



ARL-TR-9380 • JAN 2022



Quantitative Measurement of Cyber Resilience: A Tabletop Exercise

by Sidney C Smith, Stephen Raio, Robert F Erbacher,
MJ Weisman, Travis W Parker, and Jason E Ellis

Approved for public release; distribution is unlimited.

NOTICES

Disclaimers

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

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



Quantitative Measurement of Cyber Resilience: A Tabletop Exercise

**by Sidney C Smith, Stephen Raio, Robert F Erbacher,
and MJ Weisman**

*Computational and Information Sciences Directorate,
DEVCOM Army Research Laboratory*

Travis W Parker and Jason E Ellis

ICF International

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) Jan 2022		2. REPORT TYPE Technical Report		3. DATES COVERED (From - To) March 2021–July 2021	
4. TITLE AND SUBTITLE Quantitative Measurement of Cyber Resilience: A Tabletop Exercise				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Sidney C Smith, Stephen Raio, Robert F Erbacher, MJ Weisman, Travis W Parker, and Jason E Ellis				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) DEVCOM Army Research Laboratory ATTN: FCDD-RLC-ND Aberdeen Proving Ground, MD 21005-5066				8. PERFORMING ORGANIZATION REPORT NUMBER ARL-TR-9380	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES primary author's email: <sidney.c.smith24.civ@army.mil>.					
14. ABSTRACT The vulnerability of Army cyber-physical systems to cyber attack is well known, and the requirement to build cyber resilience into these systems has been firmly established. The key challenge this report addresses is that maturing this discipline requires the development of techniques, tools, and processes for objectively, rigorously, and quantitatively measuring the attributes of cyber resilience. Researchers and program managers need to be able to determine if the implementation of a cyber-resilience solution actually increases the cyber resilience of the system. There are several methodologies proposed in the literature to score or measure cyber resilience, which we will review. In addition, there are a few examples of how to use some of these methodologies; however, the literature does not contain detailed attempts to measure cyber resilience. This report documents a tabletop exercise conducted using a notional heavy vehicle on a fictitious military mission while under a cyber attack.					
15. SUBJECT TERMS cyber resilience, tabletop exercise, quantitative measurement, cyber attack, key performance parameter					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 61	19a. NAME OF RESPONSIBLE PERSON Sidney C. Smith
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (Include area code) 410-278-6235

Contents

List of Figures	v
List of Tables	v
Acknowledgments	vii
1. Introduction	1
1.1 Contribution	2
1.2 Research Questions	2
1.3 Organization	3
2. Background	4
2.1 Definition	4
2.2 Measurement Methodology	5
3. Approach	8
3.1 Cyber Resilience Definition	8
3.2 Use of the Measurement	8
3.3 Measurement Methodology	9
3.4 Measure of Success	9
3.5 Mission Scenario	10
3.6 Test Article	11
3.7 Key Performance Parameters	12
3.8 Threat Environment	12
3.9 Countermeasures	12
3.10 Example	13
4. Results	14
4.1 Unprotected Vehicle on Route 1 under a Speed Control Attack	15
4.2 Protected Vehicle on Route 1 under a Speed Control Attack	15
4.3 Unprotected Vehicle on Route 2 under a Speed Control Attack	16
4.4 Protected Vehicle on Route 2 under a Speed Control Attack	17

4.5	Unprotected Vehicle on Route 1 under a Cooling System Attack	18
4.6	Protected Vehicle on Route 1 under a Cooling System Attack	19
4.7	Unprotected Vehicle on Route 2 under a Cooling System Attack	20
4.8	Protected Vehicle on Route 2 under a Cooling System Attack	21
5.	Conclusion	22
5.1	Measures of Success	23
5.2	Lessons Learned	23
5.3	Research Questions	25
5.4	Future Work	25
6.	References	28
	Appendix A. Definitions of Cyber Resilience	32
	Appendix B. Results Tables	35
	List of Symbols, Abbreviations, and Acronyms	51
	Distribution List	52

List of Figures

Fig. 1	Representation of resilience as the area under the curve of systems functionality over time as presented by Ligo et al. ²²	6
Fig. 2	Probability weighted resilience volume as presented by Brtis ¹⁵	7
Fig. 3	Research methodology based on the four phases of design/refine implement experiment report (D/RIER)	9
Fig. 4	Map of the scenario	11
Fig. 5	Route 1 and Route 2 compared on speed and distance over time	14
Fig. 6	An unprotected vehicle on Route 1 while under a speed control attack	15
Fig. 7	A protected vehicle on Route 1 while under a speed control attack ...	16
Fig. 8	An unprotected vehicle on Route 2 while under a speed control attack	17
Fig. 9	A protected vehicle on Route 2 while under a speed control attack ...	18
Fig. 10	An unprotected vehicle on Route 1 while under a cooling attack	19
Fig. 11	A protected vehicle on Route 1 while under a cooling attack	20
Fig. 12	An unprotected vehicle on Route 2 while under a cooling attack	21
Fig. 13	A protected vehicle on Route 2 while under a cooling attack	22
Fig. 14	Iterative experimental plan for the QMoCR project	27

List of Tables

Table 1	Distance and elevation difference between point of interests (POIs) .	10
Table A-1	Definitions of Cyber Resilience	33
Table B-1	Time, Speed, and Cumulative distance for Routes 1 and 2	36
Table B-2	Time, Speed, and Cumulative distance for Route 1, speed attack, and an unprotected vehicle	38
Table B-3	Time, Speed, and Cumulative distance for Route 1, speed attack, and a protected vehicle	40
Table B-4	Time, Speed, and Cumulative distance for Route 2, speed attack, and an unprotected vehicle	41
Table B-5	Time, Speed, and Cumulative distance for Route 2, speed attack, and a protected vehicle	43
Table B-6	Time, Speed, and Cumulative distance for Route 1, cooling attack, and an unprotected vehicle	45

Table B-7	Time, Speed, and Cumulative distance for Route 1, cooling attack, and a protected vehicle	46
Table B-8	Time, Speed, and Cumulative distance for Route 2, cooling attack, and an unprotected vehicle	47
Table B-9	Time, Speed, and Cumulative distance for Route 2, cooling attack, and a protected vehicle	49

Acknowledgments

The authors would like to thank the Office of the Under Secretary of Defense Research and Engineering for funding the Quantitative Measurement of Cyber Resilience project, and Dr. Alexander Kott for his preliminary work and continuing advice and direction.

1. Introduction

The security vulnerabilities of the controller area network (CAN) bus, used in modern vehicles, have been well known since Hoppe and Dittman demonstrated them through successful attacks on the electronic window lift system.^{1,2} The dependence of vehicles on the functionality provided by the CAN bus has only grown since then, with many critical systems now relying on the CAN bus to operate. Further, while the CAN bus was once thought to be a completely isolated network, it is now exposed to the user through the on-board diagnostics ports. Not only was isolation a false assumption, due to supply chain attacks³ and physical/electromagnetic access, but the situation is worsening as new wireless communication systems are incorporated into vehicle control systems as well as connections between control buses and platform-resident mission networks. Vehicle entertainment systems often support Bluetooth,⁴ Wi-Fi,⁵ and cellular wireless networks while also being directly attached to the CAN bus, providing remote access. The wireless tire pressure monitoring system, available on most modern vehicles, provides a pathway to remotely access the CAN bus. Access may also be gained through hardware/software Trojans inserted into add-on technologies for condition-based maintenance, or through subverting over-the-air software updates.

Many solutions have arisen to address these security vulnerabilities, including network segmentation, authentication, and encryption, as well as intrusion detection and prevention.² Along with the increase in research in the cyber security of vehicle systems, is the realization that perfect security is impractical. With this realization comes a focus on cyber resilience. Cyber resilience goes beyond cyber security by focusing on completing the mission. This will necessarily incorporate cyber security but has a wider view. Specifically, the focus of cyber resilience is to accomplish the mission while systems are under attack, already compromised, or its components are degraded.

In order for the field of cyber resilience to mature, there must be "techniques, tools, and processes for objectively measuring the attributes of phenomena occurring in the systems of that discipline."⁶ There are several methodologies proposed in the literature to score or measure cyber resilience, which we will review in Section 2. In addition, there are a few examples of how to use some of these methodologies; however, the literature does not contain detailed attempts to measure cyber resilience.

We designed and implemented a tabletop exercise to test our initial assumptions about the quantitative measurement of cyber resilience.

1.1 Contribution

The key contribution of this report is that maturing this discipline requires the development of techniques, tools, and processes for objectively, rigorously, and quantitatively measuring the attributes of cyber resilience.⁶ Researchers and program managers need to be able to determine if the implementation of a cyber resilience solution actually increases the cyber resilience of the system. There are several methodologies proposed in the literature to score or measure cyber resilience, which we will review in Section 2. In addition, there are a few examples of how to use some of these methodologies; however, the literature does not contain detailed attempts to measure cyber resilience. This report documents a tabletop exercise⁷ conducted to measure the cyber resilience of a notional heavy vehicle on a fictitious military mission while under a cyber attack.

1.2 Research Questions

This report begins the process of answering the following research questions:

1. **How is cyber resilience defined?** Before something can be measured, it must be defined precisely in a way that is measurable. There are several definitions of resilience and cyber resilience in the literature. “One expert claims that well over 100 unique definitions of resilience have appeared.”⁸
2. **How will the quantitative cyber resilience measurement be used?** There are many applications for a cyber resilience measurement: (a) Researchers could use it to measure the improvements to cyber resilience when using their methodologies. (b) Project managers could use such a measurement to compare competing cyber resilience solutions. (c) Mission planners could use such a measurement to decide what materiel is appropriate for the mission.

It is unlikely that one measurement will satisfy every need; therefore, it will be necessary, initially, to focus on a single customer and their specialized need, or a small group of related customers. Further, it is unlikely that a single measurement methodology will scale across every application. As the scope of the object being measured increases, the fidelity with which each element is simulated decreases. When battles and campaigns are simulated,

the performance of each element is reduced to a set of probabilities. These methods of measuring cyber resilience may not apply in that environment; however, they may be used to inform the probabilities used to simulate the cyber resilience of individual elements within the simulation.

3. **What methodology to use to measure cyber resilience?** This measurement must be independent, rigorous, science-based, repeatable, automated and affordable. Kott and Linkov spelled out four characteristics of such a measurement. (a) It must be repeatable—if the same system is measured with the same tool, the results should be similar. (b) It must be consistent with respect to missions—similar missions should yield similar results. (c) It should have monotonicity with respect to defenses—if the defenses are strengthened, then the score should improve. (d) It should have monotonicity with respect to attacks—if the threat increases, then the score should decrease.⁶
4. **What exactly is measured to compute the cyber resilience?** Although there are many definitions for cyber resilience in the literature, most of them relate to the ability of the system to perform a task during adverse events. One of the key differences between cybersecurity and cyber resilience is that cybersecurity tends to be focused on the system while cyber resilience is focused on the mission. A crucial question here is how to measure mission success in a continuous manner that would lend itself to a quantitative measurement of cyber resilience. One possibility is to measure performance against key performance parameters (KPPs), defined as critical characteristics, which if changed would have a profound effect on mission satisfiability. Determining which KPPs to measure is a pivotal element of this research question.

1.3 Organization

The development of a quantitative measure of cyber resilience begins with a clear definition of cyber resilience. In Section 2, we review several of the definitions of resilience. In addition, the measure development will require a measurement methodology. Section 2 will also review several of the currently proposed measurement methodologies for cyber resilience. Our approach and assumptions are presented in Section 3. Our results and lessons learned are presented in Section 4. In Section 5, we provide our conclusions and outline the next steps for developing a quantitative measure of cyber resilience.

2. Background

The Quantitative Measurement of Cyber Resilience (QMoCR) project began out of the necessity for the Department of Defense (DoD) community to establish technically rigorous, science-based, repeatable, automated, and affordable methods to measure cyber resilience of military engineered artifacts. It is recognized that without a suitable quantitative measure and method for assessing cyber resilience, it is not possible to make justifiable and efficient investments and improvements in system cyber resilience. Use cases for this measure and assessment methodology include, but are not limited to, comparison of competing cyber resilience solutions for a particular cyber-physical system, making operational risk-based decisions focused on comparison of courses of action involving different systems for the same mission, and understanding the impact on cyber resilience of changes to a system or the threat environment under which it operates.

The aforementioned tabletop exercise is an initial step toward that end goal. By walking through a cyber-physical system scenario in a multi-domain operations context we gain insight into the breadth and depth of the problem space prior to advancing to a hardware-based assessment. This allows us to quickly and efficiently validate or modify the initial approach to cyber resilience measurement and automated assessment, as described in more detail throughout this report.

2.1 Definition

As stated earlier, it is estimated that there are over 100 unique definitions of resilience or resilience terms,⁹ including: (a) The National Institute of Standards and Technology defines the term information systems resilience.¹⁰ (b) The Committee on National Security Systems defines the term operational resilience.¹¹ (c) The International Council on Systems Engineering defines resilience in the context of engineered systems.¹² (d) Cyber resilience is defined by the Scottish Government, Committee on Payments and Market Infrastructure, Bank for International Settlements, World Economic Forum, Accenture, The Department of Homeland Security, as well as numerous other researchers.^{6,13–15} Appendix A provides an overview of the various definitions of resilience in cyber and related disciplines.

2.2 Measurement Methodology

In his paper, “Towards a quantifiable measure of resilience,¹⁶” Bene describes the resilience of communities to natural disasters; however, he makes a point about the need for a measure of resilience that is independent of the factors that are used to compute the resilience measure. Consider a researcher trying to find ways to improve a community’s resilience to climate change; the researcher cannot measure resilience directly, so constructs a resilience index (RI). The RI is composed of factors that the researcher learns through experience contribute to community resilience. One of these factors is the livelihood diversification index (LDI). The RI is computed before and after conducting an intervention to improve livelihood diversification. As expected, the RI is higher after the intervention. However, this is circular logic because the LDI was assumed to be a component of the RI. As a better example, he cites Sanders et al., where research was conducted into improving the health resilience of a community. In this study, tooth retention was used as the metric. Since the factors that they studied were not directly related to dental health, this gave them an independent measure of health resilience.¹⁶ Bene proposed the cost of resilience as an independent measure, defined in Eq. (1) where C_{res} is the resilience score, C_a is the anticipated cost or the cost of resilience counter measures, C_i is the cost of the impact of the event, and C_{rec} is the recovery cost.¹⁶

$$C_{res} = C_a + C_i + C_{rec}. \quad (1)$$

This measure is attractive because it expresses the cost of resiliency in terms of the total cost of ownership, which is a well understood concept. It also illustrates the point where spending more to increase a system’s resilience is no longer cost effective.

The system proposed by Bodeau et al.^{17–19} from Mitre provides a catalog of cyber resilience metrics. It encourages program managers to select the metrics that best apply to their systems from an extensive catalog and then rates the system’s compliance against the metrics. This method is subjective because it relies upon expert opinion as to the selection and priority of each metric as well as the level of compliance in the system for that metric. Additionally, it is not independent since the system only measures compliance against the metrics and not the independent measure of the cyber resilience of the system. The system is, however, discreet since

each metric is *prioritized* on a scale from 1 to 5 and then *rated* on a separate distinct scale from 1 to 5.^{17–19}

The system proposed by Whelihan et al.²⁰ assesses the mission essential function (MEF) of a system. Each MEF is then analyzed for the various failure modes that could impact it. Each failure mode is then assessed to determine if the system can detect, isolate, and recover (DIR) in time for the mission to succeed. This system is qualitative in that each failure mode receives a score of one for each DIR element if the action may be completed in time and zero otherwise. These scores are then summed for each MEF.^{20,21}

Ligo et al.²² surveyed various measurement techniques for cyber resilience in their paper, “How to Measure Cyber Resilience of an Autonomous Agent: Approaches and Challenges.”²² They propose plotting the performance of a system under cyber-attack and measuring the area under the curve, as seen in Fig. 1.

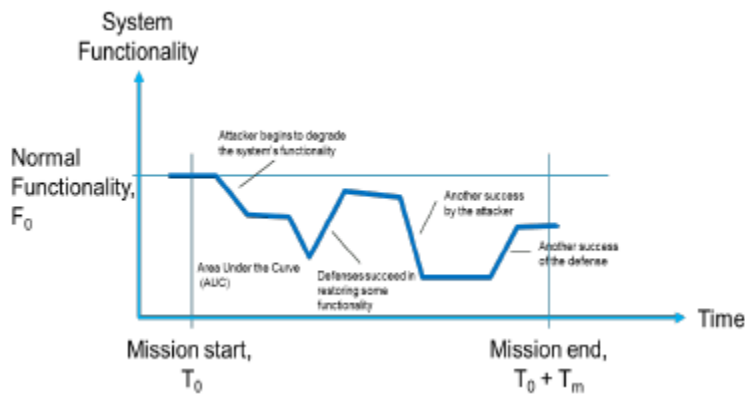


Fig. 1 Representation of resilience as the area under the curve of systems functionality over time as presented by Ligo et al.²²

In his report, “How to Think About Resilience in a DoD Context,¹⁵” Brtis recommends a framework for addressing resilience in military systems. This framework includes a metric for measuring resilience. “We evaluated 23 candidate metrics against 19 evaluation criteria. From this analysis we conclude that the best single metric for resiliency is the expected availability of the required capability.”¹⁵ He describes measuring the expected performance of a system across several mission scenarios to form a surface and measuring the area under that surface, as seen in Fig. 2.

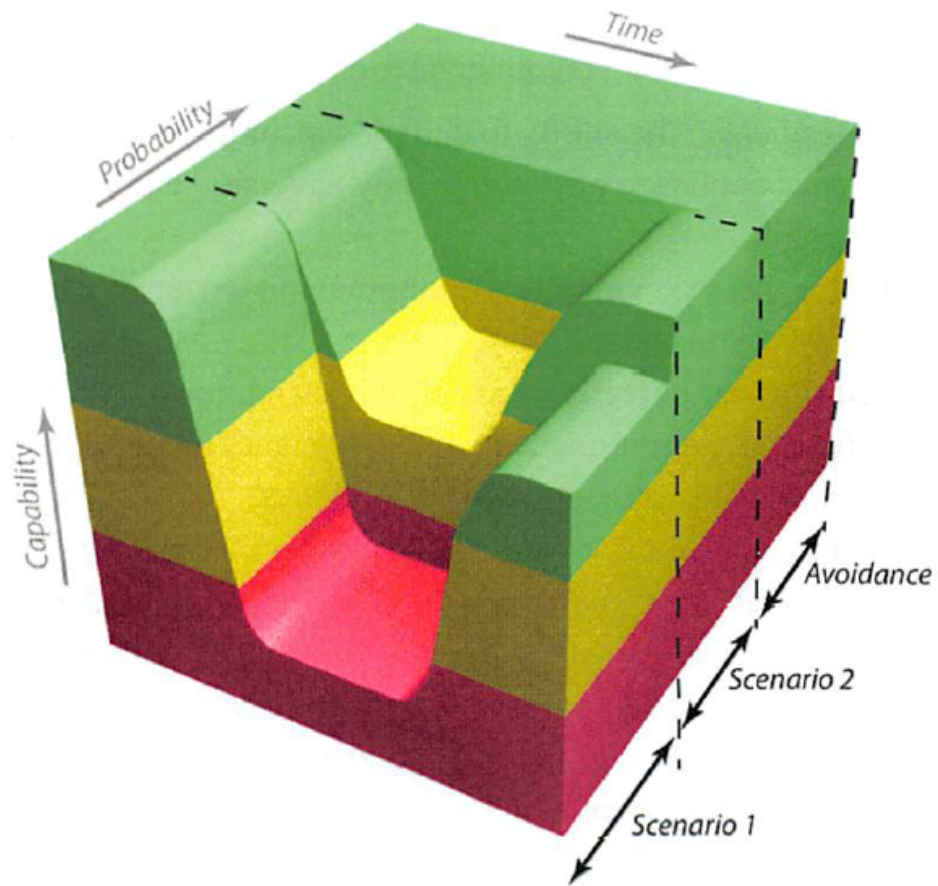


Fig. 2 Probability weighted resilience volume as presented by Brtis¹⁵

In his paper, “A Resilience Measure to Guide System Design and Management,”²³ Ferris proposes using a trade-space model to find a figure of merit (FOM) to measure resiliency. This model, he argues, would provide an objective comparison of proposals with different properties.²³

3. Approach

This project will use an iterative approach to answering our research questions and developing a methodology for quantitatively measuring cyber resilience, as seen in Fig. 3. An initial definition of cyber resilience, purpose for the measurement, measurement methodology, and measures of success have been selected from the literature review. In addition, initial mission scenarios, threat environments, vehicle simulators, and countermeasures have been crafted. One of the purposes of this tabletop exercise is to develop requirements for the automated cyber resilience assessment tool (AutoCRAT), which will implement the adversary simulator, orchestrate the mission, and implement the measurement methodology. These criteria and tools will be refined through a series of experiments. The solid shapes indicate portions that we consider to be within the scope of this project. The dashed shapes are portions that are important to the project but not within the scope. For example, this project would greatly benefit from a high-fidelity vehicle simulator; however, developing such a simulator is outside the scope of this project.

3.1 Cyber Resilience Definition

For the purpose of the tabletop exercise, we will use the following working definition for cyber resilience: cyber resilience, in this context, is the ability of systems to resist, absorb, and recover/adapt to a cyber compromise after the compromise occurs, during execution of a mission.

3.2 Use of the Measurement

Initially, we will focus on a metric that may be used by researchers to evaluate the success of their approach and by program managers who need to choose between different approaches. We will focus on cyber resilience in the mission context as opposed to the entire system lifecycle.

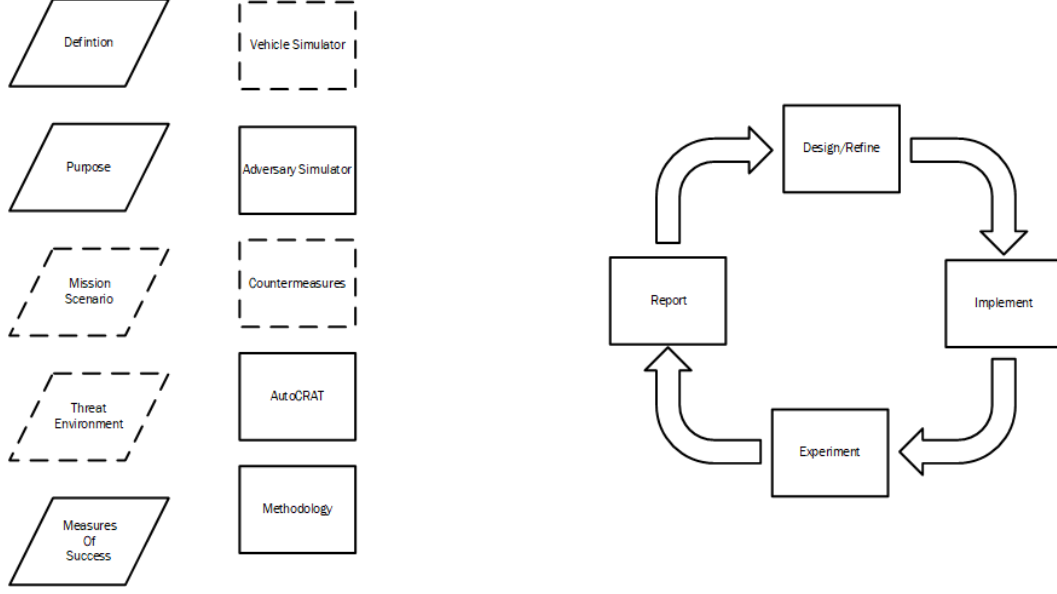


Fig. 3 Research methodology based on the four phases of design/refine implement experiment report (D/RIER)

3.3 Measurement Methodology

For this exercise, we employed the area under the functionality curve as proposed by Ligo et al.²² We selected speed and total distance to be the KPPs. We determined the planned value of the KPPs for every 10-min segment of the exercise. We then recorded the actual exercise value for each KPP for every 10-min segment of the exercise. Finally, we plotted the normalized value of the KPPs and computed the area under the functionality curve to determine the cyber resilience score. The score, S is defined in Eq. (2) where S is the score, n is the number of time segments, O_i is the observed value of the KPP at the time segment i , and P_i is the planned value of the KPP at the time segment i .

$$S = \frac{\sum_{i=1}^n \frac{O_i}{P_i}}{n}. \quad (2)$$

3.4 Measure of Success

Kott and Linkov⁶ provide the following measures of success:

1. It must be repeatable. If the same system is measured with the same tool, the results should be similar.

2. It must be consistent with respect to missions. Similar missions should yield similar results.
3. It should have monotonicity with respect to defenses. If the defenses are strengthened, then the score should improve.
4. It should have monotonicity with respect to attacks. If the threat increases, then the score should decrease.⁶

3.5 Mission Scenario

For this exercise, we considered a heavy military vehicle required to transport materiel from point of interest (POI)-1 to POI-8, as seen in Fig. 4. Further, we assume that this mission will take place in a desert climate where the temperature is typically 30 to 40 degrees. This mission plan contained two routes. The first route starts at POI-1 and moves through POI-2, POI-3, POI-4, POI-5, POI-6, POI-7, and finally to POI-8. It is 250 km long over paved roads and generally flat terrain with a gradual descent of 152 m. The second route starts at POI-1 and moves through POI-2, POI-3, POI-4, POI-9, POI-10, POI-7, and finally to POI-8. It is 249 km long over gravel roads and mountainous terrain with an ascent of 937 m and a summed decent of 1089 m. The distances and changes in elevation for POIs may be seen in Table 1. The trek from POI-1 to POI-8 over the first route is estimated to take 4 h. The trek from POI-1 to POI-8 over the second route is estimated to take 6 h. This mission requires that the materiel be delivered in 8 h.

Table 1 Distance and elevation difference between POIs

POI	Distance in km	Delta Elevation in m
1 -> 2	20.6	-15.24
2 -> 3	5.1	-15.24
3 -> 4	7.1	-15.24
4 -> 5	58.5	-45.72
5 -> 6	34.1	-22.86
6 -> 7	111.8	-30.48
7 -> 8	12.9	-7.62
4 -> 9	85.5	937.26
9 -> 10	45.0	-38.10
10 -> 7	72.6	-998.22

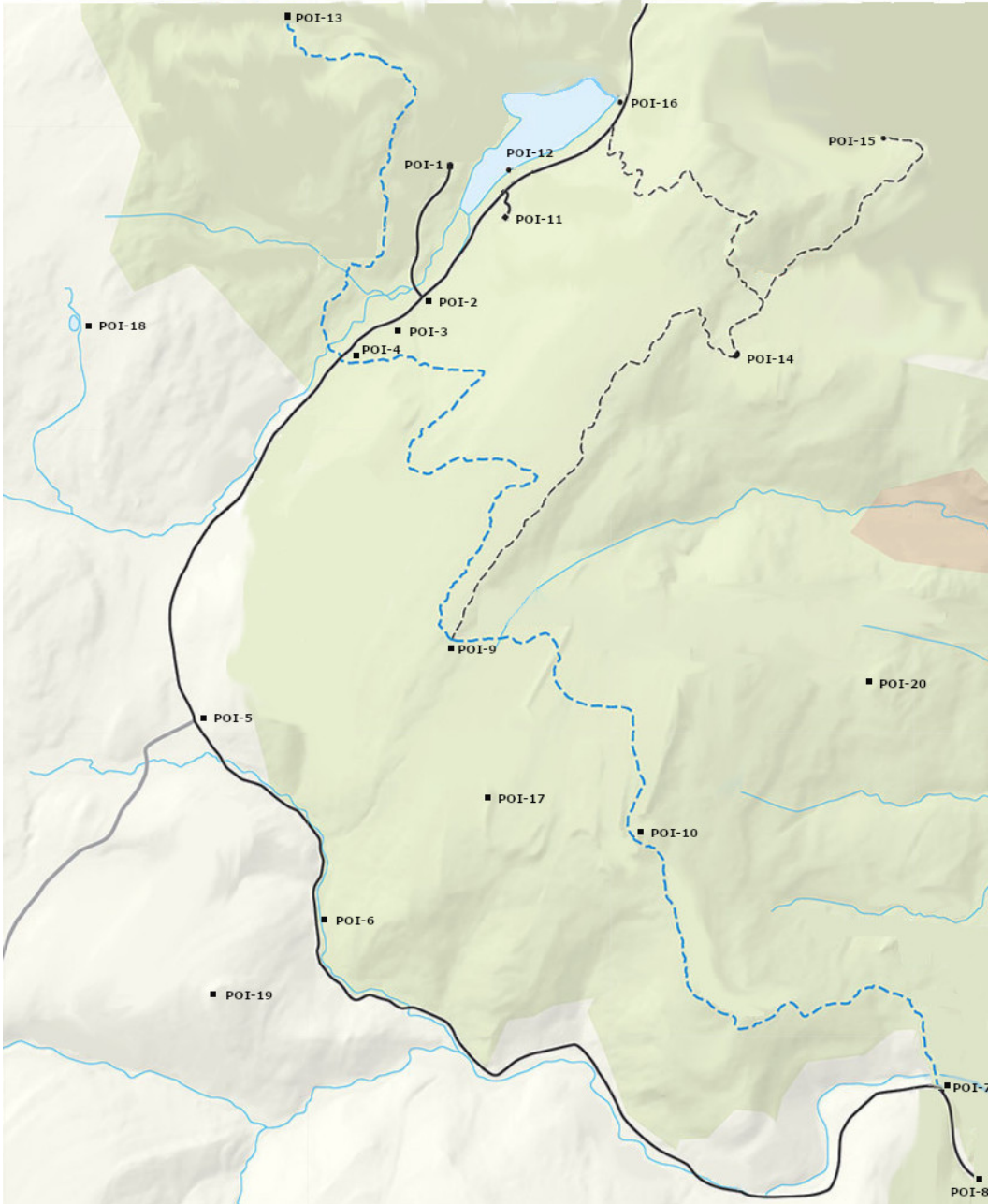


Fig. 4 Map of the scenario

3.6 Test Article

In this exercise we consider a modern heavy military manned land vehicle. It is important to note that we are considering current military manned land vehicles and what we understand their current cyber capabilities to be. This can and likely will change drastically in the future. Further, autonomous unmanned aerial vehicles

likely already have drastically different capabilities.

3.7 Key Performance Parameters

In order for a KPP to be a viable candidate for inclusion in the resilience measure it must be measurable quantitatively, relevant to the current mission scenario(s), independent, and supported by the article under test. For example, we could have used fuel economy as a KPP but computing the impact of cyber effects on fuel economy was judged to be too complex for this tabletop exercise. Alternatively, we could have used horse power as a KPP; however, that contributes to vehicle speed and would be captured by the KPP of speed. We chose speed and distance over time, which are basically the same thing, as the KPPs to measure for this exercise. Future experiments will include additional KPPs; for example, for a system with weapons, targeting accuracy would be a measurable KPP, and for systems with cameras, resolution would be a measurable KPP.

3.8 Threat Environment

The field of cyber resilience assumes that an attack can be successful and that cybersecurity alone is insufficient. To narrow the scope of the experimental setup, we assume a compromise has been successful. For this reason, and because assessing vulnerability to cyber attack requires a relevant article to test, we will initially focus on cyber-effects. For this exercise, we chose an attack to the driver's ability to control the speed of the vehicle as well as an attack on the vehicle's cooling system.

Speed. An effect on speed can be achieved by repeatedly sending a CAN bus message to the engine to idle while the transmission is changing gears. It can also be accomplished by repeatedly sending a throttle setting of zero to the engine. The attack was initiated at $T = 30$ min.

Cooling. An effect on cooling can be achieved by repeatedly sending a false engine temperature to the cooling system, which prevents the radiator fan from engaging. This attack was also initiated at $T = 30$ min.

3.9 Countermeasures

For this exercise, we considered two countermeasures. The first monitors the CAN bus and prevents messages to idle the engine except for a small window when the vehicle is actually shifting gears. The second calculates the engine temperature

based on all of the information available on the CAN bus and engages the radiator fan when its model indicates that the engine is overheating.

3.10 Example

The two planned routes provide an opportunity to illustrate how the cyber resilience score would work. For Route 1, we assume that a heavy vehicle would have no issues maintaining a speed of 60 kph on a paved road with a slight negative grade. For Route 2, we assume that a heavy vehicle will be able to maintain a speed of 40 kph on a gravel road over a mountain. The second route will take longer than the first route due to the condition of the road and the changes in elevation. We would expect the resilience score of a vehicle on the second route to be less than the resilience score of the first route. Figure 5 shows the time, speed, and cumulative distance for both routes. The raw data may be found in Table B-1 in Appendix B.

If we compute scores by summing the normalized speed and distance over time we would get a score of 1 for speed and 1 for distance using Route 1. Using the same formulas, we would get a score of 0.72 for speed and 0.82 for distance using Route 2. These figures demonstrate the performance hit in our KPPs of speed and distance using Route 2.

At a speed of 31.3 kph along Route 1, the vehicle will travel from POI-1 to POI-8 in 8 h. The score for speed is 0.52 and the score for distance is 0.64. We will use these as the minimum acceptable resilience scores that will satisfiably complete the mission.

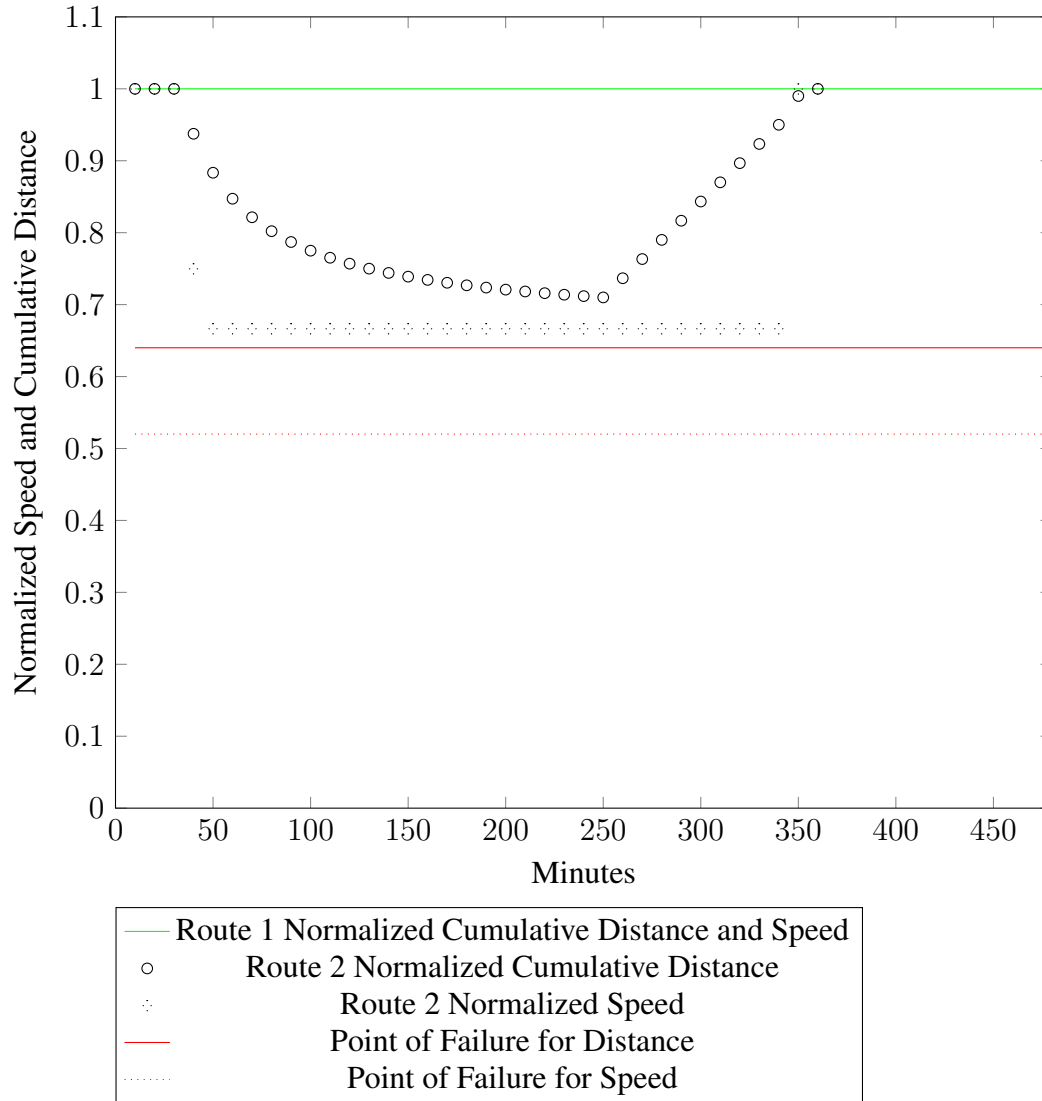


Fig. 5 Route 1 and Route 2 compared on speed and distance over time

4. Results

For this tabletop exercise we considered unprotected and protected vehicles against attacks to speed control and to the cooling system along Routes 1 and 2.

4.1 Unprotected Vehicle on Route 1 under a Speed Control Attack

In this trial, we consider an unprotected vehicle using Route 1 under a speed control attack which initiates at $T = 30$ min. This attack will cause the engine to idle, regardless of any action taken by the driver. We assume that an idling engine will be able to pull the vehicle downhill at 12 kph. The raw data may be found in Appendix B Table B-2. Figure 6 plots the normalized speed and cumulative distance over time. At 8 h 10 min into the trial, the vehicle has traversed 122 km, which is insufficient to complete the mission in the allotted time frame. This is shown by a speed score of 0.248, which is less than the minimum score of 0.52, and a distance score of 0.38, which is less than the minimum score of 0.64.

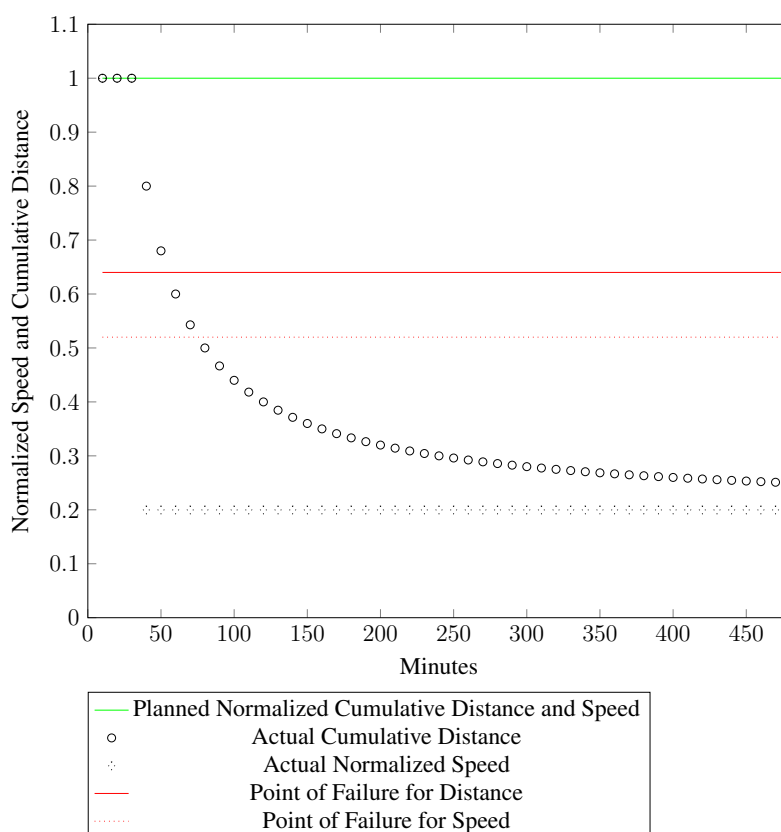


Fig. 6 An unprotected vehicle on Route 1 while under a speed control attack

4.2 Protected Vehicle on Route 1 under a Speed Control Attack

The countermeasure that we considered would only allow the engine to respond to the CAN message to idle for a small window when the transmission is actually shifting. Since proceeding down a small decline at a constant speed would rarely

require the transmission to shift gears, the countermeasure was judged to be completely effective at preventing the attack from reducing the capability of the vehicle. The results are shown in Table B-3. Figure 7 plots the normalized speed and cumulative distance over time. The score for speed was calculated to be one and the score for cumulative distance was calculated to be one.

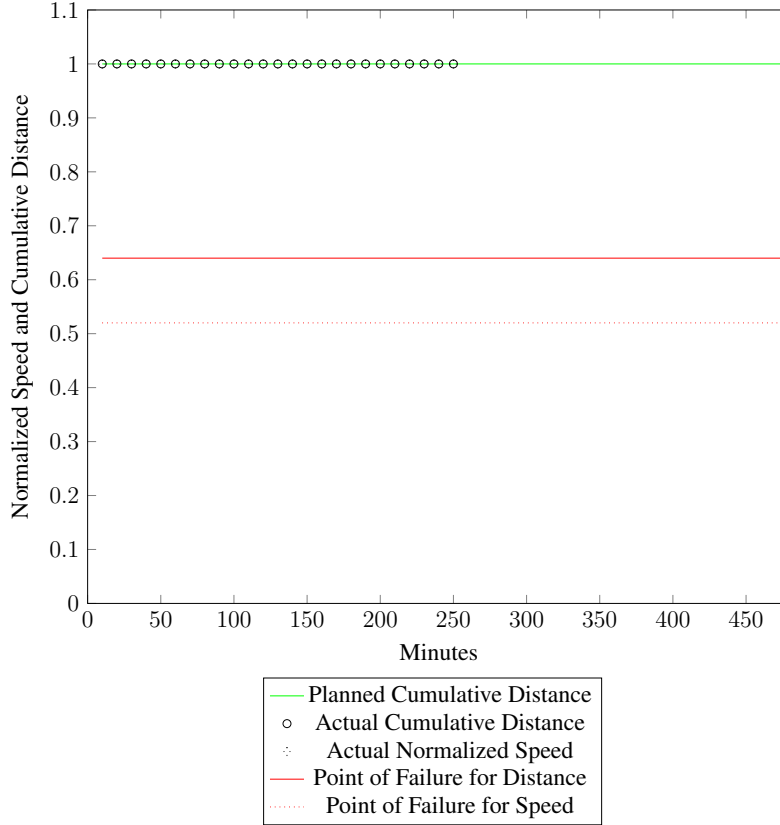


Fig. 7 A protected vehicle on Route 1 while under a speed control attack

4.3 Unprotected Vehicle on Route 2 under a Speed Control Attack

In this trial, we consider an unprotected vehicle using Route 2 under a speed control attack which initiates at $T = 30$ min. This will be 2.8 km before the vehicle reaches POI-4. At this point, the vehicle will stop because an idle engine is not capable of pulling the vehicle up the incline over the gravel road to POI-9. Table B-4 shows the time, the planned speed and cumulative distance, the actual speed and cumulative distance, and the normalized speed and cumulative distance. Figure 8 plots the normalized speed and cumulative distance over time. At 8 h and 10 min into the trial, the vehicle has traversed 32.8 km which is insufficient to complete the mission in the allotted time frame. This is shown by a speed score of 0.09, which is less than

the minimum score of 0.52, and a distance score of 0.30, which is less than the minimum score of 0.64.

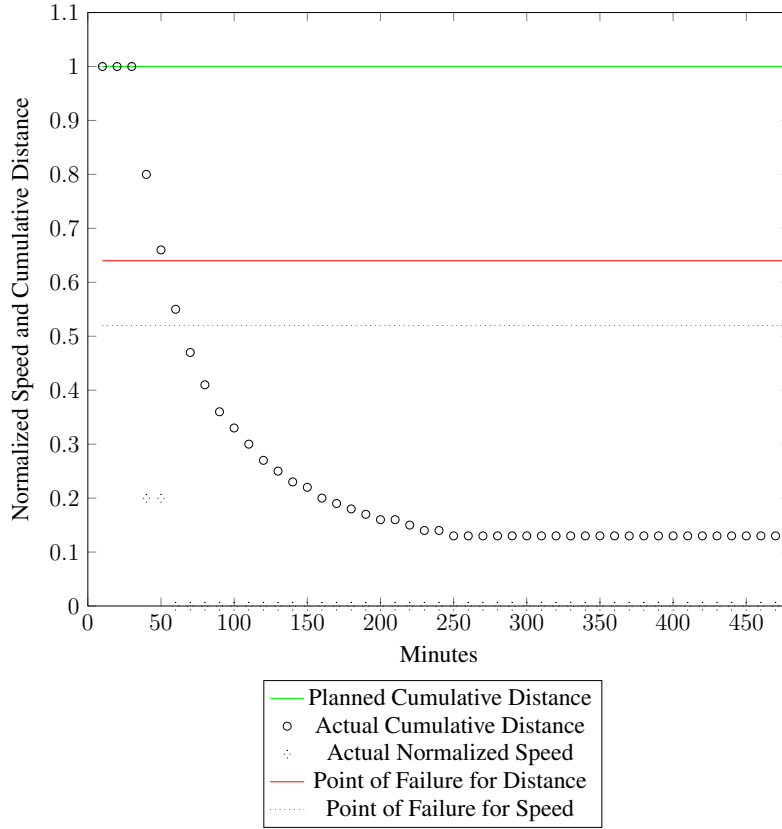


Fig. 8 An unprotected vehicle on Route 2 while under a speed control attack

4.4 Protected Vehicle on Route 2 under a Speed Control Attack

In this trial, we consider a protected vehicle using Route 2 under a speed control attack which initiates at $T = 30$ min. The attack will begin 2.8 km before the vehicle reaches POI-4. We assume that traveling from POI-4 to POI-9 over a gravel road and climbing over 937 m will require the transmission to shift gears frequently. This will provide an opportunity for the attack to reduce the engine speed. We judge this effect will reduce the speed of the vehicle over this segment from the planned 40 kph to 35 kph. Table B-5 shows the time, the planned speed and cumulative distance, the actual speed and cumulative distance, and the normalized speed and cumulative distance. Figure 9 plots the normalized speed and cumulative distance over time. At 6 h and 10 min into the trial, the vehicle has traversed 250 km and successfully completed the mission within the allotted time frame. This is shown by a speed score of 0.69, which is greater than the minimum score of 0.52, and a

distance score of 0.78, which is greater than the minimum score of 0.64.

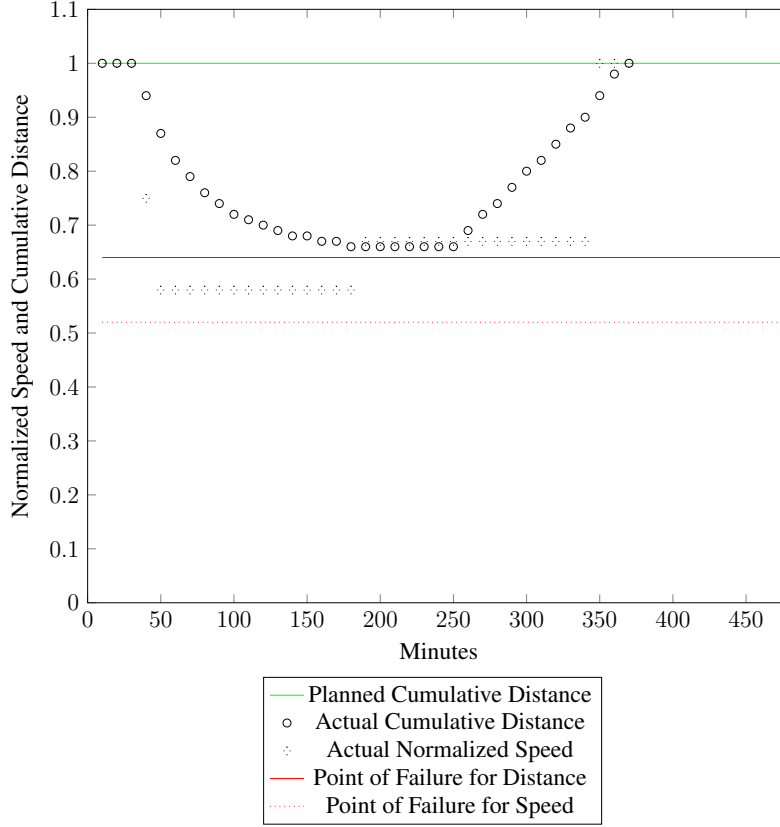


Fig. 9 A protected vehicle on Route 2 while under a speed control attack

4.5 Unprotected Vehicle on Route 1 under a Cooling System Attack

In this trial, we consider an unprotected vehicle traveling along Route 1 under a cooling system attack starting at $T = 30$ min. The cooling system attack will spoof engine temperature readings, fooling the cooling system in such a way that the radiator fan is not engaged and causing the engine to overheat. We judge that traveling downhill over a paved road at sufficient speed would not require the cooling fan as there would be adequate natural airflow over the radiator. Under these conditions, the attack would have no effect on the performance of the vehicle. Table B-6 shows the time, the planned speed and cumulative distance, the actual speed and cumulative distance, and the normalized speed and cumulative distance. Figure 10 plots the normalized speed and cumulative distance over time. At 4 h and 10 min into the trial, the vehicle has traversed 250 km and successfully completed the mission within the allotted time frame. This is shown by a speed score of 1.00, which is greater than the minimum score of 0.52, and a distance score of 1.00, which is

greater than the minimum score of 0.64.

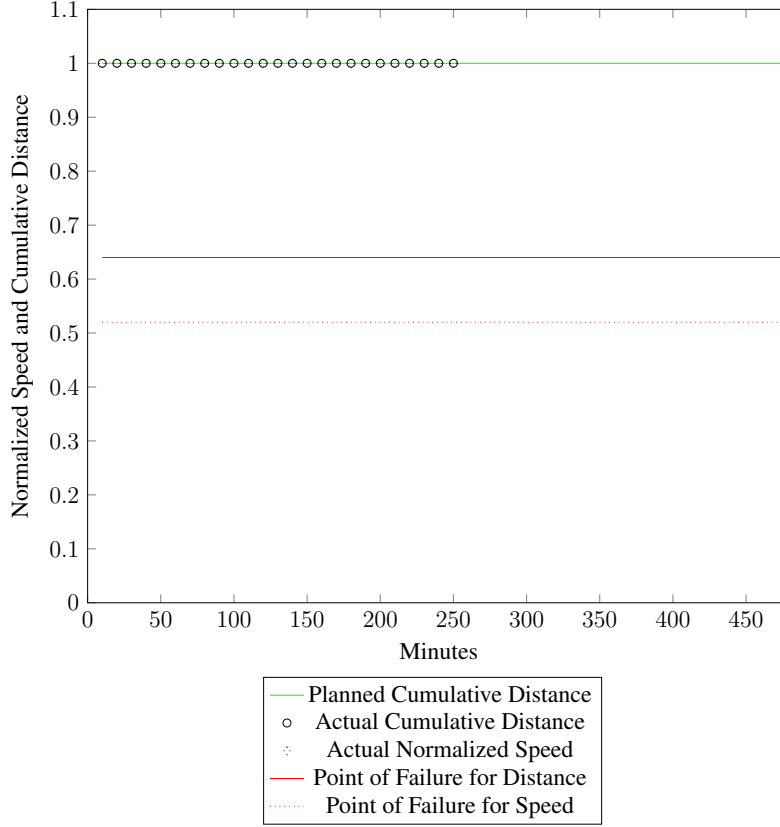


Fig. 10 An unprotected vehicle on Route 1 while under a cooling attack

4.6 Protected Vehicle on Route 1 under a Cooling System Attack

In this trial, we consider a protected vehicle traveling along Route 1 under a cooling system attack starting at $T = 30$ min. The cooling system attack will spoof engine temperature readings, fooling the cooling system in such a way that the radiator fan is not engaged and causing the engine to overheat. The countermeasure will keep track of various aspects of the engine performance, including revolutions per minute and torque to compute engine temperature. If the computed temperature is too high, then the countermeasure will engage the radiator fan. We judge that traveling downhill over a paved road would not require the cooling fan. Under these conditions, the countermeasure would be completely effective at preserving the performance of the vehicle. Table B-7 shows the time, the planned speed and cumulative distance, the actual speed and cumulative distance, and the normalized speed and cumulative distance. Figure 11 plots the normalized speed and cumulative distance over time. At 4 h and 10 min into the trial, the vehicle has traversed 250 km and successfully

completed the mission within the allotted time frame. This is shown by a speed score of 1.00, which is greater than the minimum score of 0.52, and a distance score of 1.00, which is greater than the minimum score of 0.64.

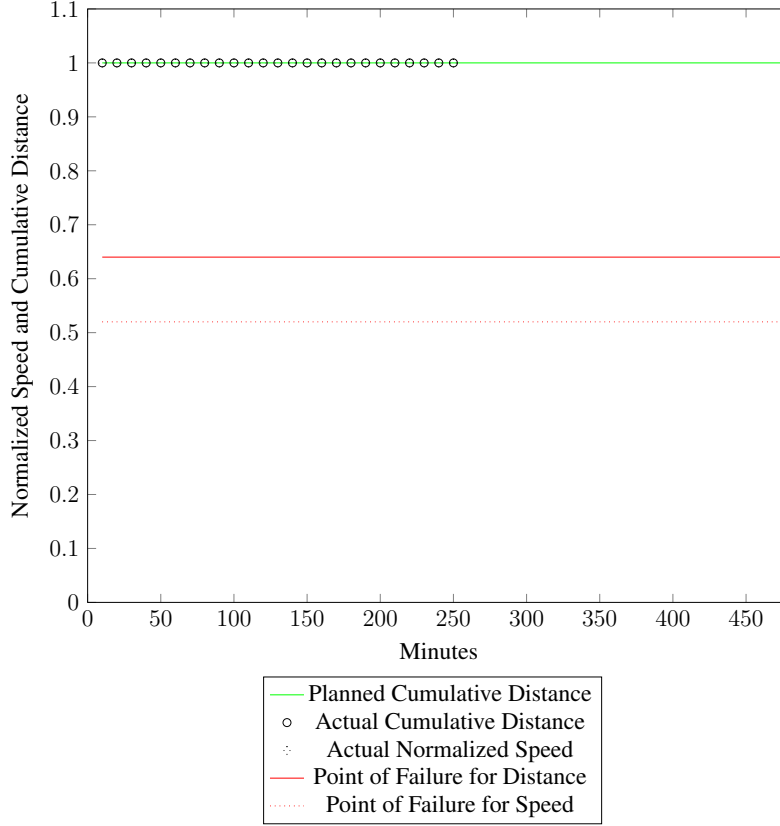


Fig. 11 A protected vehicle on Route 1 while under a cooling attack

4.7 Unprotected Vehicle on Route 2 under a Cooling System Attack

In this trial, we consider an unprotected vehicle using Route 2 under a cooling system attack which initiates at $T = 30$ min. We judge that this attack will not manifest itself until $T = 2:00:00$ because at this point the cooling system will be unable to cool the engine, which is pulling the vehicle up an incline over a gravel road. We also assume that the attack would not cloak itself to prevent the operator from being aware that the engine is overheated. After stopping for 1 h and 40 min, the engine will have cooled sufficiently to complete the climb. Once the climb is completed, the radiator will be sufficient to keep the engine cool without the fan. The vehicle will then complete the journey. Table B-8 shows the time, the planned speed and cumulative distance, the actual speed and cumulative distance, and the normalized speed and cumulative distance. Figure 12 plots the normalized speed

and cumulative distance over time. At 7 h and 50 min into the trial, the vehicle has traversed 250 km, which is sufficient to complete the mission in the allotted time frame. This is shown by a speed score of 0.55, which is greater than the minimum score of 0.52, and a distance score of 0.69, which is less than the minimum score of 0.64.

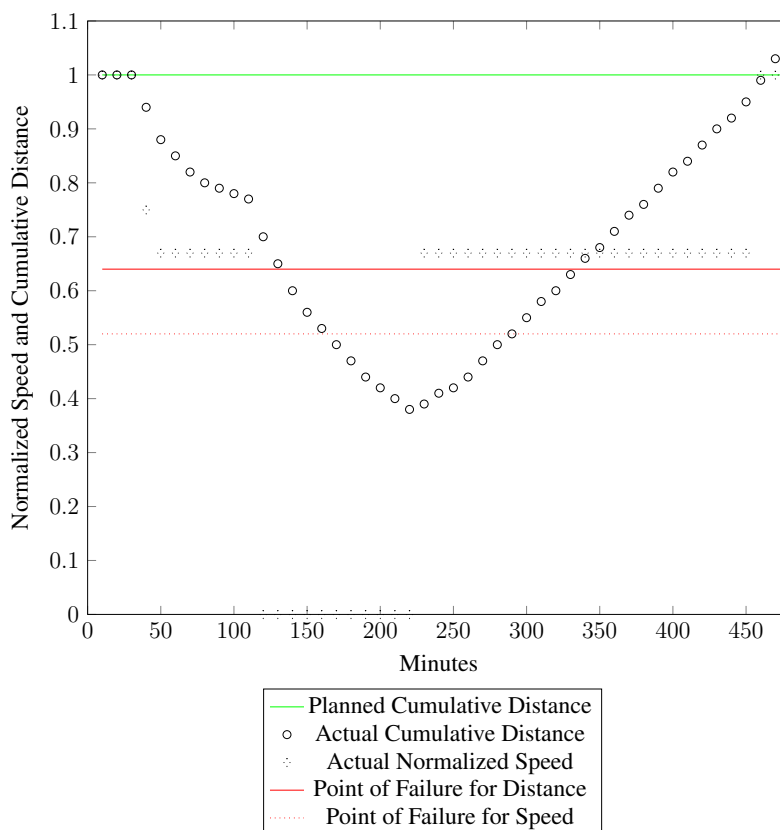


Fig. 12 An unprotected vehicle on Route 2 while under a cooling attack

4.8 Protected Vehicle on Route 2 under a Cooling System Attack

In this trial, we consider a protected vehicle traveling along Route 2 under a cooling system attack starting at $T = 30$ min. The cooling system attack will spoof engine temperature readings, fooling the cooling system in such a way that the radiator fan is not engaged and causing the engine to overheat. The countermeasure will keep track of various aspects of the engine performance to compute engine temperature. If the computed temperature is too high then the countermeasure will engage the radiator fan. We judge that traveling uphill over a gravel road would require the cooling fan. Under these conditions, the countermeasure would engage the fan and be completely effective at preserving the performance of the vehicle. Table B-9

shows the time, the planned speed and cumulative distance, the actual speed and cumulative distance, and the normalized speed and cumulative distance. Figure 13 plots the normalized speed and cumulative distance over time. At 6 h into the trial, the vehicle has traversed 250 km and successfully completed the mission within the allotted time frame. This is shown by a speed score of 0.72, which is greater than the minimum score of 0.52, and a distance score of 0.82, which is greater than the minimum score of 0.64.

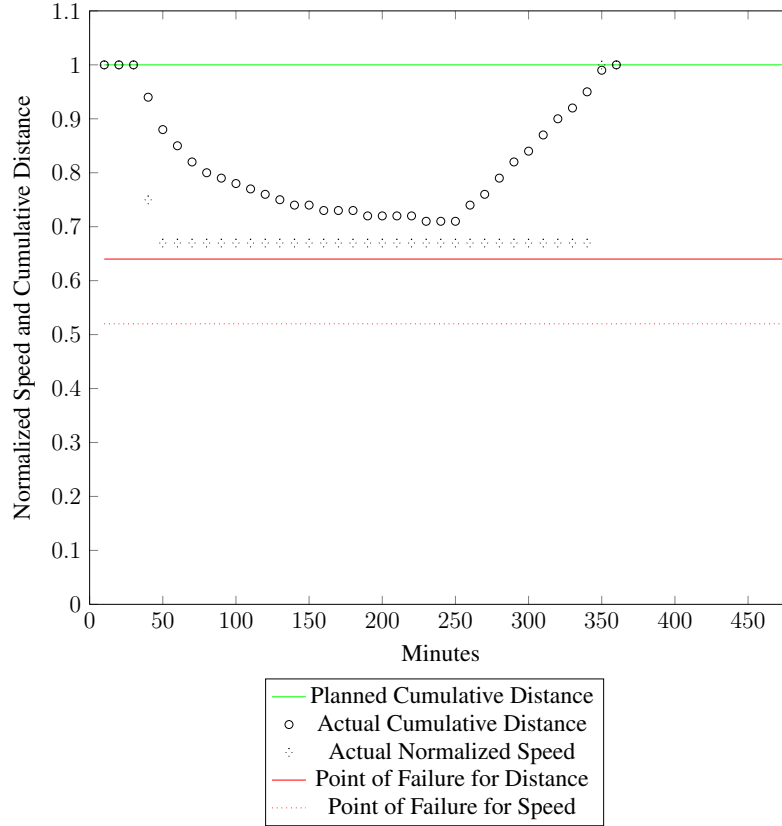


Fig. 13 A protected vehicle on Route 2 while under a cooling attack

5. Conclusion

We conclude this report by considering our initial methodology for measuring cyber resiliences against our measures of success. Next we will share some of the lessons that we have learned. We will consider our progress toward answering our research questions. Finally, we will consider future work.

5.1 Measures of Success

Based upon Kott and Linkov's work, we assert that for the measurement methodology to be successful it must be repeatable, consistent, monotonic with respect to defense, and monotonic with respect to attacks.

1. **Repeatable.** We assert that this methodology is repeatable because we fully expect that the same article tested with the same mission scenario and the same threat environment will yield similar results. We acknowledge that our tabletop exercise has not fully demonstrated this.
2. **Consistent.** We assert that this methodology is consistent with respect to missions. The same article test with similar missions against the same threat environment will yield similar results. The contrast between using Route 1 and Route 2 demonstrates a caveat in that missions appearing similar may not be similar because they stress the article in very different ways.
3. **Monotonicity with respect to defense.** Our tabletop exercise showed that protected vehicles performed as well or better than the unprotected vehicles when tested using the same scenario and the same threat environment.
4. **Monotonicity with respect to attacks.** Our tabletop exercise did not attempt to rank attacks; therefore, it is not possible for it to demonstrate that the score decreases as the threat increases.

5.2 Lessons Learned

1. As currently defined, cyber resilience is a subset of mission resilience. The key difference is not in the KPPs that are measured, but in the effects that are considered. The methodology would work as well to measure resilience against kinetic effects. This project will confine itself to effects that could be caused by a cyber attack on the system.
2. Resilience may come in many forms. Mechanisms designed to make a system resilient against mechanical failure may also make the system resilient against cyber effects if those effects either cause or mimic a mechanical failure. We saw this when the robustness of a heavy vehicle cooling system made the vehicle immune to a cooling system attack under certain circumstances.

3. Since the KPPs under measurement are specific to the mission and not to the cyber systems, many non-cyber aspects will affect the score. For example, when an unprotected vehicle takes the first route under a cooling attack, the mission proceeds exactly as planned because the route does not stress the engine to the point that the cooling fan is necessary.
4. It is important that the critical capabilities of the article under test be considered. For example, a World War II era CCKW 6X6 deuce-and-a-half tactical cargo truck could be completely impervious to cyber attack; however, its capabilities versus modern systems need to be considered. For example, the deuce-and-a-half may lack the carrying capacity, fuel economy, or off road capability to acceptably complete the mission.
5. The methodology is limited to KPPs that can be measured and the ability to sufficiently model or replicate relevant system, mission, and threat parameters. Each experiment is limited to effects that can be manifested in the article under test. For example, consider an experiment using a vehicle simulator. If the vehicle simulator does not simulate engine temperature, then attacks against the cooling system cannot be measured.
6. In this example, we used distance over time or speed as our KPP; however, the only requirement for a KPP is that it be quantitatively measurable. For example, if stealth is a requirement, and observability quantitatively measured, then any effect which impacts observability could be considered.
7. We may need to add a research question about ranking threats, cyber attacks, or cyber-effects. Certainly the cooling system attack could have been made more sophisticated by hiding itself from the operator. This improved attack could severely damage the vehicle before the operator was aware of the problem. However, on Route 1, the attack still would have failed to prevent mission success. How does one rank these attacks? The speed control attacks reliably prevent an unprotected vehicle from completing the mission; however, repair would be straightforward even if diagnosis was difficult.²⁴ The cooling system attack has the potential to inflict costly damage to a vehicle, but is not effective in every mission scenario.

5.3 Research Questions

1. **How is cyber resilience defined?** In this exercise, we used the following working definition: Cyber resilience, in this context, is the ability of systems to resist, absorb, and recover/adapt to a cyber-compromise after the compromise occurs, during execution of a mission. Our table exercise demonstrated the capacity to measure cyber resilience according to this definition; however, we noticed in our literature review that Cottam et al. would have rejected this definition because it contains the means of achieving cyber resilience.¹⁴
2. **How will the quantitative cyber resilience measurement be used?** By comparing unprotected versus protected vehicles in our tabletop exercise we were able to demonstrate that our measurement methodology is able to show the relative effectiveness of a countermeasure in some circumstances. There is a caveat, because comparing the effectiveness of the cooling system protection only on Route 1 would not have shown an improvement in cyber resilience based on the countermeasure because the vehicle itself was resilient against that attack in that environment.
3. **What methodology to use to measure cyber resilience?** This tabletop exercise used the area under the performance curve to measure cyber resilience. This measurement does meet many of our measures of success as seen in Section 5.
4. **What exactly is measured to compute the cyber resilience?** For this tabletop exercise, we measured speed and cumulative distance, which we acknowledge are basically the same thing. We still consider this an open question and will include additional KPPs in future experiments based upon the mission requirements and capabilities of the article under test.

5.4 Future Work

The definition of cyber resilience deserves more consideration. We will need to discover/select some criteria for what makes a good definition. Podsakoff et al. provide a list of 10 questions that may be used to evaluate a definition.²⁵ Cronin et al. provide a step-by-step approach for conducting a literature review.²⁶ We will combine these to create a good scientific definition of cyber resilience.

As we stated earlier and showed in Fig. 3 we plan to approach this project iteratively, conducting experiments of greater fidelity as we improve the answers to our research questions. Below is a list of currently planned future experiments.

1. **Unity.** In September, an experiment will be conducted using the vehicle simulator in the Unity Real-Time Development Platform.²⁷ This experiment will feature the first iteration of the AutoCRAT and exercise our ability to import data into and export data from the Unity platform. This is important since we intend to use the Unity platform to demonstrate this methodology. We do not expect the vehicle simulator to be of high fidelity; however, we do expect it to be sufficient for this iteration.
2. **PASTA.** We are in the process of procuring the Toyota Portable Automotive Security Testbed with Adaptability (PASTA) from Chip One Stop.²⁸ PASTA will be able to provide a higher fidelity vehicle simulator, which will allow the AutoCRAT to interface directly with the CAN bus to collect KPPs. It will also interface with the Unity platform for demonstration purposes. We expect to conduct an experiment in the early January time frame using PASTA. This experiment will exercise the ability of AutoCRAT to interface with PASTA and the ability of PASTA to interface with the Unity platform.
3. **Others.** Follow on experiments with this environment will expand the mission scenario, countermeasures, and threat environment. Figure 14 illustrates this iterative approach with increasing fidelity in the vehicle simulators to the use of actual vehicles, the expansion of mission scenarios and the threat model, as well as the refinement of the measurement methodology and the AutoCRAT. We have established a Collaborative Agreement (CA) with Penn State University Applied Research Laboratory (PSU/ARL). This CA will allow us to leverage PSU/ARL's experience with heavy vehicles and access to their vehicles for experimentation.

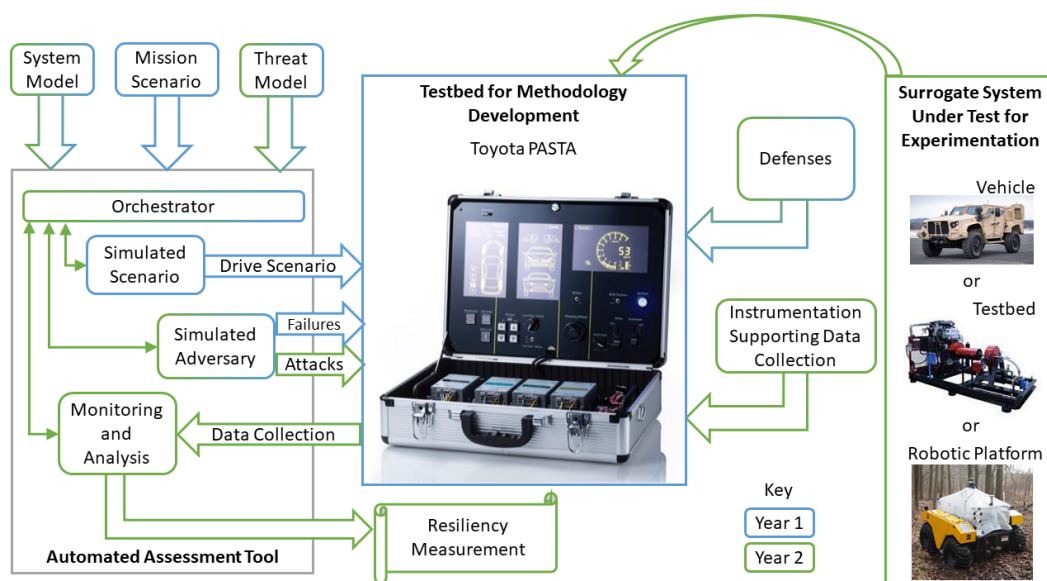


Fig. 14 Iterative experimental plan for the QMoCR project

6. References

1. Hoppe T, Dittman J. Sniffing/replay attacks on CAN buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy. In: Proceedings of the 2nd workshop on embedded systems security (WESS); p. 1–6.
2. Bozdal M, Samie M, Aslam S, Jennions I. Evaluation of CAN bus security challenges. *Sensors*. 2020;20(8):2364.
3. Bozdal M, Randa M, Samie M, Jennions I. Hardware trojan enabled denial of service attack on CAN bus. *Procedia Manufacturing*. 2018;16:47–52.
4. IEEE standard for information technology–local and metropolitan area networks–specific requirements–part 15.1a: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPAN). IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002). 2005:1–700.
5. IEEE standard for information technology—telecommunications and information exchange between systems–local and metropolitan area networks—specific requirements–part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications - redline. IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016) - Redline. 2021:1–7524.
6. Kott A, Linkov I. To improve cyber resilience, measure it. arXiv preprint arXiv:2102.09455. 2021.
7. Kick J. Cyber exercise playbook. MITRE CORP; 2014. Report No.: MP140714.
8. Brtis JS, McEvilley MA. Systems engineering for resilience. MITRE Corp; 2019 July. Report No.: MP 190495.
9. Brits J, Jackson S, Cureton K. System Resilience. Systems Engineering Body of Knowledge (SEBok); 2021.
10. Joint Task Force. Security and privacy controls for information systems and organizations. National Institute of Standards and Technology; 2017. Special Publication No.: 800-53 Rev. 5.

11. Committee on National Security Systems (CNNS) glossary. CNNS; 2015 Apr. CNSSI No.: 4009.
12. INCOSE. Systems engineering handbook: A guide for system life cycle processes and activities. Version 4.0 ed. John Wiley and Sons, Inc; 2015.
13. Björck F, Henkel M, Stirna J, Zdravkovic J. Cyber resilience—fundamentals for a definition. In: New contributions in information systems and technologies; Springer; 2015; p. 311–316.
14. Cottam BJ, Specking EA, Small CA, Pohl E, Parnell GS, Buchanan RK. Defining resilience for engineered systems. Canadian Center of Science and Education; 2019.
15. Brtis J. How to think about resilience in a DoD context. MITR COPR; 2016 Aug. Report No.: MTR160138.
16. Béné C. Towards a quantifiable measure of resilience. IDS Working Papers. 2013;2013(434):1–27.
17. Bodeau DJ, Graubart RD, McQuaid RM, Woodill J. Cyber resiliency metrics catalog. MITRE CORP; 2018 Sep. Report No.: MTR180450.
18. Bodeau DJ, Graubart RD, McQuaid RM, Woodill J. Cyber resiliency metrics, measures of effectiveness, and scoring: Enabling systems engineers and program managers to select the most useful assessment methods. MITRE CORP; 2018 Sep. Report No.: MTR180314.
19. Bodeau DJ, Graubart RD, McQuaid RM, Woodill J. Cyber resiliency metrics and scoring in practice use case methodology and examples. MITRE CORP; 2018 Sep. Report No.: MTR180449.
20. Whelihan D, Vai M, Evanich N, Kwak KJ, Li J, Britton M, Frantz B, Hadcock D, Lynch M, Schafer D, DeMatteis J, Russo D. Designing agility and resilience into embedded systems. In: MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM); p. 249–254.
21. Whitman H, Vai M, Whelihan D, Khazan R, Schafer D, Russo D. Harden: A high assurance design environment. Air Force Research Laboratory; 2019. Technical Report No.: AD1075479.

22. Ligo A, Kott A, Linkov I. How to measure cyber resilience of an autonomous agent: Approaches and challenges. arXiv preprint arXiv:2102.00528. 2021.
23. Ferris TLJ. A resilience measure to guide system design and management. IEEE Systems Journal. 2019;13(4):3708-3715.
24. Musman S, Agbolosu-Amison S. A measurable definition of resiliency using “mission risk” as a metric. MITRE CORP MCLEAN VA; 2014. MITRE Technical Report No.: MTR140047.
25. Podsakoff PM, MacKenzie SB, Podsakoff NP. Recommendations for creating better concept definitions in the organizational, behavioral, and social sciences. Organizational Research Methods. 2016;19(2):159–203.
26. Cronin P, Ryan F, Coughlan M. Undertaking a literature review: a step-by-step approach. British journal of nursing. 2008;17(1):38–43.
27. The leading platform for creating interactive, real-time content. [date unknown; accessed 2021Aug]. <http://unity.com>.
28. Portable automotive security testbed with adaptability PASTA. [date unknown; accessed 2021Aug]. https://www.chip1stop.com/sp/products/toyota-pasta_en.
29. Cureton KL, Brits JS. Resilient systems working group. INCOSE – International Council on Systems Engineering; 2015 [accessed 2022 Jan 24]. <https://www.incose.org/incose-member-resources/working-groups/analytic/resilient-systems>.
30. Glossary. ISACA; 2022 Jan [accessed 2022 Jan 24]. <https://www.isaca.org/resources/glossary>.
31. National preparedness. Office of the President (US); 2011 Mar 30. Presidential Policy Directive No.: PPD-8.
32. Critical infrastructure security and resilience. Office of the President (US); 2013 Feb 12. Presidential Policy Directive No.: PPD-21.
33. Azebbi CE. Safe, secure and prosperous: a cyber resilience strategy for Scotland. Scottish Government; 2015 Nov 18 [accessed 2022 Jan 24]. <https://www.gov.scot/publications/safe-secure-prosperous-cyber-resilience-strategy-scotland/>.

34. Committee on Payments and Market Infrastructures. Cyber resilience in financial market infrastructures. Bank for International Settlements; 2014.
35. Cheryl Markin RS. Cyber resilience playbook for public-private collaboration. World Economic Forum; 2018.
36. Faulkner A, Franz G, Dalling D, Layman J. Achieving federal cyber resilience. accenture; 2020 Aug 20 [accessed 2022 Jan 24]. <https://www.accenture.com/us-en/insights/us-federal-government/achieving-federal-cyber-resilience>.
37. Ross R, Pillitteri V, Graubart R, Bodeau D, McQuaid R. Developing cyber resilient systems: A systems security engineering approach. National Institute of Standards and Technology; 2019. NIST Special Publication No.: 800-160.
38. Linkov I, Kott A. Fundamental concepts of cyber resilience: Introduction and overview. In: Cyber resilience of systems and networks; Springer; 2019; p. 1–25.

Appendix A. Definitions of Cyber Resilience

Table A-1: **Definitions of Cyber Resilience**

Term	Context	Definition
Information System Resilience	Information Systems	The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs. ¹⁰
Operational Resilience	Organizations	The ability of a system to resist, absorb, and recover from or adapt to an adverse occurrence during operations that may cause harm, destruction, or loss of ability to perform mission-related functions. ¹¹
Resilience	Engineered systems	Resilience is the ability to prepare and plan for, absorb or mitigate, recover from, or more successfully adapt to actual or potential adverse events. ¹²
Resilience	Engineered systems	Resilience is the ability to provide required capability in the face of adversity. The scope of resilience includes the ability to avoid, withstand, and recover from adversity (the objective is required capability, not system stasis). ²⁹
Resilience	Systems or networks	The ability of a system or network to resist failure or to recover quickly from any disruption, usually with minimal recognizable effect. ³⁰
Resilience	Communities, Infrastructure sectors, the Nation	The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies. ³¹
Resilience	Communities, Infrastructure sectors, the Nation	The ability to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. ³²
Cyber Resilience	Organizations, individuals	Cyber resilience is being able to prepare for, withstand, rapidly recover, and learn from deliberate attacks or accidental events in the online world. Cyber security is a key element of being resilient, but cyber resilient people and organisations recognize that being safe online goes far beyond just technical measures. ³³
Cyber Resilience	Financial Market Infrastructure	The ability to anticipate, absorb, adapt to and/or rapidly recover from disruption caused by a cyber attack. ³⁴

Continued on next page

Table A-1 – *Continue from previous page*

Term	Context	Definition
Cyber Resilience	Systems, Organizations	the capability to detect threats, prevent their infiltration or at least confine their expansion, manage their effects and deny their recurrence; the notion of adaptability is at the core of resilience, as is being able to continue ordinary operations. ³⁵
Cyber Resiliency	Organizations	Cyber resilience brings together the capabilities of cyber-security, business continuity, and enterprise resilience. It applies holistic security strategies to help federal agencies and other organizations respond quickly to threats so they can minimize the damage and continue to operate under attack. ³⁶
Cyber Resiliency	Systems	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that include cyber resources. ³⁷
Resilience	General	Any capacity and skills, and action, strategy, investment and anticipation, which helps individual, households, and communities to anticipate, absorb, accommodate, or recover from the impacts of a particular adverse event (shock, stress, or (un)expected changes.) ¹⁶
Cyber-resilience	Systems	Cyber resilience is the ability to continuously deliver the intended outcome despite adverse cyber events. ¹³
Cyber-resiliency	Systems	Cyber resiliency – the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources. ^{17–19}
Cyber-resilience	Systems	Cyber-resilience is the ability of a system to recover or regenerate its functionality after a cyber-threat materializes and produces a degradation to the system’s performance. ³⁸

Appendix B. Results Tables

The appendix contains the raw results for the various scenarios in the table top exercise. For the sake of space, **Planned Speed** and **Planned Distance** have been abbreviated **P Speed** and **P Dist**, **Actual Speed** and **Actual Distance** have been abbreviated **A Speed** and **A Dist**, and **Normalized Speed** and **Normalized Distance** have been abbreviated **N Speed** and **N Dist**.

Table B-1: **Time, Speed, and Cumulative distance for Routes 1 and 2**

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
10	60	10	60	10.00	1.00	1.00
20	60	20	60	20.00	1.00	1.00
30	60	30	60	30.00	1.00	1.00
40	60	40	45	37.50	0.75	0.94
50	60	50	40	44.20	0.67	0.88
60	60	60	40	50.80	0.67	0.85
70	60	70	40	57.50	0.67	0.82
80	60	80	40	64.20	0.67	0.80
90	60	90	40	70.80	0.67	0.79
100	60	100	40	77.50	0.67	0.78
110	60	110	40	84.20	0.67	0.77
120	60	120	40	90.80	0.67	0.76
130	60	130	40	97.50	0.67	0.75
140	60	140	40	104.20	0.67	0.74
150	60	150	40	110.80	0.67	0.74
160	60	160	40	117.50	0.67	0.73
170	60	170	40	124.20	0.67	0.73
180	60	180	40	130.80	0.67	0.73
190	60	190	40	137.50	0.67	0.72
200	60	200	40	144.20	0.67	0.72
210	60	210	40	150.80	0.67	0.72
220	60	220	40	157.50	0.67	0.72
230	60	230	40	164.20	0.67	0.71
240	60	240	40	170.80	0.67	0.71
250	60	250	40	177.50	0.67	0.71

Continued on next page

Table B-1 Continued from previous page

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
260	60	250	40	184.20	0.67	0.74
270	60	250	40	190.80	0.67	0.76
280	60	250	40	197.50	0.67	0.79
290	60	250	40	204.20	0.67	0.82
300	60	250	40	210.80	0.67	0.84
310	60	250	40	217.50	0.67	0.87
320	60	250	40	224.20	0.67	0.90
330	60	250	40	230.80	0.67	0.92
340	60	250	40	237.50	0.67	0.95
350	60	250	60	247.50	1.00	0.99
360	60	250	60	250.00	1.00	1.00
Concluded						

Table B-2: Time, Speed, and Cumulative distance for Route 1, speed attack, and an unprotected vehicle

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
10	60	10	60	10.00	1.00	1.00
20	60	20	60	20.00	1.00	1.00
30	60	30	60	30.00	1.00	1.00
40	60	40	12	32.00	0.20	0.80
50	60	50	12	34.00	0.20	0.68
60	60	60	12	36.00	0.20	0.60
70	60	70	12	38.00	0.20	0.54
80	60	80	12	40.00	0.20	0.50
90	60	90	12	42.00	0.20	0.47
100	60	100	12	44.00	0.20	0.44
110	60	110	12	46.00	0.20	0.42
120	60	120	12	48.00	0.20	0.40
130	60	130	12	50.00	0.20	0.38
140	60	140	12	52.00	0.20	0.37
150	60	150	12	54.00	0.20	0.36
160	60	160	12	56.00	0.20	0.35
170	60	170	12	58.00	0.20	0.34
180	60	180	12	60.00	0.20	0.33
190	60	190	12	62.00	0.20	0.33
200	60	200	12	64.00	0.20	0.32
210	60	210	12	66.00	0.20	0.31
220	60	220	12	68.00	0.20	0.31
230	60	230	12	70.00	0.20	0.30
240	60	240	12	72.00	0.20	0.30
250	60	250	12	74.00	0.20	0.30
260	60	260	12	76.00	0.20	0.29
270	60	270	12	78.00	0.20	0.29
280	60	280	12	80.00	0.20	0.29
290	60	290	12	82.00	0.20	0.28
300	60	300	12	84.00	0.20	0.28

Continued on next page

Table B-2 Continued from previous page

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
310	60	310	12	86.00	0.20	0.28
320	60	320	12	88.00	0.20	0.28
330	60	330	12	90.00	0.20	0.27
340	60	340	12	92.00	0.20	0.27
350	60	350	12	94.00	0.20	0.27
360	60	360	12	96.00	0.20	0.27
370	60	370	12	98.00	0.20	0.26
380	60	380	12	100.00	0.20	0.26
390	60	390	12	102.00	0.20	0.26
400	60	400	12	104.00	0.20	0.26
410	60	410	12	106.00	0.20	0.26
420	60	420	12	108.00	0.20	0.26
430	60	430	12	110.00	0.20	0.26
440	60	440	12	112.00	0.20	0.25
450	60	450	12	114.00	0.20	0.25
460	60	460	12	116.00	0.20	0.25
470	60	470	12	118.00	0.20	0.25
480	60	480	12	120.00	0.20	0.25
490	60	490	12	122.00	0.20	0.25
500	60	500	12	124.00	0.20	0.25
Concluded						

Table B-3: Time, Speed, and Cumulative distance for Route 1, speed attack, and a protected vehicle

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
10	60	10	60	10.00	1.00	1.00
20	60	20	60	20.00	1.00	1.00
30	60	30	60	30.00	1.00	1.00
40	60	40	60	40.00	1.00	1.00
50	60	50	60	50.00	1.00	1.00
60	60	60	60	60.00	1.00	1.00
70	60	70	60	70.00	1.00	1.00
80	60	80	60	80.00	1.00	1.00
90	60	90	60	90.00	1.00	1.00
100	60	100	60	100.00	1.00	1.00
110	60	110	60	110.00	1.00	1.00
120	60	120	60	120.00	1.00	1.00
130	60	130	60	130.00	1.00	1.00
140	60	140	60	140.00	1.00	1.00
150	60	150	60	150.00	1.00	1.00
160	60	160	60	160.00	1.00	1.00
170	60	170	60	170.00	1.00	1.00
180	60	180	60	180.00	1.00	1.00
190	60	190	60	190.00	1.00	1.00
200	60	200	60	200.00	1.00	1.00
210	60	210	60	210.00	1.00	1.00
220	60	220	60	220.00	1.00	1.00
230	60	230	60	230.00	1.00	1.00
240	60	240	60	240.00	1.00	1.00
250	60	250	60	250.00	1.00	1.00
Concluded						

Table B-4: Time, Speed, and Cumulative distance for Route 2, speed attack, and an unprotected vehicle

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
10	60	10	60	10.00	1.00	1.00
20	60	20	60	20.00	1.00	1.00
30	60	30	60	30.00	1.00	1.00
40	60	40	12	32.00	0.20	0.80
50	60	50	12	32.80	0.20	0.66
60	60	60	0	32.80	0.00	0.55
70	60	70	0	32.80	0.00	0.47
80	60	80	0	32.80	0.00	0.41
90	60	90	0	32.80	0.00	0.36
100	60	100	0	32.80	0.00	0.33
110	60	110	0	32.80	0.00	0.30
120	60	120	0	32.80	0.00	0.27
130	60	130	0	32.80	0.00	0.25
140	60	140	0	32.80	0.00	0.23
150	60	150	0	32.80	0.00	0.22
160	60	160	0	32.80	0.00	0.20
170	60	170	0	32.80	0.00	0.19
180	60	180	0	32.80	0.00	0.18
190	60	190	0	32.80	0.00	0.17
200	60	200	0	32.80	0.00	0.16
210	60	210	0	32.80	0.00	0.16
220	60	220	0	32.80	0.00	0.15
230	60	230	0	32.80	0.00	0.14
240	60	240	0	32.80	0.00	0.14
250	60	250	0	32.80	0.00	0.13
260	60	250	0	32.80	0.00	0.13
270	60	250	0	32.80	0.00	0.13
280	60	250	0	32.80	0.00	0.13
290	60	250	0	32.80	0.00	0.13
300	60	250	0	32.80	0.00	0.13

Continued on next page

Table B-4 Continued from previous page

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
310	60	250	0	32.80	0.00	0.13
320	60	250	0	32.80	0.00	0.13
330	60	250	0	32.80	0.00	0.13
340	60	250	0	32.80	0.00	0.13
350	60	250	0	32.80	0.00	0.13
360	60	250	0	32.80	0.00	0.13
370	60	250	0	32.80	0.00	0.13
380	60	250	0	32.80	0.00	0.13
390	60	250	0	32.80	0.00	0.13
400	60	250	0	32.80	0.00	0.13
410	60	250	0	32.80	0.00	0.13
420	60	250	0	32.80	0.00	0.13
430	60	250	0	32.80	0.00	0.13
440	60	250	0	32.80	0.00	0.13
450	60	250	0	32.80	0.00	0.13
460	60	250	0	32.80	0.00	0.13
470	60	250	0	32.80	0.00	0.13
480	60	250	0	32.80	0.00	0.13
490	60	250	0	32.80	0.00	0.13
Concluded						

Table B-5: Time, Speed, and Cumulative distance for Route 2, speed attack, and a protected vehicle

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
10	60	10	60	10.00	1.00	1.00
20	60	20	60	20.00	1.00	1.00
30	60	30	60	30.00	1.00	1.00
40	60	40	45	37.50	0.75	0.94
50	60	50	35	43.30	0.58	0.87
60	60	60	35	49.20	0.58	0.82
70	60	70	35	55.00	0.58	0.79
80	60	80	35	60.80	0.58	0.76
90	60	90	35	66.70	0.58	0.74
100	60	100	35	72.50	0.58	0.72
110	60	110	35	78.30	0.58	0.71
120	60	120	35	84.20	0.58	0.70
130	60	130	35	90.00	0.58	0.69
140	60	140	35	95.80	0.58	0.68
150	60	150	35	101.70	0.58	0.68
160	60	160	35	107.50	0.58	0.67
170	60	170	35	113.30	0.58	0.67
180	60	180	35	119.20	0.58	0.66
190	60	190	40	125.80	0.67	0.66
200	60	200	40	132.50	0.67	0.66
210	60	210	40	139.20	0.67	0.66
220	60	220	40	145.80	0.67	0.66
230	60	230	40	152.50	0.67	0.66
240	60	240	40	159.20	0.67	0.66
250	60	250	40	165.80	0.67	0.66
260	60	250	40	172.50	0.67	0.69
270	60	250	40	179.20	0.67	0.72
280	60	250	40	185.80	0.67	0.74
290	60	250	40	192.50	0.67	0.77
300	60	250	40	199.20	0.67	0.80

Continued on next page

Table B-5 Continued from previous page

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
310	60	250	40	205.80	0.67	0.82
320	60	250	40	212.50	0.67	0.85
330	60	250	40	219.20	0.67	0.88
340	60	250	40	225.80	0.67	0.90
350	60	250	60	235.80	1.00	0.94
360	60	250	60	245.80	1.00	0.98
370	60	250	60	250.00	1.00	1.00
Concluded						

Table B-6: Time, Speed, and Cumulative distance for Route 1, cooling attack, and an unprotected vehicle

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
10	60	10	60	10.00	1.00	1.00
20	60	20	60	20.00	1.00	1.00
30	60	30	60	30.00	1.00	1.00
40	60	40	60	40.00	1.00	1.00
50	60	50	60	50.00	1.00	1.00
60	60	60	60	60.00	1.00	1.00
70	60	70	60	70.00	1.00	1.00
80	60	80	60	80.00	1.00	1.00
90	60	90	60	90.00	1.00	1.00
100	60	100	60	100.00	1.00	1.00
110	60	110	60	110.00	1.00	1.00
120	60	120	60	120.00	1.00	1.00
130	60	130	60	130.00	1.00	1.00
140	60	140	60	140.00	1.00	1.00
150	60	150	60	150.00	1.00	1.00
160	60	160	60	160.00	1.00	1.00
170	60	170	60	170.00	1.00	1.00
180	60	180	60	180.00	1.00	1.00
190	60	190	60	190.00	1.00	1.00
200	60	200	60	200.00	1.00	1.00
210	60	210	60	210.00	1.00	1.00
220	60	220	60	220.00	1.00	1.00
230	60	230	60	230.00	1.00	1.00
240	60	240	60	240.00	1.00	1.00
250	60	250	60	250.00	1.00	1.00
Concluded						

Table B-7: Time, Speed, and Cumulative distance for Route 1, cooling attack, and a protected vehicle

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
10	60	10	60	10.00	1.00	1.00
20	60	20	60	20.00	1.00	1.00
30	60	30	60	30.00	1.00	1.00
40	60	40	60	40.00	1.00	1.00
50	60	50	60	50.00	1.00	1.00
60	60	60	60	60.00	1.00	1.00
70	60	70	60	70.00	1.00	1.00
80	60	80	60	80.00	1.00	1.00
90	60	90	60	90.00	1.00	1.00
100	60	100	60	100.00	1.00	1.00
110	60	110	60	110.00	1.00	1.00
120	60	120	60	120.00	1.00	1.00
130	60	130	60	130.00	1.00	1.00
140	60	140	60	140.00	1.00	1.00
150	60	150	60	150.00	1.00	1.00
160	60	160	60	160.00	1.00	1.00
170	60	170	60	170.00	1.00	1.00
180	60	180	60	180.00	1.00	1.00
190	60	190	60	190.00	1.00	1.00
200	60	200	60	200.00	1.00	1.00
210	60	210	60	210.00	1.00	1.00
220	60	220	60	220.00	1.00	1.00
230	60	230	60	230.00	1.00	1.00
240	60	240	60	240.00	1.00	1.00
250	60	250	60	250.00	1.00	1.00
Concluded						

Table B-8: **Time, Speed, and Cumulative distance for Route 2, cooling attack, and an unprotected vehicle**

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
10	60	10	60	10.00	1.00	1.00
20	60	20	60	20.00	1.00	1.00
30	60	30	60	30.00	1.00	1.00
40	60	40	45	37.50	0.75	0.94
50	60	50	40	44.20	0.67	0.88
60	60	60	40	50.80	0.67	0.85
70	60	70	40	57.50	0.67	0.82
80	60	80	40	64.20	0.67	0.80
90	60	90	40	70.80	0.67	0.79
100	60	100	40	77.50	0.67	0.78
110	60	110	40	84.20	0.67	0.77
120	60	120	0	84.20	0.00	0.70
130	60	130	0	84.20	0.00	0.65
140	60	140	0	84.20	0.00	0.60
150	60	150	0	84.20	0.00	0.56
160	60	160	0	84.20	0.00	0.53
170	60	170	0	84.20	0.00	0.50
180	60	180	0	84.20	0.00	0.47
190	60	190	0	84.20	0.00	0.44
200	60	200	0	84.20	0.00	0.42
210	60	210	0	84.20	0.00	0.40
220	60	220	0	84.20	0.00	0.38
230	60	230	40	90.80	0.67	0.39
240	60	240	40	97.50	0.67	0.41
250	60	250	40	104.20	0.67	0.42
260	60	250	40	110.80	0.67	0.44
270	60	250	40	117.50	0.67	0.47
280	60	250	40	124.20	0.67	0.50
290	60	250	40	130.80	0.67	0.52
300	60	250	40	137.50	0.67	0.55

Continued on next page

Table B-8 Continued from previous page

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
310	60	250	40	144.20	0.67	0.58
320	60	250	40	150.80	0.67	0.60
330	60	250	40	157.50	0.67	0.63
340	60	250	40	164.20	0.67	0.66
350	60	250	40	170.80	0.67	0.68
360	60	250	40	177.50	0.67	0.71
370	60	250	40	184.20	0.67	0.74
380	60	250	40	190.80	0.67	0.76
390	60	250	40	197.50	0.67	0.79
400	60	250	40	204.20	0.67	0.82
410	60	250	40	210.80	0.67	0.84
420	60	250	40	217.50	0.67	0.87
430	60	250	40	224.20	0.67	0.90
440	60	250	40	230.80	0.67	0.92
450	60	250	40	237.50	0.67	0.95
460	60	250	60	247.50	1.00	0.99
470	60	250	60	257.50	1.00	1.03
Concluded						

Table B-9: Time, Speed, and Cumulative distance for Route 2, cooling attack, and a protected vehicle

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
10	60	10	60	10.00	1.00	1.00
20	60	20	60	20.00	1.00	1.00
30	60	30	60	30.00	1.00	1.00
40	60	40	45	37.50	0.75	0.94
50	60	50	40	44.20	0.67	0.88
60	60	60	40	50.80	0.67	0.85
70	60	70	40	57.50	0.67	0.82
80	60	80	40	64.20	0.67	0.80
90	60	90	40	70.80	0.67	0.79
100	60	100	40	77.50	0.67	0.78
110	60	110	40	84.20	0.67	0.77
120	60	120	40	90.80	0.67	0.76
130	60	130	40	97.50	0.67	0.75
140	60	140	40	104.20	0.67	0.74
150	60	150	40	110.80	0.67	0.74
160	60	160	40	117.50	0.67	0.73
170	60	170	40	124.20	0.67	0.73
180	60	180	40	130.80	0.67	0.73
190	60	190	40	137.50	0.67	0.72
200	60	200	40	144.20	0.67	0.72
210	60	210	40	150.80	0.67	0.72
220	60	220	40	157.50	0.67	0.72
230	60	230	40	164.20	0.67	0.71
240	60	240	40	170.80	0.67	0.71
250	60	250	40	177.50	0.67	0.71
260	60	250	40	184.20	0.67	0.74
270	60	250	40	190.80	0.67	0.76
280	60	250	40	197.50	0.67	0.79
290	60	250	40	204.20	0.67	0.82
300	60	250	40	210.80	0.67	0.84

Continued on next page

Table B-9 Continued from previous page

Time	P Speed	P Dist	A Speed	A Dist	N Speed	N Dist
310	60	250	40	217.50	0.67	0.87
320	60	250	40	224.20	0.67	0.90
330	60	250	40	230.80	0.67	0.92
340	60	250	40	237.50	0.67	0.95
350	60	250	60	247.50	1.00	0.99
360	60	250	60	250.00	1.00	1.00
Concluded						

List of Symbols, Abbreviations, and Acronyms

AutoCRAT	automated cyber resilience assessment tool
CA	Collaborative Agreement
CAN	controller area network
DIR	detect, isolate, and recover
DoD	Department of Defense
KPP	key performance parameter
LDI	livelihood diversification index
MEF	mission essential function
PASTA	Toyota Portable Automotive Security Testbed with Adaptability
POI	point of interest
PSU/ARL	Penn State University Applied Research Laboratory
QMoCR	Quantitative Measurement of Cyber Resilience
RI	resilience index

1 DEFENSE TECHNICAL
(PDF) INFORMATION CTR
DTIC OCA

1 DEVCOM ARL
(PDF) FCDD RLD DCI
TECH LIB

1 DEVCOM ARL
(PDF) FCDD RLC ND
SC SMITH