

MTR070331

MITRE TECHNICAL REPORT

Tactical Edge Characterization Framework

Volume 1: Common Vocabulary for Tactical Environments

November 2007

Dr. Fatma Dandashi

Jeffrey Higginson

James Hughes

Wilson Narvaez

Dr. Marwan Sabbouh

Salim Semy

Dr. Beth Yost

Sponsor: OSD (NII)
Dept. No.: E543

Contract No.: W15P7T-07-C-F600
Project No.: 0707ECSE-CA

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

Approved for Public Release; Distribution Unlimited.
Case No. 08-0037.

©2007 The MITRE Corporation. All Rights Reserved.

MITRE

Executive Summary

Many Service Oriented Architecture (SOA) approaches in common use today presume the availability of reliable, consistently available networks that provide limitless bandwidth and little or no latency. Because this is often not the case in Department of Defense (DoD) tactical environments, current development methods may not provide reliable capability to users in such environments. As shown in Figure ES-1, virtually any mission capability or thread that projects force will inevitably touch one or more edge users. In the simple case of the close-air-support thread shown below, edge users must identify and prosecute the target. Enabling these users with service-based capabilities could provide a great opportunity for improved mission success. This Capstone activity aims to assure the viability of an SOA to a broader domain of tactical users by better understanding and quantifying the edge environment. DoD programs responsible for delivering capabilities to the tactical edge include Future Combat Systems, Consolidated Afloat Network and Enterprise Services, Special Operations Command, etc. The tactical edge is also affected by DoD acquisition agents such as the Electronic Systems Center and the Space and Naval Warfare Systems Center.

This Tactical Edge Characterization Framework provides a common vocabulary that defines the conditions and identifies the disadvantaged users at the tactical edge. A second Framework paper, “Design Patterns for Tactical Environments,” describes a set of repeatable solutions to commonly occurring problems called design patterns. These design patterns specifically define solutions that help mitigate conditions at the tactical edge and enable the delivery of services to users in such disadvantaged environments.

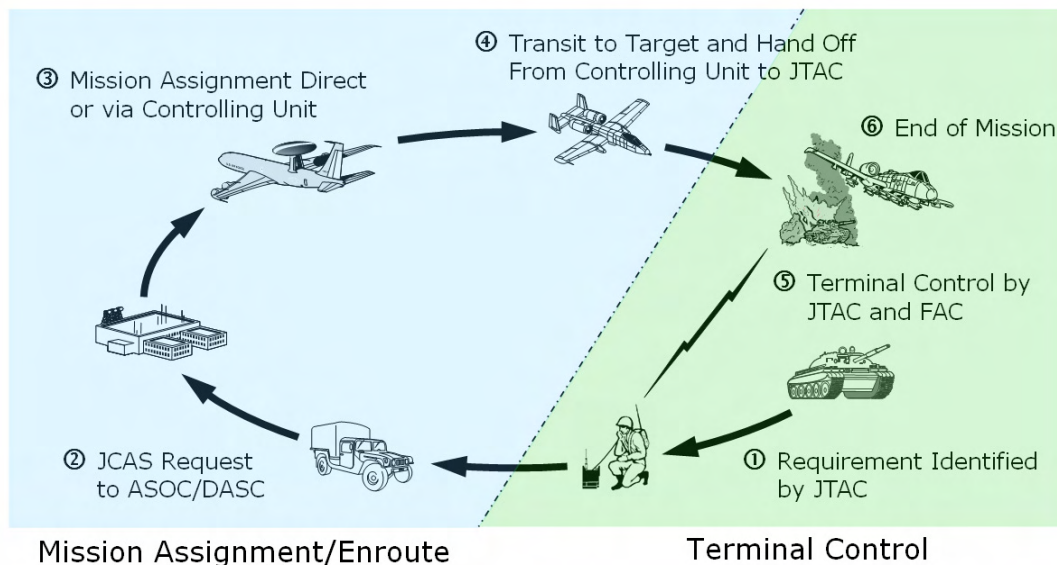


Figure ES-1. Tactical Edge Example for the Close Air Support Mission

The Tactical Edge Characterization Framework has four components:

- Common vocabulary for tactical environments
- Design patterns and templates
- Infrastructure requirements
- Reference implementations.

This paper presents the first component—a common vocabulary that describes typical constraints in the tactical environment. This vocabulary was developed by collecting and analyzing operational use cases to identify important factors that characterize the tactical edge. As a result of the analysis, four major dimensions of the tactical edge are defined:

- Network characteristics
- Resource availability
- Information assurance needs
- User interface characteristics.

Each dimension is further defined by a set of attributes. The dimensions and associated attributes collectively comprise the common vocabulary required to describe tactical environments.

Through the process of collecting and analyzing use cases and defining the factors above, a set of tactical environment classes emerged—rather than a single broad environment. These classes are illustrated in Figure ES-2 and defined as Fixed Center, Mobile Center, Mobile Swarm, and Dismounted User. The classes evolved in recognition of the complexity of the edge environment and the need to distinguish between relatively well-supported and poorly supported edge users.

Each of these classes represents a progressively less-connected and less-supported user. We begin with a Fixed Center that is well-connected to the Global Information Grid (GIG) and well-supported to execute its mission. At the next level, the Mobile Center, connectivity to the GIG is still available, but less reliable. Further out, the Mobile Swarm may have very limited connectivity to the GIG, but have reliable connectivity between elements of the swarm. Finally, the Dismounted User may only have connectivity to the local swarm and little or no connectivity to the GIG. This definition of the environmental classes is useful to help distinguish the environment, but is limited to only a discussion of connectivity to the GIG. A complete description of each class is provided in the main body of this paper.

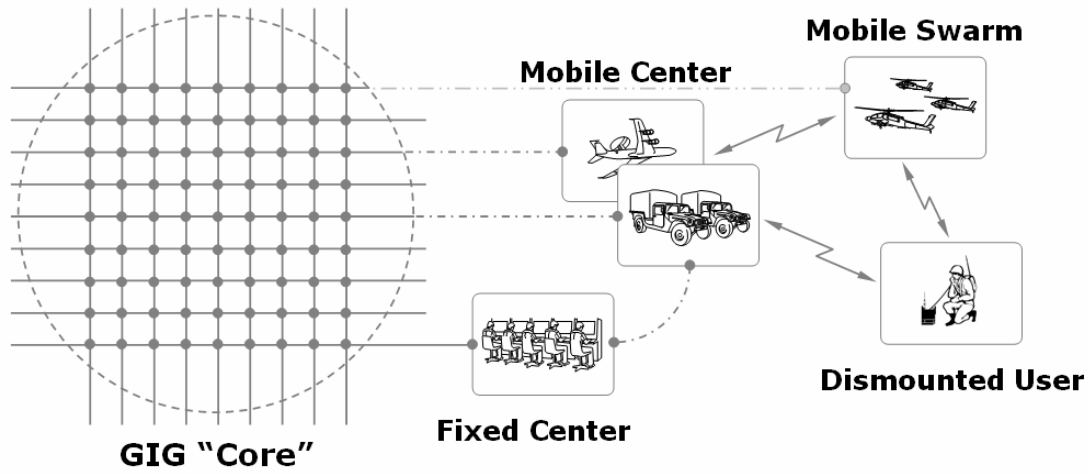


Figure ES-2. Tactical Edge Environment Classes

As we reflect on the lessons of the Capstone effort and consider future steps to support the development of SOA “to-the-edge,” we believe the DoD should consider adopting the classes defined in this paper. The classes are a starting point for a common cross-service vocabulary to describe tactical environments and the disadvantaged user. We recommend that:

1. The DoD programs responsible for delivering capabilities to the tactical edge characterize their tactical environments and reconcile differences across multiple characterizations. This will allow the programs to define and adopt a common vocabulary for describing tactical environments and associated system design patterns.
2. The DoD acquisition agents use a common vocabulary in the acquisition of tactical systems.
3. The Office of the Secretary of Defense-Networks and Information Integration use this vocabulary in all tactical edge related policies to ensure mission assurance and interoperability across tactical systems.

Adoption of a common vocabulary to describe tactical edge environments is the first critical step in developing an information-sharing reference architecture for disadvantaged users. This architecture will minimize architectural differences across DoD components and ensure that system development activities address the unique needs of the tactical edge community.

This page intentionally left blank.

Table of Contents

1	Introduction	1
2	Understanding the Tactical Edge Landscape	3
3	Technical Approach	5
4	Tactical Edge Framework	7
5	Common Vocabulary	9
5.1	Network Characteristics	9
5.2	Resource Availability	10
5.3	Data Information Assurance Characteristics	11
5.4	User Interface Characteristics	14
6	Summary of Tactical Environments	17
7	Conclusions and Recommendations	19
Appendix A	Acronyms	A-1
Appendix B	Tactical Edge Information Assurance Framework	B-1
B.1	Defense-in-Depth Model	B-2
Appendix C	Tactical Edge User Interface Framework	C-1
C.1	Objective	C-1
C.2	Method	C-1
C.3	Limitations	C-1
C.4	Impact	C-2
C.5	Tactical Edge Characterization	C-2
C.5.1	User Interface Challenges	C-2
C.5.2	Dismounted User	C-2
C.5.3	Mobile Swarm	C-3
C.5.4	Mobile Center	C-4
C.5.5	Fixed Center	C-4

List of Figures

Figure 1. Technical Approach for Defining the Characterization Framework	6
Figure 2. Example of Use Case for Combat Search and Rescue	6
Figure 3. Values for Promary Network Characteristics	10
Figure 4. Defense-in-Depth	14
Figure 5. Summary of Tactical Edge Characterization	18

1 Introduction

Many Service Oriented Architecture (SOA) approaches in common use today presume the availability of reliable, consistently available networks that provide limitless bandwidth and little or no latency. Since this is often not the case in the Department of Defense (DoD), current development methods may not provide reliable capability to users in this environment we call the tactical edge. The tactical edge can be defined from a user perspective and a technology perspective:

1. From a user perspective, the tactical edge is defined in the Network Centric Operating Environment (NCOE) Joint Capabilities Document (JCD) as the “First Tactical Mile.” Users are warfighters directly involved in executing the mission at the “tip of the spear.” In this context, the JCD defines “users” as those executing the mission in a forward deployed position.
2. From a technology perspective, the tactical edge is where users operate in certain environments that are constrained by such things as limited communications connectivity and limited storage availability. [For further details, see Ficklin, R., et al., November 2007, “Tactical Edge Gateways Functional Taxonomy,” MITRE Technical Report No. 070286.]

MITRE's Enterprise Systems Engineering Office (ESEO) started an effort in 2007 to investigate approaches and architectures that address the restrictions associated with disadvantaged tactical environments, and which will assure the viability of SOA to a broader domain of tactical users. This investigation led to the development of the Tactical Edge Characterization Framework that is documented here. The objective of the Framework is to develop a common vocabulary for identifying adverse conditions at the tactical edge and to describe design patterns that mitigate these conditions. This is done by specifying architectural guidance with infrastructure requirements and design patterns so that system developers can support the implementation of SOA-based tactical systems.

This page intentionally left blank.

2 Understanding the Tactical Edge Landscape

There are many elements of the tactical edge that require attention in any effort to codify and characterize disadvantaged users and their environment. Typically, political, operational, economic, and technical views are required to frame the problem and that is the approach taken here. From a political standpoint, the major issue is ownership of the “edge.” Because the edge has not been well-defined, each service has fenced off and supported those portions necessary for its unique mission roles. As systems and services have been pushed further out toward the edge, numerous point solutions have been adopted by stakeholders to resolve specific needs. The end result is a diverse set of solutions, each tailored to specific users, missions, and infrastructure support. Consequently, the reuse of common data and services has not been as widespread as envisioned and most general solutions must now be forced into the infrastructure. This creates a new set of economic considerations that further argues for a consolidated approach to developing and deploying information services to the edge user. DoD programs responsible for delivering capabilities to the tactical edge include Future Combat Systems, Consolidated Afloat Network and Enterprise Services, Special Operations Command, etc. The tactical edge is also affected by DoD acquisition agents such as the Electronic Systems Center (ESC) and the Space and Naval Warfare Systems Center (SPAWAR) Systems Center.

From an operational view, many stakeholders traditionally hold unique definitions of their edge environments and missions. They are only now recognizing the common nature of their needs, which have increased dramatically as joint and coalition operations become prevalent. The authors recognize that even our best efforts to provide a common edge framework, supported with design patterns and reference implementation, represent only a part of the solution. True edge interoperability requires the full spectrum of operational, doctrine, materiel, and training considerations.

Finally, the technical aspects of the edge mission must also be understood for a full appreciation of the challenge. These include the existing and evolving infrastructure, as well as emerging commercial solutions for disadvantaged users. We need to validate these solutions and create models to help us understand and predict the performance of information services in dynamic edge environments.

This page intentionally left blank.

3 Technical Approach

The approach to develop this characterization framework is illustrated at a high level in Figure 1. The effort begins with a review of numerous tactical edge use cases. These use cases provide specific insight into the challenges and restrictions faced by various users in their effort to execute particular missions. Use cases such as combat search-and-rescue, shown in Figure 2, were studied to identify their edge elements and limitations. The figure shows a survivor/evader who has limited means to communicate to a base station or recovery platform and is further constrained by the need to remain undetected. Other use cases include combat weather, call for fire, close air support, time sensitive targeting, etc.

After identifying and documenting representative use cases from the Navy, Army, Air Force, and Marines, common elements were extracted and classes of edge users began to emerge. These classes evolved in recognition of the complexity of the edge environment, and the need to distinguish relatively well-supported edge users from poorly supported edge users. The classes are Fixed Center, Mobile Center, Mobile Swarm, and Dismounted User.

Each class represents a progressively less-connected and less-supported user. We begin with a Fixed Center that is well connected to the Global Information Grid (GIG) and well supported to executing its mission. The next level is the Mobile Center, where connectivity to the GIG is still available, but less reliable. Further out, the Mobile Swarm may have very limited connectivity to the GIG, but have reliable connectivity between elements of the swarm. Finally, the Dismounted User may have connectivity only to the local swarm, with little or no connectivity to the GIG.

With the basic edge classes defined and the challenges and limitations of each better understood, the effort shifted to collecting and developing design patterns. These design patterns will be applied at the edge to support the delivery of services and improve mission capability. Finally, we validated these patterns in a tactical edge test bed, and provided a reference implementation that demonstrated improved edge capability.

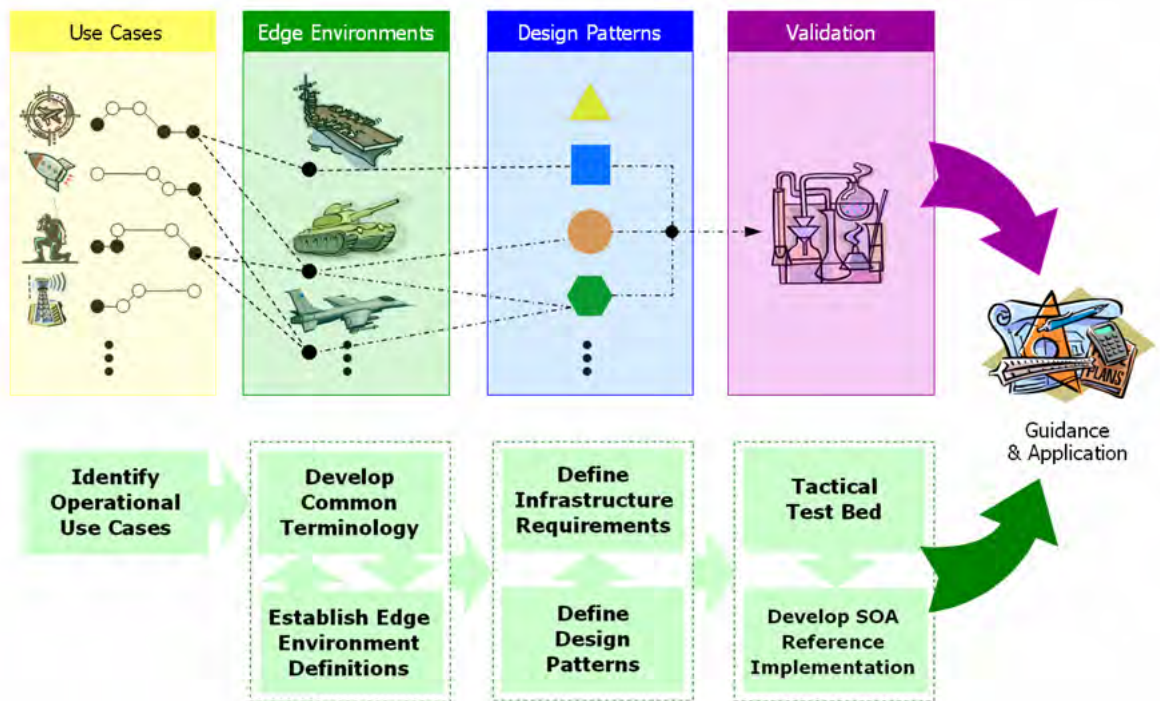


Figure 1. Technical Approach for Defining the Characterization Framework

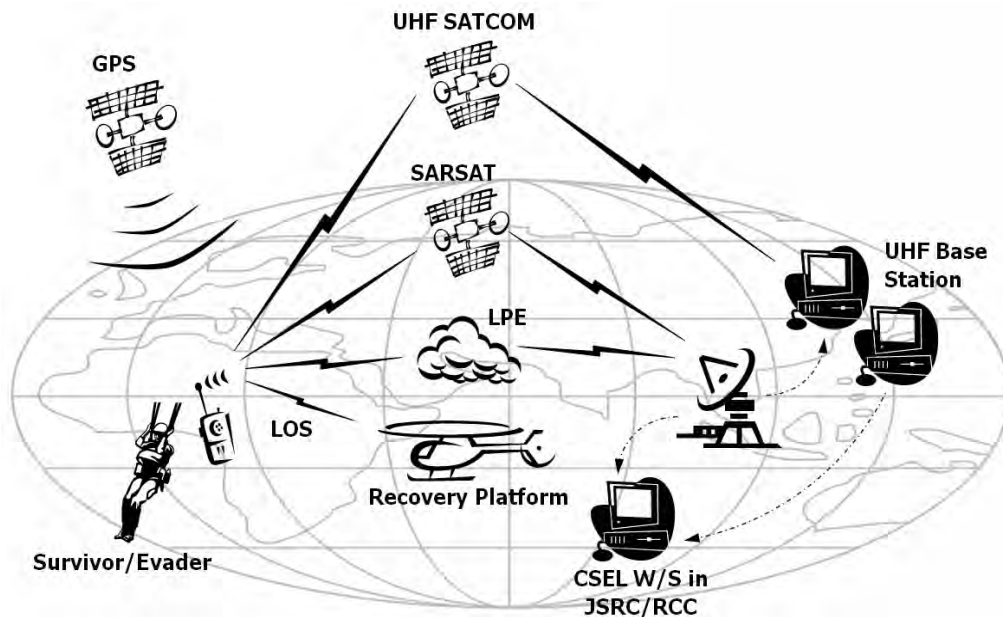


Figure 2. Example of Use Case for Combat Search and Rescue

4 Tactical Edge Framework

As a result of the technical approach described above, a framework was developed to describe the edge environment and provide guidance to the developers of information services. In general, the tactical edge framework is comprised of:

1. **A common vocabulary for tactical environments.** The vocabulary provides a terminology to describe the environmental characteristics and operational requirements in tactical environments. For purposes of characterizing the environment and aligning design patterns with particular environments, however, we will focus on the constraints of the environment.
2. **Design patterns and templates.** Design patterns and templates identify a solution set that addresses the challenges of particular classes of disadvantaged tactical environments. Specific guidance includes where to position the infrastructure, how to identify and specify enterprise services, and what best practices to use in developing application services.
3. **Infrastructure requirements.** Infrastructure requirements are derived from design patterns and specified in the context of the existing operational infrastructure. Much of this analysis is done for particular DoD components or programs of record.
4. **Reference implementations.** These implementations demonstrate the use of the characterization framework and validate the design guidance. These implementations also show how build solutions for sharing information at the tactical edge.

The focus of this report is a common vocabulary for tactical environments (Number 1). Subsequent papers will provide more details on the other components of the Tactical Edge Characterization Framework.

This page intentionally left blank.

5 Common Vocabulary

System design is often influenced by two factors:

1. Requirements placed on the system to provide a given function.
2. Constraints placed by the environment in which the system operates.

The common vocabulary provides terminology to describe both factors of system design considerations. However, for purposes of characterizing the environment and aligning design patterns with particular environments, we will focus on the constraints of the environment.

We identified the four major dimensions that will use a common vocabulary:

- Network characteristics
- Resource availability
- Information assurance
- User interface considerations.

Each of these dimensions is further defined using a set of attributes presented below. While attributes that define operational requirements are briefly described (e.g., data characteristics), they are often tied to particular operational threads and thus are not explored here in detail.

5.1 Network Characteristics

The network dimension is defined using the following attributes:

- Connectivity. The frequency with which the network is available. This can be quantified as a percentage of time when connectivity is available. “Well Connected” is analogous to an office environment (>99% connectivity); “Mostly Connected” is general cell phone coverage (85-99%); “Intermittently Connected” is cell phone coverage moving inside and outside buildings (25-84%); and “Mostly Disconnected” may be a user traveling with very spotty connectivity (5-24%).
- Bandwidth. The amount of information or data that can be sent over a network connection in a given period of time. This can be quantified as bits per second. Reference bandwidth values include:

- | | |
|-----------------------|-----------------------------------|
| o Broadband | Up to 100 Mbps |
| o 802.11g | 54 Mbps |
| o 802.11b | 11 Mbps |
| o Cell phones | 3 Mbps for 3G and 144 Kbps for 2G |
| o Dial-up connections | 56 Kbps |

- Latency. The amount of time it takes a packet of data to travel from one point to another. This can be quantitatively represented in seconds or milliseconds.

Latency and bandwidth (i.e., speed and capacity) define the *throughput* of the network when used with connectivity. The possible values for the network characteristics are summarized in Figure 3, and apply to both global and local networks.

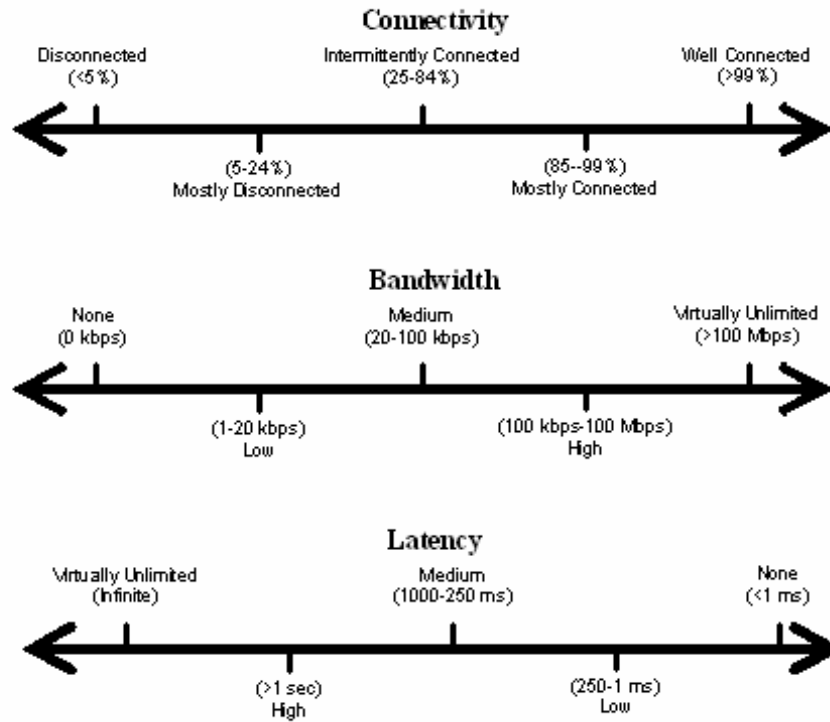


Figure 3. Values for Primary Network Characteristics

5.2 Resource Availability

The resource dimension identifies the processing and physical constraints in a particular tactical edge environment. Processing and storage are influenced by power constraints, weight, and available space. The following attributes describe the available resources:

- Processing Power. The rate at which a computing device performs operations (i.e., the clock rate or speed of the central processing unit). This can be quantified in cycles per second, or binned into: “None,” “Handheld,” “Single Workstation,” “Multiple Workstations,” or “Servers.”

- Storage Capacity. The maximum amount of data that can be retained for later retrieval. This can be quantified in gigabytes or binned into: “None,” “Handheld Memory,” “PC Hard Drive,” or “Storage Arrays.”

In addition, the following three categories are considered relevant when describing the tactical edge user, and the resources available to that user:

- Total System Weight. The maximum amount of weight in pounds for a complete system. System weight can be binned into: “>100 lbs,” “<100 lbs,” and “<10 lbs.”
- Total System Space. The maximum amount of space in square feet available for a complete system. Space in tactical edge environments can be binned into: “<10 sq ft,” “<3 sq ft,” or “<1 sq ft.”
- Power. The type of power source available such as “Grid,” “Vehicle Generator,” and “Batteries.”

5.3 Data Information Assurance Characteristics

The operational requirements for a particular use case may influence design decisions for system development. The operational requirements may be characterized by the type of data and manner in which the data is exchanged; the information assurance requirements that are necessary to protect the data; and the user interface constraints that are imposed by the tactical edge environment. The potential attributes for these dimensions are given below. It is important to note that these are general constraints and each use case will have unique challenges.

The data characteristics refer to particular attributes of the data itself as well the manner in which the data is shared. Attributes include:

- Amount of data. The average bytes per second of data sent over the network during a particular transmission.
- Type of data. The format of the data being exchanged (i.e., the MIME types). Examples include “Text,” “Imagery,” “Video,” and “Audio.”
- Priority. The relative priority of the data with respect to other information exchanged over the same network. This can be represented as “Immediate,” “High,” “Medium,” and “Low.”
- Update Rate. The frequency at which the data is updated (e.g., static, semi-static, dynamic, or very dynamic.)
- Traffic Pattern. The degree of network congestion, averaged over a particular time period. This can be represented as “High,” “Medium,” or “Low.”

- Exchange Pattern. The manner in which the data is shared among systems, including “Point-to-Point,” “Broadcast,” “Pod Cast,” “Request and Response,” or “Publish and Subscribe.”
- Number of Exchange Partners. The average number of systems and users that need to exchange data.

To address information assurance needs at the tactical edge, it is imperative to look holistically at the information assurance (IA) realm across the various tactical environments. Information assurance is defined by the U.S. Government as a set of measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. These measures provide restoration of information systems by incorporating protection, detection, and reaction capabilities.

Measures of information assurance include:

- Availability. The timely, reliable access to data and information services for authorized users.
- Confidentiality. Assurance that information is not disclosed to unauthorized persons, processes, or devices.
- Integrity. The quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. In a formal security mode, integrity may be interpreted more narrowly to mean protection against unauthorized modification or destruction of information
- Traceability. The ability to track the production and access of the data by users.
- Authorization. The ability to access information by granting all pertinent credentials to user and systems.
- Authentication. IA measures to establish the validity of a transmission, message, or the originator. It is also a means of verifying an entity’s authorization to receive specific categories of information, information services, or to perform certain role-based information system activities
- Accreditation. Official management decision, made by the Designated Approving Authority (DAA), to authorize operation of an information system. The DAA can also explicitly accept the risk to system operations (including mission functions, image, and reputation), assets, and individuals, based on the implementation of an agreed-upon set of controls.
- Certification. Comprehensive assessment of the management, operational, and technical security controls in an information system to support security accreditation. The assessment determines how controls should be implemented and how they should operate to meet the system’s security requirements.

- Management Control. A control that focuses on the management of the IA system and management of risk of the overall system.
- Non Repudiation. Assurance that (1) the sender of data is provided with proof of delivery, and (2) the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
- Vulnerability. Weakness in an information system's security procedures, internal controls, or implementation that can be exploited.

Addressing information assurance policies for various tactical environments is a two-step process:

1. Identify DOD rules, policies, and guidelines across all branches of the armed forces.
2. Recommend security perimeters for these environments.

The defense-in-depth model illustrated in Figure 4 applies the measures defined above and maintains good information assurance across all tactical edge environments. Defense-in-depth is the practice of layering defenses to provide coordinated protection against attack. Defense-in-depth mitigates the risk that a single defense can be compromised or circumvented. This strategy comprises several defense layers based on network topology (e.g., perimeters and computer enclaves) and/or protection functionality (e.g., access control, intrusion detection, and security management).



Figure 4. Defense-in-Depth

In characterizing the tactical edge environments, the following factors were considered:

- Fixed network topologies
- Network defenses
- Host defenses
- Perimeter defenses
- Data defenses
- Policies and procedures.

A more thorough discussion of IA considerations for tactical environments is given in Appendix C, Tactical Edge Information Assurance Network.

5.4 User Interface Characteristics

The end user is a critical component of emerging net-centric systems. Systems must be designed with the user in mind if we want to provide “power to the edge.” Constraints on the user interface can influence many of the other system design constraints. The following attributes can be used to characterize the user interface in tactical environments:

- Standard User Interface (UI). The typical style of user interface. This corresponds to the type of device being used. Specific design guidelines are available for the different types of Standard UIs. It can be grouped into desktop, tablet, and handheld.
- Data Complexity. The complexity of information received by a user and needed to accomplish their tasks. Complex data can result from high quantities of data, multiple data types, and multiple data sources. Data complexity is binned into complex, intermediate, and simplified.
- System Training. The amount of system training received by users. This can be a combination of time and type of training and also frequency of system use. It is binned into extensive, intermediate, and minimal.
- Receptiveness. The degree of choice an end user has in using the system and their resulting willingness to use it. Receptiveness can be classified as either receptive or discretionary.
- Decision Time. The amount of time a user has to determine if and how to act on information received. This was identified in the disadvantaged user white paper and is binned as hours to days, minutes to hours, and minutes.
- Environment. The general operating environment in which the system will be used. Values for this attribute include office, mobile office, moving vehicle, and on foot.
- Lighting. Related to the environment, the lighting conditions can be abstracted as controlled lighting (in an office) or variable lighting (day/night, indoors/outdoors).
- Display. The amount of screen space available to visually display information. Display could be described using screen size and resolution, but is binned into data walls, multiple displays, single displays, and handhelds.
- Output. The output modes available with the typical hardware. Categories include visual and auditory. A value of tactile is also possible (e.g., vibrating cell phone).
- Input. The input mode available for the end user. Input modes include keyboard and mouse, keyboard, keypad, touch, and voice.

A more detailed discussion of user interface considerations is provided in Appendix D, Tactical Edge User Interface Framework.

This page intentionally left blank.

6 Summary of Tactical Environments

Figure 5 summarizes the characteristics of the tactical edge environments described above. The Dismounted User and Mobile Swarm cases represent challenges in Network, Resource, and interface requirements. Information services designed and tested to operate in the Fixed Center or Mobile Center environment may not perform well, or at all, in constrained environments furthest from the GIG “Core” shown in Figure ES-2.

The classes shown in Figure 5 serve as the representational set of tactical environments for which design patterns can be specified. The common vocabulary discussed in the previous section is used to describe each class of tactical environments. For the network characteristics, a distinction is made between the degree of communication within a local area network and a wide area network, labeled “Local” and “Global” respectively on the vertical axis.

			Fixed Center	Mobile Center	Mobile Swarm	Dismounted	
Network	Local	Connectivity	Well Connected		Intermittently	Mostly Disconnected	
		Bandwidth	High		Medium/Low		
		Latency	Low		Medium/Low		
	Global	Connectivity	Well Connected	Mostly Connected	Intermittently	Disconnected	
		Bandwidth	High/Medium	Medium/Low		None	
		Latency	Low	Medium/Low		Virtually Unlimited	
	Resources	Processing	Servers/Workstations		Single Workstation/Handhelds		
		Storage	Large Data Storage Devices		Single Hard Drives/Memory		
		Power	Grid	Vehicle/Local Generator and Batteries		Batteries	
Space		Unlimited	<10 sq ft	<3 sq ft	<1 sq ft		
Weight		Unlimited	100+ lbs	<100 lbs	<10 lbs		
							

			Fixed Center	Mobile Center	Mobile Swarm	Dismounted	
Information Assurance	Fixed Network Topologies		WAN, LAN, Wireless LAN architectures			Limited Connectivity	
	Network Defenses		Routers, Switches, Firewalls, VPNs, etc.			HHRs, Phones, etc.	
	Host Defenses		Host IDS/Audit, Host and Data Integrity Assurance, Hardening Controls, C3, etc.				
	Perimeter Defenses		Defense against external CNA via Proxy/Application Firewalls, VPN, NIDS, etc.				
	Policies & Procedures		DoD Policy on Physical/System/Personnel Security, Countermeasures, Skills, etc.				
	Data Defenses		Cryptography, Firewall, Anti-Virus Protection, etc.			Anti-Virus, Firewall	
User Interface	App.	Content	Complex		Intermediate	Simplified	
		Standard UI	Desktop		Tablet	Handheld	
	User	System Training	Extensive		Intermediate	Minimal	
		Receptiveness	Receptive		Discretionary		
	Context	Decision Time	Hours to Days	Minutes to Hours	Minutes		
		Lighting	Controlled Lighting		Variable Lighting		
	Hardware	Environment	Office	Mobile Office	Moving Vehicle	On Foot	
		Display	Data Walls	Multiple Displays	Single Display		
		Output	Visual		Visual, Audio	Visual, Audio	
		Input	Keyboard and Mouse		Keyboard, Touch	Keypad, Voice	

Figure 5. Summary of Tactical Edge Characterization

7 Conclusions and Recommendations

This paper presents a common vocabulary to characterize a simple set of tactical edge classes. The purpose of this vocabulary is to stimulate discussion and reach agreement in the DoD on defining the tactical edge. The vocabulary can be used to identify proven design patterns that support the development of information services for disadvantaged edge user. In defining tactical edge characteristics, we considered key aspects of the information sharing environment, including network characteristics, resource availability, data characteristics, information assurance needs, and user interface characteristics.

Adoption of a common vocabulary to describe tactical edge environments will be a first and critical step in the development of consistent information sharing reference architecture for disadvantaged users. We believe this architecture will minimize differences across DoD components and promote a coherent implementation approach across disparate DoD development efforts, thus improving interoperability and providing enhanced capabilities to the edge.

Using this vocabulary as a starting point, we hope the DoD will exercise and evolve the vocabulary to support the development and deployment of information services for tactical environments. As a way to adopt the vocabulary, we recommend programs define their tactical environments using this vocabulary, capture proven design patterns of systems currently operating within the tactical edge, and integrate the vocabulary into acquisition processes.

Based on the development of the common vocabulary portion of the tactical edge characterization framework, we recommend:

1. The DoD programs responsible for delivering capabilities to the tactical edge (e.g., Future Combat Systems [FCS], Consolidated Afloat Networks and Enterprise Services [CANES], and Special Operations Command [SOCOM]) characterize their tactical environments. This will allow the program to define and adopt a common vocabulary for describing tactical environments and associated system design patterns.

MITRE recommends that the DoD programs delivering capabilities to the tactical edge reconcile differences between multiple characterizations of the tactical edge so that a common vocabulary can be developed. This paper proposes an initial definition of such a vocabulary that will enable the development of joint, cross-domain solutions to better support the warfighter. The DoD programs are encouraged to work with appropriate stakeholders to evolve this vocabulary to suit the needs of the community and to facilitate its adoption.

2. The DoD acquisition agents (e.g., ESC and SPAWAR Systems Center) use a common vocabulary in the acquisition of tactical systems.

3. The OSD (NII) uses this vocabulary in all tactical edge related policies.

A common vocabulary that defines tactical environments should be made a part of existing acquisition processes and their relevant policies. This will ensure that system requirements are based on a common definition of the tactical edge, improving systems interoperability and functionality across joint tactical environments. Existing guidance documents should also be updated with this new vocabulary.

Appendix A Acronyms

CANES	Consolidated Afloat Networks and Enterprise Services
COMSEC	Communications Security
DAA	Designated Approval Authority
DoD	Department of Defense
ESC	Electronic Systems Center
ESEO	Enterprise System Engineering Office
FCS	Future Combat System
GIG	Global Information Grid
IA	Information Assurance
IDS	Intrusion Detection Systems
IP	Internet Protocol
IPS	Intrusion Protection Systems
IS	Information Security
JCD	Joint Capabilities Document
Kbps	Kilobits per second
MIME	Multipurpose Internet Mail Extension
NCOE	Network Centric Operating Environment
NIPRNet	Non-Classified Internet Protocol Router Network
NS	Network Security
OSD (NII)	Office of the Secretary of Defense (Networks and Information Integration)
PDA	Personal Digital Architecture
SOA	Service Oriented Architecture
SOCOM	Special Operations Command
SPAWAR	Space War
UI	User Interface
WLAN	Wireless Local Area Network

This page intentionally left blank.

Appendix B Tactical Edge Information Assurance Framework

Information superiority, a mandate of U.S. defense transformational objectives, assures that the right people receive the right information at the right time in the right format, while our adversaries are denied the same advantages. In the parlance of the DoD, information security protects this "assurance."

The availability of information and the ability to distribute it for shared use significantly enhances military effectiveness and improves mission efficiencies by:

- Increasing the speed of command and enabling a higher operational tempo
- Giving greater lethality
- Reducing collateral damage and friendly fire incidents
- Increasing survivability
- Streamlining combat support
- Providing more efficient force synchronization across the battle space.

As advances in information technology increase information superiority with interconnected business processes and network centric tactical assets, the need for defensive measures to protect critical cyber assets and infrastructures becomes paramount. This drives improved security operations, the adoption of public key infrastructures, and improves integrated attack sensing and warning capabilities. Advanced information technology also improves the conduct of computer forensics and the ability to leverage information assurance.

DoD information doctrine generally comprises the following hierarchy of terms:

Information Superiority—A DoD Capstone term to establish the goal of free operation of information systems in a dominant manner analogous to air superiority or naval superiority.

Information Assurance (IA)—The most encompassing form of confidence in one's security as it relates to the integrity of information from its inception. IA protects the information and all the elements that exist to capture, transport, store, and use it. IA focuses on the confidentiality, integrity and authenticity of information. Information assurance at the various tactical levels includes:

- Plans
- Policies
- Architectures
- Services
- Certification and accreditation

- Monitoring and incident response
- Education and training
- Enterprise security program management.

Information Security (IS)—Focuses on the protection of the infrastructure and is a sub-element of IA, though the two terms are often interchanged. In information security, we often deal with Network Security (NS) that encompasses devices that secure the network including firewalls and intrusion detection systems.

Before addressing information assurance at the various classes of tactical environments it's important to address the defense-in-depth model.

B.1 Defense-in-Depth Model

Defense-in-depth is the practice of layering defenses to provide coordinated protection against various attacks. Defense-in-depth mitigates the risk that a single defense can be compromised or circumvented. This strategy comprises several separate layers of defense based on network topology (such as perimeters and computer enclaves) and/or protection functionality (such as access control, intrusion detection, and security management). Each layer provides a somewhat independent protection barrier such that an adversary must defeat multiple barriers before accessing sensitive systems or information.

Defense-in-depth is comprised of the following pieces:

1. An external digital perimeter composed of communications security (COMSEC) devices, firewalls, high-security guards, and where necessary, physical isolation serving as a barrier to outside networks such as the Non-Classified Internet Protocol (IP) Router Network (NIPRNET).
2. Internal digital perimeters, consisting of firewalls and/or router filtering capabilities, serving as barriers between echelons and/or functional communities. Internal barriers may also be augmented using COMSEC and guards.
3. A secure local workstation/platform environment, consisting of individual access controls, configuration audit capabilities, IA tools, and procedures.
4. Intrusion detection systems (IDSs) and intrusion protection systems (IPSs) located at network perimeters and even at host computers that are identified as key systems (e.g., mail servers).
5. Security management capabilities tied to network management systems to provide real-time network surveillance and reaction to network intrusions.
6. A robust and resilient infrastructure designed to contain and minimize damage from attacks and to be quickly repairable in the event of attack. The fundamental criteria

are (1) no single attack leads to failure of a critical function, and (2) no critical function or system is protected only by a single protection mechanism.

7. Wireless capabilities appropriately tied with other networks, security for Wireless Local Area Networks (WLANs) focuses on access control and privacy. Robust WLAN access control, also called authentication, prevents unauthorized users from communicating through access points. Strong WLAN access control measures help ensure that legitimate client stations associate only with trusted access points rather than rogue or unauthorized access points.

Now that the basic concepts of information assurance have been addressed, the next step is to understand how to apply these concepts across the tactical edge environments and maintain a good level of IA compliance. The objectives of maintaining a good IA compliance program across all tactical edge environments are defined as follows:

1. Depict the layered application of these capabilities to provide defense-in-depth protection, as well as detection and recovery phases
2. Provide an analysis of the security posture of the tactical edge systems including a summary of vulnerabilities, mitigation approaches, and residual risks.
3. Design information assurance capabilities to include IA management, information transport, IA devices, and operating systems. These capabilities can be leveraged using a defense-in-depth approach to provide vulnerability identification and reduction. This capability is applied across protection, detection, and recovery phases. IA status and warning information is distributed across the systems using approved protocols and message formats.

This page intentionally left blank.

Appendix C Tactical Edge User Interface Framework

Tactical edge environments can be characterized as Fixed Center, Mobile Center, Mobile Swarm, and Dismounted User. In each type of environment there are unique technological, operational, and environmental constraints. These constraints have implications for the design of the user interface and understanding them can aid in the development of new interfaces and improvement of existing interfaces. A variety of domain and system specific guidelines exist to address user interface issues. However, guidelines relevant to a particular tactical edge environment can also be useful. A description of each class of tactical edge environment is provided along with an overview of user interface considerations within that environment.

C.1 Objective

We assessed and characterized the user interface challenges in each tactical edge environment: Fixed Center, Mobile Center, Mobile Swarm, and Dismounted User. Users in each of these tactical edge environments face unique challenges due to environmental and resource constraints. As an example, users in stationary command centers have optimal lighting conditions and large displays while dismounted users may have handheld displays and suboptimal lighting. Such differences change the applicable user interface design principles.

C.2 Method

The factors that influence the user interface design in disadvantaged tactical edge environments were assessed and characterized by collecting data about a number of different systems. Systems were selected to cover a variety of domains and each tactical edge environment. They were also selected based on the quality of documentation and on the availability of people familiar with the system. Design guidelines and existing documentation was reviewed and people familiar with the system were interviewed. When possible, lessons learned during combat were obtained. The lessons learned were of the highest value because they came from end users in the field. Common user interface considerations were then identified in each tactical edge environment.

C.3 Limitations

Before applying the results of this work, some limitations need to be noted:

- The framework is an abstraction and is not a replacement for user-centered design or usability evaluation of individual systems. It is only a starting point that outlines some considerations and general guidance.
- It was unreasonable to evaluate all systems. Therefore, this work should be extended by designers to account for the unique challenges of their particular system.

- Observing users in the field is the ideal way to study user interface challenges. Because this was not feasible, lessons learned from combat were considered the most important.

C.4 Impact

Benefits from this work include:

- Improved product usability benefits users in disadvantaged tactical edge environments. Depending on the system goals, improved usability can increase user efficiency, decrease errors, and decrease training time. Increased efficiency could be crucial in situations where a few seconds determines the outcome.
- Developers benefit by using this document as a starting point to understand and meet the needs of the end user across environments.
- Emergency responders and others who operate in disadvantaged command and control environments benefit from potential improvements in user interfaces.
- The program office benefits by using the document to determine which user interfaces are best suited for particular tactical edge environments.

C.5 Tactical Edge Characterization

C.5.1 User Interface Challenges

After characterizing the user interface factors in each environment, the general user interface challenges were identified. These challenges resulted from some combination of user interface specific factors. However, user interface challenges also result from resource constraints such as battery power, network constraints such as connectivity, and information assurance factors such as DoD policies and procedures. Challenges were identified based on a variety of cases including: search and rescue, close air support, emergency response, call for fire, blue force tracking, and weather. The main challenges that emerged in each environment are described in the remaining sections.

C.5.2 Dismounted User

Dismounted Users are in the most disadvantaged environment. They typically travel on foot so they must be able to carry the complete system. The power supply must also be carried and is often extremely limited. These users operate in high-pressure environments where decisions must often be made in minutes. Dismounted Users may have limited system training and limited experience using the system in the field. Dismounted Users tend to use the most efficient means possible to obtain and provide information. Dismounted Users may have a cell phone or PDA-like device with a small visual display.

C.5.2.1. Dismounted User Considerations

The main user interface challenges that emerged from dismounted environments are:

- Appropriate use of technology
- Portability of the system
- Interfaces for variable lighting conditions
- Interfaces for handheld devices
- Users with minimal system training and device familiarity
- Users operating in time-pressured environments
- Conserving batteries without sacrificing functionality
- Limited bandwidth and network connectivity.

C.5.3 Mobile Swarm

Mobile Swarm users typically travel in a vehicle and operate in high-pressure environments where they must make decisions quickly. They generally have laptops or rugged touch screen devices. These users may have varying levels of experience with the system in the field. The information they are able to send and receive may be a bit more complex than the dismounted user. They have advantages over the Dismounted User because of the increased display space, the availability of a touch screen keyboard, and the additional vehicle-generated power supply. However, Mobile Swarm users still have limited space and are subject to the environment constraints of operating in a vehicle.

C.5.3.1 Mobile Swarm Considerations

Some of the user interface challenges that Dismounted and Mobile Swarm environments share include:

- Appropriate use of technology
- Interfaces for variable lighting conditions
- Users with minimal system training and device familiarity
- Users operating in time-pressured environments
- Limited bandwidth and network connectivity.

Challenges unique to Mobile Swarm environments include:

- Interfaces in vehicles
- Touch screens interfaces
- Transitioning from mounted to dismounted environments
- Collaboration across domains.

C.5.4 Mobile Center

While Dismounted and Mobile Swarm challenges are strongly related, Mobile Center user interface challenges tend to be more correlated to the challenges in Fixed Centers. Mobile Centers cover a range of scenarios even in a domain. A Mobile Center could be based in a small or large moving vehicle or be in shelters that were transported to a particular location. Stationary Mobile Centers tend to have better network connections and more space. Power resources are more constrained than in a Fixed Center, but less constrained than in the Mobile Swarm or Dismounted environments. The user interface challenges in Mobile Centers begin to shift from one of resource constraints to one of data complexity and collaboration. These users may have slightly more decision time, controlled lighting, multiple displays, and keyboard and mouse input.

C.5.4.1 Mobile Center Considerations

If a Mobile Center is vehicle-based, it shares the following challenges with Mobile Swarm environments:

- Appropriate use of technology
- Interfaces for variable lighting conditions
- Interfaces in vehicles
- Touch screens interfaces
- Collaboration across domains.

Challenges unique to Mobile Center environments include:

- Ability to quickly relocate
- Dealing with diverse information sources.

C.5.5 Fixed Center

Fixed Centers are included for the sake of comparison. Users in these environments are the most advantaged in available resources. They typically have an unlimited power source, no space or weight constraints, and adequate processing power. They are well connected to the network and have multiple displays for each individual and access to a large shared display. Users may be working in shifts and share their workstation asynchronously. They also may be using different machines for different networks.

C.5.5.1 Fixed Center Considerations

The main challenges in Fixed Centers result from data complexity and collaboration:

- Interfaces for collaborative work
- Large shared display interfaces
- Complexity of data
- Privacy issues.