Application of COTS Communications Services for Command and Control of Military Forces

Peter Kerr[1] Jeff McCarthy[1,2]
[1]Head Wireless Systems Group, Communications Division, Defence Science and Technology Organisation, Australian Department of Defence, United Kingdom
[2]Satellite Communications Department, DERA Defford (on attachment), WORCS WR8 9DU, United Kingdom
Contact: Peter.Kerr@dsto.defence.gov.au
JMCCarthyl@dera.gov.uk

1. Introduction

This paper describes issues related to the use of commercial communication systems in support of military command and control. These systems[1] provide paging (messaging) and telephony services with global reach using small (personal), autonomously powered terminals.

New commercial telephony and paging systems offer ready access to advanced communications technology for a range of benign and hostile forces including the military, government agencies, media organisations, emergency services, insurgents and terrorists. The size, cost, coverage and ubiquity of all of these systems combined with the availability of tools targeting internet application development creates an interesting mix of threat and opportunity for military organisations.

One of the key advantages offered by the group of new telecommunications networks is diversity. Diversity of supply may enable a future adversary to use up to five systems in order to provide a voice service. For example, a user could subscribe to voice services based on GSM, CDMA, Inmarsat, Iridium, Globalstar systems using only three terminals that could easily fit into a briefcase. These example systems would operate in five different frequency bands and all are highly independent of each other in terms of the supporting network.

This paper is structured in the following way. Section two describes some high level attributes required of these commercial systems in order to operate in a military communication environment. Section three highlights the differences that would typically exist between the commercial and military communication markets and their associated procurement strategies. Section four provides some examples of COTS solutions for military applications, which include Command and Control Warfare (C2W), and the application of COTS for Australian Defence Force (ADF) communications.

2. Military communication environment

The current thrust in military communications is towards achieving C4ISR[2] dominance in the battlespace. This dominance will provide commanders with the situational awareness and understanding that is necessary to achieve decision superiority at the tactical and operational levels of warfare.

In order to achieve the aforementioned objectives an integrated communication system will be required to provide a high level of connectivity between the various sensors, weapon systems, and Command and Control (C2) elements that exist in the battlespace. This leads to the concept of Network Centric Warfare (NCW), in which the battlespace consists of a dense grid of sensor and shooter networks that have been seamlessly integrated through communications onto a common information grid as shown in Figure 1.

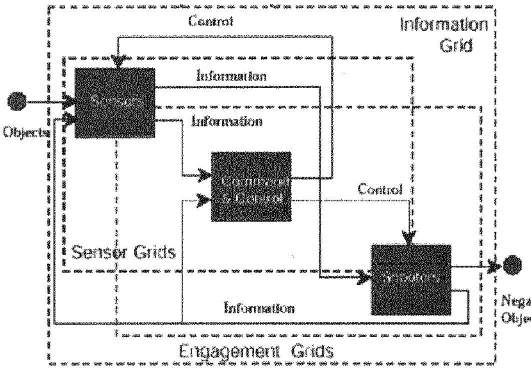

Figure 1: Integration of C2 in Network Centric Warfare

Current concepts for network centric warfare assume a communications architecture that is able to support a broad range of bandwidths over both short and long distances[3]. To a large extent this architecture is expected to depend on broadband wireless communications to support these information flows, however, the pre-eminent communication services required for command and still remain voice and low rate data.

It is the belief of the authors that the voice and low rate data command and control communication services could be provided by commercial satellite systems which, despite their commercial nature, may serve as a catalyst for future military communications and such concepts as NCW. The difficult problem for military planners, however, is tailoring these commercial systems in order to confer military attributes onto systems that have been designed for commercial operations. The first step towards solving this problem is, identifying the desired military attributes that are expected of information flows

[1] The COTS solution in this case may consist of products, services, or functionality.

[2] Command, Control, Communications, Information Surveillance, and Reconnaissance (C4ISR)

[3] Theatres of conflict are becoming increasingly characterised by greater dispersion and maneuverability of forces over wide geographic distances that may often extend deep into an adversary's territory.

Paper presented at the RTO IST Symposium on "Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS"", held in Brussels, Belgium, 3-5 April 2000, and published in RTO MP-48.

for the anticipated military environment. This occurs in the following section.

2.1 Military communications attributes

Military communication systems are generally expected to operate in environments that may be intolerable for commercial system operation. Accordingly, attributes of the military communication system, or more importantly the *environment* it is expected to operate in, have been used to characterise the system, and also to often distinguish it from commercial systems. The sustained growth in commercial telecommunication sector, however, has seen a steady increase in the demand for more military oriented attributes to become associated with commercial services. Although these services still would not meet the attribute requirements in a stringent military environment, they still may satisfy requirements for the less stringent environments that are more likely to occur[4].

The military attributes to be considered for this paper include, but are not limited to, the following descriptions;

- Quality of Service (QoS)
- Mobility
- Survivability
- Security

Each of these attributes is detailed in the following sections.

2.1.1 QoS

Quality of service is defined for these systems by the following characteristics.

- Data transfer rate
- Bit error rate, voice quality
- End-end propagation delay
- Call setup time
- Dropped call rate
- Capacity
- Communications reliability

The combination of these commercial characteristics help to define how effective a given communication service will be for C2 applications.

Comparisons to extant military communications systems such as tactical satellite communications and High Frequency (HF) show the new systems offer significant improvement in most of these measures of QoS. This is primarily due to improved source and channel coding and in response to increased demands from the commercial marketplace.

2.1.2 Mobility

Mobility is affected by the size of the terminal, the ability to establish and maintain communications on the move and the need for external sources of power. The advent of small battery powered computer such as PDA (Personal Data Assistants) and the integration with mobile communications provides numerous opportunities for situational awareness and command support systems for highly mobile forces.

Terminals requiring directional antennas tend to provide less mobility for small platforms (including troops) due to the complexity of acquisition and tracking systems.

In modern networks mobility may also include the ability to roam between networks, ie. Networks have the ability to mutually authenticate users and allow access. In this case service mobility may provide diversity and improve survivability of the service.

2.1.3 Survivability

Service survivability is a primary concern for military operations. Failure or loss of availability of a communications system in conflict can have disastrous consequences and the ability of a system to survive a range of incidental and deliberate actions is an important consideration for military planners.

Survivability can be thought of as security of supply and will be affected by the robustness and resilience of a system to a range of attacks, including factors such as congestion. Survivability must include considerations for conventional and non-conventional attacks on the air interface and on the supporting infrastructure used by each system to terminate or deliver traffic.

2.1.4 Security

Security refers to the ability to protect traffic (messages, voice and data) and traffic flow information. Because of the inherent mobility offered by most of the systems considered in this paper protecting traffic flow information may become highly important (ie. who is calling who, for how long, how often and from where).

Security is also defined to include protective measures to prevent deception through masquerading (pretending to be another user) and spoofing (injection of false messages).

All of the systems described in this paper claim to be developing security devices that offer varying degrees of end to end traffic security. The Inmarsat voice services all claim to be capable of supporting STU-III encryption. The newer systems aiming for US government markets (Iridium, Globalstar and ICO) are all developing Type-1 security products, mainly based on the FNBDT specification. This development will probably also see Type-3 and Type-4 encryption devices produced for the commercial marketplace.

[4] Note that the importance of each attribute is expected to vary according to the type of military scenario being considered.

3. Comparison of military and commercial markets

The differences between commercial and military communication attributes have been identified in the previous section, however, there still remains the problem of achieving a solution that will satisfy requirements and be cost effective in the long term. The type of solution will depend on the military planner's ability to exploit features of the commercial market, and also their willingness to modify these features according to their own market driven requirements. Furthermore, in order for this solution to be successful an understanding of the differences that exist between commercial and military products and services markets are required.
Some of these differences are outlined as follows;

- Commercial markets tend to be characterised by a more diverse, and much larger, number of users, which results in more mature products[5] that offer a wide range of features[6].
- The ability of an individual user to discard or upgrade a product or service is easier than it is for the military, which requires a "fleet" approach to procurement and maintaining compatibility between various upgrades of equipment or services[7].
- Product or service standards tend to be only valuable if they are popular, otherwise a defacto standard[8] occurs. This result is most likely to be associated with a commercial market.
- Commercial business models tend to adapt more rapidly to changing technologies than do military business models, i.e. doctrines.
- The pace of the changing commercial marketplace is faster than the military market, as evident by the much shorter life cycles of commercial products and services in comparison to those of the military[9].

3.1 Growth in commercial communications market

Rapid consumer uptake of mobile telecommunications, Figure 2, has resulted in great interest from telecommunications service providers in most countries of the world.

New companies focussed on service provision have spun off from traditional telecommunications companies and have experienced rapid growth in market capitalisation[10]. This increasing capitalisation results from rapid growth in consumer uptake compared to traditional fixed telephony services. Indeed some market forecasters are now predicting cellular telephony penetration rates of 300 percent (3 mobile phones per person) compared to 50 percent penetration of fixed services in developed countries.

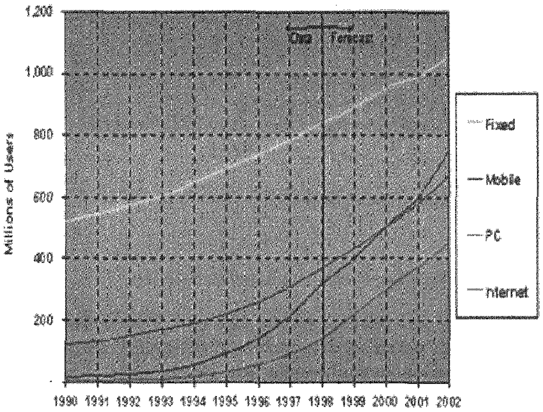

Figure 2: Growth in Commercial IT

To achieve these penetration rates implies that in the future the majority of cellular telephones will be used as embedded communications devices targeting machine to machine communications as well as for personal communicators. Furthermore, the rapid technological development and the enabling R&D investment can no longer be matched by military organisations and as a result Defence organisations risk being left behind unless it leverages the technological development in the commercial telecommunications sector.

Figure 3 shows one implication for military capability development if rapid commercial growth is not recognised as a factor. The axis marked Capability can represent any of the attributes listed in the previous section. This rapid advancement in the commercial sector may lead to an increasing technology deficit using a traditional military acquisition process. A better approach may be to adopt commercial technology in a way that adds military value yet maintain access to the commercial evolution path.

[5] A larger and more diverse number of users tends to accelerate the products "settling in" period.

[6] The large diversity in the types of users require a large range of features in order to meet the majority of requirements for these users.

[7] This would emphasise the importance of backward compatibility for military customers operating in a commercial market.

[8] Examples of defacto standards include, Windows operating system and software, and TCP/IP.

[9] This is largely due to the "fleet" procurement practice associated with the military acquisition. This acquisition approach, however is expected to change under Privately Funded Initiative (PFI) schemes, which may see a reduction in military product life cycles.

[10] For example, Japan's NTT DoCoMo is now capitalised at $527 billion dollars compared to $370 billion for its *parent* NTT. (Source: *Asia's mobile offspring dwarf their parents*, The Australian, 10/2/00, p 21)

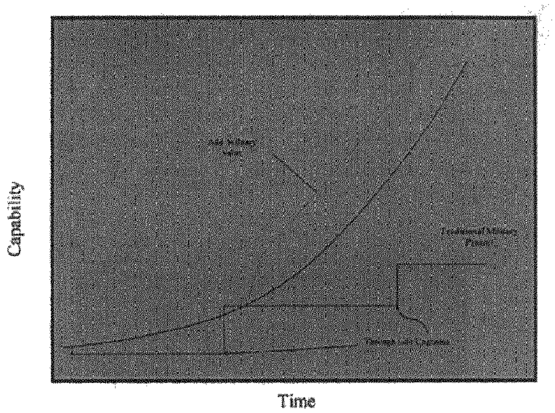

Figure 3: Implications of Exponential Growth

3.2 Marketplace procurement strategies

Ultimately, the success of the solution will be determined by its cost, which will depend on the initial procurement and upgrading strategies that are available in the military and commercial marketplaces.

A typical military investment strategy would be to provide significant up front capital investment in a product or service, as opposed to leasing commercial products or services at lower initial costs as shown in Figure 4.

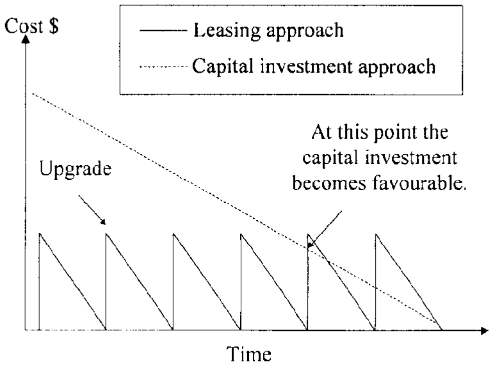

Figure 4 Leased versus capital investment strategies

Over time, the cost of leasing may eventually become higher than the dedicated military investment approach, however, access to the latest technologies and services, has been maintained over the entire period[11].

4. Application of COTS solutions for military communications

The challenge for military planners and capability development organisations is to identify those operational requirements that need specialised military communication services, and which can use military enhanced commercial services or unmodified services to meet these requirements.

They may also have to deal with the potential use by an adversary of the same advanced technology and devise methods of maintaining information superiority.

Some examples highlighting the application of COTS solutions for military communications are given in the following section.

4.1 Command and Control Warfare

One of the key challenges for future Command and Control Warfare (C2W), involving commercial communications systems, revolves around the ability to target particular users or groups of users. In many cases, both sides of a conflict will be using the same commercial communications networks. This will also be true of independent observers of conflict such as the UN, aid agencies and the media. The use of traditional means of C2W (degradation and denial) could well be counterproductive in complex conflicts

The means effective C2W strategies will allow a force to target individual subscribers or groups of subscribers. This is not a trivial task as all of these systems employ complex protocols that randomly allocate network resources to maximise capacity. Military forces need to be careful that C2W strategies do not force an adversary into using a C2 system that removes any advantage.

Area denial strategies based on dumb jammers may be effective, especially in combination with the use of smart antennas to enable friendly forces to overcome the effect of denial. Small, battery powered jamming terminals could be effective for this function but would have limited endurance for control of large areas. Airborne systems would be more effective and could support operations for longer periods of time from a reasonable stand-off distance using a directive antenna.

Other techniques for C2W could involve use of capabilities designed into the networks for fraud prevention and legal intercept requirements.

Diplomatic efforts to convince operators to enforce prioritisation may provide another simple and effective selection procedure. Most of the new commercial communications systems provide prioritisation and preemption capabilities although standard commercial practice is to assign almost all users to the same priority level. Operators would generally be hesitant to use prioritisation and preemption due to the perception that such use would adversely affect profits.

Similarly, the systems based on GSM maintain white, grey and black list of subscriber equipment. These lists are used by the commercial operators to manage fraud,

[11] Note that "break even" point will exist between the two approaches. Further note that if a customised solution were to be considered then the "serations" associated with the leasing strategy may begin to grow as the customised product begins to significantly deviate from the commercial product.

eg. the use of stolen phones or network access by a customer who does not pay the bill.

The white list contains details of subscribers who are entitled to have unrestricted access to the network. The grey list contains subscribers that may be of concern and use of the network by these subscribers generates an alarm in the network operations centre. The black list contains subscribers who are barred from using the network. These subscriber list can be readily changed by the operator and in a conflict could be used to warn of prevent network access by subscribers from a particular country or from a particular group. Operators may well seek compensation to allow such network management systems to be used as a means of C2W in a conflict.

4.2 COTS Communications in the ADF

While many nations are endeavouring to integrate COTS communications solutions into their military communication strategies, Australia has, through necessity , a considerable legacy in this area.

The Australian Defence Force currently employs a wide range of commercial communications technologies for the command and control of deployed forces. These services include leased capacity from civilian (Optus) and military (LEASAT) satellites to support broadband strategic, broadband tactical, and tactical mobile communications networks.

Australia also makes heavy use of Inmarsat and Intelsat services for off-shore deployments using commercial services with military encryption.

Further investigations into the potential application of commercial communication services are occurring through trials and evaluations in which the Defence Science and Technology Organisation (DSTO) participates in.

Current DSTO research programs are investigating the potential use of GSM, satellite PCS, broadcast technologies, ATM and IP communications products for tactical use.

Many of these systems were successfully deployed during the recent multilateral peace enforcement mission in East Timor.

5. Conclusion

New commercial satellite communications systems will be used for command and control in military conflicts of the future. The precedent was set in the Gulf war, when a large portion of military communications traffic was carried by commercial systems such as Inmarsat and Intelsat, and has followed in almost every major conflict since.

The advent of a number of systems offering new services and smaller, lower powered terminals may well create opportunities for well organised but less technically advanced adversaries to significantly improve their military capability.

The challenge is to ensure that these systems do not deliver an information advantage that could further complicate the range of military conflicts now experienced.

Similarly, as evidenced in Kosovo and East Timor, media and aid organisations using new communications technology have unprecedented mobility and this in turn could challenge military efforts in PSYCHOPS. Means of controlling benign parties such as media and aid agencies need to be devised. The danger is that some C2W techniques may inadvertently deny or degrade the communications of benign parties present in conflict scenarios and by doing so the results could well be counterproductive for the military effort.

The paper provides a brief summary of some issue related to military uptake of commercial communications systems. The focus has been on low data rate wireless technologies that might enable global command and control of national or multilateral forces. Some techniques for effective C2W against these systems based on inherent network capabilities and on external capabilities have been proposed.

Confidently Integrating COTS Software Under Worst Case Assumptions

Jeffrey Voas
Reliable Software Technologies
21351 Ridgetop Circle, Suite 400
Dulles, VA 20166, USA
jmvoas@rstcorp.com
Tel: 703.404.9293
Fax: 703.404.9295

Abstract

Most systems today are composed of hardware components, COTS software, and custom (bespoke) software. In terms of the software, the proportion of COTS software in a typical system is beginning to overtake the percentage of custom software. When a system fails, it may well be the COTS software that caused the system to fail given the well-publicized defect rates for acquired software. This paper describes a methodology for *predicting* the impact on system failure rates that a particular Commercial-Off-The-Shelf (COTS) software component might have before the component is embedded into the system.

1 Introduction

As software quality and information security becomes an increasingly well-publicized concern, the need for techniques that can accurately predict future failures and detect deficiencies grows. Voices from both industry and government are echoing this.

As an example, consider the comments of the US Department of Defense's CIO, Mr. Money, (June 17, 1999 issue of Federal Computer Week):

> *"The quality of software we are getting today is crap. Vendors are not building quality in. We are finding holes in it."*

Gary Beach, publisher of CIO Magazine, wrote on April 1, 1999:

> *"Are you tired of software vendors sending you service packs to fix bugs that should have been stamped out earlier? Off-the-shelf commercial software isn't good enough anymore. Service packs, indeed! Many CIOs I've talked to call them disservice packs."*

In my opinion, the underlying tension causing such comments to be made is directly related to the average defect density for all commercial software packages. According to Les Hatton,

> *"The industry standard for good commercial software is around 6 defects per KLOC in an overall range of around 6-30 defects per KLOC."*

Surprisingly, this rate has held fairly constant for the last two decades, regardless of the shift to object-oriented technology, automated debuggers, better test tools, stronger type safety in languages such as JAVA and ADA, etc.

If this range is correct, and given that COTS software is delivered in executable format (thus disallowing consumers to apply *white-box* techniques to assess for themselves the quality of the software) to the end users and system integrators, can the systems that rely on COTS software ever be trusted?

I will argue that the answer to this dilemma is "sometimes." And I will argue that even if the defect rate were higher than 30. While this is counterintuitive, the reason is that not all defects cause failure modes that are intolerable to the system.

The key then is to be able to predict, on a system-by-system basis, how well a system will be able to

Paper presented at the RTO IST Symposium on "Commercial Off-the-Shelf Products in Defence Applications "The Ruthless Pursuit of COTS"", held in Brussels, Belgium, 3-5 April 2000, and published in RTO MP-48.

tolerate COTS failures. This technique can also reveal what COTS failure modes the system will be able to tolerate.

To do so we employ a technique called Interface Propagation Analysis (IPA). IPA is a fault injection-based technique that simulates component and subsystem failures.

Our approach is simple. Start by simulating COTS component failures during system execution and observe how they affect the full system. If the effect is negligible, then it is fair to assume that if the component truly fails, the system will be able to tolerate real failures. If the impact is large, then the component needs additional scrutiny. The bottom line is that we do not care how poorly subsystems behave as long as their behaviors do not jeopardize the integrity of the full system.

As examples of the types of component failures that we might wish to simulate, consider events such as the COTS component hanging or failing to return a result to the system. Or it might be that the COTS component requires more memory than available and the component aborts.

IPA is normally applied once the software system is completed, thus it is a late life-cycle approach. However the analysis can still be applied before COTS components are integrated into the system provided that there exists a specification for what the component does such that we can generate failure modes from that specification. (Components that do not yet exist are termed "phantom components").

2 COTS and National Security

COTS systems cause great dependability fears. Probably nowhere is the concern greater than to information system security. The US Government considers the reliance of our military and national information infrastructure on public systems (such as the Internet and the telephone system) as severely compromising to national security. Currently, the US Government is spending billions of dollars in search of solutions to this vulnerability [1].

Biological systems use genetic diversity to enhance their survival. Each individual of a species is slightly different from another individual. The diseases that one individual is susceptible to may not damage another. This diversity increases the probability that a species will not be completely wiped out when epidemics occur. In information systems, however, we see the reverse trend occurring. We see less and less diversity being available, particularly in operating systems, due to the mainstream cry for standards and interoperability. In operating systems, we are converging towards two main platforms: UNIX and Windows. Operating systems are probably the most important of all COTS components today. Further, we are converging toward a handful of Web browsers, and this number, too, is likely to get smaller in the coming years. Because of this lack of diversity, we are all susceptible to the same types of attacks and vulnerabilities. And because our operating systems are off-the-shelf, we may also be

deficient in knowing everything going on in them and hence taking the appropriate action to protect ourselves.

The issue here is the *covert channel problem*. An executable component (other than the OS) may be making calls to the operating system that it is not supposed (and known) to. To determine whether this is happening requires a watchdog utility that has access to operating system level functionality. Tracking global environmental events requires the ability to keep track of the entire system. For example, it will probably be useful to monitor DeviceIoControl function calls. Not only will such calls need to be tracked, but isolating exactly who (or what component) is doing the calling is also required. This approach amounts to trying to wrap the operating system in order to see every request that enters or leaves the operating system. The downside to this approach is that it is both expensive to develop the utility, and expensive to execute it when the operating system is deployed. Also, this scheme would need to be implemented for each unique operating system.

3 Assessing COTS Software Failure Impacts

The first step in our approach is to determine how the system reacts to corrupted information being passed to it from COTS software functions. After all, if a COTS failure does not negatively impact the system, then concern over the dependability of the COTS component may be unwarranted.

As mentioned, the technique used here is *Interface Propagation Analysis* (IPA). The process of performing IPA is quite simple. The interfaces that are responsible for sending information out of a component to the system are first isolated. Random data generators are placed at those interfaces. As information exits a component, the generators grab the information and corrupt (modify) it. That modified information is then handed over to the system in place of the original information. This provides an analysis of how badly the system behaves when artificially corrupted information is injected into the state of the system.

One might wonder why we go through such an elaborate system to see how component failures affect the system. After all, why not just embed the components in and perform system-level testing? System-level testing will, in theory, determine this if component failures are frequent or the amount of system level testing is enormous. But if component failures are rare and the amount of system-level testing is limited, it is unlikely that system-level testing will provide any insight. So by forcing artificial component failures to occur, we can more quickly assess the tolerance of the system, even though we must always caveat our results with the realization that our injected failures were artificial.

IPA is composed of two software fault injection algorithms: "Propagation From" (PF) and "Propagation Across" (PA). PF corrupts the data exiting a real component (or phantom component) and observes what it does to the remainder of the system (i.e., what type of system failures ensue, if any). PF can also observe whether other subsystems fail and how. Thus, PF is an advanced testing technique that provides the raw information needed to measure the semantic interactions between components in order to measure their tolerance to one another.

PA corrupts the data entering a component. This process simulates the failure of system components that feed information into the component in order to see how it reacts. These simulated failures mimic human operator errors, failures from hardware devices, or failures from other software subsystems. After the component under analysis is forced to receive corrupt input, PA observes whether the component chokes on the bad data and fails. Note that PA is very similar to PF. The only difference is scale: PA is focused on standalone components and PF is focused on component/system interactions.

In summary, the main applications of IPA are: (1) making "buy" vs. "build" decisions, (2) recommending system redesigns when certain COTS failure modes have been demonstrated to be intolerable, and (3) providing intelligent heuristics for allocating testing resources. IPA provides information on how systems will tolerate the most detrimental failure modes of commercial software packages, hardware subsystems, and human operator errors. Here, for brevity, we have only focused on IPA simulating COTS component failures. (Further information on IPA can be found in [3,4,5].) By determining that even the worst failures from a COTS package are tolerable, the package can become a viable candidate for integration into the system even if it is relatively high in defects.

4 Summary

This paper has recommended methods for assessing whether a system can tolerate failures originating from COTS software subsystems. Because COTS software is often failure-prone, "defensive system designing" is prudent, and this paper has proposed one method that partially addresses this problem.

References

[1] General J. J. Sheehan. A commander-in-chief's view of rear-area, home-front vulnerabilities and support options. In *Proceedings of the Fifth InfoWarCon*, September 1996.

[2] J. Voas. Error Propagation Analysis for COTS Systems. *IEEE Computing and Control Engineering Journal*, 8(6):269-272, December 1997.

[3] J. Voas, F. Charron, G. McGraw, K. Miller & M. Friedman. *"Predicting How Badly 'Good' Software Can Behave"*. IEEE Software, 14 (4): 73-83, July, 1997

[4] J. Voas. *"Certifying Off-the-Shelf Software Components,"* IEEE Software, 31 (6): 53-59, June, 1998.

[5] A. Ghosh & J. Voas. "Innoculating Software for Survivability," Communications of the ACM, 42 (7): 38-44, July, 1999.