Misconceptions and Barriers to Adoption of FOSS in the U.S. Energy Industry

Victor Kuechler, Carlos Jensen, Deborah Bryant

Misconceptions and Barriers to Adoption of FOSS in the U.S. Energy Industry

Victor Kuechler[1], Carlos Jensen[1], and Deborah Bryant[2]

[1]School of Electrical Engineering and Computer Science
Oregon State University, Corvallis, OR, USA
{kuechlej@onid.orst.edu, cjensen@eecs.oregonstate.edu}
[2]The Bryant Group, Portland, OR, USA
{deborah@debbryant.com}

Abstract. In this exploratory study, we map the use of free and open source software (FOSS) in the United States energy sector, especially as it relates to cyber security. Through two surveys and a set of semi-structured interviews—targeting both developers and policy makers—we identified key stakeholders, organizations, and FOSS projects, be they rooted in industry, academia, or public policy space that influence software and security practices in the energy sector. We explored FOSS tools, common attitudes and concerns, and challenges with regard to FOSS adoption. More than a dozen themes were identified from interviews and surveys. Of these, drivers for adoption and risks associated with FOSS were the most prevalent. More specifically, the misperceptions of FOSS, the new security challenges presented by the smart grid, and the extensive influence of vendors in this space play the largest roles in FOSS adoption in the energy sector.

Keywords: Adoption, barriers, energy sector, case studies

1 Introduction

The energy industry in the United States is changing in many ways. Its growing and diverse energy needs have created a need to collect new types of data and network systems that have historically been "siloed". This new networked grid uses computer-based remote control and automation to intelligently manage the energy as it moves between energy producers and consumers [22]. The American Reinvestment and Recovery Act of 2009 provided $3.4 billion dollars of grant money in the form of the Smart Grid Investment Grant to support the modernization of the power grid [23]. As of July 2012, 99 projects have been funded, all of which deploy smart grid technology with a chief goal to reduce peak and overall electricity demand and operation costs; improve asset management, outage management, reliability, and system efficiency; and reduce environmental emissions [23]. The drive to establish a "smart grid" has introduced new technology, but also created new security risks and challenges [12].

As the modernization of the North American power grid continues, the security of energy delivery systems, control systems, and information sharing must be a high

adfa, p. 1, 2011.

priority. Software, whether supporting operational systems or security technology, is a key element and must be central to any related security discussion. These complex problems require collaboration between regional energy generators, government agencies, standards bodies, and security professionals. Leveraging a community of like-minded individuals who share similar needs and goals can increase the adaptability and flexibility of cyber security initiatives and software within the energy sector.

The free and open source software (FOSS) movement is one of the only distributed software development models that brings together developers from many different domains of knowledge while supporting a common goal of sharing information, collaborating to improve systems, and leveraging diverse knowledge to create some of the most effective software in cost and implementation.

We conducted an exploratory study, funded by the Energy Sector Security Consortium (EnergySec), to map out the use of FOSS software in the energy sector, especially as it relates to cyber security. The motivation for this study was rooted in the common perception that FOSS is less secure due to availability of its source code. Although this perception has existed since the initiation of FOSS, a 2010 study from Boston College supports this claim, concluding that open source software is at greater risk of exploitation [19]. Despite this perception, many government agencies have adopted FOSS, some of which consider FOSS an equal to proprietary software, including the Department of Defense [30].

Through a survey, we identified seven representative organizations and FOSS projects within the energy sector and identified the tools they use, licenses used, legal concern or solutions, and challenges and hurdles they faced or have overcome in adopting FOSS. We conducted semi-structured interviews with key members of each organization or project with a goal to:

1. Understand the extent in which FOSS participates in energy sector, and vice versa
2. Understand the barriers to the adoption of FOSS and the process of contributing to FOSS
3. Record the best practices derived from current initiatives in FOSS, the energy industry, and government.

2 Background

2.1 Introduction to FOSS

FOSS development is a collaborative process, thus understanding its culture is crucial. The open and altruistic nature of FOSS is appealing to many users and developers. FOSS development is predominantly volunteer-driven, built on a model of computer-mediated, asynchronous communication and collaboration. Many people today characterize FOSS in this way.

It may be surprising to learn that large projects like Linux, Firefox, and Apache are the exception rather than the rule; most FOSS projects are developed by a handful of people. In a 2002 study of the most active mature projects (i.e., projects not ramping-up) on Sourceforge.net, the average project has four developers, and the majority has

one [14]. In larger projects, more than half of developers only have regular contact with one to five other project members [10].

Because FOSS projects rely on volunteers, users are viewed as potential contributors. Ye and Kishida and Herraiz et al. studied "role transition" from users (using the software, motivating developers) to bug reporters (reporting and documenting problems, submitting feature requests) to active developers (contributing code) [32], [13]. FOSS communities and projects operate as meritocracy, where a programmer's ability and contributions to a project shape how the community perceives them.

FOSS's inherent volunteer nature highlights its adaptability to meet the needs of specific groups and niche markets. Volunteers work, initiate, or develop projects that either meets personal needs or the purpose and goals of other like-minded individuals [16]. FOSS has continually adapted to meet the needs of almost every domain of the software ecosystem. In 2005, Walli et al. evaluated the use of FOSS in U.S. companies. They found that 87% of the 512 companies they surveyed use FOSS [30]. They also discovered that companies and government institutions use FOSS because it reduces IT costs, delivers systems faster, and makes systems more secure. Large companies with annual revenue over $1 billion saved 3.3 million dollars, medium-sized companies saved an average $1 million, and smaller companies (<50 million) saved $520,000. They also discovered that after years of using FOSS software stacks (Linux, etc.) and web server software, companies were beginning to use other FOSS business software instead of proprietary software [30].

In 2007, David Wheeler also found that FOSS has a significant market share and "is often the most reliable software and I many cases has the best performance" [31]. Similarly, in 2011, Coverity compared open source and proprietary software quality and find "open source quality is on part with proprietary code quality, particularly in cases where codebases are of similar size" [5]. The open source ideal has been a part of government in spirit since the 1960s, but only the real potential of FOSS has only been advocated since the late 90s. Several publications, "A Case for Government Promotion of Open Source Software" by Mitch Stoltz; "Open Source Code and the Security of Federal Systems" by a multiagency working group (National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism); "Opening the Military to Open Source" by Maj. Deiferth, USAF; and "The Simple Economics of Open Source" by the Bureau for Economic Research was published in the late 90s and early 2000s. These publications started some of the first serious discussions of FOSS adoption in government and led to a variety of open source solutions being deployed by the U.S. government in the early 2000s. This included the NSA's release of SELinux—an operating system integrated with a suite of FOSS pen testing and security tools, and DHS's Homeland Open Security Technology (HOST) program in 2004.

In 2008, The Open Source Census reported that European government entities had the highest use of FOSS per computer scanned, with an average of 68 different open source packages installed per computer. The United States averaged 51 open source packages per computer [18].

Between 2009 and 2012, several advocacy groups were established to promote the opportunities of FOSS in U.S. government, including Open Source for America—a coalition of companies, academic institutions, communities, and individuals; and

CivicCommons—a community-driven app store that brings people together to share their solutions, knowledge, and best practices to improve government.

In 2003, the Department of Defense approved the use of open source in their agency [26], and later in 2012, they released a memorandum stating that open source and proprietary software are considered equal [30]. NASA also launched code.nasa.gov—a repository of FOSS projects currently in development at NASA.

So far, the energy sector has not been part of the efforts to adopt FOSS.

2.2 Software Security in the Energy Sector

Security, including cyber security, has long been an important concern for the energy sector, given the electric grids' importance as a key infrastructure. In the past, this was in large parts achieved through the isolation of control systems from more publicly accessible and exposed systems, a practice the industry refers to as "siloing." This practice, in theory, means that for control systems, cyber security largely devolved into a problem of physical security.

This model has proven difficult to implement. The temptation or need to network critical systems, be it for monitoring, maintenance, reporting, or to optimize operations means that in practice these systems have been more exposed than the industry has at time been willing to admit.

Robert J. Turk's "Cyber Incidents Involving Control Systems", published in 2005 for the U.S. Department of Homeland Security" summarizes 120 known cyber security incidents [27]. They found that forty-two percent of incidents derived from mobile malware, twenty-eight percent from hacks, twenty-six percent from misconfiguration, and four percent from penetration tests or audits. Thirty-eight percent of these incidents occurred from within the organization, sixty-one from outside the organization, and one percent were unknown. Thirty-three percent of the perpetrators were insiders (contractors, former employees, and current employees), forty-three percent were malware authors, and four percent were foreign nations, competitors and unknowns [27].

In January 2003, the "Slammer" worm disabled the computerized safety monitoring system at the Davis-Besse nuclear power plant in Ohio. Stuxnet is one of the most well-known cyber threats in history. Its primary goal was to reprogram Siemens industrial control systems, but as of September 29, 2010, Stuxnet had infected about 100,000 computers after it escaped on an employee's laptop from Iran. 60% of infected hosts are in Iran, but it has spread to more than 155 countries [8]. Since Stuxnet, other cyber attacks have occurred around the world with both criminal and commercial intent that conduct both espionage (collecting data) and sabotage (destroying data). This includes the Duqa and the Flame virus, a trojan similar to Stuxnet that scans computer systems for key private information on very specific machines around the world.

Hahn and Govindarasu explain that "The coupling of the power infrastructure with complex computer networks substantially expand[s] current cyber attack surface area […]" [12]. In 2011, the Energy Sector Control Systems Working Group released the "Roadmap to Achieve Energy Delivery Systems Cyber security." This roadmap ad-

dresses the growing vulnerabilities in energy delivery systems, including "control systems, smart grid technologies, and the interface of cyber and physical security—where physical access to system components can impact cyber security" [2].

"This update recognizes that smart technologies (e.g., smart meters, phasor measurement units), new infrastructure components, the increased use of mobile devices, and new applications are changing the way that energy information is communicated and controlled while introducing new vulnerabilities and creating new needs for the protection of consumer and energy market information" [2].

The focus on the smart grid and automated control systems like SCADA has opened up for a variety of new threats, business practices, market trends, regulations, and technologies. Among these are a few important issues [2]:

- "Growing reliance on commercial off-the-shelf technologies"
- "Increasing reliance on external providers for business solutions and services, which introduces additional cyber and physical reliability challenges"
- "Increasing interconnection of business and control system networks"
- "Increasing reliance on the telecommunications industry and the Internet for communications"

Though the energy sector does work with unique systems, and have some unique security concerns and requirements, some of these do overlap with general IT security. It is therefore not surprising to find these groups using FOSS tools such as NMAP, OpenADR, OpenPDC, and Hadoop.

The industry has also developed some unique FOSS solutions. In April 2012, Pacific Northwest National Laboratory announced they would be open sourcing a homegrown, host-based security sensor to encourage community feedback and participation. The cyber tool is called the Hone Project and it "pinpoints which applications or processes infected machines and an external network they are using to communicate" [17].

These efforts notwithstanding, there appears to be a marked dearth in energy sector FOSS projects, including cyber security related projects.

3 Study Methodology

Our goal was to catalogue experiences and attitudes with regard to the adoption and development of FOSS in and for the U.S. energy sector, especially related to cyber security. We used a mixed-method study design, implementing both online surveys—to reach a broad audience, and interviews—to gather rich data.

The first step of our process was identifying key FOSS projects, and organizations that operate within the energy sector. We started from a list of contacts from EnergySec. We scoured online sources, industry papers, and research articles for others who might provide insight.

Next we emailed each potential contact, explaining the purpose of the study and provided them with a link to our surveys. Two surveys were used, one for people

working the energy sector and another for contributors to FOSS projects used in the energy sector. Subjects who identified with both groups filled out both surveys.

Seven semi-structured interviews were conducted with selected survey respondents. Although a regimented series of questions were developed, the semi-structured approach allowed us to explore issues brought up by subjects, or their thinking.

We used open coding as our method of data analysis. Open coding is a method of grounded theory that provides a way for researchers to procedurally organize and analyze qualitative data [3]. We generated codes from our initial survey responses. These codes were discussed among the researchers and used to define categories of comments and concepts in the data. For example, when one participant commented that "business drivers force the energy industry to network their systems […]," this was tagged with the code "barrier/risk"). Interview transcripts, notes, and surveys answers were analyzed line-by-line and coded independently by two researchers. These codes were compared and refined. This process was repeated until there was sufficient agreement about the codes and their meaning. After all data elements coded, common themes were identified.

The burden of proof is relatively low in exploratory studies; the goal of this study was not to prove anything statistically, but to identify broad themes and concepts. Thus our sample sizes were small, and we did not bother with statistical analysis.

3.1 Sampling

We divided our subjects into three categories: energy producers and grid operators, the solution providers they rely on (IT contractors, software and hardware companies, etc.), and FOSS projects. All three groups were represented in our surveys, and we wanted to make sure all were represented in our interviews. We therefore chose to interview representatives from Portland General Electric, the Tennessee Valley Authority, Utilisec, Dell SecureWorks, GADS/OS, Green Energy Corp, and the Grid Protection Alliance. Table 1 shows how these organizations were classified in our study.

Table 1. List of organizations

Energy Producers	Solutions Providers	FOSS Projects
Portland General Electric	Utilisec	GADS/OS
Tennessee Valley Authority	Dell SecureWorks	Green Energy Corp
		Grid Protections Alliance

Portland General Electric (PGE). PGE serves over 800,000 customers over 52 cities in Oregon and has deployed 825,000 smart meters [24]. PGE can offer insight into their day-to-day operations in both IT and operations from the perspective of a midsize energy provider.

Tennessee Valley Authority (TVA). TVA is owned by the U.S. Government and provides electricity to 9 million people throughout the southeast United States, being

the 5th largest provider in terms of revenue [1]. TVA represents a larger energy provider with more diversified resources and needs.

Utilisec. UtiliSec offers cyber security services specifically tailored for electric utilities, with expertise in smart grid security, low-level analysis, and penetration testing. They offer training as well as guidance on real-world systems and security architecture review, penetration testing, and policy composition [28].

Dell SecureWorks®. Secureworks is a provider of information-security-as-a-service, processing more than 13 billion security events and 30,000 malware specimens each day[6]. Dell SecureWorks have extensive experience partnering with utility providers, helping them solve security challenges with industrial control systems and SCADA networks, smart grid technologies, advanced metering infrastructure and other critical IT assets. Currently, they are working on Snort 2.9 (Modbus and DNP3)—a network intrusion detection system for Unix.

GADS Open Source (GADS/OS). GADS/OS is a FOSS project that collects and analyzes performance and event data in a power grid and reports it to NERC. More than 200 companies and 3,800 generating units use GADS/OS in the United States and around the world [9].

Green Energy Corp. Green Energy Corp provides software solutions and software engineering services to communications, utilities, and energy companies. Green Energy Corp developed a FOSS platform called Greenbus, which enables utilities to integrate legacy technologies into their smart grid [25].

Grid Protection Alliance. The Grid Protection Alliance (GPA) is a non-profit aimed at supporting the development of security-related IT solutions for the energy sector [11]. GPA's projects include the PMU Connection Tester, openPDC, openPG, and SIEGate.

4 Findings

FOSS is used more extensively in the energy sector than we initially thought, though most organizations are consumers rather than producers, and most use is behind the scenes. All participants noted, in some fashion, that FOSS was not seen as unreliable or undesirable, though several commented that the FOSS support model could cause problems.

Contributing to FOSS is much more rare than adoption, primarily due to real or perceived intellectual property and liability concerns, uncertainty about how to build community, lack of best practices, and other internal roadblocks. Some concerns were raised about the need to maintain good relations with solution providers and not wanting to appear in direct competition for fear of liability or regulatory oversight. These

are common concerns of many industries where there is a lack of strong leadership and examples of FOSS adoption.

FOSS is currently used mostly for ad hoc security solutions. By this we mean that system administrators use one-off FOSS tools to complete small tasks, while proprietary enterprise software is used for critical system management and controls (e.g., SCADA). One participant claimed that "almost every tool used by testers is open source; Backtrack (Linux distribution) is a good example."

On the IT side, use of FOSS seems common, and decisions to adopt FOSS seem to be made based on an assessment of need and availability, as well as vendor support. On the operations side of these organizations, we found that security needs or concerns are downplayed and sometimes ignored due to the supposed separation between IT and production systems. This separation is not always real, and there have been many instances where control systems have been linked to IT systems, either intentionally or accidentally, and security has been breached. As the industry moves to implement a smart grid, the need to network the two sides, as well as consumers and producers, will further weaken the security through isolation model.

4.1 Themes

Eleven codes were generated from the interviews and surveys: *perceptions*, *future needs or trends*, *drivers*, *barriers*, *risks*, *potential opportunities*, *use cases*, *best practices*, *ad hoc solutions and policy*, *reasons for using open source*, *and business models.* These codes were paired down into two categories: *drivers for adoption* and *risks and barriers*. Table 2 and 3 list each theme that was shared between interviewees or unique to an organization or FOSS project.

Table 2. Drivers for adoption

EP: Energy Producer; **SP:** Solutions Provider; **FP:** FOSS Project;
#: Number of respondents who agreed

Theme	**EP**	**SP**	**FP**	**#**
FOSS has greater flexibility and functionality	X	X	X	5
FOSS solutions are already being developed internally	X	X	X	4
Smart grid initiatives require more focus on security	X	X	X	4
Control systems and IT were separate, need to integrate		X	X	4
FOSS decreases license cost	X		X	4
NERC/CIP requires compliance	X	X	X	3
Staff know FOSS tools	X		X	3
FOSS is more secure and reliable	X		X	3
FOSS security tools can be leveraged to face overlapping problems	X	X		3
FOSS decreases vendor lock-in			X	3
Homegrown FOSS solutions are currently being shared	X		X	2
FOSS is currently used ad hoc and in other contexts	X	X		2
FOSS can support niche and legacy systems		X	X	2

Companies will (and can) pay for custom development of FOSS			X	2
FOSS provides a lower support cost	X			1
FOSS provides a lower time to acquisition			X	1

Table 3. Risks and barriers

EP: Energy Producer; **SP:** Solutions Provider; **FP:** FOSS Project;
#: Number of respondents who agreed

Theme	**EP**	**SP**	**FP**	**#**
Uncertainty exists about the stability of FOSS for business support	X	X	X	5
Energy sector follows more than it leads, risk averse, regulation driven	X	X	X	5
Distrust between control engineers and other IT professionals	X	X	X	4
Energy producers rely on a small number of vendors. Vendors lack FOSS support	X		X	4
Domain expertise is needed to install/develop core services and standards	X	X	X	4
Lack of solutions (including FOSS) for control systems	X	X	X	4
Reluctance to acknowledge vulnerability of control systems		X	X	4
Energy providers prefer to buy complete solutions	X			1
Jurisdiction (e.g., federal vs. private, regional) issues limit collaboration			X	1

From these codes, we identified themes, significant converging perceptions, drivers, barriers and risks associated with the use and adoption of FOSS in the energy sector. The themes we identified are the following:

4.1.1 FOSS as an "unknown" or "hippy movement"

Many in the energy sector perceive FOSS as a "hippy movement," an ad-hoc effort rather than an effective software model. When FOSS is suggested, most people don't know where the support comes from, which is crucial in energy operations. One FOSS project manager noted that "every client ultimately asks 'how do you stay in business? Will you be there when I need you?'" This same person finds himself doing presentations because people "don't understand open source." One energy producer prefers to pay for something because it guarantees a complete product. This might explain why FOSS is currently used in an ad hoc way with very little, if any, organized discussion of open source adoption aside from small in-house teams or regional collaborators. On the other hand, these perceptions do not apply to more well-known FOSS systems like Linux.

4.1.2 Separation between controls engineers and IT

The division of jurisdiction between operations engineers and IT has impeded the broader adoption of FOSS in the energy sector. Systems are being secured by home-

grown security teams (often out of the control systems ranks). With the onset of the smart grid, utilities are forced to modernize and network their control systems. Several subjects noted that controls engineers perceive IT engineers as "cowboys". For this reason, many control engineers do not want to let the IT staff "mess around" with security on their systems. In essence, controls engineers try to shut IT folks out of the system. One interviewee noted that there are not enough security professionals in energy sector. Increasing IT numbers could offset these tensions.

4.1.3 Vendor dependence

It was emphasized that a small number of vendors supply the majority of software solutions to the energy sector. The current mentality is to buy whatever the vendor is supplying rather than advocating for new solutions from these vendors, which means that these vendors decide what software is adopted. Without the support of vendors, FOSS will not be a viable option for security. If a FOSS solution fails, the liability falls on the organization and not the software developers or the vendor. If utilities pool their resources they can get vendors to meet changes and add features they need. As noted by one interviewee, "if you get some of the bigger vendors moving in that direction [of open source] then you will have change."

4.1.4 Legal concerns

The energy sector is a risk-averse community that follows more than it leads. As one energy producer commented, "the more you use a standard practice, the less questions auditors ask." Regulatory bodies have shaped the adoption and use of software in the energy sector and there are penalties for noncompliance. Common practices, similar tools and methodologies will create simpler audits. This issue presents a variety of legal uncertainty involving the adopting FOSS, which is outside the norm. The energy sector needs one or two strong and influential organizations to prove that FOSS works. Currently, the regional division of the energy sector (e.g., Texas operates independently, the Pacific Northwest collaborates regionally, etc.) does not simplify the task, making it harder to look for role models across regions.

5 Discussion

Our findings show that FOSS is used extensively in the energy sector, though most of it is relatively informal, and few organizations are large-scale users, much less producers of FOSS. As Table 3 demonstrates, interviewees confirmed that FOSS offers significant benefits in cost and flexibility. However, FOSS is still used in most cases as a cursory solution to improve task efficiency or detect network intrusions. FOSS is not used as a primary solution for managing critical systems.

We believe that one of the main reasons for this ad-hoc use of FOSS is a lack of discussion in the energy sector community about the use of FOSS and its potential benefits. Such a FOSS discussion could create a means to petition and influence the market (e.g., vendors, etc.) to deliver more FOSS solutions. The energy community

can also leverage best practices, potential opportunities, and the community itself to subdue the risks and barriers that have inhibited FOSS adoption.

One subject noted that there is a lack of documentation that explains how organizations have successfully used FOSS, as well as their reasoning for choosing it. In an effort to broaden their participation in FOSS, the Government of Spain conducted a dossier project in 2010 to catalogue the best practices of FOSS communities and project that are heavily influenced by a public administration [4]. This helped lay the foundations for further adoption. Without sharing case studies, lists of best practices, lessons learned, or advice about legal issues, an organization will find it difficult to justify change. Similarly, the "keeping the lights on" mentality in the energy sector has demonstrated the strong connection between reliability and financial impact. Creating and sharing case studies and best practices will help circulate FOSS's reliability.

FOSS also needs to be recommended by trusted sources. Procuring support of FOSS from larger vendors in the energy sector will drive FOSS acceptance and adoption. Similarly, open sourcing commercial software can open up new revenue streams in consulting and support, which can also improve vendor buy-in.

Opportunities have also surfaced around creating and maturing open standards. Collaboration will help create common practices, tools, and audit procedures that will help shape standards. An example is the Secure Information Exchange Gateway (SIEGate), a FOSS project that provides a secure channel for transporting real-time data between a "utility control center and other control centers, utilities, and regulatory and oversight entities" [21]. This project is a collaborative effort between the Grid Protection Alliance, University of Illinois-Urbana Champaign, Alstom Grid, PJM Interconnection, and the Pacific Northwest National Laboratory. Since the FOSS development model hinges itself on the motto "release early, release often", it is designed to take in changes and deploy them quickly. This creates a responsive environment for implementing policy change and complying with new standards.

Ultimately, one of the most powerful and easiest way to promote the development and adoption of FOSS could be through a top-down initiative and promotion from a regulatory or government agency like the U.S. Department of Energy, much like the U.S. Department of Defense and the U.S. Department of Homeland Security have done for FOSS through the HOST program [14].

6 Limitations

Although we believe the cases examined in this study characterize many of the entities operating in the U.S. energy sector, there are limitations to our work. Firstly, while interviews with individuals within the projects and organizations provided an expansive perspective of FOSS and cyber security, these perspectives are not necessarily representative. Many other organizations operate within the energy sector that did not participate in the study. This includes national labs, electric cooperatives, regulatory bodies and other affiliates. Due to scheduling, policy, or other reasons, representative members of these groups were unable to participate in the study.

That said, and while more study should be undertaken to confirm and expand on their findings, these case studies provide some interesting insight into the barriers and opportunities of FOSS adoption in the U.S. energy sector.

Acknowledgements. We would like to thank EnergySec for funding this project, as well as providing insight into the energy sector. We also appreciate the participation of Portland General Electric, Tennessee Valley Authority, Utilisec, Dell Secureworks®, GADS Open Source, Green Energy Corp, and Grid Protection Alliance.

References

[1] About TVA, http://www.tva.com/abouttva/index.htm
[2] Batz, D., Brenton, J., Dunn, D., William, G., Clark, P., Elwart, S., Goff, Ed., Barrell, B., Hawk, C., Henrie, M., Kenchingon, H., Maughan, D., Kaiser, L., Norton, D.: Roadmap to Achieve Energy Delivery Systems Cyber Security (2011), http://www.cyber.st.dhs.gov/wp-content/uploads/2011/09/Energy_Roadmap.pdf
[3] Berg, B.L.: Qualitative research methods for the social sciences. Allyn and Bacon, Glencoe, IL (1989)
[4] Bryant, D. and P. Ramsamy. : Public Administrations Code Release Communities: Dossier ONSFA (2011), http://observatorio.cenatic.es/index.php?option=com_content&view=article&id=728%3Adosiier-nuevo&catid=5%3Aadministraciones-publicas&Itemid=21 (Accessed March 23)
[5] Coverity.: 2011 Open Source Integrity Report. http://softwareintegrity.coverity.com/coverity-scan-2011-open-source-integrity-report-registration.html
[6] Dell to Acquire Secureworks, http://content.dell.com/us/en/corp/d/secure/2011-01-04-ir-shld-release
[7] Department of Energy Launches Initiative with Industry to Better Protect the Nation's Electric Grid from Cyber Threats , http://energy.gov/articles/department-energy-launches-initiative-industry-better-protect-nation-s-electric-grid-cyber
[8] Falliere, N., Murchu, L.O., and Eric Chien,: W32. Stuxnet Dossier: (2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
[9] GADS Open Source, http://gadsopensource.com/
[10] Ghosh, R.A., Glott, R., Krieger, B., and Robles, G. "Free/Libre and Open Source Software: Survey and Study, Part 4: Survey of Developers." June 2002. www.flossproject.org/report/
[11] Grid Protection Alliance "Grid Protection Alliance." 2012. http://www.gridprotectionalliance.org

[12] Hahn, A., Govindarasu, M.:Cyber Attack Exposure Evaluation Framework for the Smart Grid. IEEE Transactions of Smart Grid, 2(4): 835-843 (2011)
[13] Herraiz, I., Robles, G., Amor, J.J., Romera T., Gonzalez Barahona, J.M.: The Process of Joining in Global Distributed Software Projects. Proc. of the Int'l Workshop on Global Software Development for the Practitioner, pp. 27-33, (2006)
[14] Homeland Open Security Technology, http://www.cyber.st.dhs.gov/host/
[15] Krishnamurthy, S.: Cave or Community? An Empirical Examination of 100 Mature Open Source Projects. First Monday, vol. 7, no. 6 (2002)
[16] Lakhani, K.R., Wolf, R.G.: The Boston Consulting Group Hacker Survey (2002), ftp3.au.freebsd.org/pub/linux.conf.au/2003/papers/Hemos/Hemos.pdf
[17] Messmer, E.: Research lab extends host-based cyber sensor project to open source, http://www.networkworld.com/news/2012/041612-hone-258296.html
[18] Open Source Census Tracks Enterprise Use of Open Source Globally (2008), www.osscensus.org/9.30.08.php
[19] Ransbotham, S.: An Empirical Analysis of Exploitation Attempts based on Vulnerabilities in Open Source Software. Workshop on the Economics of Information Security (2010), http://weis2010.econinfosec.org/papers/session6/weis2010_ransbotham.pdf
[20] Robles, G., Scheider, H., Tretkowski, I., Webers N.: Who Is Doing It? A research on Libre Software developers (2001), http://widi.berlios.de/paper/study.html
[21] Siegate: Secure Information Exchange Gateway for Electric Grid Operations, http://www.iti.illinois.edu/research/power-grid/siegate-secure-information-exchange-gateway-electric-grid-operations
[22] Smart Grid, http://energy.gov/oe/technology-development/smart-grid
[23] Smart Grid Investment Grant Program: Progress Report (2012), http://energy.gov/sites/prod/files/Smart%20Grid%20Investment%20Grant%20Program%20-%20Progress%20Report%20July%202012.pdf
[24] Smart Grid, Portland General Electric, http://www.portlandgeneral.com/our_company/energy_strategy/smart_grid/default.aspx
[25] Srivastava, M: Green Energy Corp Introduces Smart Grid Open Source Community, http://smart-grid.tmcnet.com/topics/smart-grid/articles/134784-green-energy-corp-introduces-smart-grid-open-source.htm
[26] Stenbit, J.P.: Open Source Software (OSS) in the Department of Defense (DoD). (2003) http://oss-institute.org/storage/documents/Resources/policy/2003_stenbit_memo.pdf

[27] Turk, R.J.: Cyber Incidents Involving Control Systems, http://www.inl.gov/technicalpublications/Documents/3480144.pdf
[28] Utilisec: Electric Utility Cyber Security, http://www.utilisec.com/
[29] Walli, S., Gynn, D., Rotz, V.: The Growth of Open Source Software in Organization (2005), http://dirkriehle.com/wp-content/uploads/2008/03/wp_optaros_oss_usage_in_organizations.pdf
[30] Wennergren, D.M.: Clarifying Guidance Regarding Open Source Software (OSS) (2009), http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf
[31] Wheeler, D.: Why Open Source Software/Free Software (OSS/FS, FOSS, or FLOSS)? Look at the Numbers! (2007), http://www.dwheeler.com/oss_fs_why.html
[32] Ye, Y., Kishida, K.: Toward an understanding of the motivation of open source software developers. Proc. of the 25th International Conf. on Software Engineering, pp. 419-429 (2003)