Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 28 (2014) 257 – 264
Procedia Computer Science

Conference on Systems Engineering Research (CSER 2014)

Eds.: Azad M. Madni, University of Southern California; Barry Boehm, University of Southern California; Michael Sievers, Jet Propulsion Laboratory; Marilee Wheaton, The Aerospace Corporation
Redondo Beach, CA, March 21-22, 2014

Resilience-based System Importance Measures for System-of-Systems

Payuna Uday[a]* and Karen B. Marais[a]

[a]*Purdue University, 701 W. Stadium Avenue, West Lafayette, IN-47906*

Abstract

Systems-of-systems (SoS) like the air transportation system and missile defense are gaining increasing attention in both the academic and practitioner communities. This research investigates one crucial aspect of SoSs: their ability to recover from disruptions, or their *resilience*. We develop a family of system importance measures (SIMs) that rank the constituent systems based on their impact on the overall SoS performance. The SIMs address some of the major weaknesses that have prevented researchers from identifying a single resilience metric. While trade-space analyses are standard practice in systems engineering, conducting trades on SoS resilience is difficult because, to date, no reliable and consistent metrics have been developed for SoS resilience. Some metrics have been proposed, but these measures assume homogenous networks, thus ignoring one of the key features of SoSs: the combination of heterogeneous systems (e.g., airports and aircraft) to achieve a common goal (e.g., transport). Instead of focusing on an overall metric, the set of SIMs provides designers with specific information on where an SoS is lacking resilience (or has excess resilience) and hence on where improvements are needed (or where downgrades are possible).

Keywords: Resilience, system-of-systems, importance measures

* Corresponding author. Tel.: +1-765-464-4966; fax: +1-765-494-0307.
E-mail address: puday@purdue.edu

doi:10.1016/j.procs.2014.03.033

1. Introduction

All systems are subject to change over their lifetimes. Resilience is the ability of a system to survive and recover from these changes. Implementing resilience is a challenging task because it is highly context-dependent. Systems may be resilient to certain types of disturbances but vulnerable to others. Long-lasting systems, such as infrastructure networks (e.g., energy, transportation, or communications), may initially be resilient to certain disruptions, but as time passes after systems are fielded, changes in the operating environment may make the networks less resilient to both old and new types of threats. Once a failure occurs, resilience is the inherent ability of a system to *survive* and *recover* from this disturbance. And so, resilience is represented as a combination of survivability and recoverability, as shown in Fig. 1. This notional representation is widely used in the literature[1,2,3] to depict the fundamental ideas behind resilience. While it appears easy to represent resilience conceptually, it is much harder to define, assess, and design resilient systems.

A system-of-systems (SoS) is a large-scale integrated network of systems that are heterogeneous and independently operable on their own, but collaborate for a common goal. For example, the national air space (NAS) and the national highway systems are SoSs. While trade-space analyses are standard practice in systems engineering, conducting trades on SoS resilience is difficult because, to date, no reliable and consistent metrics have been developed for SoS resilience. Several metrics have been proposed, but these measures assume homogenous networks, ignoring one of the key features of SoS: the combination of heterogeneous systems (e.g., airports and aircraft) to achieve a common goal (e.g., transport). Rather than attempting to create a single metric that glosses over the complexities of an SoS, we present here a family of System Importance Measures (SIMs) that capture different aspects of SoS resilience. Analogous to component importance measures in reliability theory, the SIMs provide a way to rank or prioritize the constituent systems of an SoS based on different threats. Specifically, these SIMs provide analysts and designers with informative guidance on where an SoS is lacking resilience (or has excess resilience) and hence on where improvements are needed (or where downgrades are possible).

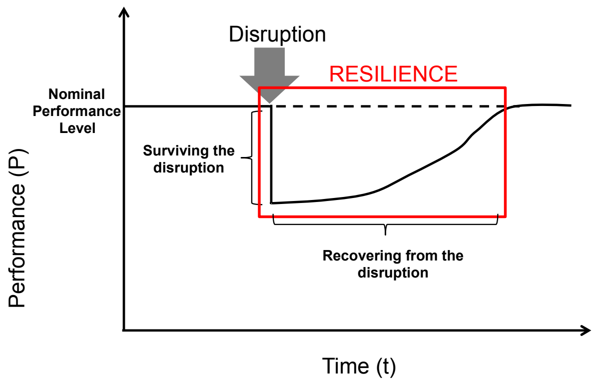

Fig. 1. Notional SoS resilience following a disruption

The remainder of this paper is organized as follows: Section 2 describes two System Importance Measures (SIMs) and presents the mathematical formulation behind these metrics. Section 3 demonstrates the use of these two SIMs with illustrative examples. Section 4 presents two additional System Importance Metrics. And, finally Section 5 concludes the paper.

2. System Importance Measures

Measuring resilience is a critical first step in any framework that aims at addressing or improving resilience. However, establishing a single, all-encompassing resilience metric will be challenging, if not impossible. Since a two-dimensional representation of resilience (see Fig. 1) is necessary to capture the main aspects of this attribute, a single metric to measure resilience could be insufficient. Given the two dimensions (time and performance), there will always exist cases where a single-dimensional metric will yield the same result for two different curves. For example, such a metric would not distinguish between a curve with a quick recovery to low performance gain and one with a slow recovery to a high performance gain. Further, while a single overall metric may enable overall comparisons between different SoS architectures, such a metric provides little, if any, information regarding specific areas within each SoS that need attention. To address this gap, our research develops a family of System Importance Measures (SIMs) that captures different aspects (time and performance) of and contributors to SoS resilience. Analogous to Component Importance Measures (CIMs) in reliability theory, SIMs provide a way to rank the constituent systems of an SoS based on their impact on the overall SoS performance during disruptions.

Component importance measures[4,5,6,7] combine system structure and component reliability to assess the importance of a particular component to the overall reliability. They indicate, for example, whether improving a particular component will improve the overall reliability, or, conversely, if a compoent can be downgraded without significantly impacting the overall system reliability. CIMs include Birnbaum's measure, risk achievement worth, risk reduction worth, and Fussell-Vesely's measure.

There have been a few attempts to modify the component importance measures to analyze the resilience of networks. Barker et al.[8] developed two resilience-based CIMs for networks, but the analysis and subsequent metrics are only applicable to networks with homogenous nodes. In addition, emphasis is placed on network flow (that is link resilience) rather than to nodes. While this approach may be beneficial in addressing network resilience, it appears to be useful only for networks where the flow between mostly similar nodes is of concern rather than particular functions carried out at the nodes themselves.

Our work focuses on developing importance measures specifically for SoS that are characterized by diversity in nodes and functions. Similar to the CIMs described above, system importance measures help identify and rank the systems that have the most and least impact on the overall SoS resilience. Consider Fig. 2. Once a constituent system, say System *i*, fails, the performance of the SoS drops from its nominal performance level to some degraded level. In the absence of any recovery measure, the SoS performance stays at this lower level for the duration of the disruption, till the failed system is repaired or replaced. However, if some recovery measure is employed, such as having another System *j* take over some of the lost functionality, then the SoS performance is raised to a higher level of performance (between the nominal and degraded level) and stays at this level till the original failure been addressed and overall performance is brought back to the nominal level. Our measures capture both the impact on the SoS of system failures, as well as the importance of using systems to recover SoS performance.

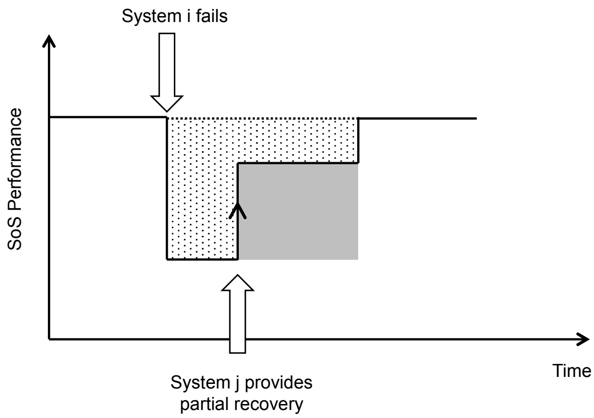

Fig. 2. Resilience curve indicating failed System *i* and recovery System *j* (for *SRI* and *SDI* analysis)

We use the resilience curve to develop four system importance measures: (1) System Recoverability Importance, (2) System Disruption Importance, (3) System Recovery Time Importance, and (4) System Performance Importance. We discuss the first two SIMs in this section and demonstrate their applicability using illustrative examples in the following section. In Section 4, we present current work on developing the next two SIMs.

2.1. System Recoverability Importance (SRI)

The first measure, System Recoverability Importance (SRI), answers the question: How important is a system to SoS recovery? Thus, $SRI_{i,j}$ measures how important System j is to SoS recovery when System i fails. Based on Fig. 2, we define $SRI_{i,j}$ as:

$$SRI_{i,j} = \frac{grey\ area}{total\ (grey + dotted)\ area} \tag{1}$$

$$E(SRI_{i,j}) = SRI_{i,j}.P_{avail}(j) \tag{2}$$

The larger the value of $SRI_{i,j}$, the more important the System j is to mitigating any disruption impact on the SoS due to the failure of System i. Now, $SRI_{i,j}$ depends on the availability of System j to actually provide this recovery. Hence, the expected $SRI_{i,j}$ is calculated using equation (2). The summation of these expected $SRI_{i,j}$ values yields the overall contribution of System j to SoS recoverability. Specifically, $\sum_{i=1}^{n} E(SRI_{i,j})$ indicates how important System j is to overall SoS recovery when the other systems fail.

2.2. System Disruption Importance (SDI)

The second measure, System Disruption Importance (SDI), answers the question: What is the impact of a system failure on the overall SoS? Thus, $SDI_{i,j}$ measures the impact of the failure of System i, given the ability of System j to provide recovery, on the overall SoS performance. Again using Fig. 2, $SDI_{i,j}$ is given by:

$$SDI_{i,j} = \frac{dotted\ area}{total\ (grey + dotted)\ area} \tag{3}$$

$$E(SDI_{i,j}) = P_{fail}(i|D).SDI_{i,j}.P_{avail}(j) \tag{4}$$

Thus, a high value of $SDI_{i,j}$ represents high importance of System i since the recovery measure does not adequately reduce the impact of the disruption on the SoS. Now, $SDI_{i,j}$ depends on: (a) the conditional probability that System i fails given a disruption D occurs, and (b) the availability of System j to actually provide this recovery. Hence, the expected $SDI_{i,j}$ is calculated using equation (4). The summation of these expected $SDI_{i,j}$ values yields the overall expected impact of a disruption on the SoS when System i fails. Specifically, $\sum_{j=1}^{n} E(SRI_{i,j})$ indicates the impact of System i failure, given that other systems are available for recovery, on the overall SoS.

3. Application of SRI and SDI: Illustrative Example

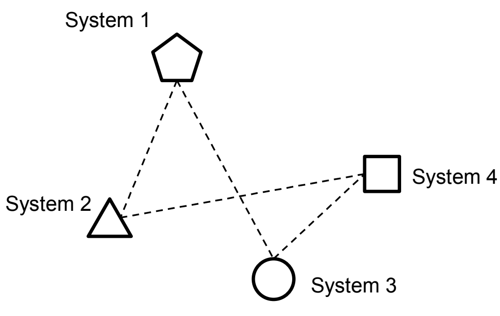

Fig. 3. Four-node notional SoS

Consider a simple four-node SoS (see Fig. 3). Each constituent system performs one or more functions, and collaborations between these systems enable higher SoS-level capabilities. The failure of each constituent system results in a corresponding drop in SoS performance from 100% to some degraded level. This degraded level depends on the failed system as shown in Table 1. We assume that, in the absence of any resilience capability, the SoS performance level is raised from the degraded level to 100% only by the repair or replacement of the failed system.

We now apply the SRI and SDI to analyze two cases of SoS resilience: (1) stand-by redundancy, and (b) stand-in redundancy. Stand-by redundancy is the traditional technique of having an identical secondary system, called a "back-up", on stand-by for each constituent system. So, if a system fails, the SoS performance level drops to the corresponding degraded level for a small (10% of total disruption time for each system) duration of time before the back-up raises the performance level back to 100%.

Table 1. Impact of system failures on SoS (baseline case with no resilience measures available)

Failed system	Degraded SoS performance level	Time duration of failure
System 1	50%	20 units
System 2	30%	30 units
System 3	10%	10 units
System 4	20%	50 units

On the other hand, stand-in redundancy is a way to compensate for a loss of performance in one constituent system by re-tasking the remaining systems. Specifically, as one entity, or node in an SoS, experiences degraded performance or a failure mode, other entities can alter their operations to compensate for this loss. In the four-node example SoS, stand-in redundancy is implemented as follows:

- When System 1 fails, Systems 2 and 3 can enable partial recovery as follows: System 2 raises the performance level to 75% after 10 time units, while System 3 raises the SoS performance level to 55% after 5 time units;
- When System 2 fails Systems 1 and 4 can enable partial recovery as follows: System 1 raises the performance level to 90% after 5 time units, while System 4 raises the SoS performance level to 40% after 10 time units;
- When System 3 fails, Systems 1 and 2 can enable partial recovery as follows: System 1 raises the performance level to 80% after 2 time units, while System 2 raises the SoS performance level to 65% after 5 time units; and
- When System 4 fails, only System 3 can raise the SoS performance level to 65% after 40 time units

Table 2 shows the probabilities used to compute the expected values of $SRI_{i,j}$ and $SDI_{i,j}$. The probability that each back-up system (1_b, 2_b, 3_b, and 4_b) is available is 1 (not shown in table).

Table 2. ($P_{fail}|D$) and P_{avail} for Systems 1, 2, 3, and 4

System	Probability system fails given disruption D occurs ($P_{fail}|D$)	Probability system is available to stand-in for failed functions (P_{avail})
System 1	0.6	0.99
System 2	0.5	0.98
System 3	0.02	0.90
System 4	0.01	0.99

3.1. Analysis of stand-by redundancy

Fig. 4 shows the results of applying *SRI* and *SDI* metrics to the stand-by case. The rows of this figure indicate the system that has failed and the columns represent the systems that are used for recovery. In the stand-by situation, the failure of each system can only be compensated for by the use of its corresponding back-up. Thus, when System 1 fails, only System 1_b can provide recovery; when System 2 fails only System 2_b can provide recovery; and so on. Wherever applicable, each cell in the matrix comprises a set of values in parenthesis (E($SRI_{i,j}$), E($SDI_{i,j}$)). These values are calculated using equations (2) and (4). Summing the expected $SRI_{i,j}$ values along each column, and then normalizing them with the maximum expected recoverability for each column, provides the expected contribution of the back-up systems to overall SoS recoverability. A high value indicates that the system contributes significantly to recovery when other systems fail, and conversely, a low value indicates that the system does not impact overall SoS recovery.

Similarly, summing the expected $SDI_{i,j}$ values and normalizing them along each row gives the overall expected impact of a failure, in the presence of a back-up, on the SoS. Here, a high value indicates that the SoS is impacted severely by the loss of the corresponding system, while a low value indicates that the system failure has a low impact on the SoS. The back-up systems have a high contribution to the overall recoverability, however this contribution is possible only when the corresponding primary system fails. Also, given the presence of these (costly) back-up systems, the overall impact of failures on the SoS is very low.

System used for recovery →

Failed system ↓

	System 1_b	System 2_b	System 3_b	System 4_b	$\sum_{j=1}^{4} SDI_{i,j}$
System 1	(0.9, 0.06)	0	0	0	0.06
System 2	0	(0.9, 0.05)	0	0	0.05
System 3	0	0	(0.9, 0.002)	0	0.002
System 4	0	0	0	(0.9, 0.001)	0.001
$\sum_{i=1}^{4} SRI_{i,j}$	0.9	0.9	0.9	0.9	

Fig. 4. SRI and SDI for stand-by redundancy

3.2. Analysis of stand-in redundancy

Fig. 5 shows the results of applying *SRI* and *SDI* metrics to the stand-in case. The rows of this figure indicate the system that has failed and the columns represent the systems that are used for recovery. As explained previously, in the stand-in situation, the failure of each system can only be compensated for re-tasking other systems in the SoS Here too, wherever applicable, each cell in the matrix comprises a set of values in parenthesis (E($SRI_{i,j}$), E($SDI_{i,j}$)), calculated using equations (2) and (4). Summing and normalizing the expected $SRI_{i,j}$ values along each column provides the expected contribution of each system to overall SoS recoverability. System 1 plays a key role in recoverability as it can provide substantial recovery when Systems 2 or 3 fail. On the other hand, Systems 3 and 4 are not useful to recovery. Although System 3 can stand-in partially when Systems 1 or 4 fail, the actual amount of recovery it provides is very low.

Summing and normalizing the expected $SDI_{i,j}$ values along each row provides the overall expected impact of a failure, in the presence of a back-up, on the SoS. Failure of System 1 has a relatively large impact on the SoS, while failure of Systems 3 and 4 do not impact the SoS significantly. Unlike the expected $SRI_{i,j}$ values, the expected $SDI_{i,j}$ depends on the probability that a system will actually fail. From Table 2 we know that the probability of failure for Systems 3 and 4 are low. As a result, even though the recovery measures in place for when these two systems fail are inadequate, the impact of their failures on the overall SoS is low.

These initial results demonstrate the use of SIMs in the analysis and design of resilient SoSs:

1. Using these importance measures, we are able to determine which areas of the SoS have excess or inadequate resilience. While an overall metric could provide some estimate of SoS resilience under both stand-in and stand-by redundancy cases, these SIMs provide specific information about: (a) systems that have *excess recoverability*, and (b) systems that have *inadequate recoverability* and hence, need more attention (resources).
2. SIMs also provide specific information to guide design decisions. For example, the results showed which type of redundancy proved better for each system. Specifically considering the expected $SDI_{i,j}$ values for stand-by and stand-in cases, we see that failure of Systems 3 or 4 has marginally higher impact on the SoS when stand-in redundancy is employed instead of stand-by redundancy. If these systems are expensive to back-up, then incurring a slightly higher initial investment in enabling other systems to perform some of System 3 and 4's functions may be a more cost-effective option to achieve essentially the same level of resilience. This observation highlights the importance of cost implications in resilience analyses. Future work will incorporate financial considerations with these SIMs to guide design decisions.

System used for recovery →

Failed system ↓	System 1	System 2	System 3	System 4	$\sum_{j=1}^{4} SDI_{i,j}$
System 1	(0,0)	(0.2450, 0.4410)	(0.0675, 0.4995)	(0,0)	0.3135
System 2	(0.7071, 0.1414)	(0,0)	(0,0)	(0.0943, 0.4479)	0.1964
System 3	(0.6160, 0.0075)	(0.2994, 0.0136)	(0,0)	(0,0)	0.0070
System 4	(0,0)	(0,0)	(0.1013, 0.0080)	(0,0)	0.0026
$\sum_{i=1}^{4} SRI_{i,j}$	0.4410	0.1814	0.0562	0.0314	

Fig. 5. SRI and SDI for stand-in redundancy

4. Additional System Importance Measures

The SRI and SDI do not place a relative value on time versus performance. The resilience curves for a system that provides a rapid, but low recovery, and a system that provides a slower, but greater recovery can have the same *SRI* and *SDI* values. To explicitly account for how fast a system can provide recovery as well as how much performance gain can be obtained, we present two additional SIMs: (a) System Recovery Time Importance, and (b) System Performance Importance. We briefly present the mathematical formulation of these measures here. Their application is left for future work.

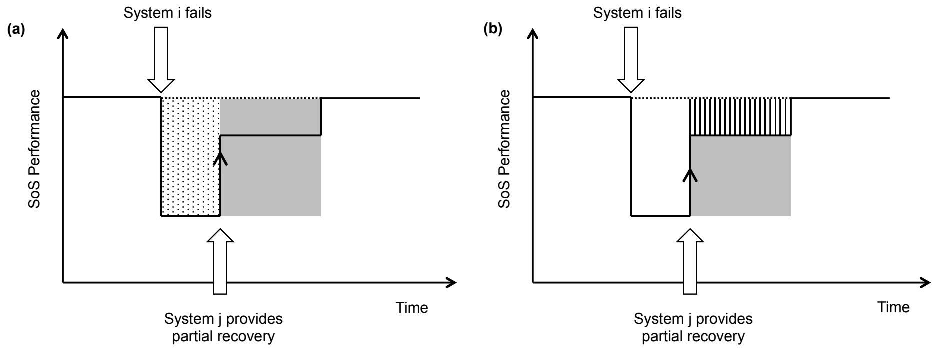

Fig. 6. Resilience curve indicating failed System *i* and recovery System *j* for (a) *SRTI* analysis and (b) *SPI* analysis

4.1. System Recovery Time Importance (SRTI)

System Recovery Time Importance answers the question: How important is a system in terms of how rapidly it can provide SoS recovery? Based on Fig. 6(a), $SRTI_{i,j}$ is given by equation (5). The larger the value of $SRTI_{i,j}$, the faster System *j* is able to recover some of the lost functionality. Similar to the expected value of $SRI_{i,j}$, $SRTI_{i,j}$ also depends on the availability of System *j* to actually provide this recovery. Hence, the expected $SRTI_{i,j}$ is calculated using equation (6). Similar to the SRI measure, the summation of these expected $SRTI_{i,j}$ values yields the overall contribution of System *j* to SoS recovery time.

$$SRTI_{i,j} = \frac{grey\ area}{total\ (grey + dotted)\ area} \tag{5}$$

$$E(SRTI_{i,j}) = SRTI_{i,j}.P_{avail}(j) \tag{6}$$

4.2. System Performance Importance (SPI)

System Performance Importance answers the question: How important is a system in terms of how much SoS performance gain it can provide? Based on Fig. 6(b), $SPI_{i,j}$ is given by equation (7). The larger the value of $SPI_{i,j}$, the higher the performance gain that System j is able to provide. Similar to the expected value of $STRI_{i,j}$, $SPI_{i,j}$ also depends on the availability of System j to actually provide this recovery. Hence, the expected $SPI_{i,j}$ is calculated using equation (8). And so, the summation of these expected $SPI_{i,j}$ values yields the overall contribution of System j to SoS performance recovery.

$$SPI_{i,j} = \frac{grey\ area}{total\ (grey + dotted)\ area} \tag{7}$$

$$E\left(SPI_{i,j}\right) = SPI_{i,j}.P_{avail}(j) \tag{8}$$

4. Conclusion and Future Work

The primary aim of this research is to provide a rigorous quantitative basis to make informed decisions about SoS resilience as opposed to the existing ad-hoc approaches. We suggest System Importance Measures (SIMs) as one way to analyze resilience with a focus on ranking resilience-critical systems. We first presented the mathematical formulation behind these SIMs, and then demonstrated their use with two cases. In future work, we will refine this initial formulation and expand it to a framework that evaluates resilience-cost trade-offs and provides guidance on designing SoS resilience. Specifically, this research will help identify areas in the SoS where greater investment of resources will considerably improve the resilience of the overall SoS, or conversely, areas where additional capital need not be spent, as these systems do not significantly impact the overall SoS. In current work, we are also applying these importance measures to a study of the Littoral Combat Ship SoS.

The key contribution of this research is to provide decision-makers with improved information and tools to make SoS-level decisions. The use of system importance measures (SIMs), and their resulting upstream effects on development policies, costs and risks, can be used by decision-makers to quantitatively assess the resilience of SoSs and by designers to better allocate risk resolution resources.

Acknowledgements

This material is based on work supported, in whole or in part, by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract H98230-08-D-0171. SERC is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

References

1. K. Tierney and M. Bruneau, “Conceptualized and measuring resilience”, TR News, 2007, 250, pp – 14-17.
2. J-F. Castet and J.H. Saleh, “On the concept of survivability, with application to spacecraft and space-based networks”, Reliability Engineering and System Safety, Vol. 99, pp. 123-138, 2012.
3. B. Ayyub, “Systems Resilience for Multihazard Environments: Definition, Metrics, and Valuation for Decision-Making”, Risk Analysis, DOI: 10.1111/risa.12093, 2013
4. M. Rausand and A. Hoyland, System Reliability Theory: Models, Statistical Methods, and Applications, Second edition. New Jersey: Wiley – Interscience, 2004.
5. E. Elsayed, Reliability Engineering, Addison Wesley Longman Inc., 1996.
6. J. E. Ramirez-Marquez and D. W. Coit, “Multi-state component criticality analysis for reliability improvement in multi-state systems”, Reliability Engineering & System Safety, Vol. 92, No. 12, pp. 1608-1619, 2007.
7. M. Van der Borst and H. Schoonakker, “An overview of PSA importance measures”, Reliability Engineering & System Safety, Vol. 72, No. 3, pp. 241-245, 2001.
8. K. Barker, J. E. Ramirez-Marquez, and C. M. Rocco, “Resilience-Based Network Component Importance Measures”, Reliability Engineering & System Safety, Vol. 117, pp. 89-97, 2013.