MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

21st Annual International Symposium
October 23-25, 2018 | College Station, Texas

Addressing the Security Requirements in Functional Safety Standard IEC 61511-1:2016

John Cusimano, Tim Gale
aeSolutions
Industrial Cybersecurity
Greenville, SC
Emails: john.cusimano@aesolns.com, tim.gale@aesolns.com

Keywords: Industrial Automation, Process Safety, Functional Safety, PSM, PHA, HAZOP, LOPA, ICS, Cybersecurity, Cyber-threat, Cyber-risk, IEC 62443, ISA-99, IEC 61511

Abstract

The 2016 edition of IEC 61511-1: 2016 added two new requirements regarding the security of safety instrumented systems (SIS). The first requirement states that "a security risk assessment shall be carried out to identify the security vulnerabilities of the SIS" and the second requirement states that "the design of the SIS shall be such that it provides the necessary resilience against the identified security risks". The standard directs the reader to ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010 for further guidance on how to comply with these requirements. While these documents are informative, the 479 combined pages do not provide concise guidance on how to address the specific security requirements. The purpose of this paper is to offer step-by-step guidance on how to address the security requirements in 61511 and to identify specific clauses in the reference standards for further information.

Why the Requirement for a Security Risk Assessment?

ISA/IEC 61511 is a functional safety standard which historically focused on random or systematic failures that could impact the ability of the safety instrumented system (SIS) to properly respond to a process demand. So why did the authors of 61511 add these new requirements for security assessments? The primary reason is that industries and governments now recognize that security threats, both physical and cyber, could significantly impact the integrity and availability of a SIS and that functional safety assessments do not historically address security threats such as physical sabotage or cyber-attacks (e.g. malware, hacking, etc.). This is particularly true for programmable electronic SIS with network communications. In other words, just because a SIS is SIL rated does not mean it is immune to physical or cyber threats.

Without performing a security risk assessment of a SIS, asset owners/operators may have a false sense of security regarding the safety of their operations.

Recent events have heightened the urgency of performing security risk assessments on SIS. Since 2010 there have been numerous publicized incidents regarding intentional attacks on industrial control systems (ICS) and SIS in critical infrastructure around the world. For example, the Stuxnet virus in 2010, the Shamoon virus in 2013, the attacks on the Ukrainian power grid in 2015 and 2016, and the Triton Malware targeted at a SIS in the Middle East in 2017.

The of Definition of Risk

Many people struggle with the term *risk* and what it means and what it doesn't mean. So, let's start with some definitions. The Oxford English Dictionary defines risk as "(exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility" (Oxford English Dictionary, 3rd ed.). This is good but it is a little too general. In risk analysis, risk is traditionally defined as a function of *probability* and *impact* where the probability is the *likelihood* of an event occurring and *impact* is a measure of the extent of the adverse circumstance (i.e. the *consequence*). The common formulaic way of expressing this is:

$$\boldsymbol{Risk = Likelihood\ x\ Impact}$$

This is also a good definition, but again, a little too general for applications where we want to assess security risk, particularly information security risk.

Security Risk

The thing many people struggle with when attempting to assess security risk, which is typically based on intentional actions, is that it is very difficult to estimate likelihood. In fact, I have heard people argue that it is impossible to assess security or cyber security risk because it is impossible to estimate the likelihood of a deliberate action. While I agree it's challenging, I disagree that it is impossible and fortunately most security professionals would agree with me. Otherwise, how would those responsible for national security or the security of major events such as the Olympic Games even begin their undertaking without some method of assessing security risk?

Actually, the solution to the "likelihood conundrum" actually quite simple. In the field of security risk analysis the likelihood component is broken down into its core elements: threats and vulnerabilities. The common formulaic way expressing this is:

$$\boldsymbol{Security\ Risk = Threats\ x\ Vulnerabilities\ x\ Impact}$$

National Institute of Standards and Technology (NIST) (Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments., 2012) explains this well by stating, "Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization."

In addition to NIST, another organization called the FAIR Institute has developed a model for understanding, analyzing and quantifying cybersecurity and operational risk called the Factor Analysis of Information Risk (FAIR) framework. The FAIR framework factors security risk into

its elements making it easier to understand and more practical to assess. Figure 1 is a visual of the FAIR model that is provided by the FAIR Institute. As you can see, the model dissects likelihood (which FAIR calls loss event frequency) into Threat Event Frequency and Vulnerability. Sound familiar? The FAIR model further breaks down Threat Event Frequency into Contact Frequency and Probability of Action. Finally, Vulnerability is broken down into Threat Capability and Resistive Strength.

As you can see, it not impossible to assess cybersecurity risk. You simply need a good framework, methodology and guidance to get started.

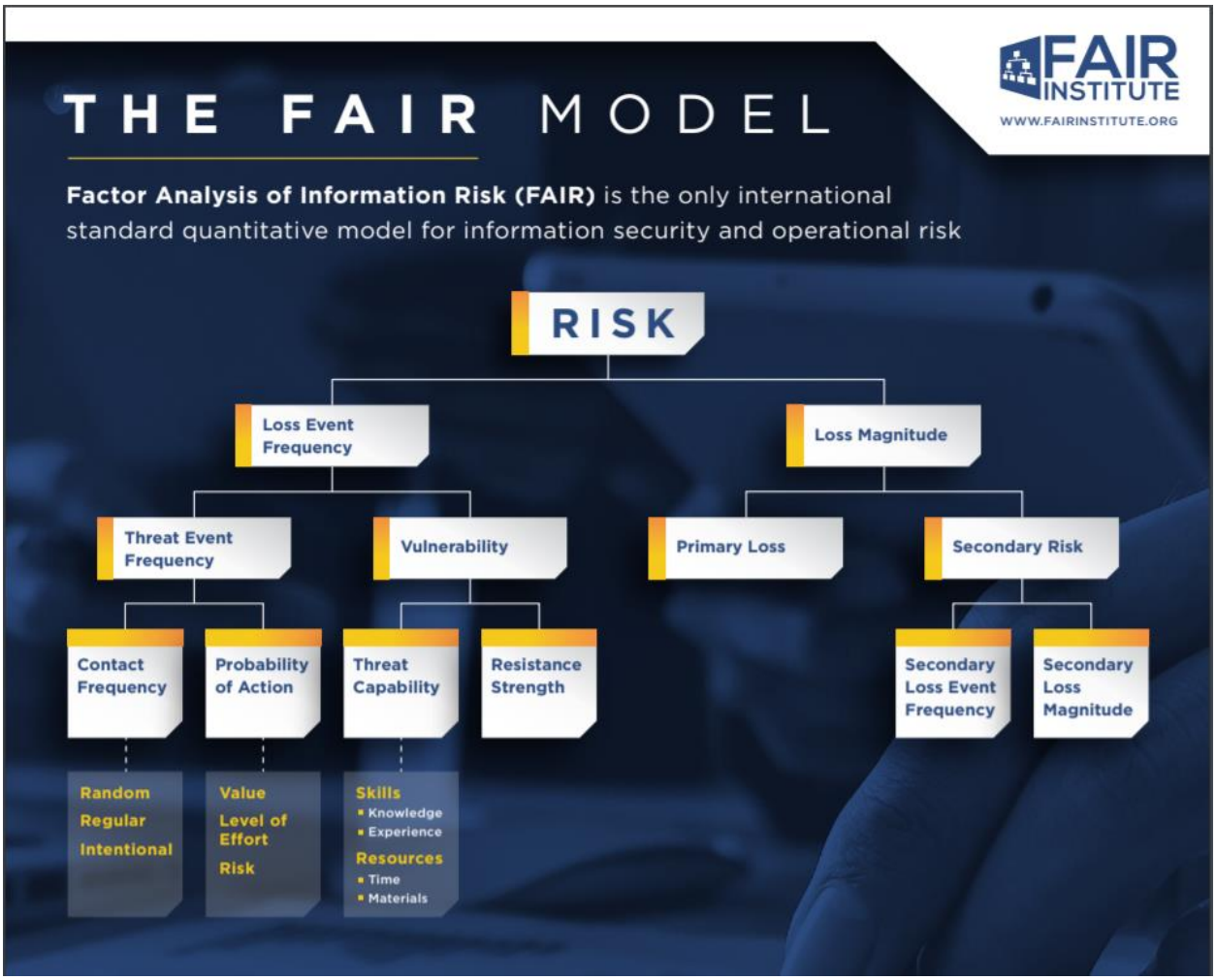

Figure 1: The FAIR Risk Model, Fair Institute, 2018 (cdn)

The 61511 Security Clauses

Now that we have established a good definition of security risk and its major components, let's take a deeper look at the security clauses in IEC 61511. Clause 8.2.4 states that a security risk assessment shall be carried out. It is followed by 6 sub-clauses that further specify the required elements of a security risk assessment.

If you read through clause 8.2.4 you will see that it requires the basic elements in a security risk assessment. For example, clause 8.2.4a requires that one define the *scope* of the assessment (i.e. the system under consideration) which is the SIS and any device connected to the SIS. Defining the scope is the first step in any security risk assessment methodology. Clause 8.2.4b requires identifying and describing *threats* and *vulnerabilities* while clause 8.2.4c requires a description of the potential *consequences* resulting from the security events and the *likelihood* of these events occurring. Clause 8.2.4.d states that the security risk assessment shall provide consideration of various system lifecycle phases such as design, implementation, commissioning, operation, and maintenance. Clause 8.2.4e states that the security risk assessment shall result in the determination of requirements for additional risk reduction. In other words, it shall define additional physical or cyber security countermeasures that will reduce the risk to tolerable levels. Lastly, clause 8.2.4f requires a description of, or references to information on, the measures taken to reduce or remove the threats. This, effectively is the documentation of existing or proposed security countermeasures. A security countermeasure is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken (Countermeasure_Computer, n.d.).

Clause 11.2.12 simply states that the design of the SIS shall be such that it provides the necessary resilience against the identified security risks and refers the reader back to clause 8.2.4.

Additional Guidance

61511 clause 8.2.4 refers the reader to several standards for additional guidance (ISA TR84.00.09 and IEC 62443-2-1:2010). These documents can be helpful as they are aligned with general security risk assessment frameworks but incorporate the unique requirements of industrial automation and control system (IACS) and SIS applications. Another document that was not referenced but is a valuable resource is ISA 62443-3-2:2018 CDV, "Security for industrial automation and control systems – Part 3-2: Security Risk Assessment and Design". The reason it was not referenced is that it was not available at the time that IEC 61511 second edition was published in 2016. This standard has been approved by both ISA and IEC and is currently being prepared for publication. It establishes requirements for:

- defining a system under consideration (SUC) for an industrial automation and control system (IACS);
- partitioning the SUC into zones and conduits;
- assessing risk for each zone and conduit;
- establishing security level target (SL-T) for each zone and conduit; and
- documenting the security requirements.

How to Perform a Security Risk Assessment on a SIS

So, all of this background information and guidance is great but how do you *actually* perform a security risk assessment on an SIS? The answer is you need to select a security risk assessment methodology that has been tailored towards assessing ICS and SIS applications. The risk

management frameworks and discussed thus far (e.g. NIST, FAIR, etc.) apply generally to assessing cyber security and information security risk. They are, as their names imply, frameworks that define the core elements. They are not, however, methodologies. A methodology is a body of methods rules and postulates employed by discipline or, in other words, it is a particular procedure or set of procedures.

One methodology that that has emerged from all of the aforementioned standards and guidance is something known as a cyber PHA or cyber HAZOP.

Cyber PHA Methodology

A cyber PHA is a detailed cybersecurity risk assessment methodology for ICS & SIS that conforms to ISA/IEC 62443-3-2. The name, cyber PHA, was given to this method because it is similar to the Process Hazards Analysis (PHA) or the hazard and operability study (HAZOP) methodology that is popular in process safety management, particularly in industries that operate highly hazardous industrial processes (e.g. oil and gas, chemical, etc.).

A cyber PHA is typically performed in phases. Figure 2 depicts a typical cyber PHA risk assessment process. The process is scalable and can be applied to individual systems, or to entire facilities or even entire enterprises. It all depends upon the scope of the assessment which, if you'll recall, is the first sub-clause in IEC 61511 8.2.4a. In this paper we will focus on applying this methodology to the assessment of an SIS.

Figure 2: Example of a cyber PHA Risk Assessment Process

The Six Phases of a Cyber PHA applied to a SIS

1. Kickoff: Kicking off a project effectively puts both the site personnel and the assessment team on the same page with regard to project expectations, data exchange requirements and schedule. The kickoff is also where the scope of the assessment is established which the first requirement in 61511 Clause 8.2.4a. A successful kickoff meeting allows all personnel to discuss the current cyber posture of the facility based on existing policies, roles and responsivities, and the SIS components and architecture. Setting expectations on information requirements allows subsequent phases to progress efficiently.

2. Assess: The purpose of this phase is to gather information about the SIS and its connections to identify vulnerabilities. This phase satisfies the remainder of the requirements in 61511 Clauses 8.2.4a and 8.2.4b by documenting the SIS and its connections and identifying vulnerabilities. This is best performed through a site visit by the assessment team as it provides an opportunity to document data flows, equipment configurations, as-built system architecture, and to interview onsite engineering, operations and maintenance personnel. It is important that only non-invasive techniques be used during this visit as it is critical that the normal operation of the SIS not be interrupted or altered in any way.

Some vulnerability assessments techniques only involve interviewing site personnel and completing a questionnaire. In our opinion, such an exercise is inadequate when assessing the security of a system with health, safety and environmental consequences. Failure to assess the actual details of the physical attributes of a SIS and all of its connections (both physical and logical) jeopardizes missing critical information necessary to truly determine risk.

The site visit also provides an opportunity to perform a gap assessment providing valuable insight into the site's position in relation to compliance with relevant functional safety and cybersecurity standards such as IEC 61511, ISA/IEC 62443, and the NIST Cybersecurity Framework. This is valuable as a means of measuring progress as a cybersecurity program moves forward and also to benchmark against best industry practices.

3. Analyze: Analyzing the data acquired during the site visit, as well as any other information collected during the project allows the team to document potential vulnerabilities that may be exploited during a cyber event. These may include physical security gaps noted during the site visit, undocumented connections, unsecure protocols, misconfigured devices, weak access controls, anomalous communications captured during network traffic analysis, or vulnerable software found during computer analysis. These vulnerabilities are documented and used as part of the cyber PHA workshop on Phase 4 to ensure scenarios considered are valid.

During analysis, markups to the architecture diagram can be made in order to document the actual current state of the ICS. This is critical for use in the Cyber PHA Workshop so all participants are clear on the system's design.

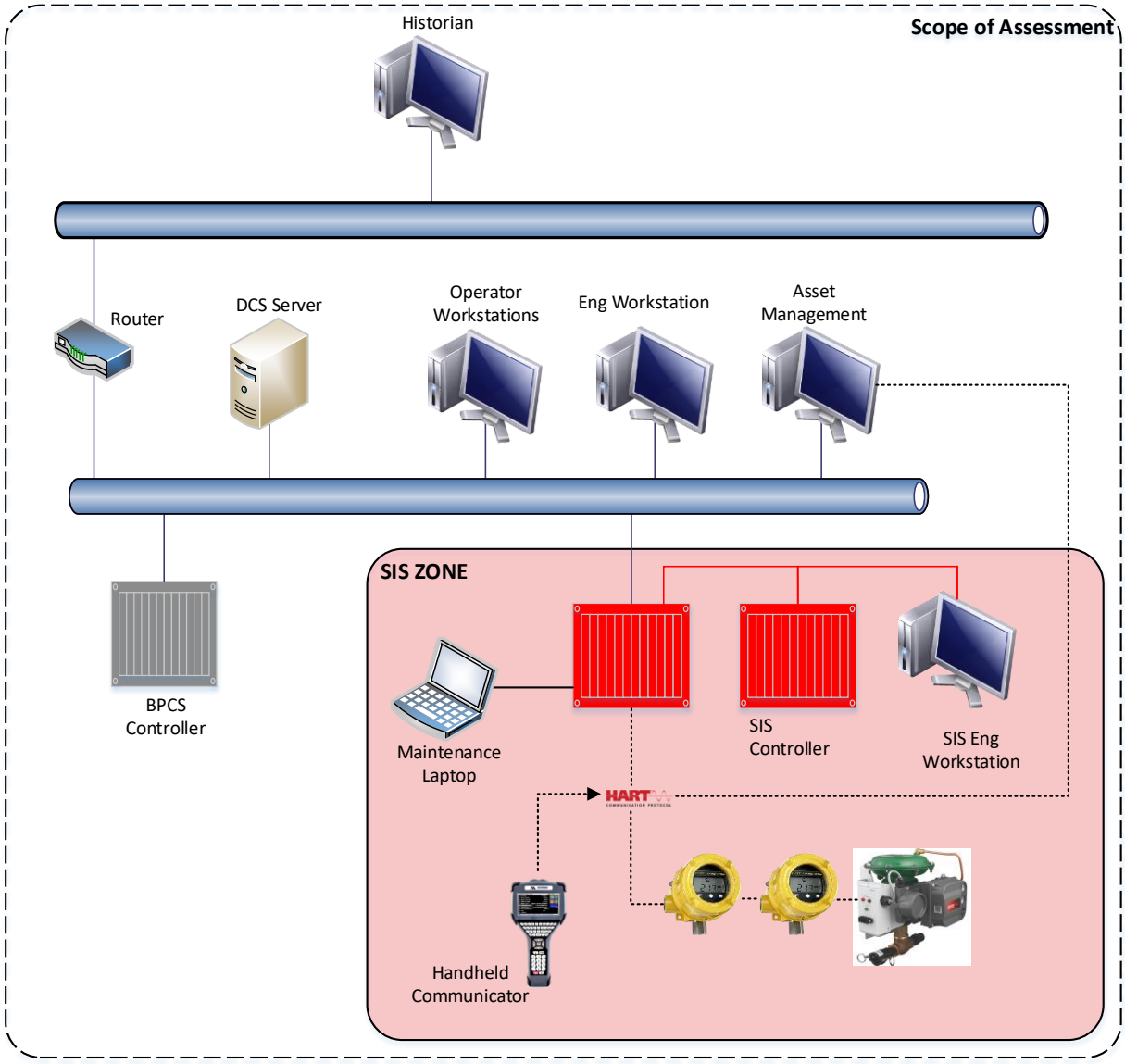

Figure 3: Example of Logical Network Diagram of Depicting the SIS and Connected Devices

4. Cyber PHA Workshop: The cyber PHA workshop is the heart of the process, where all of the information gathered and analyzed in Phases 1 – 3 is integrated with threat scenarios to develop a complete picture of risk. This phase satisfies the requirements in 61511 Clauses 8.2.4b, 8.2.4c, 8.2.4e and 8.2.4f by identifying and documenting threats, vulnerabilities, existing countermeasures, likelihood, consequences and recommendations for additional countermeasures for additional risk reduction.

The workshop is a group effort led by a facilitator and a scribe with expertise in the cyber PHA process as well as multiple subject matter experts who are familiar with the industrial process, the SIS and related ICS and IT systems. For example, the workshop team typically includes representatives from operations, engineering, IT and health and safety as well as an independent facilitator and scribe. A multidisciplinary team is important in developing realistic threat

scenarios, assessing the impact of compromise and achieving consensus on realistic likelihood values given the threat environment, the known vulnerabilities and existing countermeasures.

The facilitator and scribe are typically responsible for gathering and organizing all of the information required to conduct the workshop (e.g. system architecture diagrams, vulnerability assessments, and PHAs) and training the workshop team on the method, if necessary.

A worksheet is commonly used to document the cyber PHA workshop. Various spreadsheet templates, databases and commercial software tools have been developed to support the cyber PHA method. The organization's risk matrix is typically integrated directly into the worksheet to facilitate assessment of severity and likelihood and to look up the resulting risk score.

The workshop is conducted following a systematic approach where the system is partitioned into security zones and each zone is assessed to identify consequences of compromise and the threat scenarios that could lead to those consequences. Each scenario is assigned a risk score where risk is defined as the severity of a consequence versus the likelihood of that consequence.

First, a consequence must be defined. It include a description of what happens as a result of the scenario being considered. Typically, a consequence from the site's process safety PHA is selected where a control system failure is the initiator and/or the SIS is the safeguard. Additionally, non-safety but high impact financial consequences such as lost production or business interruption are also identified. It's important for the workshop facilitator to be familiar with process safety and cybersecurity so these scenarios are legitimate.

Next, the threat scenarios are defined that could lead to the consequence. The threat scenario includes threat actors, threat actions, and the vulnerabilities they may exploit to carry out the attack. Unlike the IT environment, cyber threats to the ICS include 3rd party contractors with high levels of privilege who may act maliciously or expose the system to non-secure laptops or portable media. These threats present a unique case were code can be changed creating safety incidents or infesting a system with a site wide malware outbreak causing an extended outage. Also, authorized users represent a significant proportion of ICS cyber attacks. These users have the potential to intentionally or unintentionally manipulate the controls in unintended ways.

Once the scenario is defined, the risk can be scored based on the severity of the consequence and the likelihood of each threat. Severity scoring uses the same system as a process safety PHA's. However, unlike process safety, there is no database of frequencies for cyber events. Likelihoods of threat scenarios are more relative to one another as opposed the more mathematical approach used in a process safety PHA. It's important that the facilitator has an understanding of this so the risk isn't under or over stated.

With a risk ranked scenario, the current state is documented by recording existing cyber countermeasures in place. Then, if required by the residual risk, recommendations are made that reduce the risk to acceptable levels. These new recommendations are directly tied to a real risk to the organization and are prioritized with the most effective countermeasures reported against the highest risk.

5. Report: Once the Cyber PHA is completed and its results analyzed, a comprehensive report is produced showing the risks to the enterprise and a plan to mitigate risk to the organization's acceptable level. A detailed risk profile provides a visual map of what zones in a

facility contain the highest risk. An executive summary provides the decision makers with a concise risk and remediation picture.

When conducing risk assessments across a number of assets (e.g. all SIS in a facility or company), a group of recommendations often become common to all the facilities. These are identified as baseline recommendations that become part of the organization's long term cyber remediation plan.

6. Mitigate: An effective remediation plan includes a prioritized list of actions, budgetary estimates, schedule and resource requirements. Typically, these plans include short term projects to mitigate high and critical risks and long term projects involving many resources, new equipment and training. Enterprises that possess multiple facilities often establish a specific project to roll out the baseline risk mitigations identified during the reporting phase. This phase satisfies the requirements in 61511 Clause 11.2.12.

Conclusion

We hope that this paper has helped clarify the purpose of performing a security risk assessment on a SIS and why it is important. More importantly, we hope that it has presented you with a proven methodology (cyber PHA) that will help you conform with the security requirements in 61511 as well as provided you with a sensible approach to assessing cyber security risk for any control system. More information on the cyber PHA methodology can be found in the whitepaper, "If it isn't Secure, it isn't Safe" **(Cusimano & Rostick, 2018)**.

Bibliography

(n.d.). Retrieved from cdn2.hubspot.net/hubfs/1616664/The%20FAIR%20Model_FINAL_Web%20Only.pdf?t=1538069566530

Countermeasure_Computer. (n.d.). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Countermeasure_(computer)

Cusimano, J., & Rostick, P. (2018, April). *If it isn't Secure, it isn't Safe.* Retrieved from aeSolutions: http://www.aesolns.com/download/2087/

Oxford English Dictionary, 3rd ed. . (n.d.). Oxford University Press.

Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments. (2012). Washington DC: National Institute of Standards and Technology (NIST) .