Defense Nuclear Agency
Alexandria, VA 22310-3398

DNA-TR-92-131

Validation of Survivability Validation Protocols

Thomas A. Stringer
Kaman Sciences Corporation
P.O. Box 7463
Colorado Springs, CO 80933-7463

May 1993

Technical Report

CONTRACT No. DNA 001-89-C-0080

Destroy this report when it is no longer needed. Do not return to sender.

PLEASE NOTIFY THE DEFENSE NUCLEAR AGENCY, ATTN: CSTI, 6801 TELEGRAPH ROAD, ALEXANDRIA, VA 22310-3398, IF YOUR ADDRESS IS INCORRECT, IF YOU WISH IT DELETED FROM THE DISTRIBUTION LIST, OR IF THE ADDRESSEE IS NO LONGER EMPLOYED BY YOUR ORGANIZATION.

DISTRIBUTION LIST UPDATE

This mailer is provided to enable DNA to maintain current distribution lists for reports. (We would appreciate your providing the requested information.)

NOTE:
Please return the mailing label from the document so that any additions, changes, corrections or deletions can be made easily.

☐ Add the individual listed to your distribution list.

☐ Delete the cited organization/individual.

☐ Change of address.

NAME: _____

ORGANIZATION: _____

OLD ADDRESS	CURRENT ADDRESS
_____	_____
_____	_____
_____	_____

TELEPHONE NUMBER: ( ) _____

DNA PUBLICATION NUMBER/TITLE	CHANGES/DELETIONS/ADDITIONS, etc.) *(Attach Sheet if more Space is Required)*
_____	_____
_____	_____
_____	_____

DNA OR OTHER GOVERNMENT CONTRACT NUMBER: _____

CERTIFICATION OF NEED-TO-KNOW BY GOVERNMENT SPONSOR (if other than DNA):

SPONSORING ORGANIZATION: _____

CONTRACTING OFFICER OR REPRESENTATIVE: _____

SIGNATURE: _____

CUT HERE AND RETURN

DEFENSE NUCLEAR AGENCY
ATTN: TITL
6801 TELEGRAPH ROAD
ALEXANDRIA, VA 22310-3398

DEFENSE NUCLEAR AGENCY
ATTN: TITL
6801 TELEGRAPH ROAD
ALEXANDRIA, VA 22310-3398

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	930501	Technical 920501 – 920831

4. TITLE AND SUBTITLE

Validation of Survivability Validation Protocols

5. FUNDING NUMBERS

C - DNA 001-89-C-0080
PE - 62715H
PR - SB
TA - SC
WU - DH057780

6. AUTHOR(S)

Thomas A. Stringer

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Kaman Sciences Corporation
P.O. Box 7463
Colorado Springs, CO 80933-7463

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Nuclear Agency
6801 Telegraph Road
Alexandria, VA 22310-3398
OTA/Yoho

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

DNA-TR-92-131

11. SUPPLEMENTARY NOTES

This work was sponsored by the Defense Nuclear Agency under RDT&E RMC Code B7664D SB SC LTHRR PRPD 1950A 25904D.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Issues associated with the validation of survivability protocols are discussed. Both empirical and analytical approaches to protocol validation are included. The use of hybrid simulations (hardware-in-the-loop, scene generators, software generators, man-in-the-loop, etc.) for the validation of survivability protocols is discussed.

14. SUBJECT TERMS

Survivability Validation
System Acquisition
Simulation
Protocol

15. NUMBER OF PAGES

22

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

CLASSIFIED BY:

N/A since Unclassified.

DECLASSIFY ON:
N/A since Unclassified.

SUMMARY

This paper identifies and describes the issues associated with the validation of survivability validation (SV) protocols. An SV protocol is a predefined, ordered set of tools and procedures that must be applied to a specific object to validate, with a measurable statistical confidence, the capability to perform a specified mission function in a defined environment resulting from a specified threat class. Application of the protocol to the specific object produces a documented collection of data establishing auditable traceability through the system survivability validation process.

A set of survivability validation protocols required to assure the specified performance of the system for its validated threat is referred to as a survivability regimen. The survivability regimen would be defined in the Test and Evaluation Master Plan (TEMP) by the Program Management Office and approved by the acquisition authority at Milestone 1.

Survivability validation protocols will consist of a specified collection of analyses, simulations, tests, and techniques that should be followed by the program manager for system components at various levels of integration to validate survivability. The question is whether each SV protocol itself is valid. That is, does following the protocol result in a system with the advertised degree of survivability?

This paper discusses two distinct approaches to protocol validation: empirical and analytical. In the first, systems whose survivability has been demonstrated by following the SV protocol are tested in "realistic" environments, and their survivability is experimentally demonstrated. With a statistically significant number of successful demonstrations, the protocol may be considered validated. In the second approach, the SV protocol is broken into its component parts and analyzed to determine if it is soundly based, with selected testing being identified and performed to validate the tools. Thus, in this context, the application of the term "analytical" to a type of protocol validation certainly does not preclude the use of testing.

Also described in this paper is the use of hybrid simulations (involving combinations of hardware-in-the-loop, man-in-the-loop, scene generators, and software simulators) for the validation of SV protocols. Validation issues associated with analyses, simulations, "approved" techniques, and tests are discussed. Related political issues are also addressed.

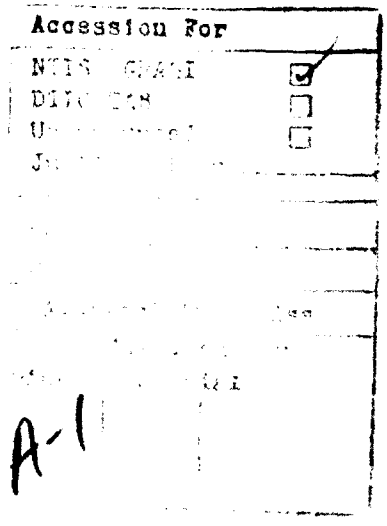

TABLE OF CONTENTS

SECTION 1

INTRODUCTION

The concept of survivability validation (SV) protocols focuses on the establishment of specific, pre-approved means by which a program manager can demonstrate system survivability. He knows *a priori* that the successful accomplishment of the appropriate protocols will be accepted as proof by the acquisition authority that his system is survivable. The key to this approach is that the protocols themselves have been accepted by the decision makers as valid.

A survivability validation protocol is a predefined, ordered set of tools and procedures that must be applied to a specific object to validate, with a measurable statistical confidence, the capability to perform a specified mission function in a defined environment resulting from a specified threat class. Application of the protocol to the specific object produces a documented collection of data establishing auditable traceability through the system survivability validation process.

We distinguish between generic SV protocols and System Program Office (SPO)-adapted SV protocols. Generic SV protocols are developed and written in general terms in order to be applicable to, and validated for, more than one system. A SPO-adapted SV protocol, on the other hand, uses the appropriate generic SV protocol as its basis, but is tailored for the specific system for which the SPO is responsible.

A set of survivability validation protocols required to assure the specified performance of the system for its validated threat is referred to as a survivability regimen. The survivability regimen would be defined in the Test and Evaluation Master Plan (TEMP) by the Program Management Office and approved by the acquisition authority at Milestone 1.

Survivability validation protocols are tools to be used and steps that should be followed by the program manager for system components at various levels of integration to validate survivability. The question is whether each SV protocol itself is valid. That is, does following the protocol really constitute a valid demonstration that the system is survivable with the advertised degree of survivability?

In this paper, we consider various levels of integration, from the highest level of integration, a "system of systems" (SOS), down to the lowest levels (e.g., piece parts and materials). Examples of complex, interdependent SOSs include Global Protection Against Limited Strikes (GPALS), Theater Missile Defense (TMD), and the Trident Submarine fleet. The terms used for the various levels of integration in this report are indicated in Table 1-1.

1.1 THE MEANING OF PROTOCOL VALIDATION.

Generic survivability validation protocols consist of a specified collection of analyses, simulations, tests, and techniques (e.g., approved or validated hardening techniques) that will be adapted by the program manager to his particular system. How can it be determined, however, whether a particular survivability validation protocol is itself valid?

Validating a survivability validation protocol means *verifying or demonstrating that if a system successfully undergoes that survivability validation protocol it will be*

Table 1-1. Hierarchy of levels of integration of a system of systems.

Level of Integration (Highest to Lowest)	Examples
System-of-systems (SOS)	GPALS, Trident, Theater Missile Defense
System element (SE)	A constellation of Brilliant Pebbles satellites
System element platform (SEP)	A radar, satellite, an individual Brilliant Pebble, a missile
Subsystem	Power subsystem of a satellite, seeker of a kinetic kill vehicle, post-boost vehicle guidance system
Component	Individual electronics boxes, lenses, mirrors
Part/material	Baffle materials, piece parts

survivable to the effects covered by the protocol with a known degree of confidence. Here, by the term "system" we mean the particular level of integration for which the protocol applies.

A related issue is the impact on confidence in survivability if the protocol is followed to some limited degree or only to some partial extent. This will sometimes be attractive or even necessary because of budgetary or time constraints. Also, it does not necessarily follow that the use of a validated generic SV protocol to formulate a SPO-adapted SV protocol guarantees that the latter is valid, or that it affords the same degree of confidence in survivability. This also raises the issue of whether the SPO-adapted SV protocol requires a complete reassessment of its validity; it is possible that the validation, and the resulting impact on confidence, can be assessed analytically.

Another relevant issue is political: how does one convince the decision makers that following the SV protocols really does result in a system that is survivable, with a known level of confidence, to the given threat.

1.2 ANALYTICAL VS EMPIRICAL VALIDATION.

Two distinct types of protocol validation procedures can be identified:

(1) An external, *empirical*, kind of demonstration or validation process, where *existing* systems and *existing* protocols are involved, and

(2) An *analytical* and indirect method, where the tools and their prescribed applications that comprise the protocol are examined and analyzed. This would involve using existing applicable databases and the results of selected additional tests examining specific issues that analysis shows are uncertain and in need of validation.

In the empirical approach, systems to which the protocol has been applied are tested in "realistic" environments and their survivability is experimentally, or empirically, demonstrated. After sufficiently large numbers of such successful demonstrations, the protocol may be considered validated. In the analytical approach, the protocol is analyzed and scrutinized in the light of known and accepted physics and engineering principles to determine if the protocol is soundly based (and hence "valid"). The term "analytical" refers to the fact that the protocol is analyzed in terms of its components. In this context, it does not mean that there is no testing involved; on the contrary, part of the procedure would be to determine where testing is needed to clarify, validate, or improve tools, and applications of tools, that comprise the SV protocol.

A *purely* empirical approach with a real test environment is not possible or practical at the highest levels of integration. It is not possible to demonstrate survivability of an SOS in a *real nuclear environment* even once, let alone the statistically significant number of times that would be required for empirical protocol validation. Hence demonstrating survivability *empirically* at the highest level of integration would involve simulation, in some mix of purely computer-based simulation and hybrid simulation (a simulation involving a combination of hardware-in-the-loop, man-in-the-loop, scene generators, and software simulations). To the extent that this validation process is done solely with computer simulation and analysis, we may consider the validation process to be essentially an analytic one. To the extent that *hybrid simulations* are used for validation, the approach may be considered partly empirical and partly analytical.

Hence, analytical validation will certainly be an important part of protocol validation at the higher levels of integration, where testing becomes impossible or impractical. It will also be a part of validation at all levels because tests have inherent limitations in fidelity and they are expensive and time consuming.

The analytical approach to protocol validation is to examine the protocol for logical consistency and for the rigor of the underlying physics. This latter aspect will involve determining what existing experimental data bears on and supports the engineering judgments and underlying physical assumptions inherent in the protocol. This analytic approach will utilize and apply results from tests that have already been conducted, in particular, results of tests involving lower levels of integration. *It will also involve determining and performing additional tests necessary to remove or reduce uncertainties associated with the component tools of the protocol.* Some other validation issues in the analytical approach are whether the various prescribed hardening techniques are based on a sound understanding of the physics of the relevant nuclear effects; whether the prescribed tests are adequate to show survivability and to uncover any hidden vulnerabilities or hardening defects in design; whether the prescribed analyses are comprehensive and based on correct physics and engineering; and whether validation at lower levels of integration can be carried forward to higher levels of integration. Concerning this last point, just because all the lower levels of integration have validated SV protocols for a given set of environments does not mean that a protocol addressing the next higher levels of integration which incorporates the lower level protocols can be validated a priori. Due to potential synergisms, each protocol validation should be considered an independent event until analysis proves otherwise.

There is an important distinction that must be made when considering analytical protocol validation. We must distinguish between validating *tools* (e.g., test facilities, computer simulations, etc.) and *validating the application of those tools* as

prescribed in protocols. That is, a tool may be valid for some applications and not others; hence the analytical approach would also ascertain whether the application of the tool in the context of a particular SV protocol is valid.

Analytical methods of protocol validation are commonly used in many contemporary technologies. There are precedents in technology for validation of protocols or procedures with many of the same limitations as in the case of survivability protocols for high levels of integration. One example is airline passenger evacuation procedures, where the procedures (protocols) are probably validated in a largely analytical manner or, where empirical, are probably hybrid simulations involving, as a minimum, real passengers and actual airplanes. A building evacuation procedure is a related example. This is an exercise or procedure whose purpose is part "readiness" and part validation (of a procedure, or protocol). In both of these examples, a real fire or any kind of a real hostile environment is not actually present when the procedure is validated.

Testing of automobiles or airplanes in adverse environmental conditions furnishes more examples: protocols for ensuring that cars or planes will survive or function adequately in such adverse environments might afford many interesting parallels for validation of survivability protocols.

In general, other technologies, both "high-tech" and "low tech", prescribe many procedures and protocols for dealing with adverse conditions which are not directly empirically verifiable, but are considered valid on the basis of hybrid simulations and analysis.

1.3 HARDNESS, OPERABILITY, AND SURVIVABILITY PROTOCOLS.

For levels of integration below the system element platform (SEP) level, demonstrating survivability will have to mean something different than it does for SOS, SE, and SEP levels. This is because of the changed emphasis on mission survivability. In the past, there has been more concern over whether components and parts break, and hence survivability has tended to mean hardness to some threat level or to some generally accepted attainable hardening level. Increasingly, in the future, survivability will be achieved in many ways (redundancy, reconstitution, inherent tolerance, avoidance, etc.), with hardness providing just a part of a component's survivability. This type of survivability (functional survivability) will often be implemented at higher levels of integration, but in some cases it can be implemented at lower levels as well. Nevertheless, survivability at the lower levels of integration (element platform level and below) for environments where actual damage or upset is the potential concern will continue to be validated or demonstrated in terms of hardness to some specified threat (or range of threats). This is in part because specification of a threat in the form of a localized set of environment parameters is only practical at these levels of integration. This specification in fact flows down from engagement scenario simulations at the higher levels. As we argue below, for environments that pose noise or attenuation concerns, survivability will be implemented in terms of operability to some specified noise background or attenuation level. Hence an SV protocol at element platform and lower levels of integration will usually involve demonstrating hardness to or operability in a specified range of nuclear environments.

When considering survivability, a distinction must be drawn between damage or malfunction effects and signal-to-noise (S/N) effects. Examples of the former are device burnout or upset, while examples of the latter are infrared (IR) sensor redout

and radio frequency (rf) sensor blackout. Traditionally, the respective "-ilities" have been referred to as survivability and operability. It is our position that these all meld into mission, or functional, survivability given the emphasis on mission survivability of complex interdependent systems. In the past, operability tended to be a concern at higher levels of integration (SEP and higher), but increasingly there will be cases where it will have to be ensured, or implemented, at the lower levels as well. Examples would be an S/N specification for an rf processor in a radar, or for the signal processor in the case of an optical sensor. Hence there will be operability specifications, and corresponding operability protocols, at the lower levels of integration (specifically the subsystem and component levels).

SECTION 2

PROTOCOL VALIDATION ISSUES AT EACH LEVEL OF INTEGRATION

The protocols will tend to be different in character at the various levels of integration. For example, protocols will involve primarily simulation testing and analysis for lower levels, while higher levels will tend toward computer and/or hybrid simulation.

2.1 SOS LEVEL OF INTEGRATION.

For an SOS, SV protocols will involve extensive computer simulations with engagement codes, as was discussed at length in a previous white paper on simulation fidelity[1]. Physical testing of an SOS, in either aboveground tests (AGTs) or underground test (UGTs), will usually be impossible, due mainly to the fact that SOSs are comprised of system element platforms that in an actual engagement would be dispersed or widely separated spatially (in space, on the ground, in atmospheric flight, etc.). For this reason, validation of protocols will also have to involve the demonstration of survivability via simulation, although these simulations should involve hybrid simulations as well as purely software simulations. The analytical approach described in the previous section will be a very important part of protocol validation at this level. It would not be a good idea to rely on "empirical" validation through computer and hybrid simulations alone due to the many assumptions and simplifications that will necessarily be implicit in them to achieve manageable run times.

Protocols either do not exist or are not well established at this level of integration because such highly interdependent complex systems were not common in the past. A corollary to this is that SV protocol validation will probably tend to be more controversial and community agreement may be more difficult to attain than it will be at lower levels, where there is a greater applicable database and a more established past history, and where direct experimental validation is more easily done.

In summary, protocol validation will have to be based on a combination of simulation and analysis. The simulations will be mostly computer simulations but some hybrid simulations, where element platforms are simulated with combinations of software and hardware (with possible provisions for man-in-the-loop) would be desirable.

2.2 SE LEVEL OF INTEGRATION.

For the SE level of integration, the same considerations as at the SOS level of integration apply. The SE is generally spatially dispersed (as with a constellation of satellites, for example), and hence tests are not practical. Again, hybrid and computer simulations will be the basis of an empirical approach to validation, with the analytical approach being used along with it to provide a higher degree of confidence in the validity of the protocol.

[1]Stringer, T. A., P. S. Book, and D. M. Rodvold, "Simulation Fidelity Issues for Nuclear Survivability Validation Protocols," Kaman Sciences Corp., Colorado Springs, CO, DNA Draft Technical Report, May 1992.

2.3 SEP LEVEL OF INTEGRATION.

For the SEP level of integration, survivability will be validated by demonstrating hardness or operability to a specified range of environments. (These specified environments flow down from the requirements definition process, engagement scenario studies, and simulations at the higher levels of integration.) Hence validating SV protocols at these lower levels will involve showing that the protocols produce systems that are hard or operable to some required level. *At these levels of integration, physical tests (albeit with some simulation fidelity compromises) are possible in UGTs and/or AGTs.* Hence proof tests, if done in statistically significant numbers, can provide confidence in protocols (and confidence at some point becomes "validation").

SV protocols, therefore, could in principle be validated in a purely empirical manner. However, the practical difficulties such as attaining a statistically significant number of demonstrations, the fact that some platforms are too large to be tested, and limitations and uncertainties involving simulation fidelity make it doubtful that the purely empirical approach alone will suffice. The analytical method will be the principal technique to validate protocols at this level.

2.4 SUBSYSTEM LEVEL OF INTEGRATION.

For the subsystem level of integration, the situation regarding validation is largely the same as at the SEP level, with the exception that it is more likely that test facilities will accommodate the size of the subsystem. There are still many cases where they will not, such as power subsystems having large solar panels.

2.5 COMPONENT LEVEL OF INTEGRATION.

Physical simulations (testing) will tend to be very important aspects of protocols at this level. Simulation fidelity and AGT/UGT/threat correlation will be validation issues here. Extrapolation to threat environments will be done via modeling and analysis. Hence validation of the effects codes used to extrapolate the test results is a protocol validation issue: is the underlying physics understood and is it being included with sufficient accuracy and fidelity to support the desired design margin?

At this level of integration, there will be a number of "approved techniques" for ensuring hardness, such as conformal coatings to minimize system-generated EMP (SGEMP) and x-ray shielding techniques, that may not require any testing or simulations as part of the SV protocol. Validation issues here include the validation of the use of the protocol tools and whether the approved technique is being properly applied in the context of the particular application. Another issue is whether the approval regarding the technique is really justified in view of current knowledge.

2.6 PIECE PARTS/MATERIALS.

Protocols tend to exist here, at least for established technologies. These existing SV protocols are heavily test oriented, although standard hardening procedures (such as use of hardened parts, rf shielding, and x-ray shielding) also comprise a large portion. As with the component level of integration, a validation question is whether these techniques are being properly applied in a particular context. Where testing is required, simulation fidelity issues are not as difficult as they tend to be at the higher levels of integration. This is partly because the exposure area requirements are more easily met, and partly because most transient radiation effects on

electronics (TREE) do not depend as much on spectrum as do x-ray SGEMP effects. Accordingly, validation will not be as difficult.

SECTION 3

COMPUTER MODEL AND SIMULATION VALIDATION

Common to many of the level-of-integration protocols is the use of computer models and simulations. Hence the validity of the protocols will depend heavily on validation of the codes. At the higher levels of integration, computer simulation tends toward engagement codes; at the lower levels it tends toward physics of nuclear effects.

When discussing validation of computer programs or software, it is conventional to make a distinction between "validation" and "verification". Validation refers to how well the models fit the real world, and verification refers to assuring internal consistency (i.e., "debugging" of the code to produce correct and consistent output with respect to the input).

The issue of computer and analytic model validation is closely linked to validation of techniques (one of the tools within the protocol), since models and theories of nuclear effects are actually implicit in the hardening techniques (i.e., the "approved techniques"). An example is in the electronics hardening, where conformal coatings are applied to exposed metal surfaces to minimize box internal EMP (IEMP). The underlying model involves recognizing that box IEMP source terms are proportional to photo-Compton electron emission levels, which are in turn minimized if range-thick low atomic number coatings are present. This is in fact an example where the underlying physics and modeling are thought to be so well understood that validation by testing may not even be required, and there are many similar examples. In such cases, technique validation can be done in an analytical manner that draws on existing nuclear effects test data.

Existing test data includes the results of "phenomenology tests". This kind of test investigates an underlying physics effect. An example is the series of high fluence cable SGEMP tests conducted by the Defense Nuclear Agency (DNA) in the late 1970s and early 1980s. These kinds of tests serve as a basis for analysis to show, or validate, that a particular area of nuclear effects and hardening is understood. In these cases, computer models with quantifiable accuracy can be constructed and used as part of the protocol.

AGT/UGT correlation is related to the issue of validation of computer models. When it can be shown that the AGT and UGT correlate in a way that is understood via the computer (or analytic) model, the model is itself to some extent validated. There are validation issues that pertain to the use of the codes also. For example, in the area of nuclear weapons effects codes, what are the zoning requirements and what dimensionality is required? That is, will a one-dimensional run suffice or does the code have to be exercised in a three-dimensional version? In the case of either effects codes or system analysis codes, we must ask how many runs are required, what accuracy and fidelity is needed, and what output is required.

SECTION 4

TEST VALIDATION

The issue of test validation is closely related to both simulation fidelity and response correlation issues. Some of the tests within the SV protocol will be of the response matching type (e.g., current injection test, CIT) as discussed in the simulation fidelity paper[2]. It may require additional testing as part of the SV protocol validation process to show that these tests are valid. The same applies to AGT radiation tests, where it may be necessary to validate the test technique (due to simulation fidelity issues, it may not be clear a priori that the test is a valid test, for example).

Validation of protocols where testing is a part of the protocol (primarily at the lower levels of integration) also involves the validation of test techniques. One aspect of this is the traditional "simulation fidelity" issue of how well a particular test facility represents or matches a real nuclear environment. However, there are many other issues as well: How many tests have to be done, how many pieces of system hardware have to be tested, what responses should be measured, how should they be measured, how does instrumenting the test affect the response, and so on.

In some cases, the system designer will be able to do only limited testing (because of limited budgets, for example). That is, he will choose to do only some of the testing within the SV protocol. Hence, a relevant validation issue is the effect of such testing reductions on the confidence in the hardness/survivability.

In some cases it may be reasonable to consider designs that afford validatable SV protocols. For example, the Department of Energy (DOE) is investigating the concept of making electronics boxes testable in existing x-ray facilities, which is essentially an approach where the design is tailored so that testing can be done with existing facilities that match responses (or that allow a high degree of correlation with threat responses).

AGT/UGT correlation is a relevant subject in this context. Since UGTs tend to represent a more realistic environment for most nuclear effects, the established degree of correlation between AGT and UGT bears on the issue of test validation.

Several prior or ongoing test related programs are relevant to protocol validation studies. One example is the series of STARSAT tests, which was a series of SGEMP tests (including both AGTs and UGTs) intended in part to show the validity of the standard practices generally followed for SGEMP hardening. Another example is the ongoing box IEMP AGT/UGT correlation work being done in DOE.

An important example of a hybrid simulation used to validate survivability is the Portable Radiation/Redout Testbed for Sensors (PORTS) test concept developed by the Strategic Defense Command (SDC) for IR sensors. The validation of this concept might serve as an interesting and illuminating example.

The issue of safety margins is a relevant validation issue. A test may have low simulation fidelity, but if the design margin is big enough the validation is easier. In some cases this can result in an overdesigned system, however.

[2] *ibid.*

Inevitably a judgment factor comes into play in deciding whether a given test technique is applicable to a given protocol. It may be difficult to quantify the validity of a given test technique.

SECTION 5

CONCLUDING DISCUSSION

Generic survivability validation protocols will consist of a specified collection of analyses, simulations, tests, and techniques that will be adapted by the program manager to his particular system. The question is whether each SV protocol itself is valid. That is, does following the protocol result in a system with the advertised degree of survivability?

There are precedents in technology for validation of protocols with many of the same limitations as in the case of survivability protocols. We have argued that our technologies prescribe many procedures and protocols for dealing with adverse conditions and adverse environments which are not directly empirically verifiable, but are considered valid on the basis of hybrid simulations and analysis. There may be useful techniques for validation in those areas that can be applied to the present issue of SV protocol validation.

We believe that current SV protocols are ad hoc and piecemeal, and are not universally accepted. This situation needs to be corrected by the development of a methodical validation process (to be done in concert with the development of the protocols themselves).

To the extent possible, the SV protocols should incorporate military standards and other hardening procedures for which there is already community consensus. However, they should be reexamined in the light of recent experience, knowledge, and new threats.

We have pointed out that the concept of protocol validation is closely related to the idea of community acceptance: convincing the decision makers (SPOs, acquisition authority, etc.) that the protocols are valid and that they do their job in the most efficient and least costly manner possible. As far as validity is concerned, it is likely that the empirical approach outlined above is more convincing to these decision makers. AGT/UGT/threat correlation is important in this context because it helps to establish the connection and correlation between AGTs and UGTs that are used in the SV protocol and threat.

We have also identified two issues that will arise when a SPO-adapted protocol is used in place of a validated generic SV protocol. One issue is whether the validation of the SPO-adapted protocol has to be entirely reassessed. Another is whether the impact on confidence in survivability can be determined through analysis and extrapolation, using in large part the results of the generic SV protocol assessment, or if a new and independent assessment must be performed on the SPO-adapted protocol.

The analytical approach, where the protocol is broken down into its component parts and analyzed for soundness and logical consistency, is a practical approach and one that can be technically sound. It is practical especially at the higher levels, where testing in real environments is not possible. This analytical approach would involve selected testing to help resolve uncertainties and to explore survivability issues associated with new technologies. It would also apply existing test results from various levels of integration. The analytic approach should be supported by hybrid simulations which can afford proof tests that are partly empirical, partly analytical. Both man-in-the-loop and hardware-in-the-loop hybrid simulations should be

considered. Of course, these hybrid simulations themselves will require validation and will necessarily involve many simplifications and fidelity limitations.

It is important to minimize uncertainties associated with all of the tools that comprise the SV protocols, as these can result in systems that are not survivable to the threat, or in overdesigned systems (i.e., with excessive safety margins) with associated penalties in cost, schedule, weight, and volume.

Specific validation issues for the protocol component tools include the following:

(1) Analyses and simulations: The validation question is whether the analytic models and computer simulations are valid. Are the models based on correct physics, are they accurate and experimentally verified, and are they sufficiently high fidelity representations of the real world? Where the program manager is relying on some set of codes to demonstrate that his system is hard, are these codes themselves validated? Are additional tests needed to validate specific analytic models?

(2) "Approved" techniques: It may still be necessary to directly demonstrate through a test that a technique really does provide hardness. Also, in some cases the underlying physics may need to be re-examined in the light of new information or new technology. For example, the technique may have been approved for technologies that have changed, or new data may have been acquired which necessitates reexamination of an existing technique. Another possibility is that there may now be better ways of achieving the required hardness.

(3) Tests: A given simulator may be approved or valid for some uses, but it can be incorrectly or inappropriately used. In other words, the utilization of the facility also needs validation. Tests at physical simulators will be important parts of SV protocols at the system element level and below. At the system element and system-of-systems levels of integration, due to their spatially dispersed nature, "threat" does not just mean an environment, but a range of enemy engagement capabilities. Validation tests in the form of hybrid simulations can be useful at these higher levels of integration.

AGT/UGT/threat correlation studies currently being actively pursued by both DNA and DOE are important to protocol validation for several reasons. This work establishes the connection between AGT and threat; hence it validates AGT techniques. The AGT/UGT correlation establishes the validity of the analytic techniques and models that are applied within the SV protocol to demonstrate survivability. By being able to trace the correlation through the models, it is demonstrated that the underlying effects and phenomena are in fact understood, and the hardening methods based on them are valid. The AGT/UGT/threat correlation studies also shows where proof tests can be done with AGTs rather than UGTs.

SV protocol validation will probably be done with a combination of the analytical and empirical approaches. We have shown that the analytical approach may involve selected tests to validate specific tools or methods within the protocol, and that this analytical approach can be effective for all levels of integration. It tends to become relatively more important at higher levels of integration, where strictly empirical demonstrations are impossible or impractical (although computer simulations and hybrid simulations can and should be used). The analytical approach will for the most part involve looking at whether the protocols are logically consistent in view of what we know about the relevant physical processes involved in nuclear

effects. This is a familiar situation by no means unique to survivability. There are many precedents where procedures and steps to follow to accomplish something are not really proved through direct experimental proof, but are well thought through and are shown to be at least consistent with what we know. This will provide program managers and acquisition authorities with confidence that the SV protocols really accomplish what they advertise, and that the system that passes all of the steps really is survivable with known confidence.

DISTRIBUTION LIST

DNA-TR-92-131

NATO

AAFCE/OOST
ATTN: SQNLDR MULLIGAN

ARTILLERIE KOMMANDO 3
ATTN: LTC JOACHIM BURTH

ATOMIC WEAPONS ESTABLISHMENT, FOULNESS
ATTN: DR DARYL LANDEG

SIEMENS PLESSEY DEFENCE SYSTEMS
ATTN: HENRY CHESTERS

TARGETS BRANCH
ATTN: ITTI

USECOM
ATTN: ECJ3-FC
2 CYS ATTN: ECJ4-LW
ATTN: ECJ5-N
ATTN: ECJ6-T
ATTN: MAJ FLEMING

DEPARTMENT OF DEFENSE

ARMED FORCES STAFF COLLEGE
ATTN: C3-JCEWS
ATTN: JCEWS-C3D

ASSISTANT SEC OF DEF (C3I)
ATTN: J BAIN

ASSISTANT TO THE SECRETARY OF DEFENSE
ATTN: DR BIRELY
ATTN: LTCOL M CRAWFORD

DEF RSCH & ENGRG
ATTN: DIR TEST FACILITIES & RESOURCES
ATTN: DEP DIR TEST EVAL

DEFENSE ADVANCED RSCH PROJ AGENCY
ATTN: ASST DIR ELECTRONIC SCIENCES DIV
ATTN: DEP DIR RESEARCH
ATTN: DIR DEFENSE SCIENCES OFC
ATTN: TTO

DEFENSE COMMUNICATION AGENCY
ATTN: JOHN SELISKAR

DEFENSE ELECTRONIC SUPPLY CENTER
ATTN: DESC-E

DEFENSE LOGISTICS AGENCY
ATTN: DLA-F
ATTN: DLA-QE
ATTN: DLA-QES
ATTN: DLA-SCC
ATTN: DLA-SCT
ATTN: DLSMO

DEFENSE NUCLEAR AGENCY
ATTN: DFRA JOAN MA PIERRE
ATTN: RAEE
ATTN: RAEV
ATTN: SPSD
ATTN: SPSP
ATTN: SPWE
ATTN: TITL

DEFENSE TECHNICAL INFORMATION CENTER
ATTN: DTIC-DE
ATTN: DTIC/FDAB

DEPARTMENT OF DEFENSE
ATTN: DEP DIR TEST EVAL

NATIONAL COMMUNICATIONS SYSTEM
ATTN: NCS-TS A H RAUSCH

NATIONAL DEFENSE UNIVERSITY
ATTN: CLASSIFIED LIBRARY

NATIONAL SECURITY AGENCY
ATTN: D/DIR
ATTN: DDI
ATTN: TECH DOC LIB

NET ASSESSMENT
ATTN: DIRECTOR
ATTN: DOCUMENT CONTROL

OPERATIONAL TEST & EVALUATION
ATTN: DEP DIR OPER TEST & EVAL STRAT SYS
ATTN: SCIENCE ADVISOR
ATTN: DEP DIR RESOURCES & ADMIN

STRATEGIC & SPACE SYSTEMS
ATTN: DIRECTOR
ATTN: DR E SEVIN
ATTN: DR SCHNEITER

STRATEGIC DEFENSE INITIATIVE ORGANIZATION
ATTN: DA DR GERRY

DEPARTMENT OF THE ARMY

ARMY RESEARCH LABORATORIES
ATTN: TECH LIB
ATTN: SLCSM-D COL J DOYLE

PATRIOT
ATTN: PROJECT MANAGER

RESEARCH & DEV CENTER
ATTN: COMMANDER

SATELLITE COMMUNICATIONS
ATTN: PROJECT MANAGER

U S ARMY AVIATION SYSTEMS CMD
ATTN: PM AIRCRAFT SURVIVABILITY EQUIP

U S ARMY BELVOIR RD&E CTR
ATTN: TECH LIB

U S ARMY LABORATORY CMD
ATTN: COMMANDER

U S ARMY MATERIAL COMMAND
ATTN: OFFICE OF PROJECT MANAGEMENT

U S ARMY MISSILE COMMAND
ATTN: PM/TO

U S ARMY MISSILE COMMAND
ATTN: AMCPM-CC/PM

U S ARMY MISSILE COMMAND
ATTN: MAJ R LUSHBOUGH

U S ARMY MISSILE COMMAND
ATTN: R LENNING

U S ARMY NUCLEAR & CHEMICAL AGENCY
ATTN: MONA-AD

U S ARMY ORD MISSILE & MUNITIONS
ATTN: ATSK-MS
ATTN: ATSK-XO

U S ARMY RESEARCH DEV & ENGRG CTR
ATTN: TECH LIB

U S ARMY SIGNAL CTR & FT GORDON
ATTN: ATZH-CDC
ATTN: ATZH-CDM

U S ARMY SPACE & STRATEGIC DEFENSE CMD
ATTN: CSSD-SA-EV
ATTN: CSSD-SA-EV R CROWSON
ATTN: CSSD-SL
ATTN: SFAE-SD-GST-E P BUHRMAN

U S ARMY SPACE STRATEGIC DEFENSE CMD
ATTN: CSSD-CS
ATTN: CSSD-OP
ATTN: CSSD-SA-E

U S ARMY STRATEGIC SPACE & DEFENSE CMD
ATTN: CSSD-H-LS
ATTN: CSSD-SD-A

U S ARMY TEST & EVALUATION COMMAND
ATTN: AMSTE-TA-F
ATTN: AMSTE-TA-F L TELETSKI

U S ARMY VULNERABILITY ASSESSMENT LAB
ATTN: SLCVA-D

USA ELECT WARFARE/SEC SURV & TARGET ACQ CTR
ATTN: COMMANDER

USA SURVIVABILITY MANAGMENT OFFICE
ATTN: AMSLC-VL-NE DR J FEENEY
ATTN: F MANION
ATTN: SLCSM-SE J BRAND

DEPARTMENT OF THE NAVY

DEPARTMENT OF THE NAVY
ATTN: DIRECTOR

GPS NAVSTAR JOINT PROGRAM OFFICE
ATTN: CHARLES TABBERT

NAVAL AIR SYSTEMS COMMAND
ATTN: AIR-5115J G T SIMPSON

NAVAL AVIONICS CENTER
ATTN: F GAHIMER
ATTN:D PAULS

NAVAL POSTGRADUATE SCHOOL
ATTN: CODE 1424 LIBRARY

NAVAL RESEARCH LABORATORY
ATTN: CODE 2627

NAVAL SEA SYSTEMS COMMAND
ATTN: COMMANDING OFFICER

NAVAL SURFACE WARFARE CENTER
ATTN: COMMANDER

NAVAL WAR COLLEGE
ATTN: CODE E-111

NAVAL WARFARE ASSESSMENT CENTER
ATTN: DOCUMENT CONTROL

NAVSEA
ATTN: J SATIN

OPERATIONAL TEST & EVALUATION FORCE
ATTN: COMMANDER

SCIENCE & TECHNOLOGY LIBRARY
ATTN: CODE 202.13

STRATEGIC SYSTEMS PROGRAM
ATTN: SP-113 D ELLINGSON

DEPARTMENT OF THE AIR FORCE

AERONAUTICAL SYSTEMS DIVISION
ATTN: ASD/ENACE
ATTN: ASD/ENSSS
ATTN: ASD/RWWI

AF SPACE COMMAND
ATTN: LKNIP MAJ S HOFF
ATTN: SM-ALC DET 25 P C LARTER
ATTN: DOCE

AIR FORCE CTR FOR STUDIES & ANALYSIS
ATTN: AFCSA/SAS
ATTN: AFSAA/SAKI

AIR FORCE INSTITUTE OF TECHNOLOGY/EN
ATTN: LTCOL R TUTTLE

AIR FORCE SPACE COMMAMD (LKI)
ATTN: CAPT WEIDNER
ATTN: LT D BARRON
ATTN: MAJ D ROBINSON
ATTN: STOP 7

ASSISTANT CHIEF OF STAFF
ATTN: AF/SAN

BALLISTICS MISSLE ORGANIZATION
ATTN: A F BURKHOLDER

DEPARTMENT OF THE AIR FORCE
ATTN: NCGS B HOPKINS

DEPUTY CHIEF OF STAFF/AF-RD-D
ATTN: AF/RD-D

DEPUTY CHIEF OF STAFF/AF-RD-W
ATTN: AF/SCMCW

DEPUTY CHIEF OF STAFF/AFRDSD
ATTN: SAF/AQSD

MILITARY DEPUTY FOR ACQUISITION
ATTN: AQQS LTCOL KEE

PHILLIPS LABORATORY
ATTN: CAPTIAN LORANG
ATTN: NTES LTCOL T BRETZ
ATTN: PL/WS L CONTRERAS
ATTN: WSP J DEGAN
ATTN: WSP R PETERKIN

ROME LABORATORY/SUL
ATTN: COMMANDER

SECRETARY OF THE AIR FORCE
ATTN: AF/RDSL

SPACE DIVISION (AFSC)
ATTN: SSD/MZS

UNITED STATES STRATEGIC COMMAND
ATTN: J 22A
ATTN: J 51
ATTN: J 53
ATTN: J 532
ATTN: J 533
ATTN: J 534
ATTN: JIC/ODM
ATTN: JIC/ODTD

WRIGHT LABORATORY
ATTN: D WATTS

WRIGHT RESEARCH & DEVELOPMENT CENTER
ATTN: COMMANDANT

DEPARTMENT OF ENERGY

DEPARTMENT OF ENERGY
ATTN: WALT KELLY

DEPARTMENT OF ENERGY
ATTN: C MEYERS

EG&G IDAHO INC
ATTN: MS ILF-2

SANDIA NATIONAL LABORATORIES
ATTN: TECH LIB-PERIODICALS

DEPARTMENT OF DEFENSE CONTRACTORS

AEROSPACE CORP
ATTN: LIBRARY ACQUISITION

ALFONTE ASSOCIATES
ATTN: WILLIAM ALFONTE

ANALYTIC SERVICES, INC (ANSER)
ATTN: LIBRARY

APTEK, INC
ATTN: T MEAGHER

BERKELEY RSCH ASSOCIATES, INC
ATTN: J ORENS
ATTN: N PEREIRA

BERKOWITZ ENTERPRISES
ATTN: H M BERKOWITZ

BOEING AIRCRAFT MARINE
ATTN: CHUCK WERTZBERGER

BOOZ ALLEN & HAMILTON INC
ATTN: J KEE

BOOZ-ALLEN & HAMILTON, INC
ATTN: J M VICE

HUDSON INSTITUTE, INC
ATTN: LIBRARY

INSTITUTE FOR DEFENSE ANALYSES
ATTN: CLASSIFIED LIBRARY
ATTN: DR H DICKENSON
ATTN: DR LESLIE COHEN
ATTN: E BAUER
ATTN: GRAHAM MCBRYDE
ATTN: I KOHLBERG
ATTN: OED W SHELESKI
ATTN: R MILLER

JASPER WELCH ASSOCIATES
ATTN: MAJ GEN J WELCH

JAYCOR
ATTN: E WENAAS

KAMAN SCIENCES CORP
2 CYS ATTN: T STRINGER

KAMAN SCIENCES CORP
ATTN: LIBRARY

KAMAN SCIENCES CORP
ATTN: DASIAC

KAMAN SCIENCES CORPORATION
ATTN: DASIAC

LOCKHEED AERONAUTICAL SYSTEMS
ATTN: CENTRAL LIBRARY

LOCKHEED MISSILES & SPACE CO, INC
ATTN: MGR VULNERABILITY & HARDENING

LOGICON R & D ASSOCIATES
ATTN: LIBRARY

LOGICON R & D ASSOCIATES
ATTN: DOCUMENT CONTROL

M I T LINCOLN LAB
ATTN: V SFERRINO
ATTN: C F WILSON
ATTN: V MISELIS
ATTN: R HALL

MARTIN MARIETTA DENVER AEROSPACE
ATTN: RESEARCH LIBRARY

MASSACHUSETTS INST OF TECHNOLOGY
ATTN: J RUINA

MCDONNELL DOUGLAS HELICOPTER CO
ATTN: B MOORE
ATTN: K PIERCE
ATTN: W SIMS

MISSION RESEARCH CORP
ATTN: DOCUMENT CONTROL
ATTN: TECH INFO CENTER

NICHOLS RESEARCH CORPORATION
ATTN: L GAROZZO

RAYTHEON - MSD
ATTN: LIBRARY

SCIENCE APPLICATIONS INTL CORP
ATTN: M ATKINS

TELEDYNE BROWN ENGINEERING
ATTN: P SHELTON

WILLIAMS INTERNATIONAL CORP
ATTN: C ANDREK

DEFENSE NUCLEAR AGENCY
ATTN: TITL/CA
6801 TELEGRAPH ROAD
ALEXANDRIA, VA 22310-3398

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300.

107200/001

DEFENSE TECHNICAL INFORMATION CENTER
ATTN DTIC/FDAB
CAMERON STATION
ALEXANDRIA, VA 22304-6145