A Useful Point of Reference for Critical Infrastructure Resilience

Don O'Neill
Don O'Neill Consulting
Montgomery Village, MD USA
ONeillDon@aol.com

Abstract— *The focus of Critical Infrastructure Resilience is on Integration Engineering process, management, and engineering considerations with full attention to the roles of the Resilience Integrator and the Intelligent Middleman and the convincing evidence of Resilience Integration Engineering earned value analytics used in calculating resilience risk.*

Keywords—*Critical Infrastructure Resilience, Resilience Integrator, Intelligent Middleman, Integration Engineering, Risk Calculation, Earned Value, Culture Harmonization, Resiliency Maturity Framework, System of Systems Architecture, Way of Working, Cascade Triggers, Recovery Time Objectives, Deterrence*

I. INTRODUCTION

Let's take a look at the elements of Critical Infrastructure Resilience.The focus is on Integration Engineering process, management, and engineering considerations with full attention to the roles of the Resilience Integrator and the Intelligent Middleman and the convincing evidence of Resilience Integration Engineering earned value analytics used in calculating resilience risk [1]. This will be a broad and deep discussion of resilience, one that will confront numerous previously unattended issues.

II. PROBLEM DEFINITION AND ITS IMPORTANCE

The critical infrastructure is the industrial base on which the competitiveness and security of the nation are dependent. The current state of the nation's critical infrastructure is at risk as the Internet has become the central nervous system of the nation both private and public. The nation's critical infrastructure continues to be vulnerable to natural disasters and cascading Cyber Security attacks. In fact, software has become the critical infrastructure within the critical infrastructure [2]. It is here in the mashup among an immature software profession, a vulnerable Cyber Security environment, and diverse and interdependent industry sectors that the challenge of system of systems resilience is born [3].

III. POTENTIAL SOLUTIONS TO ADDRESS THE PROBLEM

A more useful approach to Critical Infrastructure Resiliency is sought, one that represents new thinking, perhaps a new paradigm based on adaptive measures not simply error discovery; more selective Internet usage based on user responsibility, proven protections, and calculated risk; credible deterrence through convincing will and demonstrable capability; and earned value analytics serving as convincing evidence underlying risk assurance.

IV. ANALYSIS OF THE RESULTS

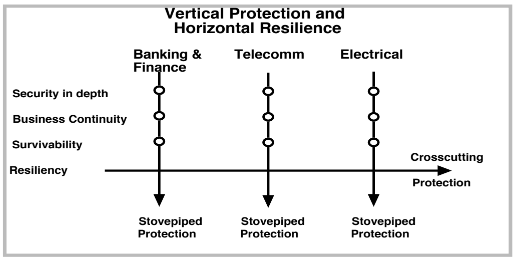
1. Contrary to some assumptions about resilience, resilience is not primarily threatened by errors. Rather, resilience is primarily threatened by multiple contexts and opposing goals. Successful approaches to resilience are primarily tied to harmonization of components and their adaptive capability.
2. Nor should the goal of resilience simply be to bounce back to the earlier state before the moment of adversity or attack. It was in fact the earlier state that proved vulnerable. Herein lies the challenge.
3. Cyber Security is not simply a problem awaiting a technology solution. Instead Cyber Security is a problem of user behavior awaiting a deeper awareness and acceptance of responsibility. Simply put, individuals and organizations who cannot afford to lose data or information should not put it on the Internet. For those who can afford to lose data or information but would rather not, these users should exercise proven user protection by employing three-factor authentication and encryption.
4. On the big stage, Critical Infrastructure resilience is part of the February 2017 Defense Science Board's Cyber Deterrence strategy and its deterrence by denial and deterrence by cost imposition. No Potemkin facade, a resilient-ready Critical Infrastructure would achieve adversary deterrence by cost imposition and perhaps even deterrence by denial of particular objectives as long as there is a convincing credible will and demonstrable capability. Like Game Theory, a strategy of deterrence is based on rationality. Rationality in the context of Cyber Security cannot be assured when unprepared managers, politicians, and lawyers are engaged in the deeply technical issues of Cyber Security where there is no unified theory. More is needed.
5. Based on nearly 50 indicators of resilience, resilience earned value analytics employ the most convincing evidence available to measure the degree to which the resilience value proposition is being achieved both collectively and in each industry sector and the degree to which unattended resilience risk continues to persist.

V. OPEN RESEARCH QUESTIONS TO BE TACKLED

One respected researcher seemed to concede the high ground of resiliency, that is, avoidance, in associating resilience with the Timex slogan, *"Take a licking and keep on ticking."* The question then becomes what perimeter is being secured? In protecting a network node or a physical facility in a geographic region, each node or facility is to be protected and made survivable.

In achieving resilience, propagation and cascading effects across the network and region must also be curtailed. This is made difficult by the context and culture challenges of the industry sectors within the critical infrastructure. The capabilities needed to impact crosscutting issues cannot be expected to evolve in a loosely coupled environment. They must be holistically specified, architected, designed, implemented, and tested if they are to operate with resilience under stress. A management, process, and engineering maturity framework is necessary to advance the assurance of software security, business continuity, system survivability, and system of systems resiliency capabilities (Figure 1).

Figure 1. Vertical Protection and Horizontal Resilience



A. Goal
Resiliency is the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity, whether natural or man made, under all circumstances of use. Resiliency applied to a system of systems focuses on crosscutting issues. Crosscutting effects stem from dependent relationships. Some dependent relationships are planned and intended interactions between industry sectors, such as, financial transactions embedded in telecommunications, electrical, transportation, and medical operations. Other dependent relationships are indirect and stem from outsourced commoditized services that bring with it opportunities for common single point failures among industry sectors, such as, the Internet, the Global Positioning System, Federal Express, IBM, and Microsoft.

B. Objectives
In order to operationalize resiliency, objectives must be matched with well coordinated features.

- The objective of *anticipating* calls for the features of harmonized domain engineering, coordinated recovery time objectives, cascade trigger identification, and digital situation awareness.
- The objective of *avoiding* calls for the features of shut down, defense in depth, operation sensing and monitoring, and distributed supervisory control.
- The objective of *withstanding* calls for the features of enterprise security, business process continuity, survivability, and alternate site.
- The objective of *minimizing* calls for the features of adaptation management, alternate mode, minimum essential mission, and shut down.
- The objective of *recovering* calls for the features of capability to reorganize, assured availability, information and data recovery, and clean up and reconstitution.

C. Industry Sectors
The critical infrastructure is composed of the numerous industry sectors that do the heavy lifting including utilities and energy, telecommunications, banking and finance, transportation, and medical systems. The architecture of each industry sector is driven by the arrangement of its business units and integrating elements and components that comprise it.

D. Business Unit Integration
Business units are organized into corporate entities, geographic regions, and operating domains of land, sea, air, and space. Integrating elements house business unit technology in the form of computers, operating systems, middleware, communication protocols, data management systems, software, and programming languages.

1. Utilities and Energy contain power generation and distribution systems, nuclear power control systems, and energy resource allocation systems.
2. Telecommunications contain network control and switching systems, satellite control and management systems, and mobile communications systems and protocols.
3. Banking and Finance contains electronic commerce and electronic funds transfer systems, transaction processing systems, security and privacy management systems, and network management systems.
4. Transportation contains route management and collision avoidance systems, avionics systems, air traffic control systems, navigation and position location systems, and embedded automobile control systems.
5. Medical Systems contain medical device control systems, patient record systems, and insurance and payment systems.

Predominately private and requiring indemnification to unlock necessary information sharing, these business units need to be infused with the spirit of "*Freedom's Forge*" by Arthur Herman [4] used to mobilize the *"arsenal of democracy"* that propelled the Allies to victory in World War II. Quite the opposite, today's Congress refuses to provide industry indemnification out of its mistrust of industry as publicly expressed by Senator Sheldon Whitehouse of Rhode Island at the 2016 Georgetown University Conference on Cyber Engagement.

E. Operations
The operations within the industry sectors of the critical infrastructure are diverse and complex. These industry sectors comprise an accidental system of systems that intersect operationally without a plan and design in advance. Each sector system was constructed within its own context and culture. In operation, these sector systems may inadvertently impose their own context and culture on others and clash with uncertain and unintended operational results.

- Industry sector practice varies widely in its domain engineering approaches resulting in diversity in architecture, models, and patterns including their representation. Formality within an architectural framework facilitates the imposition of distributed supervisory control, interoperability, and operation sensing and monitoring protocols.
- Industry sector maturity in management and engineering processes varies widely resulting in diversity in configuration management, frequency of release, conformance to requirements, and traceability among life cycle artifacts. Strong code management practices facilitate reconfiguration and reconstitution.
- Industry sector practice varies widely in fielding and operating practices resulting in diversity in accountability and control, supply chain management, civility and pushback, and willingness to expend off the clock effort. Exercising strong control over the workforce facilitates business continuity and survivability.
- Industry sector impacts from government regulation vary with respect to export control, tax policy, intellectual property, privacy, and antitrust litigation. Exercising strong government control facilitates compliance for the benefit of the commons at the expense of initiative for the self-interest.
- Industry sector public expectation and confidence vary with respect to trust, loyalty, and satisfaction. The financial and medical sectors depend on public trust. The electrical and telecommunication sectors depend on customer loyalty and satisfaction. The diverse industry sector expectations of trust, loyalty, and satisfaction must be respected, blended, and harmonized.

- Technical Debt is the organizational, project, or engineering neglect of known good practice that can result in persistent public, user, customer, staff, reputation, or financial cost [5]. In truth most Technical Debt is taken on without this strategic intent, without even knowing it, and without the wherewithal in capability or capacity to do the job right. Technical Debt must be eliminated.

VI. RECOMMENDED FOLLOW-ON ACTIVITIES

A. Resilience Integrator

There is a need for a resilience integrator to organize, integrate, and harmonize industry sectors of the critical infrastructure into a resilient system of systems. The stakeholder vision for this project is an opportunity value proposition for operational resilience.

If resilience is to be achieved, the resilience integrator must be prepared to provide resiliency engineering features capable of meeting stringent resiliency objectives.

- The resilience integrator shall harmonize the context and culture of the numerous industry sectors and anticipate domain engineering clashes in order to avoid unintended operations results stemming from diversity in management, process, and engineering approaches.
- The resilience integrator shall groom Intelligent Middlemen to pave the way in the adoption of the way of working within the industry sectors of the critical infrastructure.
- The resilience integrator shall facilitate the resilience maturity of management, process, and engineering capabilities and solutions that address security, continuity, survivability, and resilience among the industry sector system of systems.
- The resilience integrator shall specify a system of systems architecture that facilitates the harmonious cooperation among industry sectors; provides digital situation awareness; allows for distributed supervisory control under stress; and manages the assembly, delivery, and control of of common system assets.
- The resilience integrator shall prepare and coordinate a Resilience Integration Program Plan harmonizing, facilitating, specifying, engineering, developing, integrating, and fielding the integrating elements of the critical infrastructure system of systems.
- The resilience integrator shall frame a way of working to mange the communication, command, control, commitments, and performance among the industry sectors, their contractors, and the resilience integrator including executive councils, steering groups, working groups, and support groups.
- The Resilience Integrator shall calculate Resilience Risk based on Earned Value Analytics.

B. Coordinated Recover Time Objectives

The operational litmus test for harmonized domain engineering in a distributed system of systems is the coordinated recovery time objective (Figure 2). Clearly this is the responsibility of the resilience integrator in facilitating resilience maturity.

For each critical infrastructure sector, under what circumstances of use are dependent sectors not available? For each instance of non-availability, what is the immediacy of need (im) and the required recovery time objective (rrto) for each? These are expressed in seconds (s), minutes (m), hours (h), days (d), and perhaps weeks (w).

Canonical verification of the statement of critical infrastructure sector dependency is governed by the degree of correspondence where recovery time objectives (rto) are established in relationship to immediacy of need (im). Shortfall reveals technical and management feasibility and state of the practice issues.

Figure 2. Coordinated Recovery Time Objectives

Prime/Support	**S1- Electrical**	**S2- Telecom**	**S3- Banking and Finance**	**S4- Transportation**

P1- Electrical		im=s rto=s
		S2
		crto=s cl=H
			im=h rto=h
			S3
			crto=h cl=H
				im=h rto=d
				S4
				crto=? cl=L

P2- Telecom	im=s rto=s
	S1
	crto=? cl=L
			im=h rto=h
			S3
			crto=h cl=H
				im=d rto=d
				S4
				crto=? cl=M

P3- Banking and Finance	im=s rto=s
	S1
	crto=? cl=L
		im=s rto=s
		S2
		crto=s cl=H
				im=h rto=d
				S4
				crto=? cl=L

P4- Transportation	im=m rto=m
	S1
	crto=? cl=L
		im=h rto=s
		S2
		crto=s cl=H
			im=h rto=h
			S3
			crto=h cl=H	

Operational verification of the statement of critical infrastructure sector dependency is governed by the degree to which the recovery time objective (rto) has been coordinated among the prime and support sectors in arriving at a coordinated recovery time objective (crto). Shortfall reveals issues in stovepipe culture, management will, and regulatory environment. A confidence level is assigned to the outcome in terms of high (H), medium (M), or low (L).

C. Identifying Cascading and Propagating Triggers

Underlying cascading and propagating triggers hidden in the complexity of critical sector interactions and dependencies must be anticipated, avoided, and minimized [6]. Each critical infrastructure industry sector is dependent on other industry sectors. The interdependence of electric power, telecommunications, energy, financial, transportation, emergency services, water, food, and so forth is exacerbated by the embedded electronic devices relied on to provide critical controls. Electric power and telecommunications stand out as common critical dependencies for all industry sectors and require special preparation and protection measures.

Underneath the surface and hidden in the complexity of critical sector interactions and dependencies are triggers that can result in cascading and propagating effects and impacts. Anticipating, avoiding, and minimizing the effects of these triggers is a responsibility of the Resilience Integrator. For example, the Banking and Finance sector must remain ever vigilant during the trading day for evidence of triggers that might impede next day opening of the market. Here anticipation and avoidance are preferred over recovery, cleanup, and delayed market opening in maintaining trust in the Banking and Finance sector.

Hidden or in plain sight, cascade triggers are capable of invading various industry sectors in a variety of ways. The transportation sector can be brought to its knees if truck drivers cannot use credit cards to charge for gas tank fill ups. The medical sector depends on the Internet to distribute and present patient electronic medical records on demand. The electrical grid depends on a survivable electrical grid with predictable demand profiles matched to planned resources and capacities. The banking and finance sector remains ever conscious of its need to protect next day opening even in the presence of a flash crash disruption. The users of the telecommunications sector are increasingly vulnerable to Internet disruptions like DDoS and encryption-based scams like ransomware.

D. Intelligent Middlemen

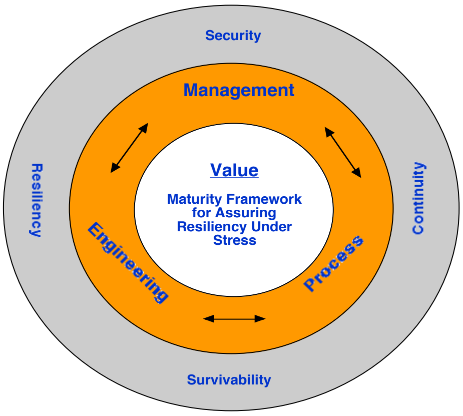
If the critical infrastructure is to be resilient, its sector managers and systems must respond to guidance from Intelligent Middlemen whose influence is felt before, during, and after a crisis [2]. Intelligent Middlemen possess the broad range of hard and soft skills spanning the cultural, ethical, legal, business, process, management, and engineering dimensions needed to meet the challenges of the critical infrastructure in anticipating, avoiding, minimizing, withstanding, and recovering from crosscutting effects and to impede the emergence of propagating and cascading effects.

The Intelligent Middlemen are positioned at the center of things and serve as the traffic cop for identifying and driving resolution of crosscutting issues. From this vantage point, the Intelligent Middlemen are able to obtain superior situational awareness. For example, they ensure that recovery time objectives are coordinated, interoperability protocols are followed, distributed supervisory control functions are coordinated, and operation sensing and monitoring functions are applied.

E. Maturity Framework for Assuring Resilience Under Stress

There exists a need for a means to harmonize the diverse and complex operations within the industry sectors of the critical infrastructure which comprise an accidental system of systems that intersect operationally without a plan and design in advance [7]. The Maturity Framework for Assuring Resiliency Under Stress provides that means and delivers value through management, process, and engineering capabilities and solutions (Figure 3).

Figure. 3 Resilience Maturity Framework



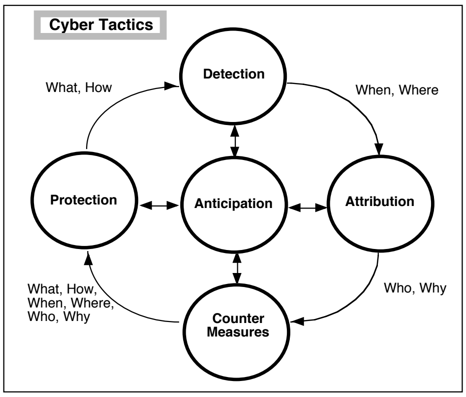
The system perimeter focus areas include commitment to a business case, security in depth, business continuity, and systems survivability. The essential focus areas needed to extend this perimeter to the system of systems context needed to demonstrate resiliency include coordinated recovery time objectives, interoperable information and data exchange, operation sensing and monitoring, distributed supervisory control, and information and data recovery. To achieve maturity in the assurance of resiliency under stress, the enterprise must satisfy the goal-based argument at each level.

F. Cyber Tactics Framework

Cyber Tactics span anticipation, protection, detection, attribution, and counter measures (Figure 4). However, these Cyber Tactics are currently underdeveloped and insufficient as implementers of the nation’s Cyber Strategy. The Cyber Tactics Framework represented here is a structure of Cyber Tactics and their intended functions and input and output semantics [8].

- Anticipation focuses on making decisions about the future based on expectation.
- Protection focuses on deploying effective barriers and safeguards.
- Detection spans digital situation awareness and operation sensing and monitoring.
- Attribution is focused on the assessment of cause and effect trace artifacts.
- Counter measures are focused on the detection and elimination of attack outcomes.

Figure 4. Cyber Tactics Framework

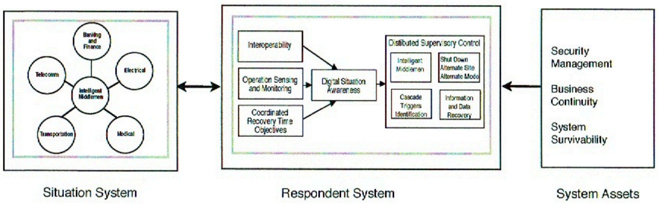


G. Software Systems Architecture

The Software Systems Architecture for Critical Infrastructure Resilience (Figure 5) calls for the following allocation of control, functions and persistent data, and assets [2].

- The Situation System is populated with the man-made Critical Infrastructure Sectors and the Intelligent Middlemen control node. Each industry sector will register its profile in order to engage with the services of the Respondent System.
- The Respondent System is populated with the System of Systems Resiliency Engineering mission focus areas intended to interact with the Situation System and its Intelligent Middleman in anticipating, avoiding, withstanding, mitigating, and recovering from the effects of adversity under all circumstances of use.
- The System Assets is populated with the facilities focus areas and their services to be instantiated by the Respondent System in its interaction with the Situation System and its Critical Infrastructure Sectors.

Figure 5. Software Systems Architecture

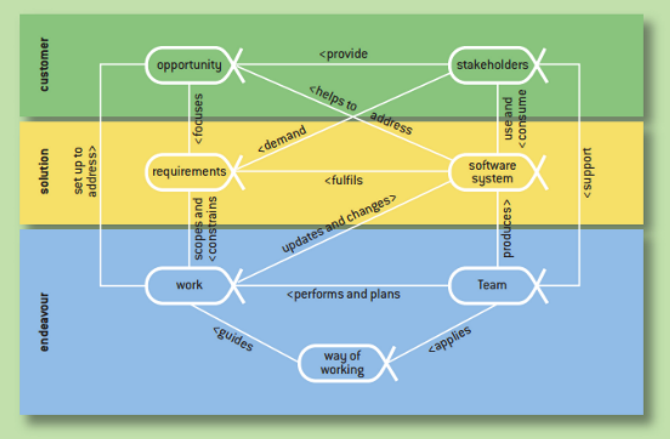

Banking and Finance
Telecomm
Electrical
Intelligent Middlemen
Transportation
Medical
Interoperability
Operation Sensing and Monitoring
Coordinated Recovery Time Objectives
Digital Situation Awareness
Distibuted Supervisory Control
Intelligent Middlemen
Shut Down Alternate Site Alternate Mode
Cascade Triggers Identification
Information and Data Recovery
Security Management
Business Continuity
System Survivability
Situation System
Respondent System
System Assets

H. Way of Working

Whether you establish criteria at the beginning of a project or not at all, there exists industrial strength objective criteria for learning the status of a project and pointing the way forward. These criteria can be found in the Software Engineering Method and Theory (SEMAT) formulation and its Essence Kernel, the essence and common ground of software engineering and a major Object Management Group (OMG) standards process (Figure 6).

- The customer space is framed by a stakeholder shared vision for a well conceived value proposition for the opportunity with convincing and consequential outcomes.
- The solution is bounded by stakeholder agreed to requirements and user stories and a software system architecture that facilitates a usable and operational software product.
- The endeavor’s work is performed by a well selected and ready team and a way of working based on established principles and foundations.

Figure 6. Software Engineering Method and Theory



As the twig is bent so grows the tree. So, to get your Critical Infrastructure Resilience project off on the right foot, expectations should be set and evidence should be sought on the following assertions and principles based on the following checkpoints:

- Stakeholders are in agreement and share a vision for the project to assure Critical Infrastructure assurance. Stakeholders include the Critical Infrastructure sectors, Intelligent Middlemen, the Resilience Integrator, and the public.
- An opportunity value proposition has been established, and there is stakeholder shared vision for achieving it revolving around the ability to anticipate, avoid, withstand, minimize, and recover from the effects of adversity, whether natural or manmade, under all circumstances of use.
- Requirements or user stories are coherent and acceptable, and there is stakeholder shared vision for them. The Resilience Integrator takes the lead in driving the fulfillment of requirements beginning with the harmonization of context and culture, the coordination of recovery time objectives, and the identification of cascade triggers along with defense in depth through Cyber Security strategy and tactics and business continuity through Supply Chain risk management assurance [9].
- The software system architecture is selected based on the Systems Coupling Diagram and comprises a domain specific architecture to guide software system implementation spanning the Situation System, the Respondent System, and System Assets. The software system implementation is made ready and operational with no technical debt.
- The team operates in collaboration, shares a vision for the project, and is ready to perform with respect to shared vision, software engineering process, software project management, software product engineering, operations support, and domain specific architecture processes, methods, and tools [10].
- The way of working by the team has established foundations for software engineering process, software project management, software product engineering, and operations support.
- The work is started only when all is prepared including coherent requirements and acceptable user stories, stakeholders in agreement, and an established foundation for the way of working.
- All work products are prepared and inspected in accordance with a defined standard of excellence assuring completeness, correctness, and consistency. Progress is assessed, verified, and validated and then expressed in terms of earned value and calculated risk.

I. Resilience Risk and Earned Value Calculation

Systematically measuring earned value resilience assurance evidence is an important step in calibrating and establishing convincing credibility of will and demonstrable capability. This tool serves as a useful point of reference for organizing integration engineering activities.This Critical Infrastructure Resilience dashboard (Figure 7) is intended to shine a spotlight on resilience risk and earned value in order to reveal gaps, suggest vulnerabilities, and point the way forward for participating industry sectors.

The worksheet is used to compile the assurance evidence element scores of 46 risk indicators for each of five industry sectors. Each indicator is scored 1 (low) to 5 (high). Note that both the assurance evidence elements and the industry sectors may be assigned weights of 1-5.

- Resilience Earned Value := Weighted Example / Weighted Maximum
- Resilience Risk := (1-Resilience Earned Value)
- Resilience Earned Value: Weighted Example / Weighted Maximum = 8101/12495 = 0.64833
- Resilience Risk: (1- Resilience Earned Value) = (1-8101/12495) = 0.35166

J. Software and Supply Chain Risk Management (SCRM) Assurance Framework

Supply Chains in the wild are intrinsically risky, vulnerable to Cybercrime and Cloud Computing risks as well as organizational neglect and unmet needs. The practice of risk management using smart and trusted tactics is necessary because software-based supply chains are inherently insecure, the risks and uncertainties are prolific, and vulnerabilities abound. The combination of unmet needs, industry neglect, and austerity coupled with the immature state of software, Cyber Security, and Cloud Computing infrastructure yield a rich environment of uncertainty and risk in establishing and maintaining infrastructure, being trusted, being competitive, and being austere (Figure 8) [9].

Figure 8. Supply Chain Risk Management Goals and Objectives

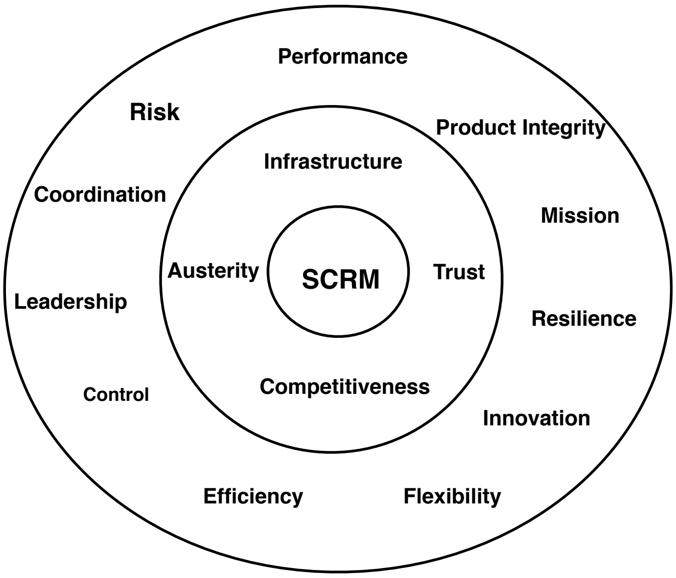


Figure 7. Critical Infrastructure Resilience Dashboard

Assurance Evidence (Weighted Example)	Risk Indicator (Score 1-5)	Indicator Weight	Electrical Sector	Telecom Sector	Banking & Finance Sector	Transport. Sector	Medical Sector	Weighted Score	Earned Value	Risk
Sector Weight			**5**	**4**	**3**	**3**	**2**			
A. Culture and Content Harmonization	164	**4**	800	624	468	312	160	2364	0.6952	0.3048
B. Intelligent Middlemen	98	**2**	240	292	144	84	48	708	0.8329	0.1671
C. Resiliency Maturity	**70**	**5**	325	260	240	210	140	1175	0.6911	0.3089
D. System of Systems Architecture Adoption	38	**5**	200	160	129	105	70	655	0.5137	0.4863
E. Integration Engineering	57	**2**	130	104	72	60	36	402	0.5911	0.4089
F. Way of Working	141	**3**	420	336	333	234	132	1455	0.7132	0.2868
G. Resilience Assurance and Risk Calculation	77	**2**	170	136	102	78	52	538	0.5274	0.4726
H. Cyber Security Strategy and Tactics	78	**3**	240	192	162	126	84	804	0.5254	0.4746
Total Indicators	723		2525	2004	1641	1209	722	8101	0.6483	0.3517

VII. REFERENCES

[1] Defense AT&L (2017-1) O'Neill, D., *"Integration Engineering and Critical Infrastructure Resilience",* Defense Advanced Technology and Logistics (DAT&L) Magazine, July/August 2017 https://www.dau.mil/library/defense-atl/_layouts/15/WopiFrame.aspx?sourcedoc=/library/defense-atl/DATLFiles/July-August_2017/O%27Neill.pdf

[2] Jacobson, I., Lawson, H.B. (2015) *"Software Engineering in the Systems Context",* Edited by Ivar Jacobson and Harold "Bud" Lawson, College Publications, Kings College, London, ISBN 978-1-84890-76-6, 2015, 578 pages

[3] Defense AT&L (2015) O'Neill, D., *"Software 2015: Situation Dire"*, Defense Advanced Technology and Logistics (DAT&L) Magazine, May/June 2015 http://dau.dodlive.mil/files/2015/04/DATL_May_Jun2015.pdf

[4] Herman, Arthur, *"Freedoms Forge: How American Business Produced Victory in World War II"*, Random House, ISBN 978-1-4000-6964-4, 2012, 413 pages

[5] Defense AT&L (2013) O'Neill, D., *"Technical Debt in the Code: Cost to Software Planning",* Defense Advanced Technology and Logistics (DAT&L) Magazine, March-April 2013 https://www.dau.mil/library/defense-atl/_layouts/15/WopiFrame.aspx?sourcedoc=/library/defense-atl/DATLFiles/Mar-Apr2013/DATL_mar-apr2013.pdf

[6] White House (2016) O'Neill, D., *Integration Engineering in the Pursuit of Critical Infrastructure Resilience: A Unified Theory ,* White House Cyber Commission on Enhancing National Cybersecurity, Kickoff Meeting , April 14, 2016 http://www.nist.gov/cybercommission/upload/Meeting_Minutes_April_14.pdf

[7] CrossTalk (2009) O'Neill, D., "*Meeting the Challenge of Assuring Resiliency Under Stress",* CrossTalk, The Journal of Defense Software Engineering, September/October 2009 http://www.crosstalkonline.org/storage/issue-archives/2009/200909/200909-ONeill.pdf

[8] CrossTalk (2011), O'Neill, D., "*Cyber Strategy, Analytics, and Tradeoffs: A Cyber Tactics Study",* CrossTalk, The Journal of Defense Software Engineering, September/October 2011 http://www.crosstalkonline.org/storage/issue-archives/

[9] CrossTalk (2014) O'Neill, D, "*Software and Supply Chain Risk Management Assurance Framework",* CrossTalk, The Journal of Defense Software Engineering, March/April 2014 http://www.crosstalkonline.org/storage/issue-archives/2014/201403/201403-ONeill.pdf

[10] Defense AT&L (2017-2) O'Neill, D., *"Renovating the Senior Executive Service",* Defense Advanced Technology and Logistics (DAT&L) Magazine, September/October 2017

4354 words