems at the Combat Training Centers, Instrumented Ranges, and for the Operational Testers. He has designed instrumentation and analysis systems for casualty assessments, training evaluations, and platform performance along with the infrastructure for communications, computing, and interoperability with Tactical C4I systems.

Wayne Koneig is the Combat Developer for the Army's Live Training Transformation - Family of Training Systems (LT2-FTS) and is currently the Division Chief of the Live Training Support Division, TRADOC Program Integration Office - Live (TPIO-Live) at Fort Eustis, VA. His previous training experience includes 11 years military service in the Army, Training and Analysis Feedback (TAF) analyst at the Combat Maneuver Training Center (CMTC) and program management of training systems for the Combat Training Centers (CTC) Program. He earned his M.E. in Math and Computer Science from California University of Pennsylvania in 1988.

Network Centric Warfare Requirements - A Live Collective Training Perspective

Paul Dumanoir
U.S. Army PEO STRI
Orlando, Florida
paul.dumanoir@us.army.mil

Rich Keller
Morgan Research
Orlando, Florida
rkeller@ideorlando.org

Wayne Koenig
U.S. ATSC
FT. Eustis, VA
wayne.koenig@us.army.mil

INTRODUCTION

The Department of Defense DoD requires that all developed systems become part of the DoD enterprise Information Technology (IT) architecture. This requirement does not seek to define the architecture of individual processing systems but how processing systems empower users' easy access to information anytime and anyplace, under any conditions, with attendant security. Since the requirement is for access to information, the Global Information Grid (GIG) Architecture is the Department's IT architecture and all DoD information systems that currently exist or that have been approved for implementation comprise the GIG. Since each new IT-related acquisition program replaces, evolves, or adds new capabilities to the GIG, program managers should consider the existing and planned capabilities of the GIG that might be relevant as they develop their integrated architectures.

DoD training systems are considered to be part of the DoD enterprise IT architecture and have some level of interoperability with the GIG defined by the Network Ready Key Performance Parameter (NR KPP). This paper describes interoperability and NR KPP concepts from a training system perspective, in particular from the Live Training Transformation Family of Training Systems (LT2-FTS) perspective. It proposes how the Net Ready KPP should be addressed for Live training range systems by enabling them to manipulate the "combat" situation to evaluate Soldiers and their operational systems from in a training context. It describes different types of interoperability required by the LT2-FTS to support Joint "Live" training and simulation as well as Live-Virtual-Constructive (LVC) training events. Finally, it provides a high level interoperability assessment of the LT2-FTS, from a System of System (SoS) perspective, based on an interoperability assessment approach developed by a North Atlantic Treaty Organization (NATO) Industrial Advisory Group (NIAG) Study Group and latter enhanced by Lockheed Martin (LM) to mesh better with DODAF architecture views (Polzer, 2005).

BACKGROUND

Live Collective Training

Live training range systems provide the means to plan, prepare, execute and provide training feedback for Force On Force (FOF) and Force On Target (FOT) training. Live collective training exercises at these ranges are characterized by the following:

- Actual soldier/vehicle activity on actual terrain under simulated combat conditions.
- FOF weapon engagement with instrumented targets is via Tactical Engagement Simulation (TES) and FOT is with actual targets and Live fire.
- Position and tracking of training audience done through the Instrumentation System (IS),
- Training system allows analyst to link observations, events, and training reports to build Cause and Effect, and After Action Reviews (AARs).
- Training "Alerts" and safety "Alarms" can be triggered, for example, when soldiers/vehicles cross control measures and enter restricted areas.
- Human and IS implemented battlefield events produce real and simulated visual and sound effects (e.g., vehicle kill indicators, smoke, pyro, barricaded bridges, etc.).

Live Training Transformation (LT2)

LT2 is an Army initiative to develop a live training range product line that includes capabilities centered on a common architecture, known as the Common Training Instrumentation Architecture (CTIA), and common plug-and-train components called LT2 components (Dumanoir, Rivera 2005). The LT2 product line strategy is required to synergize training instrumentation, targets, and tactical engagement simulation systems to ensure the efficiency and effectiveness of training during peacetime, mobilization, mission rehearsal, and in-theatre during deployed military operations. LT2 products are composed using a "family of components" approach, which maximizes software reuse, provides common functionality, interfaces and standards. LT2 training systems will also provide interfaces to virtual and constructive training domain systems, the Army's Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR infrastructure systems, FCS platforms, and to components of the Joint National Training Capability (JNTC).

The Live Training Transformation Family of Training Systems (LT2-FTS) is the Army's family of interoperable live training systems based on the LT2 product-line strategy. The LT2-FTS domain includes the following Live training programs:

- Combat Training Center Objective Instrumentation Systems (CTC-OIS) (CTC-OIS, 2006)
- Integrated MOUT Training System (IMTS)
- Homestation Instrumentation Training System (HITS)
- Instrumented Ranges (IR) (IR, 2006)
- One Tactical Engagement Simulation System (OneTESS) (OneTESS, 2006)
- Future Army System of Integrated Targets (FASIT)

NetOps and NR KPP

NetOps is the operational construct that the Commander, U.S. Strategic Command (CDRUSSTRATCOM) will use to accomplish their C4ISR mission by operating and defending the GIG (DDoD 8100.1). NetOps enables Net-centricity by shifting the DoD from a "need to know" to a "need to share" paradigm. Net-centricity is the realization of a robust, globally interconnected network environment in which data is shared timely and seamlessly among users, applications, and platforms. The three tenets of Net-centricity are: (1) robust interconnections, (2) information sharing, and (3) shared Situation Awareness (SA). Net-Centric Operations and Warfare (NCOW) is the application of net-centricity to the activities of the DoD, both day-to-day business and warfighting. It's the approach to operations and warfare by which DoD will achieve the goals and objectives of Joint Vision 2020 (Joint Vision 2020). Net-centric Warfare (NCW) is an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision-makers, and Soldiers. In other words, the application of net-centricity to just the warfighting is "NCW". The four tenets of NCW are: (1) Net-Centric Enterprise Services (NCES), (2) Net-centric Data Strategy (DoD Net-Centric Data Strategy), (3) Information Assurance (IA) Strategy, and (4) Global Connectivity.

Compliance with the GIG means an information technology-based initiative or an acquisition program that has a NR-KPP. Meeting NR KPP requirements for DoD systems is the key to enabling effective NCW. The power of NCW is derived from the effective linking geographically or hierarchically dispersed knowledgeable entities that enable them to share information and collaborate to develop shared awareness, and to achieve a degree of self-synchronization. The net result is increased combat power that can be generated by a network-centric force. NR KPP is about performance parameters for exploiting that information. NR KPP maximizes combat power by bringing more of our available information and war fighting assets to bear both effectively and efficiently, and developing collaborative working environments for commanders and soldiers to make it easier to develop common perceptions of the situation and achieve (self-) coordinated responses to situations.

The NR-KPP replaces the Interoperability KPP, and incorporates net-centric concepts for achieving IT and National Security Systems (NSS) interoperability and supportability (DoD Directive 4630.5). The NR-KPP assists Program Managers (PM), the test community, and Milestone Decision Authorities (MDA) in assessing and evaluating IT and NSS interoperability. The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The following elements comprise the NR-KPP:

- Compliance with the Net-Centric Operations and Warfare Reference Model (NCOW-RM). The NCOW-RM describes the activities required to establish, use, operate, and manage the Net-Centric Environment (NCE).
- Compliance with applicable GIG Key Interface Profiles (KIP). These KIPs describe a standard of connecting to the Grid for critical warfighting interfaces.
- Verification and compliance with DoD IA requirements as defined by the DoD Information

Technology Security Certification and Accreditation Process (DITSCAP).

- Supporting integrated architecture products (DoDAF 2004) required to assess information exchange and use for a given capability.

Each of these elements brings different but complimentary products and attributes to Net Readiness. By complying with the Net Ready KPP, systems will be Net Ready when they reach production.

System Of Systems (SoS), Family Of Systems (FoS), And Interoperability

The Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01E glossary introduces the term Family of Systems and provides a definition for it and for System of Systems that are very similar to each other (CJCSI 3170.01E, 2005). In a Family of Systems, the individual systems have a significant role or capability independent of the other systems, while in a System of Systems the individual systems could only function in a severely degraded mode if the support/functionality of the other systems is not available. As the CJCSI 3170 distinction between FoS and SoS highlights, the degree of coupling or interdependence among systems is an important metric or scale along which to assess interoperability requirements and approaches (Polzer, 2005)

As Polzer points out, "Interoperability", as it applies to information systems means something in the specific operational context of both the systems involved and their users. While there are aspects of interoperability that may be viewed as context-independent, typically at the physical and network connection level, the exchange of information between systems has a purpose. As the following definition illustrates, that purpose is to provide some service to other systems and their users in order to achieve some operational task or objective.

"Interoperability is the ability of systems, units or forces to provide data, information, material and services and accept the same from other systems, units or forces and to use the data, information, material and services so exchanged to enable them to operate effectively together." IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchanged information as required for mission accomplishment

In figure 1, Polzer provides two types of distinctions that can be used to characterize interoperability approaches: (1) top-down versus bottom up, and (2) commonality based versus interactions based. Top-down approaches typically come at the problem from an enterprise architecture or broad scope perspective (and usually directive/mandate oriented) while bottom-up seeks to bring about interoperability by adoption of specific technologies or information representation standards. Another way of looking at top-down is having a specific organization's enterprise or mission objectives drive interoperability, while bottom-up is generally focused on technical approaches that are independent of the particular organization that might adopt them.

While contrasting top-down with bottom-up approaches is a useful distinction, there is another distinction that can be made. Commonality-based approaches focus on the execution environments of systems and try to achieve interoperability across a given enterprise scope by having every system within that scope adopt a particular set of standard elements for their execution environment. These approaches usually have a strong compliance component, although some are adopted by technology adoption dynamics and market pressures as much as by mandate, such as DNS and Java. The flip side of the commonality approach is the system interaction-based approach. This approach focuses on the space between systems rather than on what the execution environment might be inside a given system's boundary. In interaction-based approaches, no one knows what your execution environment is – it's a black box approach to interoperability.

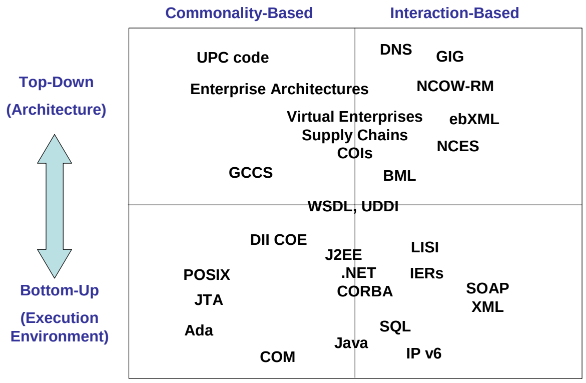

Figure 1. Common Approaches to SoS Interoperability

Polzer concludes that most actual programs will usually have element of all of these approaches. In areas where the program sponsor exerts some level of control, commonality-based approaches will apply, while in areas where interacting systems are under heterogeneous control, interaction based approaches will most likely be more appropriate and tractable. The concept of NR-KPP leans more toward interaction-based interoperability approach. One of the key elements that makes this concept work is the use of the NCOW-RM.

LT2 FTS INTEROPERABILITY

LT2-FTS is considered a Family of Systems that are bound by the use of common system components. Figure 2 provides a top level view of the different types of components, systems and architectures that interoperate with the LT2-FTS. Internally, all systems within the LT2-FTS a use client-server architecture, called CTIA (CTIA, 2006) which relies on the Common Object Request Broker Architecture (CORBA) as its main data distribution mechanism. All the plug and play training components (e.g. LT2 Components) use a common object model interface and set of services to achieve internal interoperability.

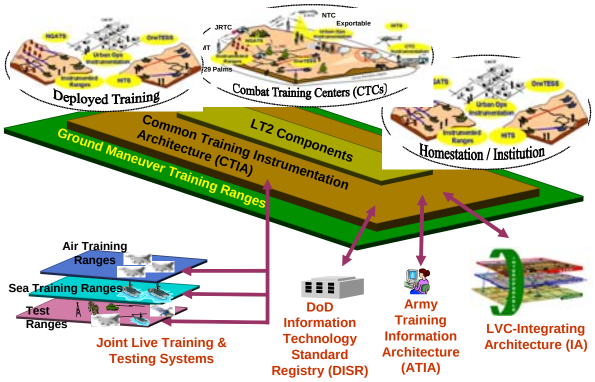
NTC
Exportable
JRTC
29 Palms
Deployed Training
Combat Training Centers (CTCs)
Homestation / Institution
LT2 Components
Common Training Instrumentation Architecture (CTIA)
Ground Maneuver Training Ranges
Air Training Ranges
Sea Training Ranges
Test Ranges
Joint Live Training & Testing Systems
DoD Information Technology Standard Registry (DISR)
Army Training Information Architecture (ATIA)
LVC-Integrating Architecture (IA)

Figure 2. LT2-FTS.

LT2-FTS interoperates with several external architectures and family of systems as well. One of those architectures is the LVC-Integrated Architecture (LVC-IA). The LVC-IA is a set of protocols, specifications and standards that support a seamless and interoperable, integrated LVC environment where common hardware, software and network components and modules are interchangeable with other LVC components and Battle Command Systems (BCS). The goal of the LVC-IA is to seamlessly interconnect and ensure interoperability with the JNTC, Joint Land Component Constructive Training Capability (JLCCTC), ATIA, CTIA, and SE Core. The LT2-FTS provide the "Live" domain capabilities for the LVC-IA and interoperate with the "Virtual" and "Constructive" simulation domains to provide a seamless Live-Virtual-Constructive (LVC) training capability for the Soldier (Dumanoir, Pemberton, Samper 2004) (LVC-IA, 2006).

Another key architecture which LT2-FTS must interoperate with is the Army Training Information Architecture (ATIA). When fully implemented, the ATIA will enable the provision of real-time training and training support to the Army worldwide (institutions, operational units, and individuals), through a logically centralized, physically distributed network (ATIA, 2006).

The LT2-FTS also implements key service areas, interfaces, and standards applicable to all DoD systems as defined in the DoD Information Technology Standards Registry (DISR). The DISR itself provides DoD systems with the basis for seamless interoperability. The DISRonline consists of a collection of web-based applications supporting the continuing evolution of the DISR and the automation of all its processes. It supports all aspects of the DISR from standards development to daily usage and compliance guidance using a web-based front-end. It provides general information for the DoD IT Standards Committee (ITSC), IT Standards Working Groups (TWG), and other DISR Communities of Interest (COI), as well as access to all versions of the archived Joint Technical Architecture (JTA) documents. In DISRonline, the JTA document was parsed and populates an Oracle database that serves as the back-end repository for all of the web-based applications. It defines the DISR services and standards applicable to all DoD information technology (IT) systems. The DISR is mandated for the management, development, and acquisition of new or improved IT systems throughout DoD. Standards and guidelines in the DISR are stable, technically mature, and publicly available.

The LT2-FTS also provides interoperability with other Joint test and training ranges through the Test & Training Enabling Architecture (TENA). The purpose of TENA is to provide the architecture and the software implementation necessary to enable interoperability among range systems, facilities, simulations, and C4ISR systems in a quick, cost-efficient manner, and foster reuse for range asset utilization and for future developments. The LT2-FTS integrates TENA middleware and a Logical Range Object Model (LROM) with the CTIA services to provide inter-range interoperability within a JNTC training environment. More information on TENA can be found in the Test Technology Symposium proceedings (2203).

LT2-FTS will also interoperate with the Family of Combat Systems (FCS) by embedding Live training capabilities in the FCS platforms and allowing them to interoperate while in LT2-FTS ranges or while deployed. Within FCS, the Warfighter Information Network-Tactical (WIN-T) provides C4ISR support for the Objective Force (OF), optimized for offensive and Joint operations. WIN-T replaces current Cold War-era communications architecture with the tactical GIG infrastructure. It will provide a new high-speed communications materiel solution, in combination with FCS, JTRS, and other supporting programs, spanning every echelon from Theater through UA. Since WIN-T employs a combination of terrestrial, airborne, and satellite-based transport options, it will be difficult to provide interoperability at each communications system level. Instead, we anticipate that training systems will interface to Command Post (CP) servers and interface at the data level achieving interoperability utilizing the NCOW-RM.

LT2 FTS INTEROPERABILITY ASSESSMENT

While there are several interoperability assessment approaches, this section focuses on the NIAG approach, as enhanced by LM (Polzer, 2005), and provides detailed perspectives from Polzer on each of the assessment dimensions. The three interoperability dimension categories that will be discussed are: (1) Net Ready Dimension, (2) Functional Capability Dimension, and (3) Technical Dimension Capability. For each of these categories a brief assessment will be made for the LT2-FTS to help formulate the conclusion of how the Net Ready KPP should be addressed for Live training range systems.

Net Ready Dimensions

Polzer maintains that Net Ready Dimensions, depicted in Table 1, help assess to what degree the system architecture and associated views for the constituent systems of a SoS map to the technical architecture views and standards. The Net Ready dimensions and levels are intended to capture the major characteristics of each system in a capability or system of systems as seen from the perspective of other systems on the network. The Net Ready dimensions measure system attributes that may support multiple capabilities. Typically these will be offered as services on the GIG that are built on top of NCES and COI-wide services by a given program. Such services will be made discoverable on the GIG by other systems and service providers through NCES discovery core services. However, even if the GIG and NCES services are not yet available to a given program, it can still be assessed based on the degree to which it offers discovery services on its own. So, if a system is isolated from the GIG for some acceptable reason, it can still be assessed as to its “net readiness”. Interoperability with training systems might be an example of this situation.

Table 1. Net Ready Dimensions

Level Category	Tighter Coupling / Less Net-Readiness			Looser Coupling / More Net-Readiness
Information Granularity	Complex obj ATO, Oplan	Record Level Mission, EDI	Data Element Standards	ASCII Text, URLs
System Arch Binding	Specific vend. Architecture	Industry open architecture	Netwrk based Interface only	Any IP net
Information Assurance	Link encrypt - SSL	Single signon support	DoD-Wide PKI support	MSL, cross-domain spprt
Service Discovery	Service specs pub at design	Service specs pub run-time	OWL spec for Services	Comparative service select
Service Evolvability	Version spec in interface	Multi-version support	Service specs extensible	Ops context aware interf
Tech Arch Life Cycle	Some current tech interfs	All current tech interfs	Some emrgng tech interfs	All emrgng tech interfs

LT2 FTS Net Ready Dimensions Assessment

The Information Granularity dimension represents the degree of pre-agreement and information representation standards compliance among the systems interacting on the network. Although LT2-FTS information requirements span from complex objects to plain text messages, it’s considered to have a looser coupling of information to external systems with which they are required to interoperate. In effect LT2-FTS have processing power, but recreating all the necessary protocols and interfaces to have a tighter coupling with external systems would be cost prohibitive and actually decrease its Net Readiness. As a matter of fact, Polzer states that a looser coupling is not necessarily bad in that it allows more flexibility in information exchange with other systems (e.g. web pages), but it also requires more processing power and sophisticated algorithms to extract a more formal information model from the information exchanged.

The System Architecture dimension assesses the degree to which the system interfaces are architecture-specific. This can range from the interface assuming all systems use a vendor-specific product or Application Programming Interface (API) set, to the interface assuming nothing but an Internet Protocol (IP) network connection. By using CORBA as its main data distribution mechanism LT2-FTS uses the CORBA Interface Definition Language (IDL) for APIs, and Extensible Markup Language (XML) for

Flexible/Extensible features. It's also a Transmission Control Protocol/Internet Protocol (TCP/IP) based open architecture. This would categorize LT2-FTS as possessing a low level of implementation architecture-specific systems interfaces.

The Information Assurance dimension spectrum implies greater information assurance awareness and enforcement at the individual interface and application service level rather than just at the "perimeter" of the network, on one side. On the other hand, network centric enterprise services have to be able to provide information services that allow application service implementation to understand access rights and enforce/enable them. For the LT2-FTS we have two approaches to IA for training. To insure that soldiers train as they fight, a training venue could provide the GIG in simulation mode. This will isolate the tactical GIG, and its security requirements, from the training application in a completely transparent way to the using units. The second approach will be to take advantage of NCES. NCES is based on a services-oriented architecture, and will apply Web services across the DoD enterprise. LT2-FTS can take advantage of NCES, allowing systems to integrate, consume and provide content to customers quicker than in traditional methods.

The degree of support for service discovery is another important dimension for net readiness. As Plozer points out, most systems "discover" services basically at design time. Even this primitive process is hampered by the lack of any DoD-wide "public" repository of service interface specifications. NCES Discovery Services will allow programs to publish their service interfaces and eventually permit run-time discovery of such services by other services to implement adaptive capabilities. Eventually, some services will become intelligent enough to select the most appropriate service provider for a given mission or capability instance at run time (point of use). Technology standards like Web Ontology Language (OWL) will provide enough information about services in NCES service directories to permit this kind of dynamic reasoning and coupling to specific services best suited to the users' current needs. Polzer asserts that Service Evolvability is closely related to Service Discovery, but is distinct and worth emphasizing separately from the discoverability of a service. This dimension measures how much awareness of service versioning is available in the service interface specification itself and to what extent the service interface definition itself is inherently extensible and operational context-aware. The key here is the NCOW-RM which will permit Net-Ready compliant systems to publish their data definitions and users to interpret the information without having to implement a precise interface specification or create a global data model.

Polzer's perspective on the Technical Architecture Life Cycle dimension indicate measures where the technologies used in the system service interfaces are in their development and industry adoption life cycle. A relatively mature technology such as CORBA is safer in the short run, but implies future lifecycle costs as it has to be replaced or adaptors have to be implemented to interact with new systems and services that will be made accessible on the network, such as web services and OWL. Polzer argues that programs that are adopting predominantly emerging technologies for service interfaces face higher risks in the short run, and greater difficulty in interoperation with legacy systems, but lower lifecycle costs in the future, assuming the anticipated emergence and maturity/longevity of these technologies actually occurs. LT2-FTS current implementation of CORBA allows it to reduce short term interoperability risk by using a mature and robust data distribution mechanism. CORBA will also minimize life cycle maintenance since it provides the interface isolation to maintain interoperability with emerging technologies. We hope that NCES will bring the same robustness to Web services being planned for future systems.

Functional Capability Dimensions

Functional Capability Dimensions help assess how well the information flows among constituent systems satisfy the operational architecture capabilities, independent of the specific technical architecture elements employed by the systems to implement the operational capabilities. Polzer maintains that the functional capability dimensions are the major focus of the JCIDS Functional Capability Boards (FCB), and reflect the specific system interface attributes that are needed to affect the full scope of the desired functional/mission capabilities. The two major categories of the functional capability dimensions are: (1) Capability Scope Measures/Levels, and (2) Capability-Specific Measures/Levels. The capability scope levels, depicted in Table 2, measure the overall scope of capabilities for the GIG, while the capability-specific categories characterize the key measures of functional/operational performance inherent in a desired capability. Polzer argues that while the latter measures are fairly well established in the capability development process, the capability scope measures are potentially more significant from system architecture and implementation cost perspective. The capability scope dimensions focus on making capability scope decisions that influence system interface requirements and have major impact on battlespace object representation and naming conventions. This in turn impacts the service interface specifications at the capability level as well as at the GIG/NCES level.

LT2 FTS Capability Scope Dimensions Assessment

As Polzer explains, the larger the overall scope, the more individual systems are likely to be involved in implementing the capability. This increases the challenge of defining the service interfaces and gaining consensus across all participating systems. In the case LT2-FTS, although the systems within the domain are focused on providing "Live training for Army ranges (e.g. single Service), they need to interoperate with other Multi-Service Live Ranges. LT2-FTS uses TENA protocols to achieve this inter-range interface.

Table 2. Capability Scope Dimensions

Level Category	Narrower Scope			Broader Scope
Overall Scope	Single Unit	Single Service or Agency	DoD-Wide	World-Wide
Enterprise Breadth	Single Functnal Domain/Service	Multi-Domain, Multi-Service	Multi-Dept, NGO, Industry	Coalition
Enterprise Depth	Single Level	Two Levels	Three Echelons	Four or More Echelons
Unity of SoS Ownership	Single DoD Acquis. Exec	Multiple DoD Acquis. Exec	DoD & US Syst. Owners	Multi-National Syst. Owners
Semantic Congruence	Single Domain Vocabulary	Multi-Domain Vocabulary	Single Language	Multiple Languages
Acquisition Congruence	All Systems on Same Timeline	Timeline within 2 years	Timeline within 5 years	Timelines >5 years apart
Information Domain	Sensor/Factual	Model-based (Cognitive)	Multi-model	Social Reality (Collaborative)
Operational Context	Single Ops Context	Multiple Ops Contexts	Future/Past Integration	Hypothetical Entities

Enterprise Breadth across which the envisioned capability is to be employed is a major sub-dimension that drives information representation and battlespace object naming standards, authorities and conventions. Cross-service and cross-functional domain information transfers create data interoperability and naming challenges, as do crossing enterprise, commercial/DoD, and multi-national scope boundaries. The LT2-FTS classification of this dimension is single functional domain since it currently encompasses a single Service – Army. This dimension might encompass a broader scope in the future if LT2-FTS are adopted by the U.S. Marine Corp and/or the Special Operation Forces for their ground maneuver training range needs.

Enterprise Depth dimension focuses on the levels of operational granularity that a given capability service must support. These might be called echelons or organizational tiers in various operational contexts. The key issue that this dimension measures is the number of aggregation and de-aggregation transformations that the service must support. Mapping battlespace representations across aggregation and de-aggregation levels create interoperability challenges. In addition, the same entities may be aggregated in different ways by different enterprise perspectives. LT2-FTS is at the narrower side of the spectrum when interoperating with systems within the LT2-FTS. The aggregation /de-aggregation scope becomes broader when it has to interoperate with constructive and virtual simulations to support LVC training environments.   A similar situation occurs when interoperating with tactical systems. Fortunately, we have been able to identify the granularity and generally focus interfaces at the "sensor" level.

Unity of ownership helps drive tight integration and interoperability. As ownership fragmentation across the systems providing a capability increase, the challenge of interoperability increases, creating pressures towards loose coupling and arms-length interoperability. From an acquisition perspective, LT2-FTS is managed by a single DoD acquisition agency so ownership fragmentation is not a risk. From a developer perspective, LT2-FTS fit at the narrower side of the spectrum since the system designs are generally under one developer's roof (High Unity of Ownership), at least from a Lead Systems Integrator view.

Polzer explains that the degree of semantic congruence across the systems and users of the collection of systems is another important driver of information model diversity. Some capabilities have fairly well defined and narrow semantics (eg, time critical targeting or air traffic control). Other capabilities, such as joint fires and maneuver tend to have a richer semantics both within the US force structure and across that of coalition partners. In cases of diverse semantics, the capability services need to accommodate this diverse semantics at the individual service provider level, or via a separate semantic translation service used by the participating services. The solution to this problem should be the NCOW-RM. If services define the dimensions of their data, we can choose to accept the data as presented and carry out our own translation or interpretation. With respect to LT2-FTS Joint interoperability we opted for a single domain vocabulary -the TENA LROM.

Acquisition congruence is similar to the technical architecture life cycle dimension, characterizing the degree to which systems contributing to a capability are on similar acquisition timelines. The greater the timeline divergence, the more of a challenge it is to make them interoperate. LT2-FTS dependency on TENA and JNTC LROM development is considered to be at the middle of the spectrum where timelines are within 2 years.

Information domain for LT2-FTS seems to be at the narrower end of the spectrum since it predominantly uses sensor data collected from the instrumentation devices, CP databases, or human interpretations of cause and effect to develop After Action Reviews (AAR).

The last capability scope dimension is that of operational context. Polzer asserts that systems using services that share their operational context are less likely to experience interoperability problems because battlespace objects exchanged will have similar or identical representations in their respective services. As we attempt to create capabilities that cross across operational context boundaries or even build bridges across alternate realities, for example, integrating planning data with exercise, training, and real world operation execution monitoring, the Operational Context could become dangerously confusing blurring the line between notional training data and real world tactical information. For this reason we propose that LT2-FTS remain at the narrower end of the spectrum for this dimension and keep all systems that interoperate with this Family of Systems within the live training range context. This means that we simulate the GIG with real tactical equipment but containing training data.

Technical Feasibility Dimensions

Polzer describes the Technical Feasibility Dimensions as a means to help assess the degree to which an operational capability is achievable given the technical architecture standards and constraints. In particular, these dimensions assess the degree to which the interface services between systems are technically feasible given the technical architecture constraints and resources available to affect the interface services. Table 3 presents technical feasibility as increasingly more challenging as one moves from left to right. This corresponds to the increasing impact on program or capability implementation cost and risk as one moves to the right.

Plozer asserts that a key technical feasibility measure is the degree of time-binding needed between systems to affect a capability. The tighter the time binding, the greater the demand on the technical architecture elements used to implement the interface service. Often the technical architecture elements make it infeasible to meet the time-binding needed to support a capability like time-critical targeting or ballistic missile defense. The degree of time-binding needed between LT2-FTS systems is at the second to millisecond level, making the technical feasibility a larger risk for that dimension.

Table 3. Technical Feasibility Dimensions and Levels

Level Category	Smaller Risk ◄			► Larger Risk
Inter-System Time Binding to Achieve Capability	Days	Minutes	Seconds	Milliseconds
GIG/NCES Resources Needed	Negligible	GIG-BE Capacity	GIG FOC Capacity	Beyond GIG FOC Capacity
Run-Time Computing Resources Needed	<1% of existing system resources	1-10%	10-50%	>50% of existing system resources
Interface Development Complexity	<1% of system size	1-10%	10-50%	>50% of system size
Technology Readiness Level for System Connections	TRL Levels 8-9	TRL Levels 6-7	TRL Levels 4-5	TRL Levels 1-3

Polzer goes on to explain that the "GIG/NCES resources needed" dimension is a resource requirement dimension needed by the systems involved to implement a given capability at some Measure of Effectiveness (MOE). Typically this would be bandwidth on some portion of the GIG network, but it could also be some service invocation rate for NCES or COI services. An initial assessment of this dimension for LT2-FTS has concluded to have a negligible need for these GIG/NCES resources since it will be running on a separate "training" network vs an operation network.

The Run-time Computing Resources dimension is a technical feasibility measure of whether a particular system interaction will require a significant portion of run-time computing resources of the current or envisioned systems. As technical feasibility becomes increasingly challenging, the resources required for a capability consume increasingly large portions of the overall system capacity. Currently LT2-FTS is implementing a high degree of scalability in the CTIA implementation to serve ranges of all sizes. The goal is to allocate system computing resources as needed to handle the interactions of entities on the range. The LT2 concept is also to provide common components to serve the family of systems. To be able to build on established technical solutions will lower the development risk.

Similar logic applies to the dimension of Interface Development Complexity, although this dimension is more an acquisition time concern than a run time concern. When an interface needed to affect a capability begins to dominate the development size of the system being acquired, sponsors may well consider it to be technically infeasible. They may also question whether the technical architecture assumptions might need to be re-examined and newer/alternate technologies and technology standards considered. LT2-FTS CTIA development of an open architecture with well defined common interfaces between the LT2 components and the CTIA services allows the technically feasibility of this dimension to have a lower risk.

The technology readiness level dimension applies in the case where an operational capability requires technical architecture elements that are not yet part of the JTA baseline. In other words, the capability is feasible if we relax the technical maturity level below production level. However, lower TRL imply added development cost and technical/schedule risks and thereby impact the feasibility of implementing a particular capability. Most, if not all of the LT2-FTS technical architecture needs are at production level TRL, thus reducing technical feasibility risk.

CONCLUSION

LT2-FTS is in the midst of defining an efficient and affordable Net Ready KPP compliance strategy that will allow the Soldier to "train as you fight". In order to do this we envision that Trainers would be interested in the GIG Joint Functional Concepts (JFC) that focus on the Net-Centric Environment (NCE) capabilities derived from the exploitation of the shared knowledge which is a critical part of both the Battlespace Awareness (BA) and Command and Control (C2) JFC, or basically the Common Operating Picture (COP). We believe that the technical aspects for achieving these capabilities for the training community can be solved as shown in this paper, especially since those solutions could be guided by the NCOW-RM. What we don't see to date is a "Net Centric Training Operations Reference Model" for the training community. This is data that can be derived from PEOSTRI experience in live, virtual, and constructive simulations but currently, no specific mandate exists to fund or implement this comprehensive model.

Why should we have a training reference model and a "training GIG"? First, let's ask: "can we consider using actual C4ISR mission data?" If we do, how do we meet the GIG IA requirements for integrity and non-repudiation of data and systems? The integrity capability ensures that data is protected from undetected or unauthorized modification or destruction and that those systems are protected against maliciously intentional or accidental changes to its configuration and resources. The non-repudiation capability provides for the timely and highly accurate ability to verify the identification of the sender and receiver of information and the authenticity of that information. But if data is modified as part of the training event, although not malicious, do we have, and does it make sense to have, methods to insure non-repudiation?

Secondly; we are designing our training systems to evaluate critical tasks while our future force is being asked to achieve Decision Superiority in force protection, force application, joint command and control, battlespace awareness, and focused logistics, based on information on the "Grid". We want the lowest level command to complete the mission by knowing how and what to "pull" from many sources of data. The GIG just makes the "pulling" technically possible – how does the trainer evaluate the "pulling the right stuff" part? -- Will the Net Ready KPP include the tactical Key Performance Factors?

So how does the LT2-FTS meet the NR KPP focus areas? Trainers can be observers of the trainees using the GIG in a limited way, or, the training system can be the source of the Global Information that is disseminated to the trainees and trainers can evaluate how well the trainees used the information provided as well as evaluating the tasks performed as a result of that information. We propose the latter is the more feasible and affordable solution for LT2-FTS, where Net Ready KPP should focus on monitoring the Soldier networks to evaluate shared awareness, self synchronization, collaboration, and NCW. Our proposed LT2-FTS training specific, NR-KPP compliance strategy is as follows:

- Focus on "knowing what the soldier is doing" during the "train as you fight" training exercise, but without having to join the C4I network or the GIG at the real mission level.
- Seek interoperability at the data level, by database query in a Local Area Network (LAN) / Wide Area Network (WAN) environment, i.e. become part of the COI both as a service provider and consumer.
- This strategy would mean that the training unit would be able to "plug-in" to a pseudo GIG provided by the range and train exactly as they fight.

Although there are several complex challenges ahead for achieving the proposed NR-KPP compliance strategy, LT2-FTS main objective will continue focus on providing a training solution that offers the desired seamless interoperability and ultimately affords our Soldiers a decisive edge during war by allowing them to train as they fight.

ACKNOWLEDGEMENTS

The authors wish to thank COL James Ralph, Project Manager Training Devices (PM TRADE) and Mr. Jorge Rivera, Assistant Project Manager LT2 (APM LT2) for their vision and leadership. Also thanks to Mr. Hans Polzer for his insight, perspectives, and expertise in the areas related to interoperability assessments.

REFERENCES

Army Training Information Architecture (ATIA) web site, retrieved 2006 from *http://www.peostri.army.mil/PM-FF/PO-CPC/atia.jsp*

CJCSI 3170.01E, Chairman of the Joint Chief of Staff Instruction (CJCSI), *Joint Capabilities Integration and Development System (JCIDS), dated 11 May 2005, retrieved from* http://akss.dau.mil/docs/CJCSI%203170-01E-Final.pdf

Combat Training Center-Objective Instrumentation System (CTC-OIS) web site. Retrieved 2006 from http://www.peostri.army.mil/PRODUCTS/CMTC-OIS/

Common Training Instrumentation Architecture (CTIA) web site. Retrieved 2006 from https://ssl.peostri.army.mil/CTIAPortal/index.jsp

DoDD 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), (2004)*

DoDD 8101.1 "GIG Overarching Policy", ASD(NII) (2002). Washington, DC. Retrieved from http://www.dtic.mil/whs/directives/

DoD Architecture Framework (DoDAF), Vol I, (2004, 9 Feb). Washington, DC: Department of Defense (DOD). Retrieved 10 Sep 2004 from http://www.defenselink.mil/nii/doc/DoDAF_v1_Volume_I.pdf

*DoD Net-Centric Data Strategy (*2003). Washington, DC. Retrieved from http://www.dod.mil/nii/org/cio/doc/Net-Centric-Data-Strategy-2003-05-092.pdf

Dumanoir, P., Pemberton, B, Samper, W (2004). *OneSAF Interoperability with CTIA – A LVC Connectivity Approach*. 2004 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), Orlando Florida.

Dumanoir, P., Rivera, J. (2005). *LT2- A Strategy for Future Army and Joint Live Training*. 2005 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC), Orlando Florida.

Instrumented Ranges (IR) web site. Retrieved 2006 from *http://www.peostri.army.mil/PM-TRADE/dmprc.jsp*

"Joint Vision 2020" (2000). Washington DC: Chairman of the Joint Chiefs of Staff. Retrieved from http://www.dtic.mil/jointvision/jv2020a.pdf

LVC-IA web site. Retrieved 2006 from http://www.peostri.army.mil/PM-FF/PO-UA/LVC.jsp

One Tactical Engagement Simulation System (OneTESS) web site. Retrieved 2006 from http://www.peostri.army.mil/PRODUCTS/ONETESS/

Polzer, H., Sr PM, Advanced Programs, LM. *Perspectives on Interoperability* presentation. Retrieved 2006 from http://www.dodccrp.org/iamwg/archive/04_08_05_Polzer_Perspectives_Interoperability.ppt

Washington, DC; U.S. Army Development Test Command (DTC). Test Technology Symposium (2003). *Test and Training Enabling Architecture (TENA) - The Foundation for DoD Range Interoperability*. Retrieved 4 Jun 2004 from http://www.dtc.army.mil/tts/2003/proceed/hudgins/