RELIABILITY OF INFORMATION-FUELED SERVICES
IN NETWORK-CENTRIC OPERATIONS

M. Tortorella
Department of Industrial and Systems Engineering
96 Frelinghuysen Rd.
Rutgers University
Piscataway, NJ 08854 USA

P. J. Driscoll
Department of Systems Engineering
Mahan Hall
U.S. Military Academy
West Point, NY 10996 USA

Report Documentation Page		Form Approved OMB No. 0704-0188

1. REPORT DATE **JUN 2005**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2005**
4. TITLE AND SUBTITLE **Reliability of Information-Fueled Services in Network-Centric Operations**		5a. CONTRACT NUMBER
		5b. GRANT NUMBER
		5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)		5d. PROJECT NUMBER
		5e. TASK NUMBER
		5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Military Academy,Department of Systems Engineering,Mahan Hall,West Point,NY,10996**		8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)
		11. SPONSOR/MONITOR'S REPORT NUMBER(S)
12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release; distribution unlimited**		
13. SUPPLEMENTARY NOTES **The original document contains color images.**		
14. ABSTRACT		
15. SUBJECT TERMS		

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**37**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

RELIABILITY OF INFORMATION-FUELED SERVICES
IN NETWORK-CENTRIC OPERATIONS

M. Tortorella
Department of Industrial and Systems Engineering
Rutgers University
Piscataway, NJ 08854 USA

P. J. Driscoll
Department of Systems Engineering
U.S. Military Academy
West Point, NY 10996 USA

ABSTRACT

The Network-Centric Operations Conceptual Framework (NCO-CF) contains many factors pertaining to the use of information in NCO. Information plays such a central role, however, that the importance of high-quality information must not be overlooked. Information that is of poor quality (even in an informal sense) is at best distracting and at worst catastrophic to NCO. In addition, a key quality attribute for information is that consumers of the information must be able to access it reliably. The highest quality information is useless if it cannot be seen so that it can be acted upon. This paper discusses aspects of service reliability for NCO information distribution services that commanders and warfighters use to obtain information. A framework for thinking about these problems and several examples from recent case studies are discussed.

1   INTRODUCTION

1.1   Rationale

Realizing the power of Network Centric Operations (NCO) depends directly not only on implementing weapon platform sophistication and lethality advances but also on how efficiently and effectively Units of Action (UofA) exploit information advantage to drive positive battlespace outcomes. We define information advantage following Driscoll and Henderson [1]: given existing intelligence gathering capabilities, information advantage is the difference between the time US Forces accurately identify opposing force operational state(s) and force disposition and the time US Force operational state and disposition is known by an opposing force. When this difference is positive, it indicates that US Forces possess sufficiently good information that affords them an ability to both decisively plan in a shorter decision cycle than the opposing force and to proactively position troops and material in the battlespace to interdict opposing force operations at a place and time where they will be.

The creation of information meeting quality criteria from intelligence source data (*e. g.*, humans, electronic sensors, etc.) and the ready availability of the resulting information product(s) to users and decision makers are key elements of the foundation of NCO. Plainly, the quality (broadly interpreted) of the information presented to the user has a strong bearing on the success of NCO [2]. If there is to be any hope of improving the situation described by von Clausewitz [3] "....three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty...The commander must work in a medium which his eyes cannot see, which his best deductive powers cannot fathom, and with which, because of constant changes, he can rarely be familiar," information must not only be provided to the commander but it must also be

(1) rich enough to overcome as many "fog of war" uncertainties as possible and (2) "good enough" to support high probability of correct decision-making. In a context of providing a commander with information that promotes successful NCO, it appears prudent to examine three system processes that bear on the information's usefulness:

- The creation of information products (an information product could be, *e. g.*, a message describing, in more compact form than the original data, a situation of interest or importance to the commander; see Section II of [2] for further details),
- The possible deterioration of information products during their useful life, and
- The distribution of information products to intended users.

1.2 Background

The NCO Conceptual Framework [4] defines key concepts and attributes pertaining to the use of information in NCO. It is worthwhile in addition to focus specifically on information quality and reliability attributes for the reasons cited in Section 1.1. Such focus augments the NCO CF with qualitative and quantitative considerations for an extremely important dimension of information value that has heretofore been less studied. The companion paper [2] provides an in-depth study of information quality issues in NCO. A brief review that provides adequate background for this reliability study is provided in Section 2 of this paper.

The fundamental ideas, concepts, and models of service reliability theory and engineering are found in [5] and [6]. These will be required for the service reliability analyses undertaken here in Sections 4.3.1 and 4.4.1.

1.3 Scope

This paper addresses quality and reliability aspects of information product distribution, the third of the processes listed at the end of Section 1.1. The purpose of this paper is to describe relevant aspects of the delivery of NCO information products to end users, to catalog failure modes and failure mechanisms that may interfere with proper acquisition of the information product by the end user, and to begin to define quantitative models that enable us to connect the characteristics of the information product delivery infrastructure (IPDI) to the reliability of information product delivery and the reliability of the information products themselves (Section 3). This research program is facilitated by the notion of service reliability [5, 6] and its associated concepts. In particular, the concept of service fulfillment ([5], Section 2) enables us to augment the NCO CF with important dynamic considerations pertaining to the evolution of information quality with the passage of time, thus enlarging the scope of the NCO CF to include not only static properties (quality) but also dynamic properties (reliability). A purely static view of information use in NCO is not adequate for this task because one of the key premises of NCO is rapid adaptation to rapidly changing conditions.

The paper aligns the characteristics of information product delivery to users in the NCO context with the basic concepts of service reliability so that we may study an important aspect of information value with quantitative models. The paper extracts relevant service reliability issues in NCO from case studies [7, 8] so that it will be clear how analyses can proceed.

2 INFORMATION QUALITY

2.1 Introduction

The phrase "information quality" can be understood in two senses that are valuable for NCO applications. The first sense is a general one: information is quality information if it is "good" in some specific sense. This sense requires us to state more clearly what "good" means, and this is accomplished with the nine information quality criteria found in Section 2.2. The second sense is a more specific one drawn from quality engineering ([9], chapter 2). Information may be

required to possess certain desirable attributes for given purposes (for example, the nine quality criteria in Section 2.2 for "quality"). The quality of an information product in this second sense comprises two factors:

- the degree to which that information product satisfies those requirements (a judgment about an individual information product), and
- the amount of between-unit and within-unit variability in the degree to which requirements are satisfied (a judgment about a population of information products).

To avoid the confusion that is naturally attendant on this situation, it would be desirable to employ two different words or phrases for these two concepts. Regrettably, common usage of the single phrase in both contexts is so firmly entrenched that introducing new terminology at this stage would almost certainly be met with resistance. Accordingly, we will try to compromise by referring to "big Q" information Quality for the "goodness" sense and "little q" information quality for the formal (second) sense brought forward by quality theory and engineering.

2.2 Review of Information Quality Criteria

Driscoll *et al.* [2] define nine critical criteria by which information Quality can be assessed (Figure 1). Briefly, these criteria are:

- <u>Comprehensiveness</u>: is the *scope* of information adequate?
- <u>Accuracy</u> (or faithfulness): is the information *precise enough* or close enough to reality?
- <u>Clarity</u>: is the information *understandable* to the user?
- <u>Applicability</u>: can the information be *directly applied* or does it have to be further transformed by the user?
- <u>Conciseness</u>: is the information *to the point* and devoid of unnecessary elements?
- <u>Consistency</u>: is the information *free of contradictions or convention breaks* from what is typically expected?
- <u>Currency</u>: is the information *up to date*?
- <u>Convenience</u>: does the information provision *correspond to the user's needs and habits*?
- <u>Traceability</u>: can the *source* of the information be *validated*?

Information quality can then be understood as the degree to which an information product meets requirements for these nine value criteria at the time of its production.   Though these criteria are deliberately broad in their general description, focusing on them in a particular context (*e. g.*, NCO/NCW) adds enough specificity to render the criteria amenable to quantitative and/or qualitative description, measurement, and modeling. Assessment of criteria in this fashion covers the static notion of quality at the time of creation of the information product because information quality is determined at the time of its creation. Dynamically assessing the ability of the system to meet user requirements beyond the point of initial information product release requires that we extend our consideration in this regard to include concepts of information reliability also.   See Section 3.
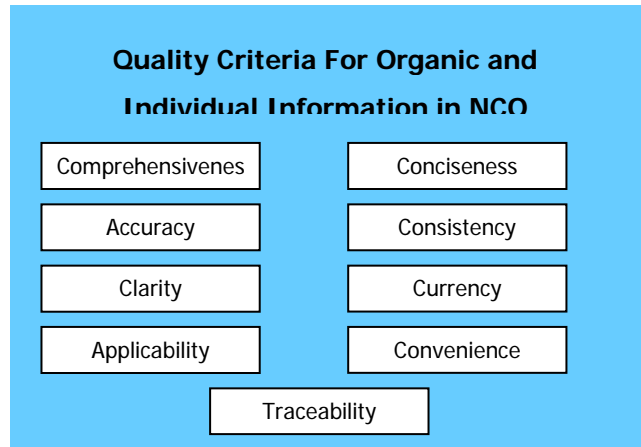
Figure 1. Nine critical elements of information quality for NCO.

2.2.1 Content Quality and Usability Quality

The nine information Quality criteria of Figure 1 may be subdivided into two categories, content Quality and usability Quality. Four criteria, accuracy, currency, comprehensiveness, and traceability, pertain to the information product's content, the part of the information product that the user will employ in making a decision based on the information product. The remaining five criteria, conciseness, consistency, convenience, clarity, and applicability, pertain to how well the user is able to apprehend and prepare to employ the content of the information product. Poor "little q" quality of the content criteria is a serious shortcoming of the information product because this by definition leads to a lower probability of making a correct decision based on the information product. Poor "little q" quality in the usability criteria may be equally serious if it causes the user to have to guess to fill in missing elements or otherwise make up for lack of immediate ability to apprehend the content of the information product.

This distinction is important for two reasons. First, we believe that when the NCO CF refers to "Information Quality," as it does in many places, it intends readers to interpret it as content Quality. Second, the distinction helps us clarify the importance of the IPDI on the overall quality (that is, along all nine dimensions) of a received information product. We will find that certain kinds of IPDI characteristics affect primarily the content Quality criteria and others affect primarily the usability Quality criteria. This is a help is nailing down the information product reliability variables and in understanding the way the information product delivery services can promote or interfere with information Quality and Reliability.

However, "big Q" quality is not enough. Study of the "little q" quality of the content attributes is important because it is necessary to understand and quantify the degree to which these attributes are present in a given information product or a population of information products. Also, it is a mistake to ignore the usability criteria because poor usability quality will destroy the value of even very high quality content. At the end of the day, we want to use this quantitative understanding to form the basis of requirements for
- The nine information Quality criteria and
- The systems (broadly interpreted) that produce the information products and deliver them to users.

3   INFORMATION RELIABILITY

As with information quality, there is "big R" information reliability and "little r" information reliability. This arises, as usual, from the fact that ordinary discourse encompasses two connotations of the word "reliability." The first sense is a common language sense of "reliable"

as something that can be counted on, something steadfast. We will use "big R" Reliability for this sense. The second sense is the technical sense found in the mathematical theory of reliability and reliability engineering: the probability that the item in question continues to function as is intended as time passes.

Information "little r" reliability refers to the preservation or persistence of initial information quality throughout the information product's life cycle. The factors influencing information reliability are the possible deterioration or loss of the information product during its life cycle and the reliability of the service(s) used to deliver the information to its users. These are the second and third processes noted in Section 1.1 because deterioration or distortion of an information product, and therefore changes to the initial quality values of the nine information Quality criteria, may occur as a result of factors arising during storage, modification, or delivery of the information product. Information reliability is also influenced by the reliability of the IPDI, the infrastructure (people and machines) that supports information delivery *services.* An information delivery service is a system process that encompasses the collection of activities targeting repeated successful delivery of information products as required by the user. Characteristics of the service may cause possible departure, during delivery and reception, of the information product's quality from its initial value, in addition to delivery malfunctions and outright failures. As presented in [11] and further explained in this paper, elements of service in this context are sufficiently unique and important to NCO success that they justify a separate consideration in their own right. An analogy that illustrates our motivation can be seen in recognizing that high quality items ordered over the internet occasionally get damaged, lost, or delayed during delivery through no fault of the product itself. To the user, the final result is unsatisfactory, or perhaps even not usable at all.

The next Sections study failure modes and failure mechanisms for information product content attributes and information product usability attributes.

3.1 Information Deterioration

As the information product travels from where it is produced and stored, through the delivery infrastructure, to the user, physical degradation may alter the information. Physical degradation refers to changes that may take place to the information product because of properties of the IPDI, enemy action, or other factors. Physical degradation may lead to quality degradation if the changes damage or destroy the information product's content or render it less usable when it reaches the user. For example, information transmitted through a noisy channel may be degraded by alteration of bits or insertion of gaps in the bit stream because of a low signal-to-noise ratio. At the extreme, we could imagine degradation so severe that the information product is unintelligible when it finally reaches its destination user. These changes are in the realm of information reliability: does the information product suffer any degradation, or changes to its initial quality attributes, during its life cycle.

3.1.1 Models for Physical Information Quality Deterioration

For purposes of this Section, we will consider the deterioration of information as it passes through the IPDI. We will assume the IPDI is a digital, connectionless network and information products are packetized messages entering at a network ingress (where information production and/or storage takes place) and exiting at a network egress (where the user is). The deterioration mechanisms are:
- Packet loss,
- Packet expected delay,
- Packet jitter, and
- Corruption of header and/or bearer bits because of low signal-to-noise ratio.

Packet loss, expected delay, and jitter (standard deviation of packet delay) are three characteristics of the packet delivery time distribution (loss is the probability that the delivery time is infinite). These network (IPDI) characteristics are controlled by attention to network design and provisioning and are usually addressed in *information assurance* studies. Specific IPDI design and provisioning actions are outside the scope of this study, but the consequences of inadequate IPDI design and provisioning do reflect in failure mechanisms for the information product delivery services supported by the IPDI. The fourth item refers to successful delivery of corrupted packets and we will see that this too is a failure mechanism for both information reliability and for reliability of the information product delivery service.

3.2 NCO Information Delivery Service Reliability

This paper focuses on the various means by which the reliability of the information product delivery services affect the information's reliability in NCO information systems, using the framework developed in [5]. Earlier work by Eppler [10], following Lesca and Lesca [11], fails to adequately differentiate between information quality and information reliability, viewing information distortion—something that renders "the original message no longer the same when it is received [as when it was created]," ([10], p. 28)—as a quality consideration. We assert that this distortion is an information reliability problem, because it takes place later in an information product's useful life cycle. Treating it as an information quality issue would mix static and dynamic elements inappropriately.

The general framework of service reliability theory and engineering [5, 6] requires that we understand the failure modes and failure mechanisms for the information product delivery services in the study. Failure modes are the overt indications that something has gone wrong; they are analogous to the symptoms of a disease. Failure mechanisms are the explanations for the failure modes: each failure mode has one or more failure mechanisms. Failure mechanisms are analogous to the causes of a disease. In the next Section, we will list information product delivery services that were used in Operation Enduring Freedom [7] and the Stryker Brigade Combat Team exercise [8] and analyze them for their contribution to information reliability.

Finally, note that another connotation of the word "reliability" is trustworthiness. Eppler [10] uses reliability and trustworthiness synonymously. This research takes the perspective that trustworthiness is one attribute of information quality, while information reliability subsumes the changes that may take place to information quality (in all its attributes, including trustworthiness) as time passes. See also Section **Error! Reference source not found.**.

4   INFORMATION DELIVERY SERVICES IN NCO

4.1 Introduction

In this context, the "service" consumed by NCO participants is the acquisition of information products that are created and stored at locations usually remote from the user/participant. Most often, data from a network of sensors are sent to some central location for processing and analysis, thereby creating some quantity of information products. It is fruitful to view this as information manufacturing, and quality engineering techniques bearing on processes, control, etc., provide useful guidance [**Error! Bookmark not defined.**]. Information products are stored in a database or other repository. Information products may be damaged or degraded during storage, and while this may be unlikely in most scenarios, it is also unreasonable to assign probability zero to this possibility, not least because enemy forces will be trying to cause such damage.

The user initiates a request for an information product from the repository and, if the request is successful, information travels through some information product delivery infrastructure (IPDI)

(typically a communications network of some kind) to the user's interface with the IPDI. The user then attempts to perceive what is offered at the interface, and closes out the request to free up the interface for the next request. This sequence of activities constitutes a single transaction in the service. The general service reliability conceptual framework concerns the conditions for repeated successful execution of transactions in a service over specified time intervals. In the NCO context, service reliability speaks to the ability to successfully deliver repeated requests for information products from the repository over some stated period of time.

4.2 Catalog of Information Delivery Services in NCO

In this section, we will list different kinds of information product delivery services used in the NCO environments of the case studies. Section 4.3.1 will describe a service reliability analysis of one of these. This listing is far from a complete catalog of all NCO information-related services but is comprehensive enough to give an idea of the range of different information product delivery services that we need to consider.

In this study, it is useful to distinguish services for which the user has to take some affirmative action to initiate a request for the service ("pull" services) from services where the delivered product is supposed to be available at all times and the user may access the service simply by turning attention to the interface displaying the information product ("push" services).

4.2.1 General Discussion of Push Services and Pull Services

4.2.1.1 Pull Services

In a "pull" service, the user must make a deliberate attempt to request an information product. The fundamental unit of service in this context is the transaction. Service reliability theory and engineering [5] classifies the service failure modes and failure mechanisms into three categories: service accessibility, service continuity, and service release. At a conceptual level, service accessibility has to do with those things that users and the IPDI need to accomplish successfully in order that a transaction may be begun, service continuity concerns the successful carrying out of a (successfully initiated) transaction to its intended conclusion, and service release concerns matters connected with being able to dismiss a transaction when it is completed.

4.2.1.2 Push Services

Some NCO information services are provided through media that are "always on." That is, a user interface constantly displays the information product and the user need do no more than turn attention to the interface to acquire the product. No deliberate action is required to initiate a request for delivery of an information product, *i. e.*, to set up a transaction. Therefore, service accessibility (at a stated time t) for push services reduces to the probability that the information product is successfully transmitted (before time t) from repository to interface so that it is perceptible at time t. It may be necessary to separate static information products (*e. g.*, email messages) from streaming information products (*e. g.*, real-time streaming video of a distant situation) when investigating service accessibility failure mechanisms. Service continuity reduces to the probability that a user can apprehend the information before it is yanked away from him/her (a failure mechanism here could be, *e. g.*, an interface failure). Since there is no formal closing to transactions in an always-on service, there are no service release failure modes.

4.3 NCO Information Services in CTF50

Adkins and Cruse [7] review aspects of network centric warfare (NCW) in the operations of the US Fifth Fleet during Operation Enduring Freedom. Information delivery services discussed in [7] are chat rooms, Knowledge Web (KWeb), and CommandNet. In addition, Adkins and Cruse [7] listed, but did not study, new capabilities that were introduced during the Global War Game 2000

exercises: Knowledge Wall, Information Workspace, and Theater Assessment and Profiling System. These latter three are not included in this study.

Chat is similar to the familiar IRC (Internet Relay Chat) service that many ISPs offer consumers. KWeb is an intranet used by the Fifth Fleet and behaves much like an ordinary http/ftp vehicle but of course has restricted access. CommandNet is a collaborative technology, similar to commercial applications like Groove™, that allows users to view and modify files separately or together, in real time. Each of these is a pull service in that the user needs to make a deliberate effort to connect with the service.

4.3.1 Service Reliability Study of KWeb

4.3.1.1 Service Definition

Warfighters use KWeb to display "lots" of information to users [7]. Adkins and Cruse quote: "The knowledge wall features a series of windows incorporating decision support tools tailored to the Commander Joint Task Force (CJTF), as well as windows with "summary status" information being "pushed" from the anchor desks used by liaison officers representing the various CJTF departments. The battlewatch captain in charge of the command center can choose which aspects of the situation to focus on by moving relevant content to the center of the wall and drilling down into deeper levels or related information. The knowledge desk uses software tools (COTS and information push Web applications) together with computer display hardware to enable the operator to create and publish value-added information to the Web. It consists of an integrated "desktop" spread across four different display surfaces. The top-right display is dedicated to routine office tasks such as preparing briefs, processing e-mail, writing memos, etc. The top-center display is dedicated to providing the tactical situation "big picture" tailored to the user's decision-making needs. The bottom center display is a dedicated place for monitoring the execution of an operational plan. The top-left display is a tool explicitly designed to facilitate sharing information. The concept uses templates to "push" information from the operator to a Web site viewable by the rest of the command staff. The information "pushed" consists of worksheets, forms, and prompts to others on the command staff that would facilitate their understanding information relevant to their decision-making tasks. The software tools cause the information pushed to be formatted in a manner that others would recognize and understand, and published to a shared database in the Web environment. The knowledge-wall hardware consists of a dual-processor Information Technology for the 21st Century (IT-21)-compliant workstation using three 4-port Appian Jeronimo Pro COTS video boards. The knowledge wall display is made up of ten 21-inch CRTs and two SmartBoard rear projection large-screen displays with internal liquid-crystal display (LCD) projectors. The displays operate as a single, integrated digital desktop, where each physical display has a resolution of 1024 by 768 pixels. This creates a digital desktop of 6144 by 1536 pixels. An additional CRT was dedicated to video and video teleconferencing requirements. The peripheral displays were intended to provide summary information for each of 14 functional areas of the CJTF command identified through knowledge engineering with the staffs of the U. S. Navy Third Fleet, Carrier Group One, and Carrier Group Three. Each summary display is formatted consistently by using a template-authoring tool that facilitates the creation of, and linking to, a variety of Web content without the operator responsible for producing content having to know HTML. Additional authoring tools were provided to facilitate the creation and publishing of map-based tactical data. All pages are implemented as HTML pages on a common server, with numerous links to more detailed pages for supplemental information. The title line indicates the functional areas described by the display. The "stop lights" in the top-left quadrant are intended to be viewable from 15 to 20 feet away, and indicate the status of activities in various time frames. Light colors indicate the severity of the alerts in terms of their deviation from the plan. The bottom- left quadrant provides space for a summary graphic or multimedia object. The right side of the screen provides space for amplifying links/headlines. The "Alerts" section describes specific problems

within this domain/ functional area that might be of interest to others. The "Impacts" links describe the impacts of alerts in terms of effects on other functional areas. The "Links" area allows access to reference and supplemental material. Any text or graphic in the page may be linked to a more detailed Web page."

It is clear from this description that the KWeb framework encapsulates both push services and pull services. We will focus in this analysis on the pull services. While there are several kinds of pull information that can be accessed through KWeb, they are accessed through a common service architecture, namely HTML over IP, or, in other words, the familiar Web browsing service. For a user, desired information product(s) are stored on Web servers accessible through KWeb. The remainder of this Section reviews service failure modes and failure mechanisms for this service. Inasmuch as service release failures are very rare, we will not cover them here.

4.3.1.2 KWeb Failure Modes and Failure Mechanisms

4.3.1.2.1   Service Accessibility Failure Modes and Failure Mechanisms

In KWeb, a transaction comprises opening a browser (if one is not already open), requesting a particular page from a server, acquiring the information in that product, and subsequent page requests and reads until the user's needs are filled. KWeb is clearly a pull service. Service accessibility, according to [5], is the probability that a user is able to successfully set up a transaction in the service at a given time.   A formal mathematical definition is given in [5]; for purposes of this section it is enough to understand that, for a pull service, a transaction must be set up successfully before any information product can be transferred to the user. Setup usually consists of a request by the user to the IPDI for a transaction, a response (or lack thereof) from the IPDI, and possibly some additional query-and-response activity, culminating (if successful) in a user application session, or transaction. In KWeb, a transaction is retrieval and viewing of a desired Web page. The following Table lists some of the failure modes and associated failure mechanisms for service accessibility in KWeb.

BREAKDOWN FAILURES		PERFORMANCE FAILURES	
MODES	**MECHANISMS**	**MODES**	**MECHANISMS**

Browser does not open when requested	▪ PC compromised
	  o Worm/virus
		Excessive delay in opening browser	▪ CPU overloaded
			  o Legitimate activity
			  o Virus/worm

No response to user request for page	▪ Server down
	▪ Request misdirected
	  o Deliberate
	    ☞ Opposing force wiretap
	  o Accidental
	    ☞ Routing table errors
		Excessive delay in responding to user request for page (starting page load)	▪ IPDI congestion
			  o Excess offered load
			  o IPDI element failures
			  o IPDI compromised
			    ☞ Physical damage
			    ☞ DOS attack
			▪ Server overloaded
			  o Excess traffic
			  o Server subsystem failures
			  o Server compromised

Table 1. KWeb service accessibility failure modes and failure mechanisms.

User error is always a failure mechanism for any of the failure modes, so it is not explicitly listed in the table. Normally, one would look to training and working conditions as factors in decreasing user error rates, but in NCO the opportunities to improve working conditions (thinking particularly of battlefield conditions) are limited, so training (particularly in remaining cool under pressure) is the primary improvement modality for this problem. Note also that in this analysis there is more emphasis on deliberate interference failure mechanisms than would ordinarily be considered in an analysis of a commercial or non-military service. This is obviously because in NCO there will always be efforts by opposing forces to deliberately disrupt these services.

Finally, note that failure mechanisms are not only the kinds of physical or software failures that are commonly understood but also include deliberate higher-layer disruptions such as spoofing, worms, and denial-of-service (DOS) attacks.

<u>4.3.1.2.2</u> <u>Service Continuity Failure Modes and Failure Mechanisms</u>

Service continuity, according to [5], is the probability that a successfully set up transaction can be carried through to its intended completion without interruption and with acceptable levels of perceptual quality. A formal mathematical definition is given in [5]. For this analysis, it is useful to note that service continuity performance failures are also called service fulfillment failures; the terminology pertains to the service's capability to provide a satisfactory user experience *during* the conduct of the transaction.

BREAKDOWN FAILURES		PERFORMANCE FAILURES	
MODES	MECHANISMS	MODES	MECHANISMS

Page load permanently stalled	▪ Packet loss <u>and</u> TCP failure
	 o Incoming
	▪ IPDI access failure
		Excessive delay in completing page load	▪ IPDI congestion
			 o Excess offered load
			 o IPDI element failures
			 o IPDI compromised
			   ☞ Physical damage
			   ☞ DOS attack
			▪ Server overloaded
			 o Excess traffic
			 o Server subsystem failures
			 o Server compromised

Subsequent page request refused/failed	▪ IPDI access failure ▪ Packet loss <u>and</u> TCP failure o Incoming o Outgoing	Incorrect page served to user	▪ Request corrupted in transit ▪ Server database corrupted ▪ Requesting page spoofed
		Audio and/or video garbled/unintelligible	▪ Packet loss ▪ Excessive packet latency

Table 2. KWeb service continuity failure modes and failure mechanisms.

4.4 NCO Information Services in the Stryker Brigade Case Study

Gonzales, Johnson, *et al.* [8] review aspects of NCW in the operations of the Stryker Brigade, a new medium-weight US Army infantry brigade. The central NCO platform is the SBCT (Stryker Brigade Combat Team) Network. The SBCT Network has five subnetworks, or capabilities:
- Satellite communications wide-area network (WAN),
- TOC-to-TOC network (TOC = tactical operations center),
- Tactical Internet
- Command Net Radio Network (CNR), and
- Global Broadcast System.

In addition to these subnets, various components of the SBCT have specialized communications equipment for such purposes as reaching back to national-level intelligence assets and transmitting UAV imagery. Each sub-net plays a role in connecting SBCT elements with one another and with non-SBCT entities. In other words, each capability provides an information product delivery service to SBCT users.

Tactical Internet contains a datacom component (the Enhanced Position Location Radio System (EPLRS) network) and a voice communications component (the CNR). EPLRS is a low bandwidth (14.4 kbps mean, 56.6 kbps max) terrestrial network that carries situational awareness data and a text messaging capability throughout the SBCT. This network is based on terrestrial line of sight communication links. It provides digital communications to vehicles while they are moving or stationary. Finally, GBS is a high-bandwidth (24 Mbps per transponder) data broadcast

network that delivers video, imagery, and other feeds from national information assets to the SBCT. GBS receivers are located at the SBCT Main CP, the BSB, the RSTA Squadron TOC, and the TOCs of the three infantry battalions. Note that GBS is a push service.

4.4.1 Service Reliability Study of GBS

4.4.1.1 Service Definition

4.4.1.2 GBS Failure Modes and Failure Mechanisms

4.4.1.2.1 Service Accessibility Failure Modes and Failure Mechanisms

Global Broadcast System is a high-bandwidth (24 Mps per transponder) data broadcast network that delivers video, imagery, and other feeds from national information assets to the SBCT. As a broadcast service, it is a push service (Section 4.2.1), so there is no special effort required on the part of the user to begin a transaction in the service. A transaction begins when the user turns attention to the interface for the service, in this case, the GBS receiver. Service accessibility at a given time therefore is equal to the probability that the GBS receiver is functioning properly at that time. That is, the receiver is powered up, operating, and receiving signals as intended.

4.4.1.2.2 Service Continuity Failure Modes and Failure Mechanisms

While GBS is a push service, a transaction that has successfully begun could still be interrupted or otherwise degraded before its intended end. The following table summarizes service continuity failure modes and failure mechanisms for GBS.

BREAKDOWN FAILURES		PERFORMANCE FAILURES	
MODES	MECHANISMS	MODES	MECHANISMS
Streaming audio or video stops, does not restart	▪ Loss of entire satellite ▪ Loss of dedicated transponder ▪ Loss of downlink ▪ Interface failure ▪ Broadcast origination failure	Streaming audio/video distorted/garbled	▪ Broadcast origination failure ▪ Interface failure ▪ Packet bearer bit errors ▪ IPDI congestion ▪ Excessive packet loss and/or delay
Static video disappears	▪ Remote refresh failure ▪ Interface failure	Gaps in streaming audio/video	▪ Intermittent satellite failure ▪ Intermittent dedicated transponder failure ▪ Intermittent downlink failure ▪ Intermittent interface failure ▪ Severe packet loss and/or delay

Table 3. GBS service continuity failure modes and failure mechanisms.

For reasons of limited space, Tables 1, 2, and 3 list only the proximate failure mechanisms for each failure mode. Using the failure mechanisms in a model to develop the probability of occurrence of a failure mode requires further analysis of the failure mechanism into elementary events in the IPDI for which system analyses have estimated probabilities of occurrence.
For example, the failure mechanism "loss of downlink" may further develop into hardware and/or software failure in the satellite CPU or downlink controller and/or the downlink equipment itself and/or opposing force action to interfere with the radio signal from the satellite to the receiver. Each possibility must be accounted for in modeling the probability of occurrence of the associated failure mode.

5   INTRODUCTION TO QUANTITATIVE MODELING FOR NCO INFORMATION PRODUCT DELIVERY SERVICE RELIABILITY

5.1   Models for Service Accessibility

We use Voice over IP (VoIP) service to illustrate how to model service accessibility in a connectionless network. VoIP is POTS delivered over an IP network such as the Internet. VoIP uses Session Initiation Protocol (SIP) as one of the (out-of-band) signaling technologies[1] used to set up calls. Before bearer voice traffic can be sent to the called party, call setup needs to determine the location of the called party and exchange call information (such as types of codecs used). In order for call setup to be successful, two steps need to be completed, assuming SIP signaling: (1)call admission from the SIP proxy server and (2)successful delivery of SIP signaling messages. Call admission determines whether enough resources are available to accept and process a call request. A SIP proxy server uses maximum simultaneous calls and processor capacity to determine if a call can be accepted. For example, during times of increased call volume, a large amount of calls could attempt to be nearly simultaneously set up. If this number exceeds what the SIP proxy server can handle, call attempts that exceed the threshold will be rejected.

Once the SIP proxy server has accepted a call for processing, the next step required is to deliver the signaling messages that need to be exchanged between the SIP endpoints. If these messages are delivered correctly, the call is set up and bearer traffic can be sent. Figure 3 shows the steps needed to successfully setup a VoIP call using SIP.
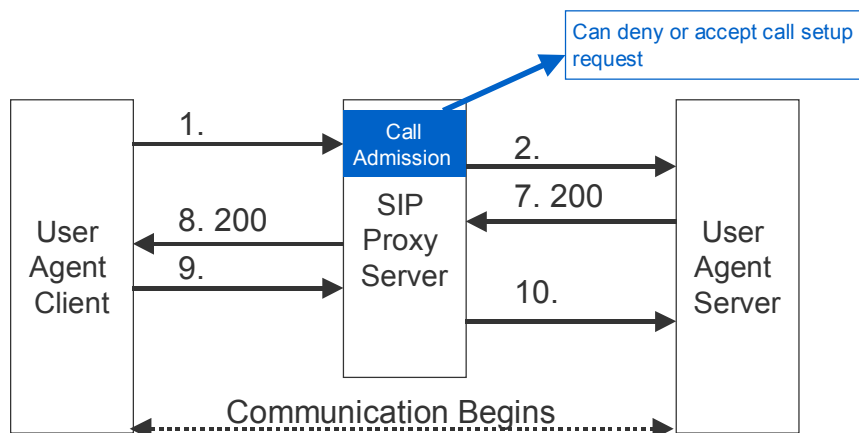

Figure 3. SIP VoIP setup messages

If signaling messages are lost due to packet loss or congestion, transmission control protocol (TCP) retransmission procedures resend them. The number of times TCP will attempt to resend a message depends on the TCP configuration (retransmission number and timeout thresholds, etc.). The SIP originating endpoint can also be configured to abort a signaling setup request independent of TCP connection retries. Therefore, the UAC can end the setup request at a set threshold even if TCP is still trying to connect. For example, if the UAC time limit is 1 second, after one second UAC will abort the connection even if TCP has not yet successfully set up the connection. This can be used as an upper bound on the time allocated to set up a call.

---

[1] Others include IEEE H.323, but SIP seems to be the most prevalent.

Service accessibility is then the probability that the SIP proxy accepts the request and that all signaling messages complete within the UAC time limit. These events, in turn, depend on the state of the network at the time of the call setup request. Network element failures during the exchange of SIP messages play a role, but usually network congestion is the primary driver of service accessibility. It is frequently necessary to resort to simulation to develop this model further.

5.2 Models for Service Continuity

To illustrate service continuity modeling in connectionless networks, we here give a procedure for studying VoIP service fulfillment, which describes how well a call adheres to standards of perceptual (in this case, audio) quality, or how intelligible is the information being transferred to the user. For voice services, intelligibility is often summarized as a mean opinion score (MOS) [12]. MOS provides a numerical measure of the quality of human speech at the destination end of the call. MOS ranges from 5 to 1 with a decreasing quality rating: 5: excellent (toll quality), good, fair, poor, and 1: unsatisfactory (not intelligible). MOS is established using subjective tests that are statistically analyzed to obtain a quantitative indicator of human perception of audio quality.

The probability $P_m = P\{\text{MOS} \geq m\}$ that MOS is above a specified value for a VoIP call is calculated given values for packet loss and delay using the E-model proposed by the ITU [13]. The E-model posits first an R-value that is influenced by five factors: the basic signal-to-noise ratio, three "impairment factors" corresponding to echo, delay, packet loss and codec distortion, and user tolerance for distortion. MOS is an increasing function of R-value [14]. The model proceeds by finding the R-value R_m for which $R \geq R_m$ is equivalent to MOS $\geq m$. Then, based on packet loss, delay, and jitter, values for the factors contributing to R_m are determined and the probability computed. Many details have been omitted from this summary. See Section 7.2 of [15] for a full treatment.

5.3 Models for Service Release

In commercial telecommunications, service release problems are very rare. Additional investigation will be required to determine whether this is also the case for NCO information product delivery services carried on the types of IPDI discussed above.

6 CONCLUSIONS AND FUTURE WORK

The NCO CF makes clear that NCW stands or falls on the quality of the information that it uses as fuel. It is equally clear that information of even the highest quality is of no value to a user who cannot acquire it in a form close enough to its original form that its quality is not degraded. We are therefore committed to study the reliability of the services that users employ to get NCO information products from remote repositories.

Service accessibility tells us whether users are able to set up the transactions they need to ask for the information products. Service continuity tells us whether users are able to acquire the whole information product without interruption and whether the quality of the information product is degraded during its journey from repository to user. Service release tells us whether, once having completed a transaction that transfers an information product from repository to user, the IPDI may be reset so that another transaction may take place. This paper gives an introduction to these concepts as applied to NCO information product delivery services and illustrates the ideas with service reliability analyses for KWeb and GBS, two such services that have been used in CTF50 and Stryker Brigade Combat Team operations. The paper also introduces some ideas for quantitative modeling of service reliability in the NCO context.

REFERENCES

1. P. J. Driscoll and S. Henderson (2005), A Meta-model Architecture for Fusing Battlefield Information. Submitted to *J. Milit. Oper. Res. Soc.*.

2. P. J. Driscoll, E. Pohl, and M. Tortorella. (2005), Information Product Quality in Network Centric Operations: Case Study Analysis. In preparation.

3. K. von Clausewitz (1982), *On War*. Peter Paret translation. New York: Viking.

4. Signori, D. (2002), A conceptual framework for network centric warfare. Joint RAND & EBR presentation at the Workshop on Network Centric Warfare and Network Enabled Capabilities, December 17-19.

5. M. Tortorella (2005), Service Reliability Theory and Engineering, I: Foundations. *Quality Technology and Quantitative Management* **2** no. 1, 1-17.

6. M. Tortorella (2005), Service Reliability Theory and Engineering, II: Models and Examples. *Quality Technology and Quantitative Management* **2** no. 1, 18-40.

7. M. Adkins and J. Kruse (2003), Case Study: Network Centric Warfare in the U. S. Navy's Fifth Fleet. University of Arizona Center for the Management of Information.

8. D. Gonzales, M. Johnson, *et al.* (2004), Network Centric Operations (NCO) Case Study: The Stryker Brigade Combat Team. RAND Corporation report DRR-3338-OSD.

9. H. W. Wadsworth, K. S. Stephens, and A. B. Godfrey (1986), *Modern Methods for Quality Control and Improvement*. New York: John Wiley and Sons.

10. M. J. Eppler (2003), *Managing Information Quality*. Berlin: Springer-Verlag.

11. H. Lesca and E. Lesca (1995), *Gestion de l'information, qualité de l'information, et performance de l'enterprise*. Paris: Litec.

12. ITU-T Recommendation P.800, Methods for subjective determination of transmission quality.

13. ITU-T Recommendation G.107

14. Sun, L. and Ifeachor, E. C. (2002), Perceivced Speech Quality Prediction for Voice Over IP Based Networks. *Proc. IEEE International Communications Conference*, 2573-2577.

15. Office of the Manager, National Communications System (November 2002), Network Topology Report. Arlington, VA: Technical and Programs Division (N2).

INFORMATION QUALITY: RELIABILITY OF NCO INFORMATION PRODUCT DELIVERY SERVICES

Michael Tortorella, Ph. D.
Rutgers University

THEME

❖ NCO stands or falls on the quality of information delivered to the user

   ❑ User develops accurate situational awareness

   ❑ User makes good decisions

❖ Even information of the highest quality is useless if the user can't get at it

   ❑ Information product delivery *services* must be *reliable*

❖ This research targets the information producer-distributor-user *system*

OVERVIEW

❖ Information product delivery services in NCO
  ❑ Examples
  ❑ General framework

❖ Information product delivery service reliability
  ❑ Definitions
  ❑ Figures of Merit and Metrics
  ❑ Models
  ❑ Examples

❖ Case study findings

❖ Discussion

❖ Conclusions and future work

NCO INFO PRODUCT DELIVERY SERVICES

❖ Examples
- ❑ CTF50
  - ✛ <u>Knowledge Web</u> (KWeb)
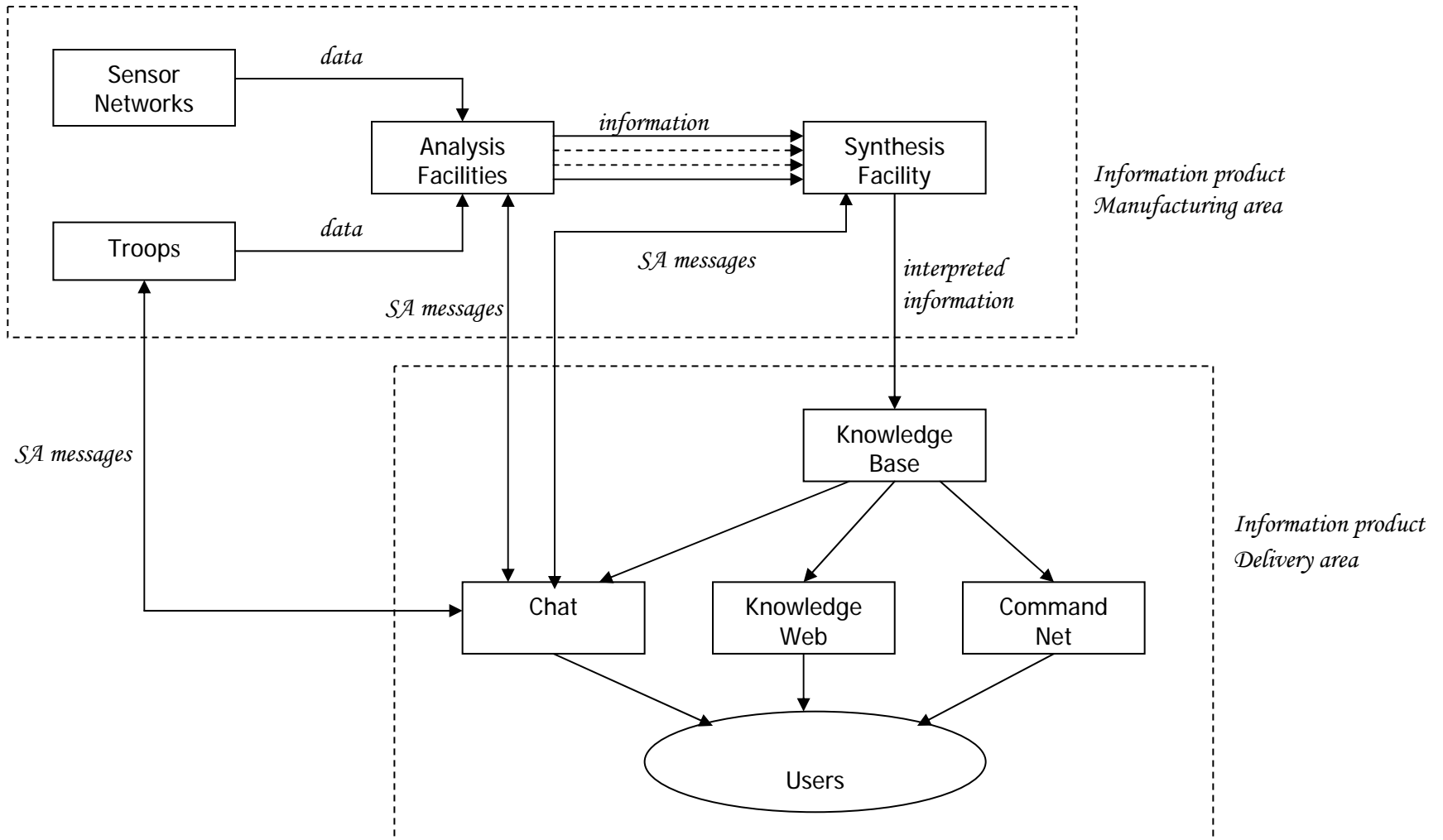 - ✛ Chat rooms
  - ✛ CommandNet
- ❑ **Stryker Brigade**
  - ✛ SBCT Network
    - Satellite communications wide-area network (WAN),
    - TOC-to-TOC network (TOC = tactical operations center),
    - Tactical Internet
    - Command Net Radio Network (CNR), and
    - <u>Global Broadcast System</u>

NCO IP DELIVERY SERVICES RELIABILITY

❖ Each instance of an information product's being transferred to a user constitutes a *transaction* in the service

❖ Example: KWeb pull services
  ❑ User requests a particular page (URL)
  ❑ Server accepts request & sends page
  ❑ User reads page
  ❑ User finishes with that page

NCO IP DELIVERY SERVICES RELIABILITY

❖ KWeb, whatever else it may be, is a delivery service for pages stored on a remote server

❖ For these pages (information products) to be useful, the delivery service must be reliable

SERVICE RELIABILITY DEFINITIONS

❖ Service accessibility
- ❑ Can start up a transaction in the service when desired

❖ Service continuity
- ❑ Successfully-started transaction carries through to completion without interruption
- ❑ All perceptual variables (*e. g.*, audio, video) have satisfactory quality throughout

❖ Service release

❖ $\alpha(t, \underline{v}) = P\{$transaction setup attempt at time t is successful when prevailing conditions are $\underline{v}\}$

❖ $\gamma(t, h; \underline{v}) = P\{$a transaction successfully set up at time t and lasting for duration h is successfully completed at time $t + h$ when prevailing conditions are $\underline{v}\}$

❖ Figures of merit are developed from models of the IPDI and its operations

SERVICE RELIABILITY METRICS

❖ Metric is a statistic that estimates a figure of merit

$$\hat{\alpha} = \frac{\text{\# of successful transaction setups}}{\text{total \# of transaction setup attempts}}$$

$$\hat{\gamma} = \frac{\text{\# of successfully completed transactions}}{\text{total \# of successful transaction setups}}$$

SERVICE RELIABILITY MODELS

- ❖ **Queueing networks**
  - ❑ Packet delay distribution

- ❖ **Stochastic flow networks**
  - ❑ IPDI failures in OSI 7-layer model context
    - ✛ Accidental
    - ✛ Deliberate
  - ❑ Information deterioration in transit

- ❖ **In all cases, connect to service accessibility and continuity FOMs via the relevant failure modes and failure mechanisms**

SERVICE RELIABILITY EXAMPLES

❖ Wireless telephony
- ❑ Failure mode: dropped call
- ❑ Failure mechanisms: weak signal, base station failure, MSO failure,…

❖ Package delivery
- ❑ Failure mode: late delivery
- ❑ Failure mechanism: numerous!

❖ Electric utility
- ❑ Failure mode: incorrect bill
- ❑ Failure mechanism: numerous!

$$\text{FOM}(t, h; \underline{v}) = P\left(\bigcup_{i=1}^{m} \{\text{Failure mode } i\}\right) =$$

$$= P\left(\bigcup_{i=1}^{m} \left\{\bigcup_{j=1}^{n_i} \text{Failure mechanism } j \text{ for failure mode } i\right\}\right)$$

SERVICE RELIABILITY REQUIREMENTS

❖ Set requirements for desired service reliability characteristics

❖ Use the framework (slide 13) to see how to arrange the IPDI reliability requirements so that the desired service reliability requirements are met

KWEB ANALYSIS
SERVICE ACCESSIBILITY

BREAKDOWN FAILURES		PERFORMANCE FAILURES	
MODES	**MECHANISMS**	**MODES**	**MECHANISMS**

Browser does not open when requested	▪ PC compromised
	o Worm/virus
		Excessive delay in opening browser	▪ CPU overloaded
			  o Legitimate activity
			  o Virus/worm

No response to user request for page	▪ Server down
	▪ Request misdirected
	  o Deliberate
	    ☞ Opposing force wiretap
	  o Accidental
	    ☞ Routing table errors
		Excessive delay in responding to user request for page (starting page load)	▪ IPDI congestion
			  o Excess offered load
			  o IPDI element failures
			  o IPDI compromised
			    ☞ Physical damage
			    ☞ DOS attack
			▪ Server overloaded
			  o Excess traffic
			  o Server subsystem failures
			  o Server compromised

NCO INFORMATION QUALITY & RELIABILITY

KWEB ANALYSIS
SERVICE CONTINUITY

BREAKDOWN FAILURES		PERFORMANCE FAILURES	
MODES	**MECHANISMS**	**MODES**	**MECHANISMS**

Page load permanently stalled	▪ Packet loss <u>and</u> TCP failure
	 o Incoming
	▪ IPDI access failure
		Excessive delay in completing page load	▪ IPDI congestion
			 o Excess offered load
			 o IPDI element failures
			 o IPDI compromised
			  ☞ Physical damage
			  ☞ DOS attack
			▪ Server overloaded
			 o Excess traffic
			 o Server subsystem failures
			 o Server compromised

Subsequent page request refused/failed	▪ IPDI access failure ▪ Packet loss <u>and</u> TCP failure o Incoming o Outgoing	Incorrect page served to user	▪ Request corrupted in transit ▪ Server database corrupted ▪ Requesting page spoofed
		Audio and/or video garbled/unintelligible	▪ Packet loss ▪ Excessive packet latency

GBS ANALYSIS
SERVICE ACCESSIBILITY

❖ Global Broadcast System is a push service
  ❑ Transaction begins when user turns attention to the interface

❖ Service accessibility is equal to the probability that the GBS is operating properly at the desired time
  ❑ As a system
  ❑ Receiving signals and displaying them
    + Near zero latency

GBS ANALYSIS
SERVICE CONTINUITY

BREAKDOWN FAILURES		PERFORMANCE FAILURES	
MODES	**MECHANISMS**	**MODES**	**MECHANISMS**
Streaming audio or video stops, does not restart	▪ Loss of entire satellite ▪ Loss of dedicated transponder ▪ Loss of downlink ▪ Interface failure ▪ Broadcast origination failure	Streaming audio/video distorted/garbled	▪ Broadcast origination failure ▪ Interface failure ▪ Packet bearer bit errors ▪ IPDI congestion ▪ Excessive packet loss and/or delay
Static video disappears	▪ Remote refresh failure ▪ Interface failure	Gaps in streaming audio/video	▪ Intermittent satellite failure ▪ Intermittent dedicated transponder failure ▪ Intermittent downlink failure ▪ Intermittent interface failure ▪ Severe packet loss and/or delay

DISCUSSION

❖ Information assurance studies concern operation of the IPDI

  ❑ But without understanding the effect of IPDI anomalies on the user, we are stuck with "less [bad stuff] is better"

❖ Explicit consideration of user needs enables setting requirements for IPDI behavior on a rational basis

CONCLUSIONS

❖ Reliability of the information product delivery service bears on key information parameters

- ❑ Quality
- ❑ Reliability
- ❑ Risk to Use

❖ We have begun to understand how this works in NCO

❖ Much remains to be done

FUTURE WORK

❖ Complete a service reliability analysis in detail for a prospective NCO information product delivery service to show how early attention to service reliability concerns will positively influence the service architecture.

❖ Incorporate the effects of deliberate disruptive actions (e. g., opposing force action and/or software attacks such as denial-of-service attacks, worms, and the like) into service reliability studies.

FUTURE WORK

❖ Further enhance the application of service reliability theory to NCO by developing IPDI reliability models for failures at the transport, network, protocol, session, and application layers as well as the physical layer.

❖ Develop a model for the deterioration of information as it passes through a connectionless network of noisy channels.