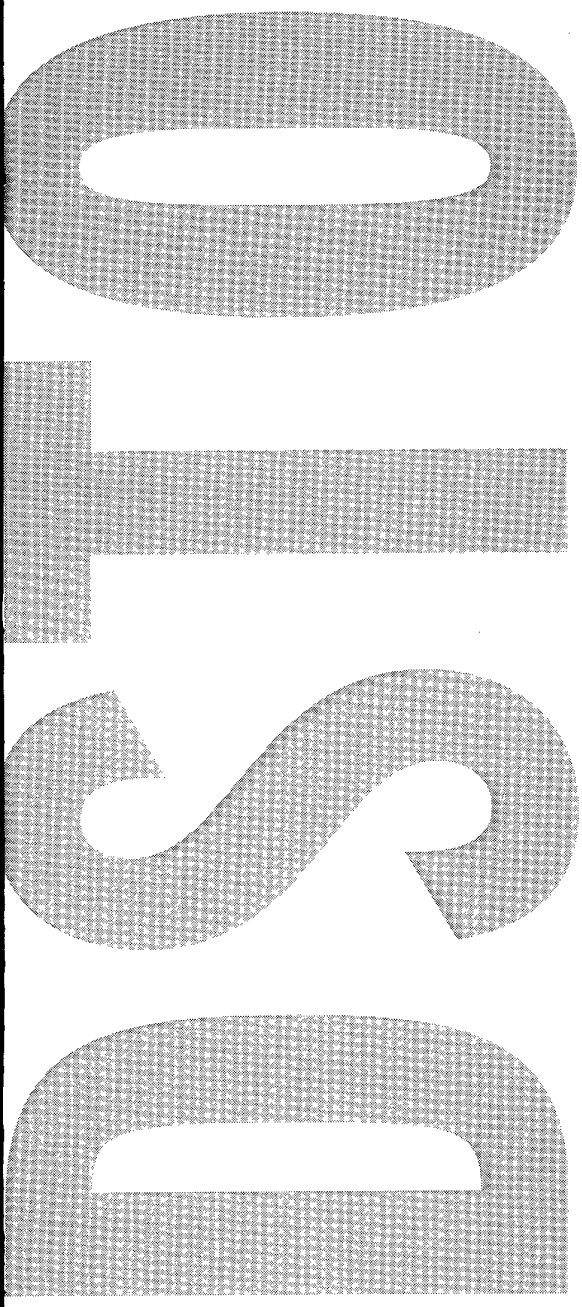
DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO



Aspects of Command and Control System Vulnerability Analysis

Lewis Warren

DSTO-TR-1123

Aspects of Command and Control System Vulnerability Analysis

Lewis Warren

Information Technology Division
Electronics and Surveillance Research Laboratory

DSTO-TR-1123

ABSTRACT

This report describes several different approaches to Command and Control System vulnerability analysis. The focus is on practical heuristics that can be used without a significant loss of accuracy. Topics covered are qualitative criticality evaluation of C2 nodes, identification of degradation sources, and dependability evaluation of digital C2 support systems. The use of the possibility measure for data with higher-order uncertainty forms is discussed, and dependability results using the possibility measure are contrasted with those of probabilistic methods.

RELEASE LIMITATION

Approved for public release

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO

Published by

DSTO Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury South Australia 5108 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-011-807
March 2001

APPROVED FOR PUBLIC RELEASE

Aspects of Command and Control System Vulnerability Analysis

Executive Summary

Vulnerability analysis of military command and control (C2) systems is an increasingly important field of study as awareness grows of the leverage that Information Operations can provide in adversarial conflicts. However, there are many kinds of vulnerability analysis and which is the appropriate form for any given C2 situation is not always obvious. Initially, the concept of nodal criticality is examined and several types of criticality are described so that the most appropriate version for a given C2 situation can be assessed. Next, C2 system vulnerability is discussed based on elemental dysfunctions of diverse types. The Failure Modes, Effects and Criticality Analysis technique of systems engineering is described for evaluating system vulnerability based on the potential combination of diverse elemental dysfunctions. Finally, the concept of C2 network dependability is discussed based on combinatorial network communication failures. Two types of failure likelihood measure are applied in the network combinatorial computations: the conventional probabilistic failure likelihood, and the possibilistic likelihood measure. Whereas the probabilistic likelihood estimates the likelihood that communication between sets of nodes will not occur due to link failures, the use of possibilistic likelihoods estimates the communication failure likelihood that could feasibly occur for any set of nodes. It is suggested that the more conservative estimates derived using the possibility measure are especially relevant to military situations due to the use of subjective estimates for component failure likelihoods, and the limited relevance of historical evidence since the adversary will search for new ways to attack a system. An approximate probabilistic method is also demonstrated, and for some example networks the results are shown to exhibit small error from the more complicated exact probabilistic methods. This report aims to provide a broad perspective of the field of vulnerability analysis so that a suitable analytical approach, or combination of different approaches, can be selected to match the needs of a given C2 system and situation context. Overall, the emphasis is on practical methods, with relatively low computational requirements so that application in the field may be more readily achieved and not be dependent on the presence of technical analysts.

Author

Lewis Warren

Information Technology Division

Lewis has a background in industrial mathematical analysis and modelling for application development. He has a B.E.(Hons.) in Industrial Engineering from the University of Melbourne, a Master of Systems Engineering from RMIT University, and a PhD in Business Modelling from Swinburne University of Technology. In recent years he has focused on soft OR and AI techniques, especially uncertainty analysis for information processing and model definition. His research interests include hybrid uncertainty modelling and its application to strategic decision analysis and performance evaluation of complex systems.

Contents

1. Introduction

A command and control (C2) system consists of:

1. Flexible human agents
2. Information technology networks
3. Information traffic flows (patterns).

In threat situations these three types of elements interact and provide the foundation for military decision making. Military Information Operations is then concerned with identifying vulnerabilities across all three types of elements. Comprehensive vulnerability analysis would examine the behaviour of all three elements, and use various techniques to capture different aspects. This report will concentrate only on vulnerability analysis of the information technology networks and their outputs. Vulnerability analysis of the human elements would require the identification of key personnel, while vulnerability analysis of information flows would require dynamic network mapping tools to visualise information flow patterns for the identification of key nodes and links. A frequent objective of C2 system vulnerability analysis is to identify structural weaknesses so that the overall system can be designed to be robust, or hardened later against degradation attempts. Although this is largely a defensive objective, an adversary's network that has been mapped may also be analysed to detect weaknesses, and this can be valuable for planning offensive information operations.

Vulnerability analysis of complex military systems with human elements has several levels:

- Determination of critical nodes, subsystems, components, and links
- Evaluation of subsystem or component dysfunction modes
- Evaluation of C2 support network reliability and dependability.

While human C2 networks may appear similar to telecommunication networks, they are uniquely different in certain respects. In telecommunication network analysis, functionality measures are based on considerations such as: number of alternate paths, path lengths, path type, and number of routers. However, human C2 systems are more hierarchical and modular, and rather than combinatoric path alternatives, different considerations are important, such as the information influences and dependencies between nodal elements. Nevertheless, the communication functionality of C2 networks is obviously still important and should be monitored and evaluated. While the preferred performance measure for evaluating telecommunication networks has changed over the years, the general trend [12] has been from using the design criterion of probabilistic system "unreliability", to "unavailability" (for example, 4 hours downtime in 20 months). Thus, the trend has been towards *a posteriori* end-user metrics rather than *a priori* design metrics. For the theoretical estimation of unavailability, system exogenous information is required concerning the characteristics of the restoration process. Not only is *a priori* availability estimation more complex than reliability estimation, but it is also more tentative and potentially inaccurate. (A concise introduction to the theory of availability estimation can be found in [16]). It is also important to note that the steady-state, or long term value of interval availability of a network, is not the same as the point availability, or probabilistic reliability at a particular time. In relation to

digital C2 support networks, "survivability" [19] is another performance concept that is becoming more prevalent. Similar to availability, this measure factors in extra considerations such as susceptibility to penetration and ease of reconfiguration. Rather than being a prescriptive measure, it is also an *a posteriori* type of measure. A further term, "dependability" has also claimed some popularity in recent years. Frequently, dependability is used to include system maintainability characteristics, which may also include system exogenous factors in addition to the endogenous system reliability characteristic. In this report, dependability will be taken to mean reliability in the presence of various types of dysfunctions, some of which may be caused by system exogenous factors such as network intrusions and unauthorised access. In this way, dependability is intended to be a broader concept than reliability. However, a separate meaning for dependability may also be encountered - as the inter-dependence that can exist between system components - but that meaning will not be adopted in this report.

For evaluating the performance of C2 networks in the following discussion, the number of demands that are not met due to some dysfunction, will be taken to indicate the lack of dependability (unreliability) of C2 links. Each component undependability may be caused by hardware, software, or human dysfunctions, and the subjective evaluation of undesirable event likelihoods inevitably plays a large part in the initial stages of a vulnerability analysis. There are two main categories of *qualitative* vulnerability analysis: the first category aims to identify all the possible combinations of events that can cause degradation- a state space specification of degradation situations, while the second category requires the subjective evaluation of dependencies between C2 elements, which enables critical elements or nodes to be identified. In contrast, *quantitative* vulnerability analysis evaluates system and subsystem failure likelihoods and dependabilities, from combinations of component degradation event likelihoods. This report will focus on the following types of vulnerability analysis:

1. Criticality evaluation of C2 elements
2. Dependability evaluation as the likelihood of C2 communication success.

It is well known that the exact evaluation of statistical network reliability for large networks is a NP-hard problem. Discussion of the theoretical complexities of statistical network reliability analysis can be found in Shier [17], Colbourn [5], and Harms *et al.* [7]. There are also special issues relevant to C2 vulnerability analysis that are not addressed in this report. One such issue is how to formulate a network hardening strategy (for information assurance) subject to optimal use of budget funds. A recent approach to that problem for network hardening, or alternatively for network tampering, has been proposed by Lyle et al [11]. Overall, this report focuses on more general issues and the selection of practical solutions to the above two types of vulnerability analysis.

Section 2 first discusses several qualitative approaches to criticality evaluation of nodal elements within C2 systems. Section 3 then discusses the Failure Modes, Effects, and Criticality (FMECA) analytical technique for combining complex degradation modes with elemental degradation event likelihoods to estimate the system dysfunction likelihood. Section 4 then presents examples of static system dependability estimation, using the possibility measure for subjective estimates of degradation event likelihoods, and also describes some important aspects of

dynamic dependability monitoring. Finally Section 5 summarises the principle notions of this report.

2. C2 Node Criticality Evaluation

2.1 Introduction

A C2 cell can be separated into its component elements and decomposition may be on the basis of hardware systems, or utilise more abstract higher-level decision units composed of people, hardware, software, and applications. One approach to criticality evaluation is to use specialised network visualisation tools that can identify nodes and links with high information flows. However, with this type of analysis criticality is equated with traffic volume and the significance, or relevance, to the whole system is not considered. Several approaches that follow for C2 node criticality evaluation are based upon qualitative influence ratings for a node in relation to other nodes, which reflect the degree of relevance of a node's information output to the other nodes' information processing activities. These qualitative influence ratings are simply influence ratings between 0, for no influence at all, and 1 for total influence, meaning the source node totally determines the sink node. A linguistic scale may also be used to rate the relative influence strengths. However, any subjective dependency evaluation is very context dependent, especially when nodes represent flexible human individuals or groups. For this reason, rating them out of context, or for well-defined threat situations, may well be unrealistic. In addition to influence strength based methods, the technique of C2 process mapping is also described.

2.2 Node Criticality Based-on Sum of Nodal Output Influences

The qualitative inter-nodal influences or dependency ratings can be represented in a matrix and simple summation across rows is sufficient to prioritise the influence strengths of the ouputs from the source nodes. For asymmetric networks, such a matrix is not symmetrical, not additive ($a_{ij} \neq a_{ji}$), and not multiplicative ($a_{ij} \neq 1/ a_{ji}$). For this simple type of criticality evaluation, techniques for higher-order uncertainty modelling are not required because the influence strengths are not likelihoods. Such criticality prioritisation by aggregate output influences at a node, does not consider a node's relevance or importance with respect to the total system, and the output links may be at a low level in the C2 cell or be concerned with some non-essential aspect of the situation.

2.3 Node Criticality Based-on a Nodal Domination Measure

This approach is based on a relative power measure that was proposed [20] for use in social networks. That measure is the *β-measure* and for any pair of source and sink nodes in a directed network it is the ratio of the influence strength between the pair, over the sum of nodal influences into the sink node i.e. the proportional influence of the source on the sink node. For any directed network a matrix of *β-measures* can be derived according to the network structure. These values can then be summed across columns (sinks) for each row (source) indicating the total domination power of each node with respect to the whole network. By ranking these dominance sums the more critical nodes at the top can then be determined. Although the authors of the *β-*

measure do not apply it in exactly this manner, they have also investigated the previous sum of outputs method (called the "score measure" in their terminology) and conclude that both relational power measures yield similar results.

2.4 Node Criticality Based-on Path to System Output

This qualitative approach evaluates criticality in relation to the number of links a node is displaced from the top-level system output. The assumption implicit in this approach is that system output (or decisions) are more dependent on higher-level nodes because they process more aggregated, or richer forms of information. In such simple qualitative influence diagrams, the influence of a node on the system output node is simply the multiple of the dependency or influence strengths along the uni-directional path. The uni-directional path of greatest value then defines the criticality of a node. For this type of top-down analysis, the general type of information synthesis operation at each C2 element must be taken into account. Nodal inputs may be processed by summarisation (the AND operation), which fuses all inputs into some global metric or summary evaluation. Alternatively, nodal inputs may be processed by a disjunctive operation (the OR operation), which selects between a variety of inputs. For AND type information processing, top-down analysis must evaluate influence strength multiples along all paths. However, for OR type information processing, only the path along the input link with the lowest influence strength need be considered; if the child node is a leaf node. But if the OR node's children has children, all its childrens' criticality values must be determined by multiplying their path influence strengths. From such top-down multiplications, values are determined for each node which provide a criticality ranking whereby higher-level nodes are inherently more critical. The weakness with this approach is when a node has a direct link to the top (say), but is still only of peripheral interest in a situation. This again points to the need to consider the intrinsic value or importance of a node's output in relation to the hierarchical C2 structure and the top-level decision.

2.5 Node Criticality Based-on Relative Importance Ratings

Different types of threat or military situations have different information processing needs. For example, a terrorist attack threat may not require much detailed geographic information since there is no attacking force of objects. It may be useful to evaluate the individual importance or value of C2 nodal outputs for different threat situations. An element may be compared to each and every other element in a C2 cell, and its importance subjectively rated in relation to the overall goal. From these pairwise comparisons, a matrix of relative values can be developed from which a priority vector can be synthesised showing the relative importance of each on a proximity scale [0,1]. Alternatively, instead of *directly* comparing the relative effect of two elements on the overall goal, a hierarchical set of relative importance measures (weights) could be subjectively developed by pairwise comparisons, as in the popular decision theoretic called the Analytic Hierarchy Process (AHP) [14]. This hierarchy would reflect the intrinsic hierarchical nature of C2 information processing, and the importance of any nodal element would be the product of the prioritised weights along the branches leading to the element. These nodal importance weights could then be factored into the previous three methods to make them somewhat more credible (i.e by using weighted influences). However, care should be taken when selecting a procedure to synthesise a priority vector from the

matrix of pairwise ratings, as there are some problems concerning the common eigenvector method used in the AHP. Barzilai [1][2] discusses some hidden dangers of the AHP technique and has proposed procedures to satisfy the requirements for an adequate prioritisation method.

2.6 Node Criticality Based-on Alternative Path Analysis

In communication network analysis, alternative path and combinatoric analysis is fundamental because paths represent routing options of messages between nodes. However, with C2 decision networks, the alternative path problem is less relevant to criticality analysis because the routing choices are generally less in hierarchical structured C2 systems. (For communication dependability analysis in the following section, alternative path evaluation is necessary to determine the exact solutions.) When alternative path options are considered for higher-level C2 system models with inter-nodal dependencies, a decision criterion must be defined to determine the criticality over all alternate paths between two nodes. One approach that has been proposed [13] uses the MaxMin decision rule, which takes the Max of the Min link dependency within each alternative path between two nodes, as the inter-dependency value for the two separated nodes in the C2 network. A prioritisation vector of nodal criticalities can then be determined, as above, from the nodal set dependency matrix. While the Max Min decision strategy may be justifiable for game type decision problems, where payoff tables are used, it would seem hard to justify its use in C2 systems without a clear reason. So C2 node criticality evaluation by alternative path analysis is somewhat hard to justify, and those considerations are more relevant to C2 system communication dependability analysis.

2.7 Node Criticality Based-on C2 Task Mapping

For a C2 node, or a group of C2 activities, the information flows with inputs and outputs at the various process stages can also be defined on a map using any of the various formalisms available for process mapping (such as IDEF0). On such a map, the information technology and other resources that are required by the different process stages and tasks can then be identified clearly. Consequently, the information resource requirements can be identified within the C2 cell, and the criticality of the various process stages are inferred from their resource dependencies. However, it is somewhat difficult to determine which resources are more critical in this type of process and activity mapping. In the commercial world, process mapping is widely used to identify inefficiencies and redundant activities within well defined resource transformation processes. When applied to military decision making, these objectives can only be achieved in a limited capacity due to the less well-defined resource transformation processes. Although there may be accepted stages of military decision making as described by the OODA loop, and sub-tasks defined by the universal task list, which aspects are most important actually depends on the situation and context. But perhaps the primary reason that process mapping has limited value for vulnerability analysis is that it mixes tools, activities, outputs, and resources in a fragmented linear picture. Within such a picture, it is difficult to identify which activity support services are more important. What may be more appropriate is to map only the information outputs from C2 elements, in a multi-tier model with both hierarchical and network aspects. Then for each support service, such as LAN, INTEL feeds, telephone, and computer applications; on separate maps show all the information outputs on the multi-tier

model that depend on one of these resources. Vulnerabilities would then be easier to identify visually, especially taking into account the importance of the different levels in the multi-tier model. For example, if the whole C2 cell depended on a single fibre optic cable into a node at the bottom tier, it would be clearly highlighted. In this way, such a model would represent the C2 elements in a manner whereby it is easier to identify critical resource dependencies.

2.8 Node Criticality Based-on Dynamic Analysis

The dynamic behaviour of a C2 network, with dependency ratings on links between nodes can also be investigated by means of the Fuzzy Cognitive Mapping (FCM) technique [8], used for dynamic analysis of directed cyclic networks. The nodes in FCM networks represent qualitative variables, or abstract concepts that are inter-linked in the overall problem. The knowledge outputs from C2 system elements (humans, digital systems, applications etc.) can be considered to be such qualitative variables. In FCM the activation levels of nodal states are usually [0,1] and link strengths are {-1,0,+1} or [-1, 1]. The complex feedback effects on the overall system behaviour can be explored in various ways. By fixing the states of variables, or turning them on or off, their relevance and hence criticality on the overall system can be examined. As a qualitative exploratory technique, sensitive nodes which have a relatively large impact on the overall system may thus be detected. Similar to neural nets, FCM use squashing functions for nodal transfer functions, and these squashing functions need to be specified so that they bear some correspondance to the information processing characteristics of C2 nodes.

When the directed dependency links of a FCM are subjectively assigned influence strengths, the FCM can be viewed as a dynamic system and its stability analysed. Kosko [9] has noted that the latent stability of static fuzzy associated memory (FAM) systems may be analysed using the eigenvalue of the edge connection matrix. Such static FAM systems act as sets of IF-THEN rules and do not iterate through multiple cycles, as do dynamic systems. In these cases, latent equilibrium is inherent if *all* the eigenvalues of the system have negative real parts [15], and potential instability is indicated when some eigenvalues have positive real parts. But the complex feedback patterns of dynamic FCM prevent this type of prescriptive analysis, and the dynamic stepped behaviour must be investigated empirically for the chosen squashing function and edge matrix. The dynamic behaviour of FCM must either stabilise as a repeating set of values, called a limit cycle which is a fixed set of values (including a fixed point), or else must exhibit constantly changing chaotic behaviour. The initial set of nodal state values does not determine whether a limit cycle develops or whether chaotic behaviour prevails; only the edge matrix (and especially the combination of positive and negative directed edges) determines the dynamic behavioural chracteristics.

With negative inter-nodal influences, increases in the state value (knowledge output) of a source node cause decreases in the state value (knowledge output) of the sink node. Assuming that there are seldom negative dependency links in C2 networks, in general, mainly limit cycles will develop for C2 networks. For this type of limit-cycle behaviour, the criticality of different nodes can be explored as follows. Since the fixed dependency matrix determines the limit cycle, the *time taken* to reach an observed limit cycle could be used to evaluate the disturbing effect a node can have

on the system. More critical nodes would then be those nodes whose degraded functionality would cause the system to oscillate for longer times before reaching the inherent limit cycle, or stable information processing capability. By clamping a node's value as low (say 0.1), and initialising the others, either randomly or at a reasonably high value (say 0.8), nodes which cause the system to oscillate for relatively longer time intervals can then be identified empirically. However, all that one could hope to learn from this type of qualitative investigation would be an intuitive feel for the significance of a node in relation to the whole C2 network. FCM analysis is also of limited value when there are definite importance levels or tiers in the C2 system.

3. C2 System Dysfunction Analysis

The evaluation of different ways by which C2 subsystems and components may fail or degrade is another aspect of vulnerability analysis. It has been noted that large complex system failures are frequently caused by surprising, or highly unlikely combinations of events. The nuclear disasters at Chernobyl, and more recently in Japan, were both caused by such combinations of human errors (as deviations from standard operating procedures). A standard systems engineering technique called Failure Modes, Effects and Criticality Analysis (FMECA) can be used to systematically explore the possible combinations of events that could cause problems, the nature of their effects, and the criticality of the effects. Using this technique, these details can be graphically represented on a fault tree using logical connectives (AND, OR, EXOR, etc.), appropriate to the significance of the different event combinations. Probabilistic likelihoods are traditionally used for the root events, and combined via the logical operators with probability laws to yield the likelihood of the head event; or failure of the system under study. The very small probabilities of the root events are frequently subjectively estimated, or taken from an industrial database in the case of common pieces of technical equipment. Although it is widely applied, the FMECA technique is somewhat limited by one's ability to conceive of all the possible problems, and the accuracy of the guesses for component likelihoods or of the failure data in industrial databases. For digital C2 support systems, the method may be most appropriate for evaluating problems caused by combinations of procedural anomalies and electronic component failure. For more critical systems, all the support services, such as telephone, power, water, gas; would obviously need to have redundant back-up readily available on stand-by. But a FMECA of less critical systems may help to identify those systems which need back-up, or the degree of back-up required to achieve the necessary level of system dependability. This author suggests that more realistic failure estimates from FMECA analysis may be derived if possibilistic likelihoods (PN) for the subjective component estimates are used instead of probabilities in the fault tree analysis stage of FMECA. Lower and more conservative dependability estimates would then result. Thus, another type of C2 system vulnerability analysis is to perform a FMECA study to identify potentially dangerous combinations of events, and it is suggested that possibilistic fault tree analysis is more appropriate when vague subjective likelihood estimates are the only inputs available. Although there have been many fault tree analyses using fuzzy probabilities, there have been far fewer studies using possibilistic likelihoods. A concise description of conventional probabilistic fault tree analysis and FMECA procedures can be found in [18], and a practical approach to

possibilistic fault tree analysis, which may be also applied to C2 system vulnerability analysis, can be found in [22][24].

4. C2 Support Network Dependability Analysis

4.1 Introduction

Since C2 is highly information dependent, the dependability of the supporting communication system is also critical and should be constantly monitored and evaluated. There are two types of communication network dependability evaluation: theoretical evaluation based on the synthesis of combined degradation event likelihoods, and practical evaluation by the simulation of stochastic traffic flow patterns based on channel capacities and random degradation event occurrences. The second approach using stochastic simulation is beyond the scope of this report. While an increase in network complexity can theoretically increase the total network reliability due to the increase in alternative paths, it also increases the vulnerability to potential communication disruptions. (For (n) fully connected nodes, there are (n(n-1)/2) links where communication degradation can potentially occur.) But in highly distributed C2 systems, the likelihood of communication degradation between a subset of nodes is generally of more interest than that of whole system degradation, which can be compromised merely by a single failure somewhere. Theoretical dependability estimation can be used as the first stage in designing more survivable and fault tolerant systems, including the evaluation of tradeoffs between dependability and vulnerability. (This reliability/vulnerability tradeoff problem is also beyond the scope of this report but techniques to address it can be found in [11] [23].)

As previously mentioned, it is not uncommon to use link unavailabilities as the proportion of time a link is down over a long period, for failure probability in network analysis. This is unsatisfactory because the probability functions express the probability that the link will die (or be alive) at any time, which is the chance that the system will not function on demand *due to forces of mortality.* This chance is different to the proportion of time a link is in a down state. The instantaneous or time-varying failure rate is sometimes called the force of mortality (or hazard rate), and this represents a certain probability of satisfying a demand at any point in time. If failures follow a stationary random process with a constant hazard rate, dependability (and reliability) deteriorates exponentially over time. On the other hand, interval availability is dependent on the size of the interval window, and is a composite function of reliability, ease to repair, and repair efficiency. While unavailability (% downtime) is critical for planning purposes, the proportion of time down does not reflect the type of probability required in network dependability analysis, even with a steady state assumption. So we will take dependability to be the chance that a link will die, or be killed at any instant, which may be updated as new evidence from system monitors comes available, or as new situations arise.

4.2 Higher-Order Uncertainty Modelling

This section will demonstrate how higher-order uncertainty modelling can affect computer system dependability evaluation when various types of subjective estimates are required for the diverse problems that can affect the

hardware/software system and its operators. Higher-order uncertainty (HOU) refers to multiple layers of uncertainty in situations where the amount of information available is small. The probability of a probability value is one such example, as is the possibility of a possibility value. This author has proposed [22][24] a practical approach to HOU representation when using the possibility measure, which enables the difference between ambiguity and vagueness to be clearly defined and measured. In that semantic framework, ambiguity (and conflict) refers to the existence of multiple possible values, while vagueness refers to indistinctness of values, inherently induced by the presence of indistinct set elements due to limitations of available information. Fuzzy probabilities are then examples of ambiguity, as approximate belief values that events (or states) *will* occur, while vague likelihoods are to be interpreted as approximate belief values that events *can* occur. It should be noted that only things that can happen, will happen (as per Murphy's Law), so the possibility metric is always greater than the corresponding probability metric (referred to as the Consistency Principle [24]). A detailed discussion of HOU representation for dependability analysis can be found in [23].

For many types of military models it is suggested that the possibility measure is very meaningful because:

- there is frequently only a small amount of factual evidence in combination with many uncertain estimates, or subjective guesses.
- "potentiality" evaluation is relevant to war because it refers to a feasible *range* of events, rather than indicating the predicted behaviour of the adversary based on probabilistic chance.

The main difference when using the possibility measure in dependability analysis is with the OR operator, as used for series system analysis or disjunct event evaluation. Simply speaking, when indistinct set elements are present there is an additional dimension of possibility (a higher-order) which must be managed carefully in disjunctive operations. In practice, this translates to simply adding the possibilistic event likelihoods instead of multiplying the success, or no event, likelihoods in probabilistic analysis. This simple summation of degradation event likelihoods is demonstrated in the following examples and always results in a lower system dependability estimate than the probabilistic estimate.

4.3 Some Simple Dependability Analysis Algorithms

4.3.1 Introduction

Von Collani [21] has proposed that the probabilistic reliability of any set of links in a network can be determined using a very simple approximation, in most cases with small error from exact solutions obtained by graph methods. In general, the magnitude of the approximation error is shown to be well within the error magnitude expected in the input subjective estimates for component event likelihoods. This approximation will also be used to demonstrate the difference between probabilistic estimates, and those based on possibilistic event likelihoods. Although von Collani's probabilistic approximation is the exact formula for possibilities with the disjunctive OR operator, another computational difference at the preliminary stage when using possibilistic likelihoods, where component sources of failure are aggregated into a single link unreliability estimate by the Series OR

operator (as below), leads to a quantitative deviation for possibilistic analysis from the results of von Collani's simple probabilistic approximation.

4.3.2 Preliminary Edge Unreliability Estimate

Consider a distributed C2 system composed of disparate local digital networks. A link between any two distributed C2 nodes {1,2} in the system consists of five communication stages, each of which may fail or be degraded. For simplicity, consider the likelihood of failure (0.07) to be the same for all five stages.

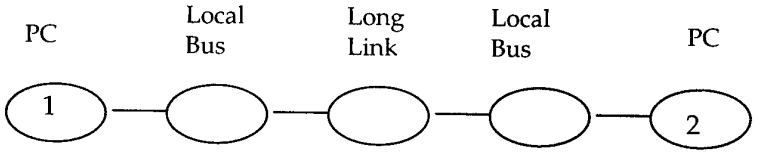


Figure 1: *Link Unreliability Components*

For probabilistic reliability analysis:

Link reliability	= (0.93)(0.93)(0.93)(0.93)(0.93)	= 0.6957
Link unreliability	= 1 - .6957	= 0.3043

For possibilistic reliability analysis:

Link unreliability	= 5 x 0.07	= 0.35
Link reliability	= 1 - 0.35	= 0.65

Von Collani presents three algorithms for network reliability computation: for any 2 nodes, for any set of nodes greater than 2, and for any set of nodes in networks which can obviously be partitioned into subnetworks. In essence, the approximations simply consider the simultaneous failure of all links at all of the specified nodes (which may be the whole network), and the algorithms approximate the minimal cut set equations. A detailed explanation of the rationale can be found in [21] and the objective of presenting these examples is only to highlight the difference between probability and possibility estimates. Examples 1,2, and 3 below assume identical unreliabilities for all links with the above values (0.30, 0.35) for probability and possibility. Example 4 demonstrates the method with non-identical link unreliabilities. Table 1 summarises the example computations and their deviations from the exact solutions as found in Beichelt [3], Blechschmidt [4] and von Collani [21]; and validated by Kraetzl [10] using Monte Carlo simulation techniques.

4.3.3 Some Example Network Evaluations

Example 1: Hexagonal Network

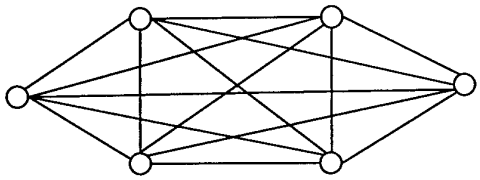


Figure 2: *Hexagonal Network*

Approximate Probabilistic Reliability:

$$R\{\text{All Nodes}\}=1-\{6(0.3)^5\}$$
$$= 1 - 0.1458$$
$$= 0.98542$$

Possibilistic Reliability :

$$R\{\text{All Nodes}\}=1-\{6(0.35)^5\}$$
$$= 1 - 0.03151$$
$$= 0.96849$$

Example 2: ART1 Network, as in Von Collani Figure 15.1 and also in Blechsmidt.

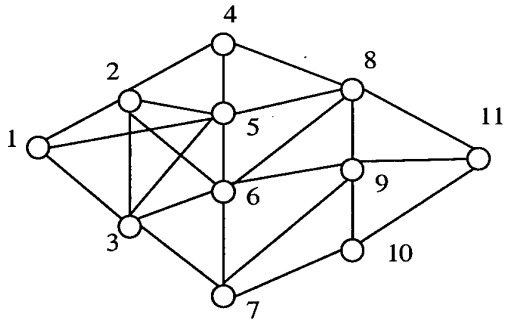


Figure 3 : ART1 Network

Node set { 1, 11 }

The implementation of the approximation algorithm can be explained from a cut-set viewpoint. If all the links out of each of the nodes in the target set are down, communication is impossible. However, when 2 terminal reliability is required (in a non-partitionable network) additional subsystems must be considered associated with each of the terminal nodes. Thus all links associated with *each path out* of each terminal node must be added to the composite failure of all links at each terminal node itself. The same reasoning (and equation) applies for simultaneous possibilistic and probabilistic failure likelihoods.

Let E be number of edges. Then $E_1 = 3$, $E_{11} = 3$

Plus $E_{1\text{-}2} = 6$, $E_{1\text{-}5} = 7$, $E_{1\text{-}3} = 6$, $E_{8\text{-}11} = 6$, $E_{9\text{-}11} = 6$, $E_{10\text{-}11} = 4$.

Approximate Probabilistic Reliability:

$$R\{1,11\} = 1-\left\{2(0.3)^3+(0.3)^4+4\,(0.3)^6+(0.3)^7\right\}$$
$$= 1 - 0.0652$$
$$= 0.9348$$

Possibilistic Reliability :

$$R\{1,11\} = 1-\left\{2(0.35)^3+(0.35)^4+4\,(0.35)^6+(0.35)^7\right\}$$
$$= 1 - 0.108752$$
$$= 0.8913$$

Node set { All Nodes }

Approximate Probabilistic Reliability:

$$R\{\text{All Nodes}\} = 1-\left\{4(0.3)^3+(0.3)^4+4\,(0.3)^5+2(0.3)^6\right\}$$
$$= 1 - 0.1273$$
$$= 0.8727$$

Possibilistic Reliability :

$$R\{\text{All Nodes}\} = 1-\left\{4(0.35)^3+(0.35)^4+4\,(0.35)^5+2(0.35)^6\right\}$$
$$= 1 - 0.21119$$
$$= 0.7888$$

Example 3: Network as in Beichelt's Figure 3.4 (14 nodes, 35 arcs)

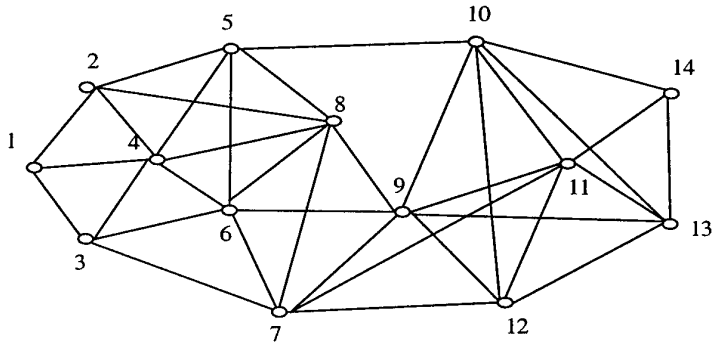


Figure 4: Beichelt's Figure 3.4

Node set { 1, 13 }
Approximate Probabilistic Reliability:

$$R\{1,13\} = 1-\left\{(0.3)^3+3(0.3)^5+(0.3)^6+(0.3)^7+(0.3)^8+2(0.3)^9\right\}$$
$$= 1 - 0.03534$$
$$= 0.96466$$

Possibilistic Reliability :

$$R\{1,13\} = 1-\left\{(0.35)^3+3(0.35)^5+(0.35)^6+(0.35)^7+(0.35)^8+2(0.35)^9\right\}$$
$$= 1 - 0.06149$$
$$= 0.93851$$

Node set { 1, 5, 13 }
Approximate Probabilistic Reliability:

$$R\{1,5,13\} = 1-\left\{(0.3)^3+2(0.3)^5\right\}$$
$$= 1 - 0.03186$$
$$= 0.96814$$

Possibilistic Reliability :

$$R\{1,5,13\} = 1-\left\{(0.35)^3+2(0.35)^5\right\}$$
$$= 1 - 0.05337$$
$$= 0.94663$$

Node set { All Nodes }
Approximate Probabilistic Reliability:

$$R\{\text{All Nodes}\} = 1-\left\{2(0.3)^3+2(0.3)^4+3(0.3)^5+6(0.3)^6+(0.3)^7\right\}$$
$$= 1 - 0.08208$$
$$= 0.91792$$

Possibilistic Reliability :

$$R\{\text{All Nodes}\} = 1-\left\{2(0.35)^3+2(0.35)^4+3(0.35)^5+6(0.35)^6+(0.35)^7\right\}$$
$$= 1 - 0.14408$$
$$= 0.85592$$

Example 4: A Small Network (10 nodes, 10 links)

This example will demonstrate the computations for a small network with low connectivity and exposure of end nodes to isolation. It will first be demonstrated how an individual arc unreliability can be derived for the link (1 – 7). For simplicity, consider a link has 3 parts, with an end node subject to 6 possible modes of dysfunction (a – f) and their likelihoods (probabilities or possibilities) per unit time

as below. Any of these may cause node failure and these crisp values could equally well be approximate or linguistic ratings with fuzzy computations applied.

a =	Operator accidental error	= 0.010
b =	Operator intentional error	= 0.005
c =	Hardware random failure	= 0.0015
d =	Hardware attack caused failure	= 0.010
e =	Software random error	= 0.010
f =	Software attack caused error	= 0.010

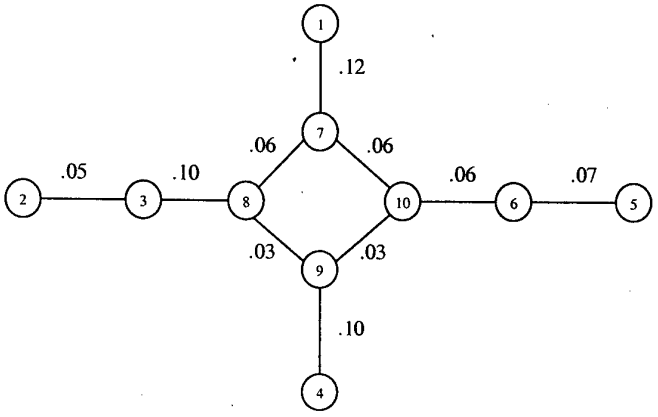


Figure 5: A Small Network

For simplicity, the fact that "a" and "b" are mutually exclusive will be ignored since the numerical error in using the probabilistic OR (instead of EXOR) operator will be small, for two values among the six.

Probabilistic unreliability of node = $1 - (1-.01)^4 (1-.005) (1-.0015)$ = 1- 0.9544
= 0.0456

Possibilistic unreliability of node = $4 \times .01 + .005 + .0015$ = 0.0465
Say both ≈ 0.05

In this manner, the dysfunction likelihoods of the three components of a link (2 nodes plus link) could be aggregated from the likelihoods of the potential degradation modes for each component.

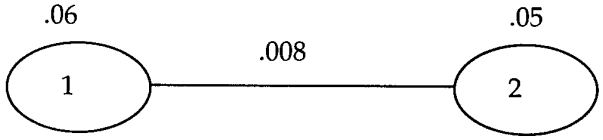


Figure 6: Link Unreliability Example

Since any of the three possible component dysfunctions of a link can result in communication failure, the OR operator can also be used to determine the single link unreliability.

Probabilistic unreliability = 1 - (1-.06)(1-.05) (1-.008) = 1- 0.885 = 0.115
Possibilistic unreliability = .06 + .05 + .008 = 0.118

Let both composite unreliabilities for the link ≈ 0.12

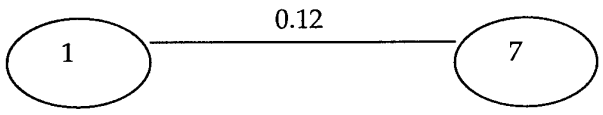


Figure 7: *Link Composite Unreliability*

Exact Probabilistic Reliability of the Small Network
Each composite arm of the small network can then be considered as a series system of links. In each arm of this cross network, the double connection to the central network is represented as a single link, with unreliability being the product of the two central links. By series system evaluation, the probabilistic reliability of each of the composite arms of the cross network are:

Rel (1,7)	= (1 - .12) (1 - .0036)	= .8768
Rel (2,8)	= (1 - .05) (1 - .1) (1 - .0018)	= .8535
Rel (4,9)	= (1 - .1) (1 - .0009)	= .8992
Rel (5,10)	= (1 - .07) (1 - .06) (1 - .0018)	= .8726

And failure of any composite arm (A,B,C,or D) results in network dysfunction, thus:

Network Unreliability = A Fails OR B Fails OR C Fails OR D Fails
(a logical Series system)
and Rel (Network) = .8768 x .8535 x .8992 x .8726
= .5872

This value represents the degree of belief in the exact chance that the system will be functional. The low value illustrates the inherent dangers of a star configuration where branch nodes have no alternate paths.

Approximate Probabilistic Reliability of the Small Network
By von Collani's algorithm : Consider all links at every node.

Rel (Network) = 1 - { .12 + (.06)(.06)(.12) + .05 + (.05)(.1) + (.1)(.06)(.03) + .1
+(.1)(.03)(.03)+ .07 + (.07)(.06) + (.06)(.06)(.03) }
= 1 - .3500
= 0.6500

This result is 10% higher than the exact value illustrating that the approximation accuracy decreases in less connected networks.

Possibilistic Reliability of System
Possibilistic composite arm unreliabilities:

Unrel (1,7)	= .12 + .0036	= .1236
Unrel (2,8)	= .05 + .10 +.0018	= .1518
Unrel (4,9)	= .10 + .0009	= .1009
Unrel (5,10)	= .07 + .06 + .0018	= .1318

Then by possibilistic OR operator :

Unreliability of Network	=	.1236 + .1518 + .1009 + .1318
	=	.5081
And, Rel (Network)	=	1 - .5081
	=	.4919

This value represents the degree of belief that the system can potentially be functional. Thus, using event likelihoods as possibilities for this small system the network reliability estimate is reduced by 16% from the exact probabilistic estimate of 0.5872. All results are summarised in Table 1.

4.4 Dynamic Dependability Monitoring

Elements within C2 systems can change in various ways, as can their working environment. Equipment degradation processes may change from stationarity to non-stationarity, operator behaviour may get lax or become error prone, and levels of national threat may increase. For diverse reasons, degradation event likelihoods may change at C2 system elements and this situation requires that network C2 elements be continuously monitored to detect when behavioural change becomes significant. There are many approaches one can take to update a variable's estimate on the basis of new evidence: Dempster/Shafer theory, Bayesian methods, genetic algorithms, and so on. However, the popular Bayes Net analytical technique is not so appropriate for this network dependability updating problem for the following reasons. Bayes Nets propagate a change at a node (or cue) across a uni-directional network by means of a set of inter-connected (joint) conditional probabilities. This may be appropriate for events whose effects can spread as with viral attacks, although conditional probabilities for viral transmission would also seem to be rather unrealistic in light of the mechanics of transmission. In general, Bayes Nets are suitable for reasoning in systems where the same symptoms (or instances) can arise from a number of different causes, or for updating proposition truth values on basis of inter-related evidence. But network dependability is affected via systemic dependability relationships, rather than by uni-directional conditional probability propagation through a network of components. Rather than conditional probability relationships between components, it is the logical relationships between components that determines overall system performance. What is most important for C2 system dependability control is to update the individual nodal and link degradation likelihoods on the basis of new events at a node, and subsequently, to determine the effect on network functionality by means of the overall network dependability function. With respect to this kind of monitoring, Bayes rule itself is appropriate for updating isolated states while Bayes Nets are suitable for updating a

Node Set	Probabilistic Network Reliability R { node set }		Possibilistic Network Reliability	Possibilistic Reliability Difference From R (Exact)
	Exact	Approximate		
Example 1: Hexagonal network				(6 Nodes 14 Links)
{all nodes}	.98497	.98542	.9655	-4 %
Example 2 : ART 1				(11 Nodes 22 Links)
{ 1, 11}	.93149	.93480	.8912	-5 %
{ all nodes}	.86550	.87272	.7890	-10 %
Example 3 : Beichelt Fig. 4.3				(14 Nodes 35 Links)
{ 1, 13}	.96358	.96470	.9385	-3 %
{ 1, 5, 13}	.96358	.96814	.9466	-3 %
{ all nodes}	.91461	.91792	.8559	-7 %
Example 4 : Small Network				(10 Nodes 10 Links)
{ all nodes}	.5872	.6500	.4919	-16 %

Table 1: *Example Network Reliability Estimates*

set of states with probabilistic interdependencies. However, Bayes Nets cannot determine the overall system state of system performance.

One complication with updating degradation event likelihoods in military situations is that the input information is often very sparse, vague, or imprecise. Frequently, initial likelihood estimates are guesses, with only sporadic data available to update those estimates. Caution should be adopted when applying Bayesian updating in this situation since it may take considerable time to adjust to new event likelihood values if they are substantially different to the initial *a priori* estimates. These information characteristics place fuzzy set methods, fuzzy statistics and fuzzy Bayes methods, amongst the more feasible techniques with which to address this updating problem. However, the exact nature of the information set should determine the ultimate selection of the revision and tracking method. For example, a discontinuous fuzzy time series may be induced by a limited number of sporadic events, when each event is associated with a qualitative rating that may be subjectively derived. Such series may be produced from INTEL streams, or be summaries of the outputs from

several different network intrusion detection algorithms at the end of each day. This particular type of macro-anomaly detection is to be distinguished from data-rich dynamic anomaly detection which is usually addressed by real-time analytical approaches. When monitoring such rough series, the core problem is to detect promptly any anomaly when it occurs, not only for detecting increased degradation in C2 network functionality, but also for rapid implementation of remedial actions before overall C2 network transmission is greatly affected.

5. Summary

This report has discussed various approaches to C2 system vulnerability analysis covering the following aspects:

- Criticality analysis of C2 system elements.
- System dysfunction analysis from the combination of distinct degradation events.
- Communication system dependability based on the synthesis of link dependabilities.

For nodal criticality evaluation, some qualitative approaches have been described based on subjective estimation of information influence strengths and the degree of a C2 element's intrinsic importance. These simple heuristics are highly context dependent since the characteristics of a threat situation determine which C2 elements are critical to a large degree. However, beyond that, there are hierarchical aspects of C2 decision making that also affect the criticality of elements. Although methods have been described that address both the context and hierarchical level of a C2 element, the criticality state can have no definite or absolute value since it is only a qualitative concept. Hence, these methods must be appreciated only as general exploratory approaches. Next, C2 system dependability has been defined to include both intrinsic system reliability and the vulnerability of a system to exogenous sourced degradation events. The use of the possibility measure to represent the higher-order uncertainties inherent in the input to much C2 network analysis was contrasted with the use of the more traditional probability measure of uncertainty. The possibility measure relates to what can potentially happen, in contrast to the probability measure which is a measure of the belief in what will happen. Overall, it is suggested that the prevalent use of subjective estimates in system dependability analysis renders the use of possibilistic likelihoods appropriate, especially in the simple algorithms demonstrated. For several example networks, exact and approximate probabilistic results were compared with dependability estimates using possibilistic likelihoods. The deviation of the approximate probabilistic method from the exact probabilistic results was shown to be small, and with the exception of the small less-connected network, well within the error magnitude expected in any input subjective estimates for network elements (say $\pm$ 5%). The deviations between the exact probabilistic and possibilistic system dependability estimates were around 10%. While this may not seem very significant in light of the uncertainty in the input event likelihoods, the deviations may be greater in times of conflict when the event likelihoods increase. But ultimately, the magnitude of the difference between probabilistic and possibilistic dependability estimates is determined by the network configuration, and these examples are only intended to demonstrate that dependability is always less when possibilistic likelihoods are used. Consequently, more conservative estimates are derived. For real-world C2 system vulnerability control, dynamic dependability analysis should also be employed, whereby unusual

degradation events at nodes are continuously monitored in a systematic way that is appropriate to the fuzzy nature of data. In conclusion, the practical techniques that have been presented in this report are intended to foster a wider base of vulnerability analysis in the field, especially where analytical resources may be scarce.

6. References

1. Barzilai, J. (1997) Deriving Weights from Pairwise Comparison Matrices, *J. Operational Research Society*, **48**(12), pp. 1226-1232.
2. Barzilai, J. (1998) Understanding hierarchical processes, *Proc. 19th Annual Meeting of American Society for Engineering Management*, pp. 1-6.
3. Beichelt, F. (1993) Decomposition and reduction techniques, in *New Trends in System Reliability Evaluation*, K.Misra (ed.), Elsevier.
4. Blechschmidt, A. (1993) Rechnergestutzte Zuverlassigkeitsanalyse stochasticher Netzstrukturen auf der Basis von Dekompositions- und Reduktion-stechniken, *Ph.D. Dissertation*, School of Engineering, Mittweida University.
5. Colbourn, C. (1987) *The Combinatorics of Network Reliability*, Oxford University press: New York.
6. Fuzzy Thought Amplifier Software (1994) - from Fuzzy Systems Engineering, Poway, California.
7. Harms, D., Kraetzl, M., Colbourn, C. and Devitt, J. (1995) *Network Reliability*, CRC Press: Boca Raton Fl.
8. Kosko, B. (1986) Fuzzy cognitive maps, *Int. J. Man, Machine Systems*, **24**, pp. 65-75.
9. Kosko, B. (1997) Additive fuzzy systems, in *Fuzzy Engineering*, Prentice-Hall: New York, pp. 116-121.
10. Kraetzl, M. (2000) Personal communication.
11. Lyle, D., Chan, Y. and Head, E. (1999) Improving information-network performance: reliability versus invulnerability, *IIE Transactions*, **31**, pp. 909-919.
12. Malec, H. (1998) Communications Reliability: A Historical Perspective, *IEEE Trans. Reliability*, **47**(3), pp. 333-345
13. O'Neill, P. (1999) Assessing Network Vulnerabilities, *Proc.TTCP Symposium on C2RT*, Rhode Island, 1999.
14. Saaty, T. (1980) *The Analytic Hierarchy Process*, McGraw Hill: New York.
15. Sharov, A. (1996) Equilibrium: Stable or Unstable, http://www.gypsymoth.ento.vt.edu/~sharov/popecol/lec9/equilib.html
16. Sherwin, D. and Bossche, A. (1993) T*he Reliability, Availability and Productiveness of Systems*, Chapman Hall: London.
17. Shier, D (1991) *Network Reliability and Algebraic Structures*, Clarendon Press: Oxford.
18. Sundararajan, C. (1991) *Guide to Reliability Engineering: Data, Analysis, Applications, Implementation, and Management*, Van Nostrand Reinhold: New York.
19. Survivable Network Technology Team (1997) *Survivable Network Systems: An Emerging Discipline*, Technical Report ESC-TR-97-013, Carnegie-Mellon Software Engineering Institute.
20. van den Brink, R. and Gilles, R. (2000) Measuring domination in directed networks, *Social Networks*, **22**, pp. 141-157.
21. von Collani, E. (1998) A simple algorithm for calculating approximately the reliability of almost arbitrary large networks, in *Advances in Stochastic Models for*

Reliability, Quality and Safety, Kahle W. et al. (Eds.) Birkhauser: Boston, pp. 213-234.

22. Warren, L. (1997) *Dynamic Benchmarks for Operations Evaluation in an Aluminium Ingot Mill*, PhD Dissertation, Grad. School of Management, Swinburne University of Technology.
23 Warren, L. (2000) *On the fuzzy representation of ambiguity and vagueness*, Report in process.
24 Zadeh, L. (1978) Fuzzy sets as a basis for a theory of possibility, *Fuzzy sets and systems*, **1**, pp. 3-28.

Aspects of Command and Control System Vulnerability Analysis

Lewis Warren

(DSTO-TR-1123)

DISTRIBUTION LIST

	Number of Copies
AUSTRALIA	
DEFENCE ORGANISATION	
Task sponsor:	
CDRE Russ Crane (DGISC)	1
COL Peter Lambert (DIOPC)	1
S&T Program	
Chief Defence Scientist)	
FAS Science Policy)	1 shared copy
AS Science Corporate Management)	
Director General Science Policy Development	1
Counsellor, Defence Science, London	Doc Control Sheet
Counsellor, Defence Science, Washington	Doc Control Sheet
Scientific Adviser to MRDC Thailand	Doc Control Sheet
Scientific Adviser - Policy and Command	1
Navy Scientific Adviser	1 copy of Doc Control Sheet and 1 distribution list
Scientific Adviser - Army	1
Air Force Scientific Adviser	1
Director Trials	1
Aeronautical & Maritime Research Laboratory	
Director	1
Electronics and Surveillance Research Laboratory	
Director	1 copy of Doc Control Sheet and 1 distribution list
Chief Information Technology Division	1
Research Leader Command & Control and Intelligence Systems	1
Research Leader Military Information Enterprise	1
Research Leader Advanced Computer Capabilities	1
Research Leader Joint Systems	1
Head, Enterprise Visualisation, Instrumentation and Synchronisation Group	Doc Control Sheet
Head, Trusted Computer Systems Group	Doc Control Sheet
Head, Systems Simulation and Assessment Group	Doc Control Sheet
Head, C3I Operational Analysis Group	Doc Control Sheet
Head, Information Exploitation Group	Doc Control Sheet
Head, Intelligence Group	Doc Control Sheet
Head, Human Systems Integration Group	Doc Control Sheet

Head, C2 Australian Theatre	1
Head, Distributed Systems Group	Doc Control Sheet
Head C3 Information Systems Concepts Group	1
Head, Military Systems Synthesis Group	Doc Control Sheet
Head, Systems of Systems Group	Doc Control Sheet
Head, Advanced Network Integrity Group	Doc Control Sheet
Head, Information Warfare Studies Group	1
Task Manager (Mr Jeff Schapel)	1
Author (Dr Lewis Warren)	1
Publications & Publicity Officer, ITD /Executive Officer, ITD	1 shared copy

DSTO Library and Archives

Library Fishermans Bend	Doc Control Sheet
Library Maribyrnong	Doc Control Sheet
Library Salisbury	1
Australian Archives	1
Library, MOD, Pyrmont	Doc Control Sheet
US Defense Technical Information Center	2
UK Defence Research Information Centre	2
Canada Defence Scientific Information Service	1
NZ Defence Information Centre	1
National Library of Australia	1

Capability Systems Staff

Director General Maritime Development	Doc Control Sheet
Director General Aerospace Development	Doc Control Sheet

Knowledge Staff

Director General Command, Control, Communications and Computers (DGC4)	Doc Control Sheet
Director General Intelligence, Surveillance, Reconnaissance and Electronic Warfare (DGISREW) R1-3-A142 Canberra ACT 2600	Doc Control Sheet
Director General Defence Knowledge Improvement Team (DGDKNIT) R1-5-A165, Canberra ACT 2600	Doc Control Sheet

Army

Stuart Schnaars, ABCA Standardisation Officer, Tobruck Barracks, Puckapunyal VIC 3662	4
SO (Science), Deployable Joint Force Headquarters (DJFHQ) (L), MILPO, Gallipoli Barracks, Enoggera, QLD 4052	Doc Control Sheet
NPOC QWG Engineer NBCD Combat Development Wing, Tobruk Barracks, Puckapunyal, 3662	1

Intelligence Program

DGSTA Defence Intelligence Organisation	1
Manager, Information Centre, Defence Intelligence Organisation	1

Corporate Support Program

Library Manager, DLS-Canberra	Doc Control Sheet

Universities and Colleges	
Australian Defence Force Academy	1
Library	1
Head of Aerospace and Mechanical Engineering	1
Serials Section (M list)), Deakin University Library	1
Hargrave Library, Monash University	Doc Control Sheet
Librarian, Flinders University	1
Other Organisations	
NASA (Canberra)	1
AusInfo	1
State Library of South Australia	1
Parliamentary Library, South Australia	1
OUTSIDE AUSTRALIA	
Abstracting and Information Organisations	
Library, Chemical Abstracts Reference Service	1
Engineering Societies Library, US	1
Materials Information, Cambridge Scientific Abstracts US	1
Documents Librarian, The Center for Research Libraries, US	1
Information Exchange Agreement Partners	
Acquisitions Unit, Science Reference and Information Service, UK	1
Library - Exchange Desk, National Institute of Standards and Technology, US	1
SPARES	5
Total number of copies:	**56**

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Aspects of Command and Control System Vulnerability Analysis

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Lewis Warren

5. CORPORATE AUTHOR

Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury SA 5108 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-1123	AR-011-807	Technical Report	March 2001

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
9505/19/199	JNT 99/028	DGISC	29	24

13. URL ON THE WORLD WIDE WEB

http://www.dsto.defence.gov.au.corporate/reports/DSTO-GD-TR-1123.pdf

14. RELEASE AUTHORITY

Chief, Information Technology Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, SALISBURY, SA 5108

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CASUAL ANNOUNCEMENT Yes

18. DEFTEST DESCRIPTORS

Vulnerability analysis, Computer security, Information warfare, System failures, Communication failures

19. ABSTRACT

This report describes several different approaches to Command and Control System vulnerability analysis. The focus is on practical heuristics that can be used without a significant loss of accuracy. Topics covered are qualitative criticality evaluation of C2 nodes, identification of degradation sources, and dependability evaluation of digital C2 support systems. The use of the possibility measure for data with higher-order uncertainty forms is discussed, and dependability results using the possibility measure are contrasted with those of probabilistic methods.