7th International
Command and Control Research and Technology Symposium
September 16 – 20, 2002
Quebec City, QC, Canada

Interoperability, Procedures and Standards

Framework for Achieving Joint Operational Interoperability

Submitted by
John E. Kirzl
Evidence Based Research Inc.
1595 Spring Hill Drive
Suite 205
Vienna, VA 22182

Framework for Achieving Joint Operational Interoperability

1. Purpose

The purpose of this paper is to describe a methodology that yields a consistent set of interoperable C2 functions to monitor, assess, plan, and execute in the environment.

Achieving Joint C2 interoperability presents several challenges. From a legacy standpoint, the existing fielded C4I systems are generally Service-specific and are not designed to be interoperable with systems of other Services. This situation is further exacerbated in terms of potential solutions in that Joint doctrine, CONOPS, and C2 architectures are still in the development stage, and requirements documents for systems in the acquisition pipeline generally do not address interoperability.

Joint Pub 1-02 defines interoperability as follows:

a. The ability of systems, units or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together.

b. The condition achieved among communication-electronics systems or items of communications-electronic equipment when information or services can be exchanged directly or satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases.

For the purposes of this paper, the interoperability definition is expanded to include the levels of services to be provided and accepted. It can be stated that C2 interoperability exists when the right information is provided at the right time to the right element, and, that information has the same meaning to the recipient as to the originator.

The type and nature of the information to be exchanged determines the degree or level of interoperability necessary for systems and/or equipment that facilitate information exchange. For example, if the information exchange requirements can be satisfied through the exchange of e-mail, this imposes quite a different set of equipment design characteristics than if the requirement is for the real-time exchange of complex graphics. Therefore, in order to describe the correct level or degree of interoperability required, one must first determine the information requirements of all the elements and their capacity to collect, transmit, and understand that information. This implies processing the data in such a way that the information provided is meaningful to the decisionmaker.

Later in this paper, the interoperability objectives are described which can inform the selection of the necessary levels of interoperability in terms of those objectives that, when achieved, provide the requisite interoperability.

2. Levels of Interoperability

The C4ISR Architectures Working Group, in its final report dated April 14, 1998, recommended adoption of the Levels of Information Systems Interoperability (LISI) developed by the MITRE corporation. The author first became aware of LISI when functioning as co-chair of the Ballistic Missile Defense Organization (BMDO) Theater Air Defense (TAD) interoperability working group. The working group felt that this would be a good tool in determining interoperability requirements.

The LISI model looks at interoperability with respect to requirements for information exchange where interoperability requirements can range from the simple exchange of e-mail to collaboration using multimedia information and common databases. LISI proposes five increasing levels (levels 0 – 4) of sophistication with each level providing an increase in capabilities over the previous level. Figure 1 depicts the five levels.

Level 0. Isolated Interoperability in a Manual Environment – this level comprises stand-alone systems with manual interfaces using manual re-keying or extractable media.

Level 1. Connected Interoperability in a Peer-to-Peer Environment – this level includes systems that can be electronically linked to provide simple exchanges of information. These systems are generally used for passing text e-mail or fixed graphic files such as GIF, JPEG, or TIFF images.

Level 2. Functional Interoperability in a Distributed Environment – this level includes local networked systems used to pass data sets from system to system. They include increasingly complex media exchanges.

Level 3. Domain-Based Interoperability in an Integrated Environment – this level comprises systems on a wide area network with multiple user-multiple access capability. Information can be shared between independent applications. Central or distributed data repositories may be shared.

Level 4. Enterprise-Based Interoperability in a Universal Environment – this level includes systems operating across a distributed global information space and across multiple domains. Multiple users can interact with complex data simultaneously using fully shared data and applications and advanced forms of collaboration.

LISI also couples the levels with the attributes Procedures, Applications, Infrastructure, and Data (PAID). For each level, the most salient of the PAID attributes is identified as a critical enabling function. At the strategic and operational levels (the focus of this paper) interoperability levels 3 and 4 are the most germane. For these interoperability levels, the PAID items Data and Procedures are the critical enabling functions. The Data attribute focuses on the information processed by the system. The Procedures attribute includes, among other things, overarching enterprise standards and architecture guidance as well as operational and functional program guidance. This paper is concerned with the information aspects of data and the operational portion of procedures.

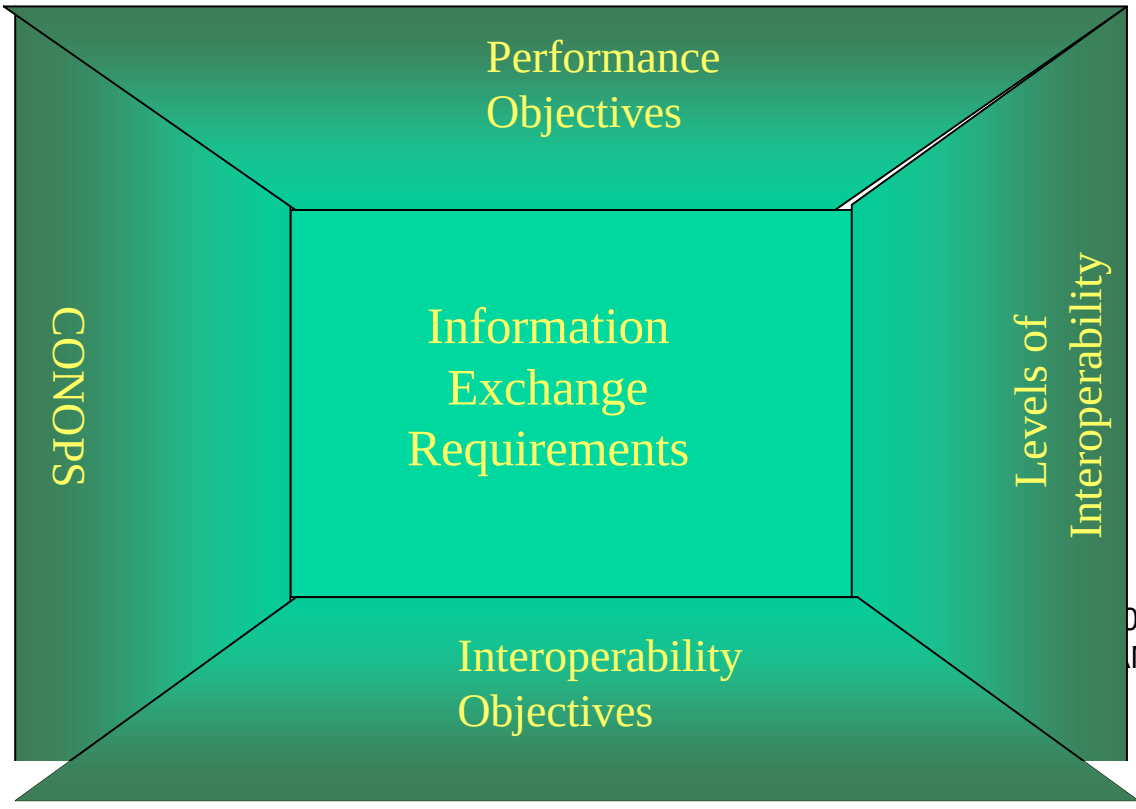
Information Exchange	Level
Cross-domain Information and applications sharing Advanced collaboration (Interactive COP update, event-triggered global database update)	4 Enterprise Interactive manipulation Shared data and applications
Shared databases Sophisticated collaboration (Common Operational Picture)	3 Domain Shared data “Separate applications”
Heterogeneous product exchange Basic collaboration (Annotated imagery, maps w/ overlays)	2 Functional Minimal common functions Separate data and applications
Homogeneous product exchange (FM voice, tactical data links, text files, messages, e-mail)	1 Connected Electronic connection Separate data and applications
Manual gateway (diskette, tape, hard copy exchange)	0 Isolated Non-connected

Figure 1. LISI Levels of Interoperability

It is not the intent of this paper to assign levels of interoperability to objectives, rather to provide high level objective functions and measures of success that can be used to specify information exchange requirements and levels of required interoperability.

3. Strategy/Methodology

The heart of the strategy for achieving interoperability is a methodology that provides for assessment of interoperability needs and an evaluation of interoperability accomplishments. This methodology is depicted in Figure 2. The methodology has as its backbone the information exchange requirements, starting with the operational concept from which are derived the C2 interoperability objectives and performance objectives. The



interoperability and performance objectives form the basis for evaluating operational performance.

Figure 2. Interoperability Methodology

The operational objectives are divided into four major categories: Common Relevant Operational Picture (CROP); Positive combat identification; Sharing intelligence and surveillance data; and Joint Planning. The effectiveness measures of these broad objectives can be simply stated as "providing the right information at the right time at the right command echelon." A set of performance objectives has been defined for each of the operational objectives and is couched in terms of information accuracy and timeliness. The associated effectiveness is determined by applying performance measures to Joint doctrine and TTP.

The functions that, when performed, achieve the performance objectives are characterized as:

1. Monitor the environment
2. Receive the information
3. Analyze the information
4. Decide what to do about it
5. Transmit the decision/order/alert/cue
6. Implement the decision (execute)

The systems that comprise a C2 architecture are characterized in terms of: monitoring, preprocessing, assisting in assessment and planning, post-processing, and implementing. Full systems interoperability is realized when there is a common infrastructure.

4. Strategy-to-Objective, Objective-to-Test (SOOT)

The SOOT process is a method that describes a thread from an operational concept through operational and performance objectives needed to make that concept work, to design and implementation of a systems or systems. The thread also proceeds through the testing cycle from component/system testing, through functional and performance testing, to objective and operational effectiveness.

The operational concept states what needs to be accomplished in broad terms. These broad needs are decomposed into a set of operational objectives, the accomplishment of which allows the concept to be carried out. For each operational objective a set of performance objectives is developed. These performance objectives are stated in terms that can develop into effectiveness and performance measures, and are complete. Once

performance objectives are agreed upon, in order to achieve them, a new system or systems must be designed, or modifications need to be made to existing systems. The resulting equipment must then be implemented in a battlefield environment.

This development strategy also provides the test community with a test and evaluation strategy. Each stage of the development cycle determines what needs to be evaluated for that stage and also defines success for that stage. Traditional testing provides for component and system testing during the development phase. This is followed by operational testing: does the system work as designed when placed in an operational environment? Operational testing would also provide an indication of the achievement of performance objectives and overall effectiveness. With the advent of sophisticated modeling and simulation capabilities, and by viewing the design development and testing process as a whole, it is possible to perform evaluations for any stage of the cycle prior to building of any systems. This allows for the determination of the effect of a change in a component technical parameter on operational effectiveness.

The C2 process is viewed in the context of its ability to produce the right information, at the right time, at the right place. The process can be viewed as a cycle whose commencement is the discovery of an event requiring an action to be taken, and whose end is the taking of some action or the decision to do nothing. (Note: The reporting of the results of the action could well be the start of another cycle.) This cycle comprises the functional areas of monitor, analyze, decide, and act. Each of the functional areas can also be viewed as a cycle that can be decomposed into smaller elements, each with its own cycle.

The C2 cycle can be seen as a continuum that comprises the other cycles. This continuum is called “overall cycle time.” The length of this time varies with the situation, however, it is bounded by threat actions and timelines. For example, if a decision to engage is made outside the time envelope required for a weapon to reach its target, that decision will be ineffective. Because of the different time domains involved, it makes sense to look at cycles from three perspectives, or levels of operation. The highest level, with the longest cycle times, is the theater or operational level. This level is concerned mainly with long range planning, and cycles at this level are generally in terms of weeks, days, and hours. The second level is the control level. This level is involved more in the day-to-day operations with cycles in terms of days, hours, and in some cases, minutes. The third level is the tactical or weapon/sensor level. This level is involved in the current battle with cycle times in the hours, minutes, and seconds range. As is readily evident, the timeframes for moving information around the battlefield are different for each level, as are the content and accuracy requirements.

The function of a C2 system is to facilitate the successful completion of these cycles through effective and efficient information exchange. The information to be exchanged has three main attributes: timeliness, accuracy, and relevancy. Information arriving at a

command must be received and understood in time for it to be acted upon; it must be of sufficient accuracy to permit the requisite action to be taken; and, it must be of interest to the recipient and in a such a form that it can be easily understood.

Interoperability can be viewed as an enabling function that increases battle management capability, flexibility and efficiency. It achieves this through the provision of more efficient and effective exchange of information. This increased information exchange capability leads to improvements in the performance of the decision cycles, both in the quality of the decision and the time required at all levels.

Interoperability will cause processed information to be made available sooner from a variety of disparate sources. This allows for either an earlier decision, or more time to refine the information, if required. This improvement in the cycle time results from a combination of two factors. First, the information is available earlier. Second, the accuracy of the information is improved by bringing more sources into play. The availability of more sources and more players does have a downside: information overload. The amount of information provided can exceed the capacity of the systems and/or humans to process it. The important factor, where information is concerned, is whether the information is timely, accurate, relevant, and is received in time to allow the commander to take the required action. This time/information requirement can be summed up as the requirement for the right information at the right level at the right time.

Interoperability needs to exist between the three levels: Strategic, Operational, and Tactical. It is required that, within the concept of operations, Joint and coalition systems can use the services of any other Joint or coalition system and be interoperable. This is necessary not only for systems at the same level, but also between levels.

5. Design, Development Process

The design, development process for C2 interoperability, applies the SOOT methodology to the specifics of C2. It defines the performance objectives and system/component technical parameters that are necessary to achieve interoperability. The process also includes the selection of evaluation methods suitable to the development phase and the scope of the test event.

The functional decomposition process of strategy to testing provides the operational effectiveness attribution and required ability to track information. Lack of interoperability at the systems and operational levels are reflected in a lower level of operational effectiveness in terms of detections, cueing, kills, etc.

Figure 3 depicts the SOOT development and testing process as applied to C2. The left side of the figure describes the design to build the process. The “strategy to function” process starts with the operational concept and works through operational objectives such as providing a CROP and providing positive combat identification, to the performance

objectives for achieving the operational objectives. The design development process includes the design parameters to provide for event detection, transmission and receipt of information, the ability to analyze the information, decision support functions; and the implementation of common hardware, software, symbols, and messages. The right side of the figure depicts the testing hierarchy, starting with component and systems testing to determine the degree of commonality achieved at the technical level, proceeding on to performance testing to determine the timeliness, accuracy and completeness of the information provided. Testing is conducted to determine whether the operational objectives have been achieved, and that the required information is provided in a timely manner to (and understood by) those who need it. Operational effectiveness includes the force effectiveness measures such as kill ratio, event cycle time, and cost-benefit measures. The interoperability test and evaluation methodology makes use of modeling and simulation techniques to allow evaluation to take place at any phase of the cycle, thereby enabling the evaluation of concepts and/or system parameter changes without having to design and build the systems first.

The interoperability test and evaluation process should provide a means to test, evaluate, compare, and integrate disparate C4I systems and their use. The legacy systems were generally designed to meet Service-specific requirements, and not necessarily to interoperate with systems of other services. These systems will, however, need to operate in a Joint environment and will be required to interoperate to some degree with each other. The evaluation methodology needs to account for this requirement for varying levels of interoperability to ensure that an accurate assessment of interoperability shortfalls can be accomplished.

The evaluation process should be comprehensive enough so that, when individual or combinations of systems are evaluated in accordance with the methodology, a passing grade means that the systems are, in fact, interoperable.

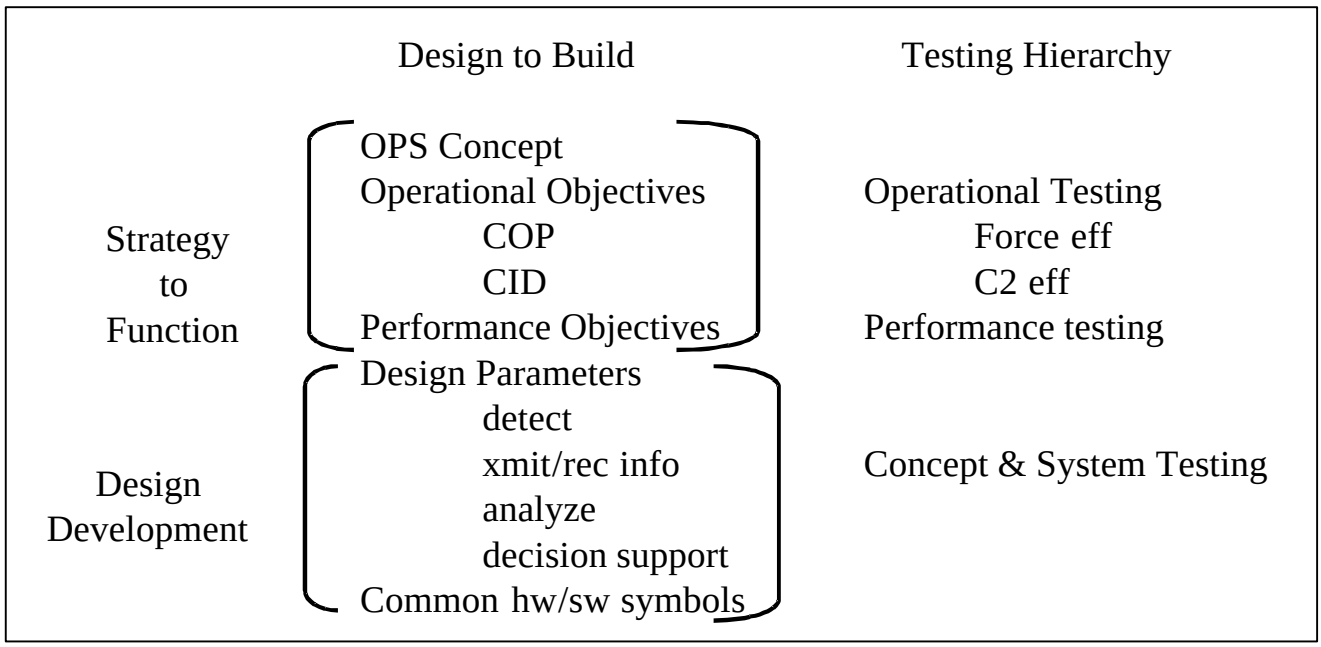


Figure 3. SOOT Development and Testing Process

The initial goal of the interoperability evaluation process should be to establish measurable benchmarks, against which to determine the need for, and the actual benefits realized, from the introduction of new and/or modified systems. With adequate benchmarking, a workable migration plan to an interoperable suite of systems can be developed.

In designing a plan for test and evaluation there is a logical sequence of steps that must be followed:

- A logical model is needed to guide the Services in the development of new systems. This model should be applicable across the full spectrum of C2 operations and systems.
- Evaluation criteria must be specified for the required level of interoperability. These criteria must be relevant to the tasks that need to be performed by the systems users and their information requirements.
- The evaluation criteria must be measurable, and must state the values that indicate success.
- Test designers must know what technical parameters have to be specified for two systems to be interoperable at the required level

Interoperability performance testing can take the form of measurement, in which performance measures are taken during actual operations or exercises, simulation, which is the use of models and automated tools to determine performance, and analytic modeling which uses analytical methodologies and mathematics to determine performance

6. C2 Objectives/Sub-objectives

A primary consideration of the Interoperability Technical Panel was to develop a process that coupled system and operational interoperability to command and control interoperability and hence, operational effectiveness. A coupling of operational effectiveness to technical performance parameters provides a traceable means to relate system and system to system performance to user needs. A set of operational

interoperability objectives was developed to provide the process with the required coupling mechanisms.

These operational interoperability objectives were then decomposed into more definitive sub-objectives that can be related to or transformed into functional and system level test objectives and MOE/MOP.

In consonance with the Concept of Operations, the Interoperability Technical Panel developed the following Operational Objectives.

6.1. Objectives For Common Relevant Operational Picture

There is no single picture that has attributes to meet the needs of all users at all times. However, the data that each user accesses to paint the picture must be consistent across all users. Access will be provided by "information push" processes where information needs are pre-established, and/or by "information pull" where information needs are not pre-established.

6.1.1. Units can contribute any relevant data to the CROP

Information that is sensed or derived, that has value to other units, should be made available for sharing with the timeliness and quality appropriate to its application.

6.1.1.1. Determine the desired content, fidelity, and timeliness of the information that will be produced and transmitted by these sources.

Each node will have different requirements for information depending on the tasks it is performing and the level at which it is operating (e.g., theater, operational, or execution).

6.1.1.2. Determine the sources of information from which a CROP will be built.

There are a myriad of sensors and observers on the battlefield. Not all will have data relevant to the CROP.

6.1.1.3. Provide capability to add locally derived information to displayed picture.

Each node will have information sources that are not participants on the C2 nets. Some of this information will be of purely local interest, but should be part of that node’s picture. Each node should have the capability to include this information on its display, and to insert it into the applicable net if relevant.

6.1.2. Units have access to all relevant data as needed.

Relevant data can come from both organic and non-organic sources.

6.1.2.1. Relevant data must meet user mission requirements to include:

a) Timeliness (latency)

b) Accuracy

c) Update Rate (frequency)

d) Fidelity

e) Content

f) Granularity

6.1.2.2. Determine whether or not these C2 nodes have the necessary hardware and software to receive the information from which a CROP will be built.

6.1.3. Units can correlate and aggregate data so that no ambiguity exists between units.

One of the most difficult problems to solve for the CROP is that of multiple INPUTS on a single entity, or entities not reported because the entity is erroneously thought to be one that already being reported.

6.1.3.1. Ensure that C2 nodes must have a common geo-spatial reference when coordinating with others on CROP information.

Units need to know accurately where they are with respect to other units and to common reference points, for correlation to be successful.

6.1.3.2. Determine which information, when received from the network, needs to be correlated with organically produced data before it is displayed.

Some organically produced information will be on entities not part of the CROP, and some will be part of the CROP. Units need to know which ones need to be correlated with existing entities.

6.1.3.3. Establish procedures for correlating organically produced information with similar information already on the network to preclude redundancy of transmissions.

Specific procedures are necessary to ensure that this task is performed correctly.

6.1.3.4. Determine whether or not the information sources have the necessary software and hardware to do the necessary correlation and once accomplished, produce and transmit the required information in the required format.

6.1.3.5. Determine procedures for proper correlation.

6.1.3.6. Determine whether or not the necessary software is available to accomplish the required correlation.

6.1.3.7. Provide capability to communicate decisions (or disagreements) regarding the supplied picture when it is different from locally derived information.

This will allow an operator who perceives a discrepancy between what is being reported over the network and what is being reported by local organic sensors to alert other network participants to this discrepancy.

6.1.3.8. Employ a consistent identification labeling process, regardless of what source provided the initial information.

This will preclude problems arising as a result of different labeling schemes.

6.1.4. Management

Authority for managing common battlespace information will be placed at organizational levels appropriate to the process of fusion, integration, and association.

6.1.4.1. All nodes must receive common battlespace data from which they will tailor to meet their needs (e.g. status and location of resources, readiness, engagement zones, etc).

Nodes have different requirements for what they want to display. Provisions for a consistent picture should include the ability to access the data required to develop the picture.

6.1.4.2. Objects in the CROP must have an appended file (drill down) describing as much information about the object as is known with indication of degree of confidence in the information.

This information is necessary to provide the required level of confidence in the veracity of the information.

6.1.4.3. Display must be flexible so that "layers" of filters can be applied.

This is necessary to prevent cluttering the screen when large numbers of objects are present.

6.1.4.4. Establish the lowest level where changes can be made to the CROP. (who can modify the CROP?)

There needs to be strict rules for who has authority to change data that is used to develop the CROP.

6.1.4.5. Local C2 nodes should be capable and not denied capability to manage local displays.

Each C2 node needs to be able to control the information used to produce the display.

6.1.4.6. Rank order for these sources and determine a hierarchy to ensure "correct" picture.

A scheme is required that allows the system or a data manger to determine what inputs to use when multiple sources are reporting the same events.

6.1.4.7. Establish guidelines to ensure information provided does not saturate users.

The quantity of information available will be more than enough to overwhelm a command if intelligent filtering is not performed so that only relevant information is presented.

6.1.4.8. Develop and implement a Joint training program that mandates techniques and procedures for developing a battle space picture.

In order to ensure that all commands operate from a consistent battlespace picture, the techniques for developing and displaying this picture need to be standardized.

6.2. Objectives for Combat Identification

Satisfaction of this objective will provide all units the ability to differentiate friendly elements and threat targets

6.2.1. Determine requirement for the passing of combat ID information among participants (i.e., who should have the capability to do combat ID, timeliness of information).

6.2.1.1. Determine nodes/commands/participants who have responsibility/authority to make ID determination.

6.2.1.1.1. Establish criteria for what constitutes positive ID.

All units that input ID data use consistent criteria for determining ID.

6.2.1.1.2. Determine at what level IDs can be changed and who has the authority to make those changes.

6.2.1.1.2.1. It is imperative that all concerned understand how ID is assigned, how it is changed if need be, and who has authority to make what type of changes.

6.2.1.1.3. Ensure that declaration of ID has a "confidence level" associated with sources.

A confidence level designation is necessary so that the assignors of ID can make a proper determination.

6.2.1.1.3.1. Determine organizations that require confidence level.

Once ID is assigned by appropriate authority, confidence level is superfluous and could cause screen clutter (i.e., shooters don't need confidence level).

6.2.1.1.3.2. Transmit source of Identification as a label with track data. Source should include C2 node and identification method.

6.2.1.2. Establish methodology for evaluating various combat ID TTP based on benefit, accuracy, and risk incurred.

6.2.1.3. Ensure units have a minimal capability to display CID information (not necessarily mandatory that they possess advanced identification systems).

C2 nodes with CID need to be able to correlate that data with local sensed data and provide to network participants.

6.2.1.4. Evaluate security issues.

Combat ID techniques can disclose information to an enemy that one would prefer to remain hidden.

6.2.1.4.1. Provide C2 networks the capability of operating at security levels that allow participation in Intel source feeds or develop a multi-level secure system that can appropriately provide and deny certain track label information.

For Joint and coalition operations, participants will have different access privileges, requiring procedural and system safeguards to protect sensitive information.

6.2.1.4.2. Develop safeguards to prevent corruption of Combat ID by enemy countermeasures.

Deception and imitative techniques are likely to be employed by an enemy. Systems must be able to detect these tactics.

6.2.1.4.3. Ensure source identification can be removed to allow transmittal at proper security level (sanitization).

This needs to be done to protect sensitive information sources from compromise.

6.2.2. Develop tailored combat ID and threat assessment systems and procedures to support each unit force level.

Different command levels will have different requirements for CID information (e.g., a sector control center's requirements will be different than an engagement/maneuver unit).

6.2.2.1. Develop correlation algorithms for combining of ID data from various sources.

The time constraints make it an impossible task for a human to assimilate the CID expected to be available from various sources and the associated confidence levels. Automation of the process is necessary to ensure timely assignment of ID.

6.2.2.1.1. Develop common algorithms.

6.2.2.1.2. Develop data elements.

6.3. Objectives for Sharing Intelligence and Surveillance Data

The requirements for sharing intelligence data are different than the requirements for surveillance data. Therefore, they are treated separately.

6.3.1. Share Intelligence Data

C2 nodes will disseminate and receive existing intelligence as needed, including information from organic, non-organic, Joint, national, and non-military sources.

6.3.1.1. Determine types and content of information required by users.

Not all users require the same information, nor could they assimilate all the available information.

6.3.1.1.1.Determine providers and users of national intelligence data.

This is a logical first step in any information requirements determination. Who needs the data and where does it come from?

6.3.1.1.2.Tailor data to show intent at higher command levels, while supporting execution at lower echelons.

Higher echelons are more interested in long range planning and therefore need information as to enemy intentions, while execution echelons need information describing what the enemy is doing.

6.3.1.1.3.Generate process for converting intelligence into a form understandable by tactical users

Intelligence information comes in many forms, some of it highly technical. This needs to be provided to users in a manner that is relevant to their situation.

6.3.1.1.4.Develop Joint theater intelligence databases with real time update capability.

Updated databases would allow users to obtain information without having to request it from a collection agency.

6.3.1.1.5.Determine time requirements.

Not all information is required within the same time frames and not all users need information at the same time.

6.3.1.1.6.Define what non-military information is desired.

With the plethora of information in the non-military world, a methodology is required to determine what subsets of that information needs to be collected and analyzed

6.3.1.1.6.1.Identify methods for sorting non-military data to avoid over-saturating the operators with information.

6.3.1.2.Determine fusion and correlation requirements.

6.3.1.2.1.Use data on different platforms in the same way.

6.3.1.2.2.Append (tag) intelligence data to objects for unambiguous association.

6.3.1.3.Develop information management procedures.

Networks must manage information in addition to connectivity in order to ensure nodes with interests in intelligence data receive the data not knowing in advance that the data are available

6.3.1.3.1.Determine who can input and who can extract data, and in what standard format.

This is a critical net management issue. Control needs to be maintained over the networks to prevent saturation and redundant reporting.

6.3.1.3.1.1.Establish processes for a user to quickly request and receive intelligence data from sources that do not routinely provide information to those users.

Instances will occur when sensors are in position to collect and provide data of use to users not in their usual reporting chain

6.3.1.3.1.2.Develop procedures to alert friendly forces that are in proximity of projected threats that they are at risk.

This area requires careful study. A balance needs to be struck between ensuring that all commands that could be affected are warned in a timely manner, and avoiding the taking of needless protective measures by those not affected.

6.3.1.3.1.3.Establish protocol for informing potential users of the existence of possibly useful intelligence information.

It is highly likely that, in an information pull environment, users will not know of the existence of useful information.

6.3.1.3.1.4.Develop systems to provide networks/nodes automated knowledge of the sources of information available, so that information can be readily pulled using general queries.

6.3.1.3.2.Identify sensor controllers.

Users are expected to have more control over sensors than that they currently have. To exercise this control they will need to communicate directly with the sensor controlling authorities.

6.3.1.3.3.Generate process for assessing relevance of specific intelligence.

The large quantities of data expected to be available mandate that there be some form of control over what information is disseminated over what transmission media.

6.3.1.3.4.Establish rules and criteria for use of civil/commercial sources at the theater level.

Information available from the civil and commercial sectors is likely to be in non-standard formats and disseminated over non-interoperable systems. Rules need to be established as to what information will be accepted and how it will be translated into useable formats.

6.3.1.3.4.1.Determine future availability of civil/commercial information sources such as civilian air traffic control systems.

6.3.2. Share Surveillance Data.

C2 Nodes can share and utilize Joint, national, theater, and non-military surveillance data.

6.3.2.1.Specify what information users require.

Not all users require the same information, nor could they assimilate all the available information.

6.3.2.1.1.Determine providers and users of surveillance data.

This is a logical first step in any information requirements determination. Who needs the data and where does it come from?

6.3.2.1.1.1.Clearly state the role of organic sensors on service weapons platforms compared with that of national sensors as sources of Joint surveillance data.

6.3.2.1.2.Determine timeliness requirements.

6.3.2.1.3.Determine accuracy requirements.

6.3.2.2.Determine fusion and correlation requirements.

6.3.2.2.1.Use data on different platforms in the same way.

6.3.2.2.2.Avoid duplicate tracks.

6.3.2.3.Develop information management procedures.

Networks must manage information in addition to connectivity in order to ensure nodes with interests in intelligence data receive the data not knowing in advance that the data are available.

6.3.2.3.1.Determine who can input and who can extract data, and in what standard format.

This is a critical net management issue. Control needs to be maintained over the networks to prevent saturation and redundant reporting.

6.3.2.3.2.Identify existing national sensors and determine their coverage and strategic workload.

6.3.2.3.3.Specify the role of the Space Warfare Center in collection, correlation, fusion, and dissemination of appropriate theater-level data.

By providing national sensor data directly to the theater, the role of the Space Warfare Center in the dissemination of missile defense data is likely to change. Decisions need to be made on how to best take advantage of these extensive capabilities.

6.3.2.3.4.Alert friendly forces which are in proximity of threat impact points.

This area requires careful study. A balance needs to be struck between ensuring that all commands that could be affected are warned in a timely manner, and avoiding the taking of needless protective measures by those not affected.

6.3.3. Exchange intelligence data only with authorized users.

6.3.3.1. Develop security classification procedures that do not prevent nor delay important information from being used effectively.

6.3.3.1.1. Develop access procedures that do not inhibit use of national data by those who could gain the most benefit.

6.3.3.1.2. Generate rules for dissemination without compromise of sources.

6.3.3.1.3. Determine how much information regarding intelligence sources can be disclosed to warriors and C2 designers.

6.3.3.1.4. Decompartmentalize selected national level intelligence data.

6.3.3.2. Design, develop, and test appropriate fusion nodes and connectivity from sensors to distribution centers.

6.3.4. Utilize Joint sensors in-theater in an efficient and effective manner.

6.3.4.1. Identity "in-theater users" and specific data requirements.

6.3.4.1.1. Specify the standards for detection, identification, correlation, tracking, and prioritization of target sets.

6.3.4.1.1.1. Determine what sensor data requirements are met in-theater by what nodes.

6.3.4.2. Enable dynamic reallocation of sensor assets.

6.3.4.2.1. Specify protocols and procedures for transferring control of sensors.

6.3.4.2.1.1. Specify which commands/nodes will have capability to control sensor assets.

6.3.4.3. Define the procedures for sensor information management for theater sensors' data such that users get only the data they need so as to prevent network and information overload.

6.3.4.3.1. Resolve issue of automated control vs. man-in-loop.

6.3.4.3.2. Establish means to fuse sensor data from both similar (e.g. surveillance) and dissimilar (e.g. non-cooperative) sources.

6.3.4.3.3.Integrate sensor data into a common battlespace picture.

6.3.4.3.3.1.Establish means to incorporate IPB data in sensor allocation and use.

6.3.4.3.4.Establish the required level of granularity, which includes time constancy and sensor quality, for the common battlespace picture.

6.3.4.3.5. Generate rules for access to national sensors

6.3.4.3.5.1.Identify requirements for gateways into the theater from the strategic level

6.3.4.3.6.Determine future availability of civil/commercial communications systems such as satellites, Internet, landlines, etc.

6.4. Objectives for Joint Planning

Joint planning systems can produce effective plans that are understood at all echelons.

6.4.1. Joint C2 planning systems can evaluate operational and tactical effectiveness of candidate Courses of Action (COA) before selection and execution.

6.4.1.1.Tools must be provided to support assessment of alternative defense strategies (what if'ing) and determine merits and limitations of each, leading to a preferred selection. This should be a collaborative process seeking input/concurrence from all appropriate subordinate elements (and coordinating elements) during the formulation and evaluation process.

6.4.1.1.1.Provide the battle manager with a "simulation" capability to input and run the candidate COA-based on alternative plans in order to evaluate potential outcomes.

6.4.1.1.1.1.Simulation workload for detailed effectiveness evaluation will require a separate node on the planning net in addition to the effectiveness analysis tools with each service planner.

6.4.1.1.1.2.Timely effectiveness analysis will be available at all levels of command where plans are formulated. This includes campaign level planning, ATO/MTO, and near real time tactical planning of imminent engagements by individual aircraft crews.

6.4.1.1.1.3.Establish appropriate configuration control for weapons system effectiveness models embedded in the planning tools.

6.4.1.1.2.Interoperability methods of effectiveness and performance can be applied to the functions addressed by the application, as well as to the aggregate actions that a commander may initiate (MOE/MOP on functions and actions).

6.4.2. The Joint C2 dynamic planning process can produce and revise, as necessary, plans that will achieve required defense effectiveness.

6.4.2.1.The ability to continuously "re-plan" must be built into the process.

6.4.2.2.Ensure planning tools account for engagement results of previously executed plans and ongoing execution.

6.4.2.3.Timely dynamic planning requires a real time planning network.

6.4.3. Plans should be developed under a collaborative, interactive environment with the affected parties participating in plan generation in real time, minimizing the subsequent coordination and change process.

6.4.3.1.Determine requirements for the conduct of distributed collaborative planning.

6.4.3.1.1.Planning applications should be collaborative and distributed, and provide responsive alternatives when presented with realistic, actual scenarios.

6.4.3.2. Joint dissemination of collaborative C2 Plans will be accomplished in a timely manner.

6.4.3.2.1.Establish timeliness requirement for distribution.

6.4.3.2.2.Determine mechanisms for dissemination of the plans.

6.4.3.3.Identify receivers of the plans.

7. Measures of Effectiveness (MOE)

Measurements of effectiveness for combat units are generally straightforward because the results of a battle or an exercise are readily apparent. The measures are generally couched in terms such as a loss exchange ratio or force exchange ratio. On the other hand, C2 systems make an indirect, albeit significant, contribution to the events on the battlefield. It is therefore often difficult to establish a direct empirical connection between C2 effectiveness and measures such as force exchange ratio. The function of a C2 system is to provide a decisionmaker with sufficient information for an intelligent decision to be made and in sufficient time for that decision to be implemented. The C2 system must also provide adequate means of transmitting the decision to executing units. Battle

management systems must also provide fire control and guidance information to the employed weapons. As can be seen, the primary function of the BMC4I system is to provide for the efficient and effective movement of information. It can be stated, therefore, that the C2 systems are effective if they provide the right information at the right time at the right level. At the theater and operational levels, this information is used to make decisions, while at the execution level the information is also provided directly to weapon systems. Therefore the command and control measures of effectiveness are based upon the quality of information at each decision and action level, the correctness of the decision or the action taken, and the time taken to make and implement that decision. The tables that follow provide measures of effectiveness as applied to the operational objectives and sub-objectives, as well as to the individual system functions that satisfy those objectives and sub-objectives.

Measures of performance support the measures of effectiveness by providing data on how accurately and timely a system collects and processes information. Measures of performance are therefore related to system and systems functionality. Interoperability measures of performance are more complex in that they provide evaluation criteria for common functionality, data, and infrastructure. The individual measures of performance can be further broken down into system performance parameters, and technical performance parameters.

Appendix A provides a decomposition of the interoperability objectives into performance objectives and performance effectiveness (MOE/MOP). These measures are for objectives only, and need to be developed for sub-objectives.

8. Conclusions

The combining of operational measures of merit with the LISI levels of interoperability can be a powerful tool in achieving Joint and coalition interoperability. The levels need to be informed by the information exchange requirements that are derived from the concept of operations. This is an iterative process, however. As interoperability is achieved, new methods of operating may be discovered which will lead to changes in the concept of operations.

Operational Objective	**Objective Effectiveness**	**Performance Objective**	**Performance Effectiveness (MOE/MOP)**
CROP	Right information at the right time at the right echelon	Demonstrate that units have access to data as required	*Timeliness* All units have data within xxx seconds of event detection *Data accuracy* Location of elements w/i xxx meters difference between nodes *Update rate* All nodes can update every xxx seconds Network does not achieve saturation *Fidelity* Data at node A = data at nodes A - n *Granularity* Units can aggregate to desired level without loss of accuracy
		Demonstrate that data can be efficiently managed	*Reporting Rules* Rules allow for accurate and timely reporting and display of tracks without over stressing communications and data processing systems. Rules are established for integration of local data. Human interfaces have necessary commonality. Applicable human override procedures exist.

Operational Objective	**Objective Effectiveness**	**Performance Objective**	**Performance Effectiveness (MOE/MOP)**
CROP	Right information at the right time at the right echelon	Demonstrate that units can contribute relevant data to the CROP	*Format* Units have the capability to format information IAW applicable network requirements *Timeliness* Data can be transmitted within xxx seconds of detection *Quality* Data transmitted meets quality standards of applicable network
		Demonstrate that units can correlate and aggregate data with no ambiguity between units	Units can reference data to appropriate location on the battlefield. Correlated tracks are accurate to w/i xxx meters and xxx km/s. Units can correlate track data so that single tracks are shown as single tracks and multiple tracks are shown as multiple tracks. Units can correlate organic and non-organic data. Units can correlate data from non-like sources. System can correlate $\geq$ xxx tracks. Existence of discordant data is made known to participants.

Operational Objective	**Objective Effectiveness**	**Performance Objective**	**Performance Effectiveness (MOE/MOP)**
Sharing Intelligence and Surveillance Data	Right Information at the right time at the right echelon	Demonstrate that Joint Nodes can Share and Utilize: Joint, National, Theater; and Non-Military Surveillance Data;	*Networks* All units have xxx % of required data within xxxx seconds of event detection Requests for information are acted upon within (timeframe) Networks do not exceed saturation Applicable nodes can access national sensor information w/i xxx (time) Updates rates meet reporting requirements *Applications* Units can correlate track data so that single tracks are shown as single tracks and multiple tracks are shown as multiple tracks Units can correlate data from like and non-like sources
		Joint Nodes Will Disseminate & Receive Existing Intelligence as Needed, Including Information From: Organic, Non-Organic, Joint, National, & Non-Military Sources	Existing intelligence is available to all nodes requiring it. Units can correlate organic and non-organic data. Units can aggregate to desired level without loss of accuracy. Data received at a node is understood by that node. Joint Theater Intelligence databases can be updated in real time. Network does not achieve saturation. Conversion formats provide information fidelity for data received from non-military sources. % of events for which additional data is requested.

Operational Objective	**Objective Effectiveness**	**Performance Objective**	**Performance Effectiveness (MOE/MOP)**
Sharing Intelligence and Surveillance Data	Right Information at the right time at the right echelon	Intelligence Data Will be Exchanged Only With Authorized Users	Classified data is provided only to authorized users Intelligence data is not compromised Authorized users are not denied needed data Sanitized intelligence can be exchanged in a timely fashion
		Demonstrate that Joint Message Sets reflect all Requirements	*Format* % of required information not included in message sets % of units not capable of receiving/transmitting required message sets *Dissemination* Unwanted message sets received at a node expressed as a percentage of all message sets received
		Demonstrate that Joint Nodes can Establish Links and Connect as Required to Other Nodes	*Network* 100% of required nodes can enter their respective nets with a delay <xxx secs. Message sets exist for required data. Net manager can reconfigure network as required with delay<xxx secs. Mission area and Service conflicts are resolved IAW an established protocol. 100% of required information can be transmitted across networks 100% of the time.

Operational Objective	**Objective Effectiveness**	**Performance Objective**	**Performance Effectiveness (MOE/MOP)**
Joint Planning	Joint Planning systems can produce effective plans	Demonstrate that effective plans are generated	% of: mission, assets, boundaries, and schedules changed as a result of surprise Time to develop plans is w/i xxx secs Plan has desired effect % of total available planning nodes that actually participate in generation of the plan
		Demonstrate consistent course of action evaluation	Given equivalent inputs, recommended COA for node a = that for nodes b – n
		Demonstrate ability to rapidly replan	Plans are revised at nodes a - n w/i xxx min(hr) of event detection. Time to develop new plans/modifications is w/i xxx secs Plan has desired effect. % of total available planning nodes that actually participate in revision of the plan.
		Demonstrate that common procedures are used	Procedures ensure that all necessary information is used in the plan generation process.
		Demonstrate ability to simulate alternative courses of action at all nodes	Tools provide accurate estimates of friendly and threat system performance. Number of alternative courses of action simulated. Accuracy of simulation. Adequacy of results.

Operational Objective	**Objective Effectiveness**	**Performance Objective**	**Performance Effectiveness (MOE/MOP)**
Joint Planning		Demonstrate that planning applications are collaborative, distributed, and timely	Number of nodes participating in plan development. Timeliness of interection Input received w/i xxx secs of initiation, response received w/i xxx secs of initiation. Number of alternatives considered.
Combat Identification	Right Information at the right time at the right echelon	Demonstrate that applicable units can differentiate friendly elements and threat targets	*Identification* Units correctly identify threat as threat xxx % of the time. Units correctly identify friendly as friendly xxx % of the time. Units label <xxx % of friendly units as hostile Units identify <xxx % of hostile units as friendly Units fail to identify <xxx % of units ID achieved w/i xxx secs of detection ID achieved at a range of $\geq$ km from ? *Correlation* System can correctly correlate various inputs into a combined identification. Units can display combined ID as part of track data. *Targeting* <xxx % of threat targets not attacked because of lack of positive ID. No friendly units attacked because of incorrect ID.