EAST CAROLINA UNIVERSITY

# Incident Response Planning In Industrial Control Systems

ICTN 6823 Information Security Management

**Bill Clark**

**July 20, 2016**

Abstract

This paper discusses what Incident Response (IR) Planning is, what Industrial Control Systems (ICS) are, and how IR Planning pertains to ICS security. IR Planning is the process of preparing for any type of adverse event, also known as an incident, which can cause a process degradation or failure in a system. A system can be hardware, software, or a combination of both. An event can be man-made or natural in origin. An ICS is a combination of hardware and software processes that use extreme precision to automate or control most of today's manufacturing product lines, water and power utility production plants, and transportation systems for people and products. For ICS applications and data, availability is the first priority.

We can assume that all businesses are in existence to provide a beneficial service of some type, to all or some subset of society. In most cases, this service or services are provided in exchange for profit to the business owners or investors. Unless the business is the sole provider of a given service, the business or organization must provide this service at the lowest possible cost to society, to accommodate the majority of the service users. In smaller or startup businesses, a single owner or executive must make daily planning decisions to ensure that the company is financially capable of withstanding any unplanned, adverse event or incident without affecting its support or service that is provided for the customer base. These incidents can originate from natural occurrences such as prolonged power outages from ice storms, hurricanes, or floods. They can also originate from man-made incidents such as accidental accounting record deletions, database server reboots, or corrupted inventory files. Along with accidental incidents, there is also the possibility of intentional database corruptions, stolen files, and account record erasure by disgruntled or terminated employees and external adversaries. All of these types of incidents can disable an organization's ability to provide needed services to the customer base and cause the customer base to close accounts or discontinue business transaction with the organization. The ability to protect and access accurate customer, inventory, billing, and delivery tracking data when needed can provide an organization with the leading edge that is required to stay ahead of other competitors in any industry. These services could also be in the context of a life support system such as a traffic light system, fresh water processing pumps and filters, or a flood water management system. The document that conveys an organization's objective toward maintaining the Confidentiality, Integrity, and Availability (CIA) of operations, processes, and data during an incident is known as the *Incident Response* (IR) Policy. The CIA triad, as shown in Figure 1, demonstrates the association of Confidentiality, Integrity, and Availability in relation to security protection modeling for operational processes and data. The IR Plan provides the measures that are taken to execute the IR Policy and maintain during or restore as soon as possible this security triad to operational

processes and data during and after an incident. IR Planning consists of the actions to create three deliverables: The IR Policy, the IR Plan, and the IR Team (IRT).

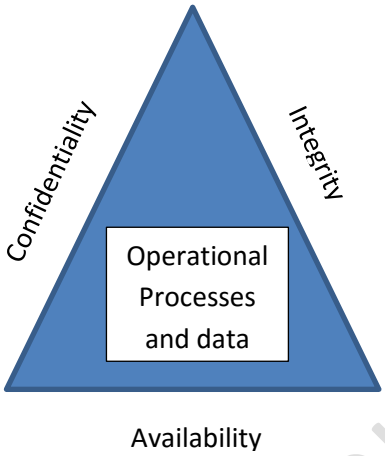


Figure 1: IT CIA Triad

According the *NIST SP600-61-R2 Computer Security Incident Handling Guide,* the IR plan should at a minimum address the following elements:

- Mission
- Strategies and goals
- Senior management approval
- Organizational approach to incident response
- How the incident response team will communicate with the rest of the organization and with other organizations
- Metrics for measuring the incident response capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization (* Cichonski, Paul., Tom Millar., Tim Grance., Karen Scarfone., 2012)

Gaining senior management approval for the IR Policy and Plan will often determine the success of the IR plan. Without senior management acceptance and support, the plan will lack adequate resourcing and the drive to succeed. The IR plan should be reviewed annually to ensure the strategies and goals are relevant and continue to support the organization's mission.

As mentioned with the IR Policy, the IR plan should have senior management approval and support. The IR plan should provide provisions to address the following elements:

- Awareness training: Provide processes to educate users and staff on abnormality identification and how to handle or report these abnormalities.
- Implement procedures to verify that an incident has occurred: Provide methods to identify that an actual incident occurred.
- Maintain information CIA / AIC or restore business continuity before, during, and after the incident: Provide procedures to contain the incident and maintain normal business functions.
- Eradicate the incident: Define procedures and actions to eradicate the incident based on the incident footprint and scope.
- Recover the elements affected by the incident: Provide guidance to verify that the affected operations are clean and return them to full operations.
- Implement procedures to determine the attack vectors and how the incident occurred: Implement processes to develop new processes from lessons learned to prevent future attacks/incidents.
- Keep management informed and follow proper chain of command procedures: Provide routine reporting procedures to keep management up to date on IR readiness.
- Test the IR Plan: Provide procedure and schedules to evaluate the IR Plan and update it against the latest vulnerabilities.

Another element of IR Planning is the selection of the IR team. The IR team should be selected, not appointed. The members of the IR team should be well-trained in incident response task and investigative processes. The members should have daily work responsibilities allow them to leave or hand off the responsibility to others in support of incidents. Depending on the requirements and resources of the organization, the team should have representatives from the following areas:

- Senior management
- Information Security (InfoSec)
- Information technology (IT)
- IT auditor
- Security
- Legal
- Human Resources
- Public Relations
- Finance (* Borodkin)

An Industrial Control System (ICS) is a combination of hardware and software processes that use extreme precision to automate or control most of today's manufacturing product lines, water, and power utility production plants, and transportation systems for people and products. These systems ensure that every bottle of water is safe to drink, every medication is the exact combination of toxic and inert elements, the electric power is a constant 120V or 208V at 60Hz, and that every highway intersection allows traffic to only flow in the prescribed direction. Because these systems must operate with extreme precision and extended time schedules, security is not the primary concern of the system owners. The primary concern is system availability. These systems must always be online and accurate. In the early days of ICS, the control and monitoring of networks that connected these systems were proprietary and isolated

from public exposure. However, in today's Internet of Things (IOT), extremely reliable Commercial Off-The-Shelf (COTS) vendor equipment, and operating cost reductions, most all of these ICS networks are connected to the business networks. Along with the applications and data in the business networks, the applications and data in the ICS must also be protected from external entities, but with a different scope. The business network requires that the applications and data be kept confidential as the first priority. For ICS applications and data, availability is the first priority. As mentioned, an ICS system can be deployed in any type automation application. For the purpose of this paper, we will focus on a flood water control system shown in Figure 2.

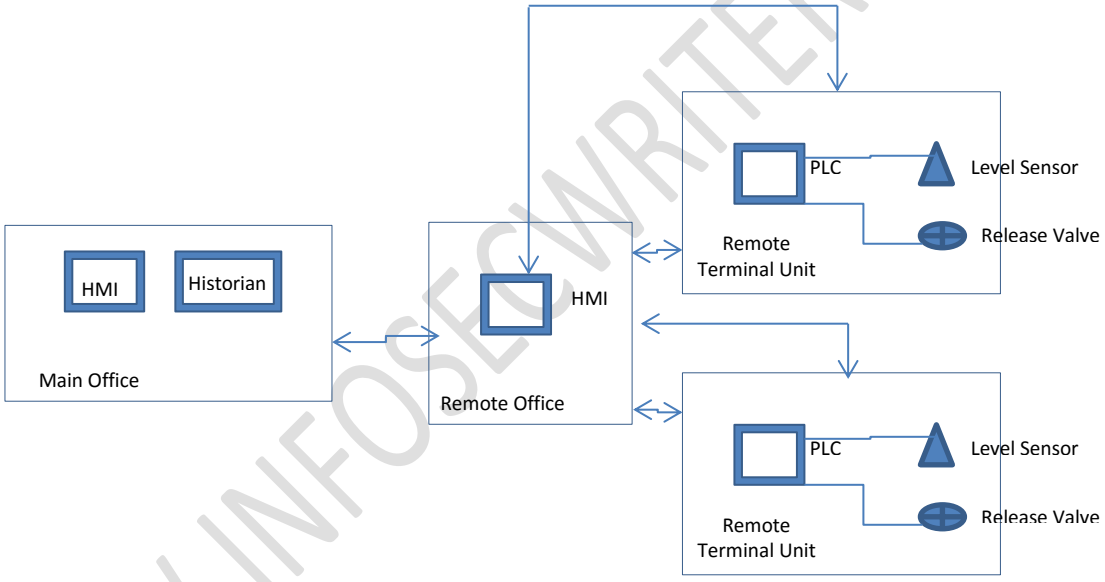


Figure 2: Flood Water Control ICS

Our flood water control system has sensors along the banks of the water release canals throughout the city. In the event that a flash flood occurs, the sensors trigger the PLC to open control gates at the end of the canals and release the flood waters in to the nearby river. These controls manage the canal water release levels to maintain a balance between the runoff water levels in the city canals and the river.

A generic ICS system consists of the following operation zones:

- Business Zone: This zone supports the following networks:
    - Enterprise Business
    - Plant (Business applications to plant supervisor and workers)
- Demilitarized Zone: This zone supports the Demilitarized (DMZ) network
- Operations Zone: This zone supports the following areas:
    - Operations Network
    - Process Control and Supervisor Control and Data Acquisition (SCADA) Zone. This zone supports the following subzones:
        - Supervisor Control Network
        - Control Devices Network
        - Process Control Instrumentation Network
- Safety Zone: This zone supports the safety shutdown and control processes
- Enforcement Zone: This zone supports the other zone's segregation and protection devices. Figure 2 displays a common ICS zone association diagram.

Although most of the components in an ICS environment seem to be similar, or in some cases, the exact components deployed in an Information Technology (IT) environment, there are critical physical and process differences that make an ICS environment more operationally critical than informational. One basic difference is that access criticality is placed on availability over confidentially in relation to data management. As mentioned earlier, in an IT environment, users can tolerate delays in accessing processes and data in most desktop applications. However, in an ICS environment, even the slightest delay can be catastrophic for processes, and in some cases, human lives. This real-time data requirement within an ICS environment is what distinguishes the environment as an Operational Technology (OT) as opposed to the delay-tolerating IT environment.

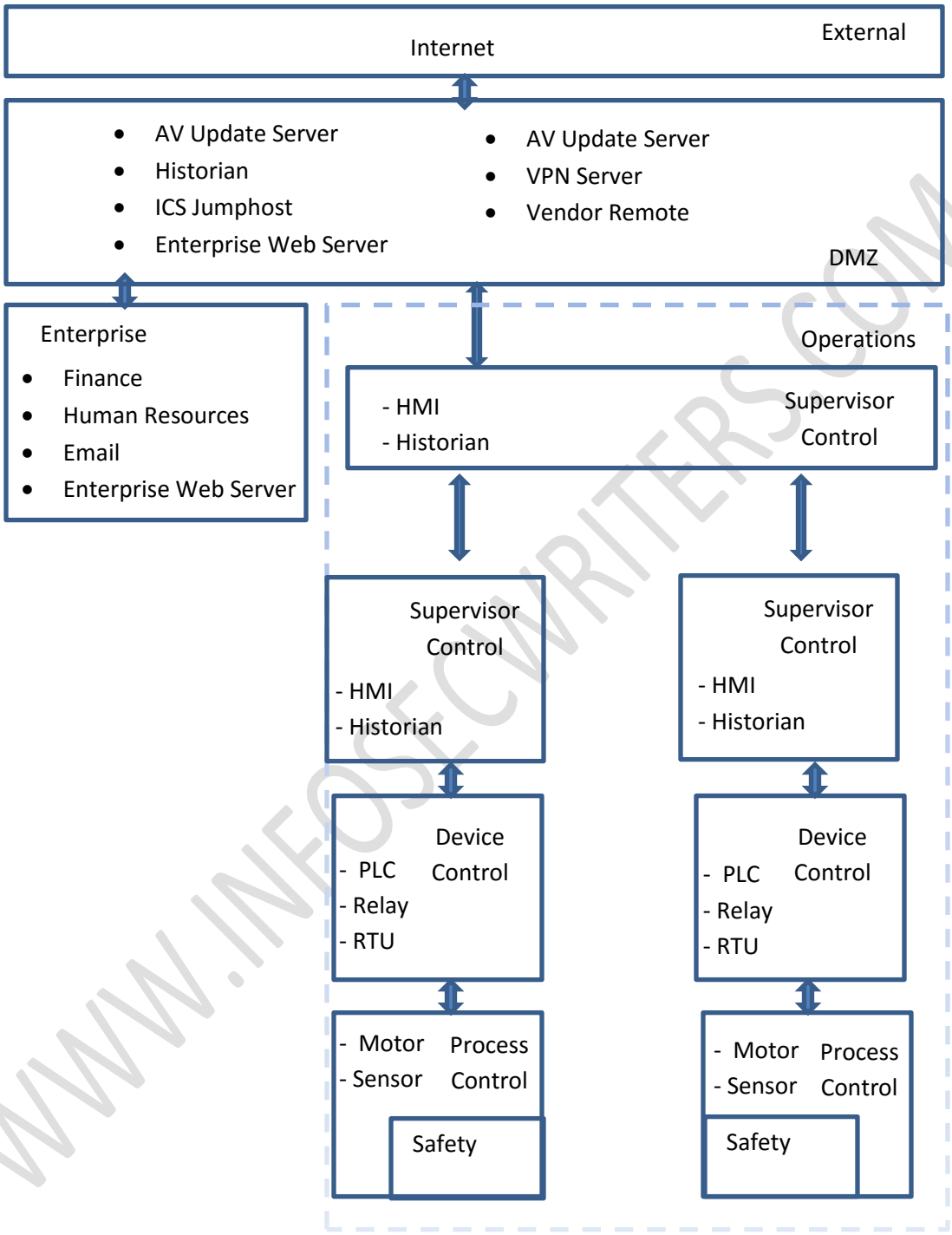


Figure 3: Generic ICS Zone diagram

As shown in Figure 4, the data modeling of an OT environment is more like the AIC triad, as the availability to data processes is critical over confidentiality. Process and data integrity is critical in the OT environment just as it is in an IT environment.

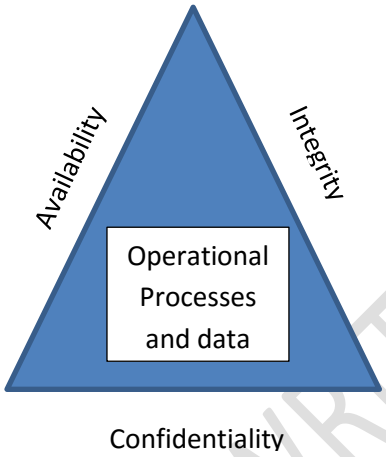


Figure 4: ICS AIC Triad

Another critical difference between OT and IT environments is the protocols used by the processes. Most IT environments rely heavily on the IPV4, IPV6, SIP, CDP, or IPX protocols. The dominate protocols used within most ICS systems are CIP, MODBUS, DNP3, OPC, and Profinet (* Collantes, 2015). During the early development of IT protocols such as IP and IPX, the connectivity was not considered very reliable and could not support the availability requirement of ICS processes. As mentioned earlier, ICS systems required near real-time availability and responses between Programmable Logic Controllers (PLC), sensors, and actuators. This requirement led to the development of the more responsive, but proprietary protocols as CIP, MODBUS, DNP3, OPC, and Profinet. Because these protocols were generally kept local to the ICS environment and were not expected to provide connectivity beyond the Supervisor Zone of the ICS system, there was no capability for routing or security features embedded in these protocols.

Now that we have a good understanding of what an ICS system is, the type of processes that are managed by ICS systems, and the common components of an ICS, we will discuss the vulnerabilities that exist in a common ICS environment. A PLC is a device that can be programmed to perform a specific action based on a specific value. An example could be to open an automatic tank drain valve when a liquid level sensor indicates the full level has been reached in a mixing tank. This is a simple example, however a more complex operation would be to open multiple valves to allow a precise amount of different liquids in a mixing tank. Delays in the response of the valve to respond to the controls from the PLC can cause the measured amount to be incorrect. Also, if the level sensor becomes compromised, it could send a false-level indication to the PLC and cause an overflow or underflow. Also these PLCs, sensors, and actuators often operate in very harsh environments that would cause average IT equipment to rapidly fail. As mentioned, the protocols used by the devices provide no security or authentication mechanism to provide data integrity. If corrupted data or signals were sent to the devices accidental or intentionally, the result would be unpredictable. The device could make incorrect movement or shut down completely. Also deployed in an ICS environment are rugged computer systems that are installed with Windows, UNIX and Linux (Xnux) operation systems (OS). These Windows and Xnux systems vary in versions from Windows XP to Windows 2008R2 and Hewitt Packard (HP) UNIX to Redhat Linux. This diversity in operating systems within the ICS is mainly due the processes that have remained unchanged for over 15 years, or were not cost effective for the organization to upgrade. As these PC systems were orginal isolated from other environment, there was more of a failure risk from a flawed patch than an attacker accessing the system. So patches were rarely applied. Another issue affecting the upgrade or process improvement lifecycle within ICS systems is the availability of specific process applications and application patches. In the late 1980s and 1990s, applications for ICS processes were mainly proprietary for a specific type of process. They were not updated unless a major process flaw existed in the code affecting the operation, but not the vulnerability of the

system. The objective of this section is not to explain every type of ICS or every type of industry ICSs are currently managing, but to bring a level of awareness that many of the life support systems we as humans interact with daily are managed by ICS, and how the IoT has placed the ICS in a new vulnerable environment that they were never designed to interface with. The electrical power we use, the fuel oils we consume, the automobiles we drive, and the beverage and nutrients we digest are tested for safety and packaged by ICSs. With this in mind, in the next section we will focus on the best to plan Incident Response to minimize the effects of accidents, intentional disruptions, and external intrusions on these systems.

IR planning is the responsibility of senior management and should yield the IR policy, IR plan, and an IR team (Whitman, 2016). The ICS IR policy should be specific to the ICS environment and document the creation of the ICS IR team and the IR plan. The ICS policy could be a sub item of the organizations overall security response policy. The functions should include provisions for human resource (HR) and legal actions taken to discipline internal and contractor employees responsible for causing an incident. The policy should address how an investigation will be conducted and recorded. If the ICS is regulated by any state or federal regulations, the IR policy should ensure that all ICS employees are aware of these regulations. Directives should include how information relating to the incident will be disclosed, who it should be disclosed to, and by whom. This policy directive should include provisions for notification of disclosure of intellectual property (IP) belonging to the organization or equipment vendors. The IR policy should also define the positions of authority during the incident and the reporting levels, including the sub-levels, in the absence of daily authority personnel (* Homeland Security, 2009). Finally, the IR policy should establish, at a minimum, an annual policy review by upper management.

The IR plan provides the procedures and operations to execute the IR policy. The IR plan should contain a sub-section for every type of incident that is considered a risk to the

business organization. The incident sub-section should support the following sections: (* Homeland Security, 2009)

- *Overview:* Description of the business service.
- *Incident Description:* Definition of the type of incident. Type classifications could be accidental, intentional, attack, hardware, or code failure and the processes affected.
- *Detection:* Description of symptoms or events that characterize the incident. Methods should be descriptive in nature to eliminate false positive alerts.
- *Notification:* Listing of employee, contractors, and vendor contact numbers relating to the devices or process affected by the incident. This listing should also include upper management and internal departments.
- *Analysis:* This section provides guidance on determining the type and extent of the incident to the operation of the organization. This section should also provide guidance to determine the state of employee and public safety.
- *Response:* This section describes actions taken in response to initial detection, containment, and eradication of the incident. The actions should include provisions for off-hour, weekend, and holiday occurrences. The actions should also cover restoration of services, escalation procedures to external support agencies, and collection and handling of forensic evidence such as logs and files.
- *Communications and Contracts:* This section consists of any contact information for internal and external employees, hardware and software vendor contacts, law enforcement and public safety contacts, prepared media statements, and the media method to convey these communications.
- *Forensics:* Depending on the analysis of the incident type, this section describes what type evidence should be collected and processed.
- *Reporting:* This section lists the internal and external reporting templates, including the information that is reported to what level of management or product vendors.

With the IR policy and IR plan defined and published, the final element is the IR team. It is critical that the IR team be well trained and knowledgeable of the organization's processes and departments. The number of members and positions of the team will vary depending on the requirements of the business operations and processes. The best practice is to maintain the IR team in a central location with easy activation and deployment to any incident. However, many ICSs are configured in a distributed fashion with a few remote operation locations in which

distributed IR teams would have a better reaction time. In this scenario, many of the assignments will be duplicated at each site. A well-documented IR policy and in-depth IR plan will lay out the responsibilities of the IR team. The common responsibilities will include further development of the IR policy and plans, serving as the primary point of contact for incident prevention and analysis, testing the IR plan, reporting incident analysis and status to upper management and external agencies, and most importantly, responding to and rectifying incidents (* Homeland Security, 2009). In order to effectively respond to incidents of different origins and domains, the IR should consist of at least one employee and vendor from every possible business area. It is important to note that when contractors or vendors are members of the IR team, a Non-Disclosure agreement (NDA) should be in signed and in place. The IR team should have one or more members from each of the following areas:

- *Executive Management*. This position will give leadership, sponsorship, and leadership to the team. The executive manager will also have the authority that is needed to resolve department conflicts.

- *IT Engineer*. This position will have insight into the overall company asset connectivity and an in-depth knowledge of software and hardware vulnerabilities. This position will most likely have access to licensed security and reporting tools used in the ICS connectivity domain.

- *Security*. This position will have extensive knowledge of the logical and physical security domains deployed in the organization.

- *ICS Management*. This position will have the in-depth knowledge of the control system operating system configuration requirements, connectivity and access methods deployed with the ICS, and the authority to make critical decisions on process requirements during an ICS incident.

- *ICS Engineer*. This position will provide the process expertise on ICS signal paths, functionality and have a relationship with application and hardware vendors. A relationship with equipment vendors will be valuable during incident isolation and recovery, with minimal ICS functionality degradation.

- *Others*: These positions could, if needed, be covered by an HR representative, legal representative, and IT system administrators.

## Summary

As more and more systems move from the protection of air gaps, private networks, and complete isolation from the daily business networks, we read how these systems fall victim to some form of cyber-attack or failure. From script kiddie to amateur hackers to state-supported attackers, it seems that every device that has any type of data stack is under attack. Some for fun, some for espionage, and some for ransom, but all are vulnerable to disclosing the data and processes that make daily human existence possible. It is believed that our critical ICS systems have been affected by ransomware and data exfiltration code for some time and the exploiters of the attacks are only waiting for the correct time or event to cause a catastrophic event. A catastrophic event could be to cause a power plant to exceed safe voltage output levels or power grids that cause distribution equipment to explode and devices to overheat. Up to now we have been fairly fortunate that the embedded safety systems have prevented this from happening at a catastrophic level. In the documents we have discussed the measures that organizations should adopt, implement, and improve upon to have in place an Incident Response policy, plan, and team that is capable to minimize the effects of an incident, not if it occurs, but when it occurs.

* Borodkin, M. (n.d.). *Computer Incident Response Team.* Retrieved from www.san.org: https://www.sans.org/reading-room/whitepapers/incident/computer-incident-response-team-641

* Cichonski, Paul., Tom Millar., Tim Grance., Karen Scarfone. (2012, August). *NIST Special Publication 800-61.* Retrieved from NVLPubs.nist.gov: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

* Collantes, M. H. (2015, May). *Protocols and Network Security in ICS Infrastructure.* Retrieved from www.incibes.es: https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_protocol_net_security_ics.pdf

* Homeland Security. (2009, October). *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability.* Retrieved from ics-cert.us-cert.gov: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

Anderson, D. (2012, June 1). *Protecting today's SCADA systems with a 'defense-in-depth' strategy .* Retrieved from www.epmag.com: http://www.epmag.com/protecting-todays-scada-systems-defense-depth-strategy-678461#p=4

Ashford, W. (2014, Oct 14). *Incident response: a common failing.* Retrieved from www.computerweekly.com: http://www.computerweekly.com/news/2240233470/Incident-response-a-common-failing

Caswell, J. (2011, 12 8). *Survey of Industrial Control Systems Security.* Retrieved from www.cse.wustl.edu: http://www.cse.wustl.edu/~jain/cse571-11/ftp/ics/

Davis, K. W. (2015, June 1). *Defending SCADA systems against the growing cyber threat.* Retrieved from community.energycentral.com: http://community.energycentral.com/community/intelligent-utility/defending-scada-systems-against-growing-cyber-threat

Houmb, S. H. (2015, August 21). *Protecting industrial control systems.* Retrieved from www.controleng.com: http://www.controleng.com/single-article/protecting-industrial-control-systems/c07ce49f515a643842a41060a1d2e177.html

Weiss, J. (2016, Jul 19). *Assuring Industrial Control System (ICS) Cyber Security.* Retrieved from csis-prod.s3.amazonaws.com: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/080825_cyber.pdf

Whitman, M. E. (2016). *Management Of Information Security.* Boston: Cengage Learning.