Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019

Investing in Cyber Defense: A Value-Focused Analysis of Investment Decisions for Microgrids

Bryan J. Hudgens
Naval Postgraduate School
bryan.hudgens@nps.edu

Cameron Hartner
United States Marine Corps
Cameron.hartner@usmc.mil

Brian Adams
United States Marine Corps
Brian.adams@usmc.mil

Eva Regnier
Naval Postgraduate School
eregnier@nps.edu

Abstract

To mitigate disruptions to commercial power grids, and to achieve operational efficiencies by managing energy use, many organizations are fielding smaller, local, self-contained microgrids. The computer control systems that operate the microgrids create new vulnerabilities to a rapidly-escalating array of cyber attacks. This creates a tension between the need to improve energy assurance and efficiency through microgrids, and the need to protect against cyber attacks that can disrupt and damage the organization's energy systems. Through a series of interviews with subject matter experts and end-users, this exploratory study surfaces the decision-makers' important values in this decision space and develops a network of those values to guide decision-makers to make better decisions in balancing these competing needs.

1. Background

As disasters, such as Superstorm Sandy in the Northeastern United States demonstrate, even relatively brief lack of energy can curtail critical services including transportation, healthcare, communication and security [4]. Protecting critical infrastructures, such as energy, has become a national security issue, e.g., [13], [15], [34]. Reliance on commercial power grids is important for the United States (US) Department of Defense (DoD), which is the United States' top consumer of electricity, and which relies on the commercial power grid to supply essentially all its electrical power, including power to 91% of its "most critical" infrastructure [8]. The DoD is vulnerable to natural and intentional outages and "[i]n 2015 alone…experienced approximately 127 outages that lasted 8 hours or longer, caused by…weather and equipment failure" [8].

One way to address this vulnerability is through microgrids – smaller, local, power grids that can function in concert with, or isolated from, commercial power grids [19]. Because they can operate independently of commercial grids they can provide electricity when commercial grids are down [2], [19], [25]. They provide capability for operational management of the local grid that can lower costs [19].

These benefits come at a cost, however, because microgrids rely on computerized control systems to govern their activity, and these control systems introduce the potential vulnerability to cyber threats [2]. Control systems, or Supervisory Control and Data Acquisition (SCADA) systems, have the capability to adjust the energy system [5], [16]. Such SCADA systems are often interoperable, which improves the potential benefit via information sharing and greater efficiencies, but also increases the risks of cyber intrusion, as instances such as the Havex attacks beginning in 2013 [15] and the Ukraine cyber attacks of 2015 [15], [34] demonstrate. As the DoE notes [8], from 2001 to 2015, the number of devices connected to the internet grew from 400 million to 25 billion. Concomitant with this growth in connects has come an increase in cyber threats and attacks [13], [14], [15], [21]. Attackers include both state and non-state actors [15], and experts expect attacks to continue [34].

Decisions about control system cyber security often require trade-offs between greater resilience and greater vulnerability, and the impacts of cyber-security interventions are difficult to evaluate [31]. For example, is providing off-site access to a control system good, as it allows installation personnel to quickly repair problems, or is it bad as it creates an additional vulnerability to cyber attack? Is the cost of one worth the benefit of the other?

In the context of Navy installations, we explore the values of energy managers and control system engineers responsible for making these decisions at US Navy installations. Using Value-Focused Thinking (VFT) [17], we interview these stakeholders to identify, synthesize and organize the relevant values. This process can lead stakeholders to identify values that might not be explicit, and how values contribute to the organization's fundamental values. For example, in our study, cyber security is only a means

URI: https://hdl.handle.net/10125/59720
ISBN: 978-0-9981331-2-6

to the end of providing reliable energy to sustain the mission at bases. Understanding this can help clarify whether interventions that reduce cyber-vulnerability are worth any degradation of functionality of the energy system. In addition, VFT can reduce the perceived tension between competing values and lead stakeholders to identify creative alternatives that improve all objectives. In adopting this approach, we follow other information scholars, e.g., [10], [27], and [30], who have used it to understand information systems security; we contribute to this conversation by exploring this approach in a context requiring important trade-offs which can have significant national and international security implications.

Keeney's value-focused thinking [17] formulates decisions not as problems, but as opportunities. Keeney defines values as "principles used…to evaluate the actual or potential consequences of action and inaction, of proposed alternatives, and of decisions." [17, loc. 157]. Value-focused thinking seeks to surface values that decision-makers hold, perhaps implicitly. These implicit values, when considered explicitly, often present *un*considered objectives that can lead to new, also unconsidered opportunities for potentially better solutions. Objectives, on Keeney's view, are simply "a statement of something someone desires to achieve" [17, loc. 482]. Objectives take two forms: fundamental objectives are "essential reason[s] for interest in a decision situation" [17, loc. 482], whereas means objectives simply enable achieving fundamental objectives [17]. Additionally, value-focused thinking encourages decision-makers to clarify their values explicitly, both in terms of definitions and in terms of a hierarchy of importance, which can lead to more measurable decision objectives and outcomes, which in turn enables more measurable costs and benefits to trade against each other in making better decisions.

In our study, we formulate the decision opportunity as, "which cyber product(s) do we buy to protect our control system and microgrid?" In formulating the decision opportunity this way, we extend Dhillon & Torkzadeh's research [10] on the value of information security, who note that information security lacks an inherent value proposition, by providing an explicit trade-off, the benefits of increased energy assurance. This insight – that cyber security is a means to an end – reliable energy – emerged from this work as well.

2. Research approach

We recruited our participants by identifying organizations in US Navy installations that both work with control systems and have a primary mission to provide energy services. We interviewed nine participants from three organizations [18], [29], representing a purposeful sample [6], [28] of facility managers and engineers responsible for making and/or informing decisions about cyber security of US Navy energy SCADA systems; these participants are both potential end-users as well as subject matter experts in the area. While representative of personnel at other US Navy installations, and reasonably representative of those at other DoD installations, these personnel in some ways represent an extreme case relative to non-DoD organizations [28] in that the consequences of losing energy assurance can lead to serious national and international security consequences [7].

During these interviews, we elicited values and objectives, and the participants clarified those values and objectives; we then organized the objectives into a means-ends network, in which we present the objectives graphically in a relational hierarchy [17]. The contribution of the analysts was to get participants thinking about the issues, eliciting expressions of value, clarifying into objectives, and organizing their objectives according to how and why they are important.

We developed an initial comprehensive interview protocol of eleven possible questions, based on previous research (particularly, e.g., [20], but our literature review more broadly). In practice, we narrowed the protocol to the first three questions, based on time constraints for each interview (three primary questions typically generated an hour-long interview for a participant). These questions were designed to surface values relating to SCADA system performance generally, SCADA system performance under cyber attack, and potential worst-case consequences of such an attack. Our original interview protocol included these eleven questions:

1. List what is important to you regarding the performance of CS networks.
2. Describe the ideal performance of a microgrid under a cyberattack (or electrical grid if no microgrid).
3. List the consequences of a worst-case scenario (within reason).
4. List what is important to you regarding cybersecurity performance for CS networks.
5. What are your current concerns relating to security threats on CS networks?
6. What can be done to raise awareness of cybersecurity threats on CS networks? (Maitland et al., 2013)
7. What are some of the issues that prevent the

effectiveness of CS networks? (Maitland et al., 2013)

8. How would you evaluate cybersecurity threats on CS networks?
9. How would you evaluate your vulnerability to cyber threats?
10. What would you tell other energy engineers to do to maintain cybersecurity, CS networking performance?
11. What can the owners of commercial-run power plants do to increase safety against cybersecurity threats?

We recorded participant answers on white board for ease of reference, and then asked two follow-up questions designed to clarify their answers and to convert their answers into objectives: "why is that important?", which helps identify fundamental objectives, and "what do you mean by that?", which helps identify means objectives [17], [20]. We captured the raw interview data for future analysis.

3. Analysis and results

3.1. Applying value-focused thinking

To illustrate our interview approach, a common initial answer to our question about consequences – an answer consistent with the extreme sample - was either "death" or "casualties". Participants typically clarified this answer ("what do you mean by that?") to an objective of "minimizing casualties", and then explained ("why is that important?") casualties meant loss of life, a fundamental failure and thus a fundamental objective. (Casualties, our participants explained, can affect mission accomplishment, but moreover, casualties from our participants' view, are inherently bad.) Similarly, another typically important aspect of SCADA system performance was "maximize resiliency", which our participants clarified meant "minimizing down time". This clarification process helped distinguish resilience from other characteristics, such as durability and flexibility; for our participants, resilience referred to responding to a problem (how long until it is resolved?), whereas flexibility referred to preventing outages and managing reductions in capability to sustain the most important functions.

From our interviews, we developed a means-ends network, graphically displaying the fundamental, or ends objectives in the smaller grouping at the top; the means objectives in the larger grouping; and their hierarchical interrelationships, represented by arrows showing how lower-level means objectives lead to higher-level objectives (see Figure 1). We discuss each objective below.

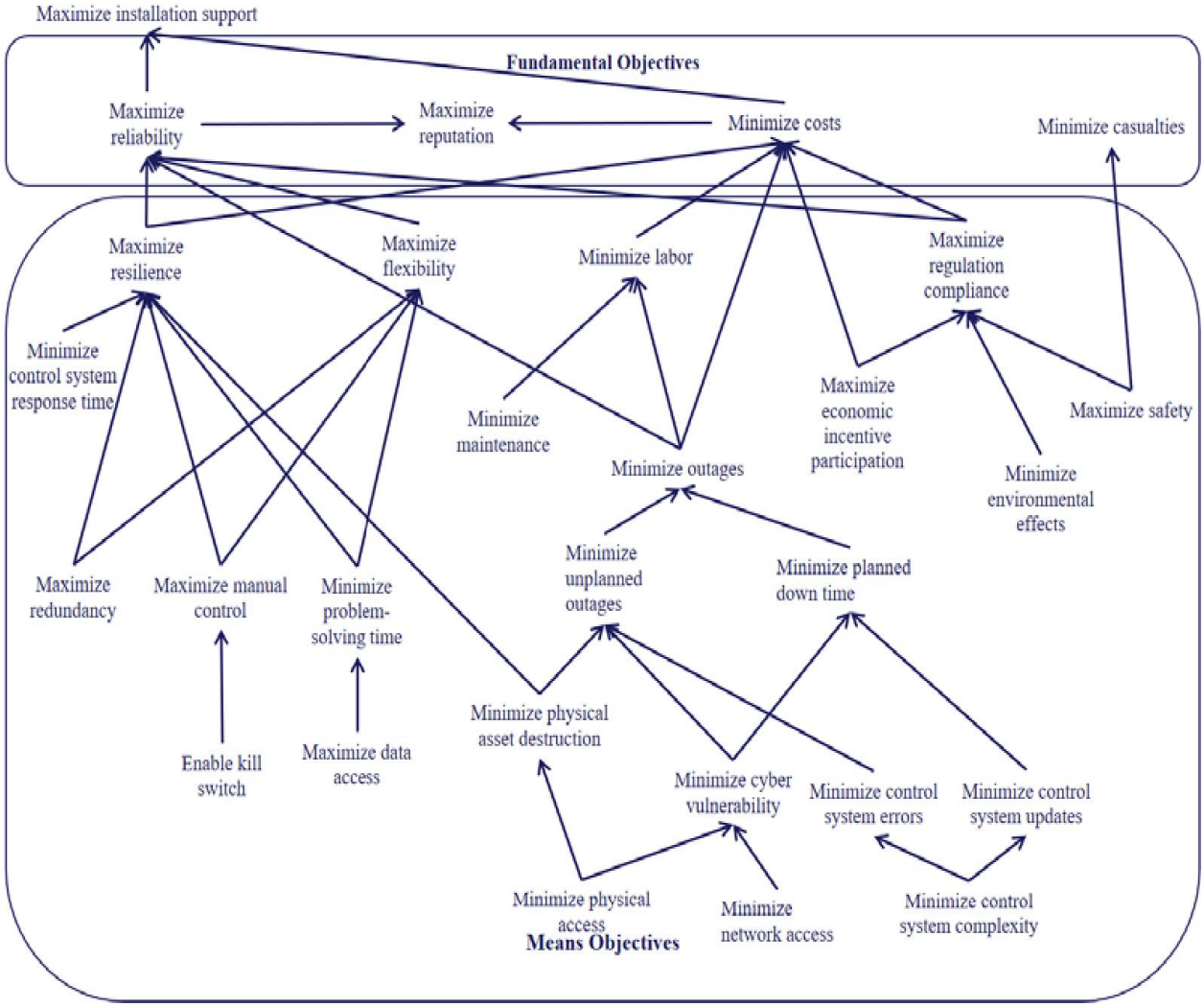

Figure 1: Means-ends objective network

3.2. Fundamental objectives

Our participants surfaced four fundamental objectives, which were common to all nine participants: maximizing reliability, maximizing reputation, minimizing cost, and minimizing casualties; two of these ends objectives contribute to a third ends objective, with maximizing reliability and minimizing costs contributing to maximizing the organization's reputation. The participants also surfaced a strategic fundamental objective, maximizing installation support, roughly defined as "providing the best possible energy support necessary to accomplish the mission". This defines the reason for operating the installations, thus it is a strategic objective, one of a "decision maker's broadest objectives" [17, loc 2348]. We discuss each fundamental objective in turn.

3.2.1. Maximize reliability

Each participant initially defined this objective somewhat differently, based in part on their organization, its mission, and their role in that organization. A synthesis of their definitions, however, is very similar to "the ability of an energy production system to provide consistent and expected levels of energy under stated conditions for a specified period of time" [12]. Participants identified several recurring means objectives as contributing to maximizing reliability, including minimizing outages, maximizing regulatory compliance, maximizing resilience and maximizing flexibility.

3.2.2. Maximize reputation

The participants all expressed a belief that their organization's reputation was both valuable and important. This was initially surprising as reputation does not immediately seem fundamental to Navy installations. However, several participants expressed that without the trust of their customers – those depending on installation services – the customers would stop relying on them which would degrade their ability to do the mission and incur additional costs. This fundamental objective appears to manifest two other fundamental objectives, maximizing reliability and minimizing cost. This is consistent with a general belief that government functions better when the public trusts it [24].

3.2.3. Minimize cost

All nine participants mentioned minimizing costs – labor, materials, time, and money – as important. SCADA systems contribute to greater efficiency, thus decreasing costs, and microgrids provide redundancy against commercial grid outages. One participant noted that by keeping energy costs low, that provider was able to bill its customers on the installation at a lower cost, thus preserving its customers' resources to spend on their organizational missions.

3.2.4. Minimize casualties

Perhaps because of the larger Navy and DoD missions, all participants were concerned with preventing death and casualties. This belief appears based in part on both regulatory guidance and experience. Safety is a "vital enabler" to the mission [23], and [3] reports over 150 deaths per year are related to electrical systems.

3.3. Means objectives

The nine participants identified twenty-four means objectives, organized in a network in figure 1. While all participants agreed on the four fundamental objectives, not every participant mentioned every means objective. Here, we discuss six of the most important means objectives, including the most-frequently mentioned means objectives, maximizing resilience, minimizing labor, maximizing regulatory compliance, maximizing flexibility, minimizing cyber vulnerability and minimizing control system complexity. As means objectives move further away from fundamental objectives they can become more like options or alternatives – the kill switch objective in the bottom left of Figure 1 is an example. We generally kept the network to objectives, stopping before specifying decision-specific alternatives or options (parts of alternatives).

3.3.1. Maximize resilience

All nine participants viewed resilience as an important means objective, contributing directly to two ends objectives, maximizing reliability and minimizing costs. As discussed elsewhere, resilience for our participants meant recovering from disruptions [9]. Control systems maximize resilience, e.g., by minimizing response times in disruptions, and identifying the location and likely cause of disruptions, this minimizing problem-solving, trouble-shooting, and repair times. Participants observed that redundancy improves resilience. Finally, one participant noted that having the ability to disconnect the control system and use manual controls was an important aspect of resilience.

3.3.2. Minimize labor

SCADA systems increase efficiency, thus reducing the amount of labor required to do a job [33], and ultimately contributing to the ends objective of minimizing costs. For example, these systems can minimize necessary maintenance and optimize maintenance times. Such labor savings were important to all nine participants.

3.3.3. Maximize regulatory compliance

Regulatory compliance enables both cost minimization and greater reliability. One participant noted that compliance avoids costs, an ends objective; to illustrate this, the Navy installation at Joint Base Pearl Harbor paid a fine approaching $100,000 based on an environmental violation [22]. This fine reduced resource available for other needs, including ensuring reliable energy, another ends objective.

3.3.4. Maximize flexibility

Our participants believed greater flexibility increased reliability, an important ends objective. A flexible control system can maintain its distribution despite supply and demand fluctuations [26], thus contributing to reliability. The greater availability of renewable energy sources, such as hydroelectricity and solar, increase, energy systems has increased the need for flexibility as well [26].

3.3.5. Minimize cyber vulnerability

All nine participants surfaced concerns about cyber vulnerabilities, but not all nine agreed on the magnitude of those vulnerabilities. Some were more concerned with nation state attacks, such as that on the Ukraine, while others discussed non-state hackers as a threat. All agreed that minimizing physical and network access is an important safeguard. This means objective contributes directly and indirectly to several other means objectives, and ultimately to both maximizing reliability and minimizing costs as ends objectives.

3.3.6. Minimize control system complexity

Our participants noted that minimizing control system complexity is an important means objective that contributes to minimizing errors and updates, both of which operate through several other ends objectives to reduce reliability and increase costs.

3.4. Identifying tradeoffs

Our participants routinely identified two important trade-offs they must consider in making decisions in this context. First, they consider trade-offs between functionality and security. Perhaps based on their functional backgrounds, our respondents viewed functionality and security as potentially-competing objectives; improving security, in their view, could require decreasing functionality. For example, while providing off-site access to the system might enable managers to respond quickly to failures, it would also create an access point for a cyber attacker. As one participant noted, "The most secure system is one that doesn't work." All nine participants agreed on what functionality and security mean, and that both functionality and security are important; they were divided on how to balance the trade-off between the two considerations.

Participants' preferences on the best way to balance the trade-off seems to be related to the participant's role in the organization. A correlation that appeared in our small sample is that those with greater responsibility, e.g., over many installations, seemed to weigh (cyber)security as a greater (but not overriding) need. Conversely, an engineer responsible for one installations' system, with a primary concern of ensuring customers had the power necessary to perform their missions, reported a greater (but again not overriding) concern for functionality. Rather than worrying over cybersecurity, this participant reported that their installation lost power to an entire circuit when a gecko electrocuted itself on a wire; this participant was more concerned about making investments that would ensure uninterrupted access against these non-cyber disruptions. Regardless of their respective roles in the organization, all participants agreed that the two considerations must be weighed in every situation.

The second trade-off our participants commonly noted was between user control and automated control. While not a universal consideration for all nine participants, the importance of being able to assume manual control was very important to some participants.

4. Discussion, conclusions, limitations, and recommendations

Our participants' means-ends objective network tells a story. Their overarching mission is to maximize installation support, and that involves maximizing four fundamental, or ends, objectives: developing the reputation of providing reliable energy at minimal cost, while minimizing casualties. A hierarchy of means objectives contribute to achieving these ends objectives, and thus their mission.

All our participants were clearly oriented towards the strategic objective of mission support, but they were split on how best to achieve it. While the network in Figure 1 accurately reflects the relationships among the ends and means objectives, it does not necessarily reflect each participant's individual ends objectives, nor does it reflect the relative importance – which differed among participants – they apply to those objectives.

That said, achieving this balance is important, and we suggest subject matter experts closer to the end user – where the mission is actually supported – are best able to make these tradeoffs, with those higher in the organization providing oversight of the decisions.

Our participants valued customer support; they believed maximizing reliability is an important ends objective. Cybersecurity was important to varying degrees to all participants, but for all it was clearly a means objective – important because it influences the other objectives, and the ability to meet the mission, i.e. maximize installation support. All participants were very cognizant of the installation's mission, especially the most critical functions. One of the benefits of VFT and understanding which objectives are means (vs. ends) and which ends they contribute to is that it can help stakeholders reduce focus on tension and trade-offs and instead identify new alternatives or "potential choices to pursuing your [means] objectives," which can increase the ability to achieve the fundamental objectives [32].

Our study focuses on three naval installations. We've suggested our sample is reasonably representative of other military installations, but the small sample size is nonetheless a limitation of our study. Future research should explore whether and how our findings apply to other installations across all services, and to organizations beyond the military. Our results also suggest that decision-makers' values can depend on their position and role in the organization, but our sample clearly limits our ability to draw strong, well-supported conclusions. Future studies could address how the position and role in organizational hierarchies influences the development of ends-means objectives.

Ongoing and future research can consider how best to implement the means-ends network and the tradeoffs. For example, ongoing research within the Navy is formulating a return on investment model for cybersecurity investment based on user values. Different decision-making approaches can also inform the analysis. For example, multiple-objective decision analysis [11] can assess qualitative outputs, such as value focused thinking delivers, quantitatively. Finally, future research might explore developing standard measures the means and ends objectives we identify.

5. References

[1] B.J. Adams and C.C Hartner, Cyber-Defense Return-on Investment for NAVFAC Energy Technologies, Naval Postgraduate School, Monterey, CA, 2017.

[2] S.V Broekhoven, N. Judson, J. Galvin, and J. Marqusee, "Leading the Charge: Microgrids for Domestic Military Installations", IEEE Power and Energy Magazine, *11*(4), pp. 40–45. doi: 10.1109/MPE.2013.2258280

[3] Bureau of Labor Statistics, National Census Of Fatal Occupational Injuries in 2015, Washington, DC, Bureau of Labor Statistics. 16 December 2016.

[4] Center for Naval Analysis Military Advisory Board, National Security and Assured U.S. Electrical Power, Arlington, VA, Center for Naval Analysis, November 2015.

[5] G. Clouser, SCADA getting smarter. Retrieved from https://www.schneider-electric.com/solutions/ae/en/med/691367152/application/pdf/2414_scada-getting-smarter-_-midstream-business-ap.pdf, 1 April 2013.

[6] J.W. Creswell, Qualitative Inquiry & Research Design: Choosing Among Five Approaches, Thousand Oaks, CA, Sage Publications, Inc., 2013.

[7] Department of Defense (DOD), "About Department of Defense", Retrieved from https://www.defense.gov/About/, 27 January 2017.

[8] Department of Energy (DOE), "Valuation of Energy Security for The United States", Retrieved from https://energy.gov/sites/prod/files/2017/01/f34/Valuation%20of%20Energy%20Security%20for%20the%20United%20States%2 0%28Full%20Report%29_1.pdf, 2017a.

[9] Department of Energy (DOE), "Department Of Defense Installation Energy Resilience" [PowerPoint slides], Retrieved from https://energy.gov/sites/prod/files/2017/06/f34/5_Storage%20and%20Microgrids%20Panel%20-%20Ariel%20Castillo%2C%20DoD.pdf, 2017b.

[10] G. Dhillon and T. Gholamreza, "Value-Focused Assessment of Information System Security in Organizations", Information Systems Journal (16), pp. 293-314, 2006.

[11] R. Dillon-Merrill, G. Parnell, D.L. Buckshaw, W.R. Hensley, and D.J. Caswell, "Avoiding Common Pitfalls in Decision Support Frameworks For Department Of Defense Analyses", Military Operations Research, *13*, pp. 19–31. https://doi.org/ 10.5711/morj.13.2.19, 2008.

[12] Energy-101.org, "Reliable", Retrieved November 14, 2017, from http://www.energy-101.org/topics/choose-topic/definitions/reliable, 2017.

[13] S. Gorman, "Electricity Grid in U.S. Penetrated By Spies", Wall Street Journal, Retrieved from https://www.wsj.com/articles/SB123914805204099085, 8 April 2009.

[14] L. Graham, "Cyberattacks Are Surging and More Data Records Are Stolen", Retrieved from https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html, 20 September 2017.

[15] Idaho National Laboratory, "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector", Retrieved from https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the% 20U.S.%20Electric%20Sector.pdf, August, 2016.

[16] Inductive Automation, "What is SCADA? [Commerical]", Retrieved from https://inductiveautomation.com/what-is-scada, 2017.

[17]. R.L. Keeney, Value-Focused Thinking: A Path To Creative Decisionmaking, Harvard University Press, Cambridge, MA, (1992).

[18] S. Kvale, and S. Brinkmann, Interviews: Learning The Craft of Qualitative Research Interviewing (2d). Sage Publications, Inc., Thousand Oaks, CA, 2009.

[19] A. Lantero, "How microgrids work", Retrieved from https://energy.gov/ articles/how-microgrids-work, 17 June 2014.

[20]. N. Maitland, C. Barclay, and O.B. Kweku-Muata, "A Value Focused Thinking (VFT) Analysis to Understanding Users' Privacy and Security Dynamics on Social Networking Services". In Proceedings of SIG GlobDev Sixth Annual Workshop. Milan, Italy: Special Interest Group for ICT in Global Development. Retrieved from http://globdev.org/files/proceedings2013/paper_19.pdf , 14 December 2013.

[21]. McConnell, J.M. (2008). Annual threat assessment of the director of national intelligence for the senate select committee on intelligence. Washington, D.C.: Director of National Intelligence.

[22]. "Navy Pays EPA Fine To Settle Cesspool Case", Honolulu Star-Advertiser, Retrieved from http://www.military.com/daily-news/2017/04/11/navy-pays-epa-fine-settle-cesspool-case.html, 11 April, 2017.

[23]. Naval Facilities and Engineering Command, Safety Plan 2013, Retrieved from https://navfac.navy.mil/content/dam/navfac/NAVFAC%20Atlantic/NAVFAC%20Southwest/PDFs/SF_docs/sw_sf_2013_safety_plan.pdf, 2013.

[24] Organization for Economic Co-Operation and Development (OECD), "Trust in Government", Retrieved from http://www.oecd.org/gov/trust-in-government.htm, 2017.

[25]. E. Ortiz, "Microgrids Sustain Power During Natural Disasters", Retrieved from http://www.govtech.com/dc/articles/Microgrids-Sustain-Power-During-Natural-Disasters.html, 20 October 2015

[26] G. Papaefthymiou, K Grave, and K. Dragoon, Flexibility Options in Electricity Systems. Berlin, Germany: ECOFYS. Retrieved from https://www.ecofys.com/files/files/ecofys-eci-2014-flexibility-options-in-electricity-systems.pdf, 10 March 2014.

[27]. G.S. Parnell, Value-Focused Thinking Using Multiple Objective Decision Analysis, Methods for Conducting Military Operational Analysis: Best Practices in Use Throughout the Department of Defense, pp. 619–656, 2007.

[28]. M.Q. Patton, Qualitative Research & Evaluation Methods: Integrating Theory and Practice (4th). Sage Publications, Inc., Thousand Oaks, CA, 2015.

[29]. H.J. Rubin, and I.S. Rubin, Qualitative Interviewing: The Art Of Hearing Data (3d), Sage Publications, Inc., Thousand Oaks, CA, 2012.

[30] J. Simon, E.D. Regnier, and L. Whitney. A Value-Focused Approach to Energy Transformation in the United States Department of Defense, Decision Analysis 11(2) pp. 117-132, 2014.

[31] J. Romero-Mariona, R. Hallman, M. Kline, G. Palavicini, J. Bryan, J. San Miguel, L. Kerr, M. Major and J Alvarez, An Approach to Organizational Cybersecurity. In: Chang V., Ramachandran M., Walters R., Wills G. (eds) Enterprise Security. Lecture Notes in Computer Science, Vol 10131. Springer, Cham, pp. 203–222, 2017.

[32] J. Siebert, Ralph Keeney´s (Duke University) Talk on Value-Focused Thinking at the University Of Bayreuth [Video file], Retrieved from https://www.youtube.com/watch?v=5nhBDgvjOy4, 30 July 2013.

[33] J. Weinberger, "SCADA Benefits Without SCADA Costs", Retrieved from www.wwdmag.com/analytical-equipment/scada-benefits-without-scada-costs, 11 November 2010.

[34]. K. Zetter, "Inside The Cunning, Unprecedented Hack Of Ukraine's Power Grid", Retrieved from https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, 3 March 2016.