

Automation & Network Disaster Recovery Planning (ANDRP)

By

Rockie S. Wolfe

December 2014

Submitted to the Graduate Faculty in partial fulfillment of the requirements for the degree

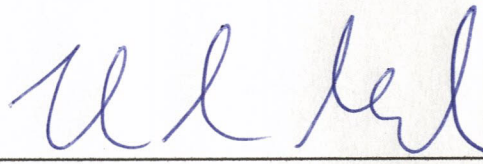
Master of Science in Industrial Management in the Department of Engineering

of the Pott College of Science and Engineering at the

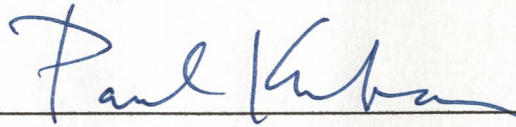
University of Southern Indiana

December 2014

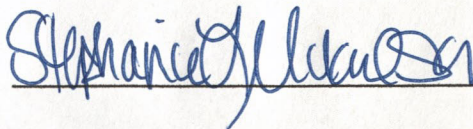
Accepted by the Graduate Faculty of the University of Southern Indiana,
in partial fulfillment of the requirements of the degree of
Master of Science in Industrial Management

A handwritten signature in blue ink, appearing to read "T. McDonald", written over a horizontal line.

Dr. Thomas McDonald, Assistant Professor of Engineering

A handwritten signature in blue ink, appearing to read "Paul Kuban", written over a horizontal line.

Dr. Paul Kuban, Professor of Engineering

A handwritten signature in blue ink, appearing to read "Stephanie Mikulski", written over a horizontal line.

Stephanie Mikulski, Sr. Engineer of Manufacturing and Process Automation

ABSTRACT

Wolfe, Rockie S. Master of Science in Industrial Management, University of Southern Indiana, December, 2014. Automation & Network Disaster Recovery Plan (ANDRP): Production floor automation and network become one. Major Professor: Dr. Thomas McDonald, Ph.D.

Automation has evolved into many levels of complexity and points of failure. In this research paper the focus is on automation disaster recovery methods and examples. Also, extra effort was put into the growing interdependency of automation and Information Technology (IT) in the modern manufacturing facilities of today.

Disaster recovery plans under the business continuity model is briefly discussed as research and articles in this area have been in print for decades if not centuries. Some discussion is covered in the benefit-cost analysis section. This short discussion is not meant to take away from the importance of benefit-cost analysis to artfully sell needed projects to procurement and upper management.

The research is broken down into five different yet related disciplines: Automation, Disaster Recovery Plans, Information Technology, the new Hybrid, and Benefit Cost Analysis. After covering the five different disciplines there is a follow up with an example application for Automation / IT Disaster Recovery Plan.

The intent of this paper is to create guidance for starting a disaster recovery plan in a manufacturing setting. Unfortunately no “one size fits all” and the many challenges of natural and intellectual negative effects on business continuity will demand a lifelong commitment to investment, education, and awareness.

ACKNOWLEDGEMENTS

I would like to thank my wife, family, and friends, as I have basically disappeared from the face of the earth, in my pursuit of higher education and research. I want to thank the professors at University of Southern Indiana (especially, in memory of Dr. David Schultz for accepting me into the graduate program) for believing in me and taking me to the next level in professionalism. Finally I want to thank all the good folks at Mead Johnson Nutrition and third party suppliers for giving me the opportunity to grow and apply my talents in the food industry.

TABLE OF CONTENTS

	Page
1. INTRODUCTION: Automation & Network Disaster Recovery Plan (ANDRP).....	1
Challenges: Yesterday, Today and the Future.....	1
Complacency is Not an Option.....	3
Five Areas of Study	3
Can't We Just Get Along.....	4
2. REVIEW OF LITERATURE AND RESEARCH	5
Break it Down	5
Challenges and Lessons Learned.....	17
3. PROCEDURE: Building a Disaster Recovery Plan.....	19
Building the Plan.....	19
Building the Data List.....	20
Brief Description with Examples.....	20
Do Nothing Scenarios	26
4. SUMMARY.....	28
Data Choices and Treatment.....	28
5. DISCUSSION	30
Conclusions.....	30
Recommendations.....	30
WORKS CITED.....	32

1. INTRODUCTION: Automation & Network Disaster Recovery Plan (ANDRP)

In the past couple of decades the manufacturing floor has experienced immense changes in technology. The days of operators interfacing with hardwired contacts and walls of gauges have been replaced by the Personal Computer (PC) screen with virtual contacts and gauges communicating with Programmable Logic Controllers (PLC's). Another technological change is the advent of IT and Information Management (IM). The IT and IM technology includes hardware like servers, switches, routers, PCs, and smart phones all connected by various forms of cables and wireless technology. Software may be dominated by, for example, Microsoft[®], Cisco[®], and Rockwell[®] to name a few; others are quickly gaining ground making inter-connected communications challenging.

Automation and Network Disaster Recovery Plan should be a top priority in every company. The first thing that must be understood is what is considered a disaster and to what level is feasible for backup and recovery. All downtime is costly, but when does it reach disaster level? This varies per company - it can be seconds, minutes, and if lucky hours before it becomes costly. Finally, what funding will a company put into a disaster recovery? Disaster recovery can range from as small as the component level to a large investment of a secondary redundant manufacturing facility.

Challenges: Yesterday, Today, and the Future

In the 1970's and 1980's a lot of the manufacturing systems were either stand alone or had limited communication structures as compared to today. There were communication platforms using serial and data highway interfaces, where field devices would communicate with PLC's. What changed was the desire to see data at PC's in

management's office. With this data, trends were built and the use of statistical measurement tools was added. The days of typing data into spread sheets were replaced by data automatically populating spread sheets.

Today's manufacturing plants are becoming increasingly more complicated. The marriage of automation and business side information systems has been troublesome. The two sides are two different disciplines, train of thought, and approaches to issues that arise in manufacturing. Common networks in manufacturing are configured with core, distribution, and access servers. Top level core switches are paired redundantly for fail-over capability. Second level involves distribution switches which are, also paired for redundant fail over capability. Strategically located throughout the plant floor are the access switches. A network will communicate and pass data to and from several hundred PLC controllers, Human Machine Interface (HMI), PC's and other automation electronic equipment up to and back from various servers. All servers and the core switches usually reside in a secure room separate from manufacturing. The distribution switches reside in the manufacturing area and centrally located to the access switches.

An example of a food manufacturing plant might have the liquid plant field switches and devices separate from the powder plant switch and field devices located in a different on-site building. One plant operation may be large and need redundant distribution switches between the core and access switches. The other plant operation may be small enough that a single access switch will communicate directly to the core switches. The redundancy system keeps downtimes in the seconds as opposed to hours in rebuilding a new switch. Switch failures are usually hardware or security breaches. A worst case scenario is a security attack or natural disaster and this can cause a network

system to be down for days, maybe weeks.

The automation side can use Rockwell® software “*Factory Talk Asset Centre*” for PLC, HMI software and automation communication configurations back up. Unfortunately, most companies use a wide variety of automation and software components. As much as possible should be backed up on a server. Server data should also be backed up, whether on backup tapes or perhaps the use of the “Cloud”.

Future challenges will only add to the need for an ANDRP to be in place. The idea of doing away with a room full of complicated servers and replacing them with Cloud storage, will add to security issues. Trusting hardware built by countries known for security issues will make manufacturing all the more susceptible to attack.

Complacency is Not an Option

Small as well as large companies need to have disaster recovery plans in place. The ideology of thoughts like, “who would want to attack us, natural disasters is rare, and we have virus protection software” is complacency only asking for trouble. The five areas of study below, will discuss the many ways disasters can occur and possible ways of risk mitigation to limit the effects of impending disasters.

Five Areas of Study

After months of research and my years of experience in the automation field, the focus for this paper is broken down into five separate areas of study.

- a. Automation: More and more plant floor devices and PLC’s use Ethernet to communicate within and outside of manufacturing,

creating more points of failure and intrusion.

- b. Disaster Recovery Plans: Disaster recovery, also known as business continuity, is now reaching down to the plant floor.
- c. Information Technology: focused disaster recovery on the business side is now challenged with, how to integrate with automation.
- d. Hybrid: In today's industry it is even more important now than ever that IT and Automation groups learn to work together.

Common ground must be found to protect the health and vitality of today's industries.

- e. Benefit and Cost: Economic studies must be done to justify cost to mitigate disaster for funding prevention and recovery measures.

Can't We Just Get Along?

There are studies in the human involvement of disaster recovery plans dating back centuries. Business side and Information Technologist have been working together for decades to prepare and protect companies from disasters. Now the new player in town is Automation and the weather has been stormy. Automation and IT Engineers work in two different worlds and have different approaches to disasters and how to protect against them. The IT professional is focused on protecting and maintaining flow of data for business continuity. The Automation professional is focused on reliability and efficiency of manufacturing and the safety of humans, environment, and automation equipment for business continuity. Even though both focus on business continuity and risk mitigation, conflict can arise from differing priorities and approaches.

2. REVIEW OF LITERATURE AND RESEARCH

Literature research for network disaster recoveries is easily available. Disaster recovery that includes factory floor automation is becoming more available as this relatively new frontier is evolving into a science of its own. The challenge is integrating this with other business needs. There is no “one size fits all” disaster recovery. Every company is unique and so will be its Automation and Network Disaster Recovery Plan.

Break it Down

In this section of the research paper, the focus will expand on the five different areas of disaster recovery disciplines. With emphasize put on Automation, Information Technology (IT), and the Hybrid of the two. Copious amounts of information and research are available for Disaster Recovery Planning (DRP) / Business Continuity and Benefit / Cost Analysis (BCA). Not to take away from the importance of the latter two, this research paper is the focus on the ever changing challenges to Industrial Control Systems (ICS) in the twenty first century.

Automation

This new segment of disaster recovery is quickly becoming a global concern. The days of stand-alone PLC's and Computer Integrated Systems (CIS) not connected to the World Wide Web are becoming a thing of the past. Unfortunately, the path that automation took was contradictive to a secure system. As factories advance technologically, the push is to limit human intervention and automate as much of a

process as possible. With automated controls, malware can infect a system and allow someone to take control of any or all of the system.

Standards have been created to help automation engineers fight cyber threats. ANSI/ISA-99 gives guidelines for improving control systems security. The challenge is “operators and engineers are under pressure to isolate automation systems at the same time as management is asking for greater interconnectedness” (Byres 26). Data compiled by the repository for industrial security incidents from 1982 to 2009 show only 24% of incidents were due to malware with the remaining being accidental in nature (Byres 27). With a quarter of disasters being cyber threat in nature, this adds a new level of awareness to automation.

Malware is not the only form of cyber-attack. With more of the chip manufacturing done out of the United States, lithography masks may be altered with undetectable backdoor accessibility or a kill switch built in. With a back door open, not only is malware a threat, but the use of False Data Injection Attack and Denial of Service (DoS), as well. The False Data Injection Attack is injecting a false number like pressure on a Human Machine Interface (HMI) monitor. The operator will think things are fine when in reality the attacker is sending pressure to dangerous levels. The DoS is more familiar, that is the operator or automation engineer no longer has control of the automated systems or PC's. The kill switch allows the attacker to stop the software when a certain code is sent. These types of attacks are overlooked; because, “hardware backdoors create significant security vulnerability since hardware is the root of trust, which software builds on” (Salem 2).

Cyber-attacks are not the only disasters to an automated system. Other disasters

that can be gauged from major to minor also happen. Major ones include natural disasters, terror attacks, and employee causes (intentional and non-intentional). Minor disasters can include power outages and hardware failures. Power spikes can affect software programs in PLC's, HMI's, Robotics, and Data Acquisition. The list is large and an ANDRP is essential to mitigate disaster. It is important to have backups not only of static data, but plant floor programs, as well. There are software packages that can help in backup, restoration, and change tracking for automation programs:

When a company needs to get back on its feet after a software crash, they can restore previously used programs and manage backup and recovery services with an automation control center that centralizes, manages, and maintains information (Fussel 2).

According to a web survey by ARC Advisory Group Inc. less than 50% of respondents have a disaster recovery plan (Callaway 1). Hopefully these percentages have increased from seven years ago.

Shown in figure 1, is an example of a typical Distributive Control System (DCS) in manufacturing. This figure shows the floor level automation components, computer interfaces, and communication branches.

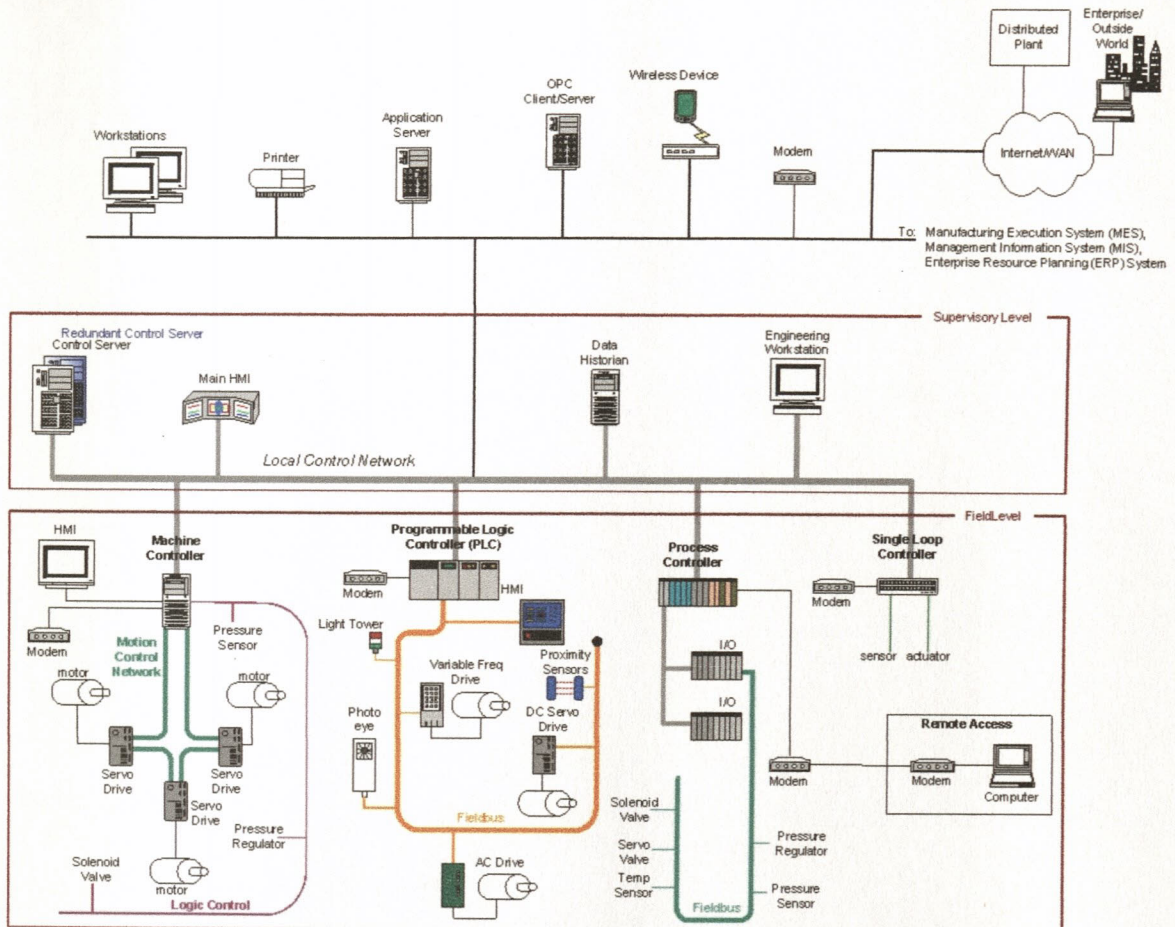


Figure 1 DCS implementation example (Falco, Scarfone, and Stouffer 2-11)

Disaster Recovery Plans

Disaster recovery plans have been around for a long time in the simplest form. Sometimes the wording of prevention versus recovery was used interchangeably. The mitigation and success of disaster recovery is derived from a well-planned prevention program. In terms of cost, manufactures will buy some prevention and some recovery; the real decision is how much of each to buy (Anderson 17). Today Reliability Engineering is a growing corner stone to disaster prevention. Reliability engineering, attacks predictable phases of disasters by using historical data and related cost to build a

value-based case. Automation and IT engineering has more focus on disaster related planning in addition to prevention.

Two phrases that are used interchangeably is disaster recovery and business continuity. The Business Continuity Plan (BCP) is necessary for keeping the business model working during a disaster recovery phase. There will need to be a way and perhaps a new place to conduct day to day operations. The ability to stay in contact with customers, pay employees, and provide a work environment for employees with communications abilities within and outside of the organization. Until the manufacturing facility or new facility is up and going there has to be a business plan to maintain customer confidence and loyalty until the disaster has passed.

Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored (Peters 2). The RTO level will vary for different business and technical areas. An example would be a core switch, which may be minutes (as it affects the entire plant) as opposed to a field switch or PLC that may be hours. Recovery Point Objective (RPO) is the place in time (relative to the disaster) to which you plan to recover your data (Peters 2). For example on the backup server, decide at what intervals to do partial or full back ups and which interval backup tapes are stored in a vault. Up until recently the disaster recovery plans included business continuity, IT, and infrastructure; but left out automation on the plant floor.

Information Technology

Information technology or information management DRP have been associated mostly with the business side in industries like telemarketing, banking, or health care

industries where data lost is devastating to business continuity.

IT includes hardware for data storage and retrieval from servers and communications with switches and routers. Standalone approaches have created major problems; whereas, if one piece of hardware goes down so does the entire network. To remedy this, redundancy is built in. Three typical DRP redundancy strategies found in the market are cold, warm, and hot standby (Al-Harbi and Soha 502). Cold standby is similar to warm but with less frequent mirroring and used for non-critical data sources. Warm standby as in cold standby uses two servers where a secondary server captures data from the primary server but at more regular intervals. Warm standby failover is quicker than a cold standby yet still the data may not be the same on either server. The hot standby is by far the best solution and used most often today. The hot standby is two identical servers and data is sent simultaneously to the redundant servers. High Availability (HA) clusters use software for redundancy, if one server fails the data traffic is quickly diverted to the remaining operating server. Load Balancing (LB) servers share the work load of data read/write to optimize response times. Taking this a step further, some servers have several identical hard drives called a Redundant Array of Independent Disks (RAID). In this case if one of the hard drives fails others are present and identical on the one server to take over. RAID storage disk zoning affects the disk array bandwidth, at present there are seven levels of RAID (0 – 6):

Weaknesses: data mirroring takes initially a very long time when issuing a backup server. Hot standby may be considered expensive for non-critical data. The HA clustering suffers from split brain which may cause data corruption (Al-Harbi and Soha 505).

All of these servers and computer nodes in the field will communicate through switches in some form of architectural topology. Most are familiar with the Cisco® family of switches and routers. Even at the communications level there is redundancy to build in on the manufacturing facility. Typically there will be two redundant core switches located in a high security area with the servers. These two core switches will talk to two redundant Distribution switches that fan out to numerous access (field) switches, which communicate with computers and automation equipment:

As corporate networks have converged with industrial networks, there have been many integration projects where proprietary networks or equipment were replaced with TCP/IP networks and commercial-off-the-shelf equipment. This shift in technology has greatly increased the complexity and “interconnectedness” of control systems. As a result, they now have many of the same vulnerabilities that have plagued enterprise networks. In addition, the controllers in these networks are now subjected to new threat sources that they were never designed to handle. (Byres 27)

The Hybrid section of this research paper will cover how and why IT is becoming a vital partner of Automation.

Hybrid

Today Engineers and Technologists are finding the growing necessity to not only have a strong knowledge in manufacturing automation, but also, an in-depth knowledge of information management and technology. Even if a person is not an expert in all fields, they must get educated to a high level in all disciplines to maintain and protect business

continuity. The Engineer and Technologist must be able to have an intellectual conversation with suppliers for what can and cannot be accomplished in house. This higher level of knowledge is imperative to guarantee your company is getting its returns on investments.

So which is it? Train the Automation Engineer / Technologist in IT / Information Management (IM) discipline or hire the IT/IM Engineer/Technologist and train them in Automation? Depending on the size of the company there will most likely already be both employed. The important thing is that both understand each other's responsibilities and objectives so an intellectual line can be drawn as to where one discipline stops and the other starts. Generally both the business and automation side will have networks and a firewall will most likely be the dividing line of ownership. IT must constantly install updates and security patches whereas this can bring down the automation side if research and caution is not used. So normally business side IT will have a firewall to the outside world and then a firewall (or sometimes referred to as a demilitarized zone (DMZ)) between business side IT and plant floor automation. To keep manufacturing and business side running, multiple layers of prevention will be installed (see fig. 2).

It is imperative that the ability to understand the importance of maintaining functionality during a network failover condition on the automation side is critical. When this fail over occurs the network traffic must be controlled or a cascading event will occur and cause communications to fail between automation equipment. Plans for outages are used to test updates since there is limited simulation capability in network updates and its effects on Industrial Control Systems (ICS). Also, stopping automation control systems without a controlled stop or shut down can be costly in time and product loss:

Additionally, in some instances, third-party security solutions are not allowed due to ICS vendor license and service agreements, and loss of service support can occur if third party applications are installed without vendor acknowledgement or approval. (Falco, Scarfone, and Stouffer 3-2)

In addition, in a manufacturer with regulated and validated systems, network and ICS changes may require the cost and time of revalidation of systems affected.

Not only does a sudden stop of ICS create the potential for loss of data, downtime and products, there is potential for bodily injury or loss of life. Risk management must be implemented in accordance with Occupational Safety and Health Administration (OSHA), Code of Federal Regulations (CFR), and Job Safety Analysis (JSA) to minimize hazards to humans in the work place. ICS that is not properly designed for fail conditions could also cause environmental impacts. A proper cross function of IT and Automation professionals must share their knowledge to mitigate risk that would expose proprietary data or cause manufacturing disruption. So a properly staffed organization is imperative as manufacturing advances in an ever changing and challenging environment. These are the major differences between IT networks and Industrial Control Systems in that disruption or damage to ICS have significant risk to humans, the environment, micro and macro economies, and loss of proprietary information.

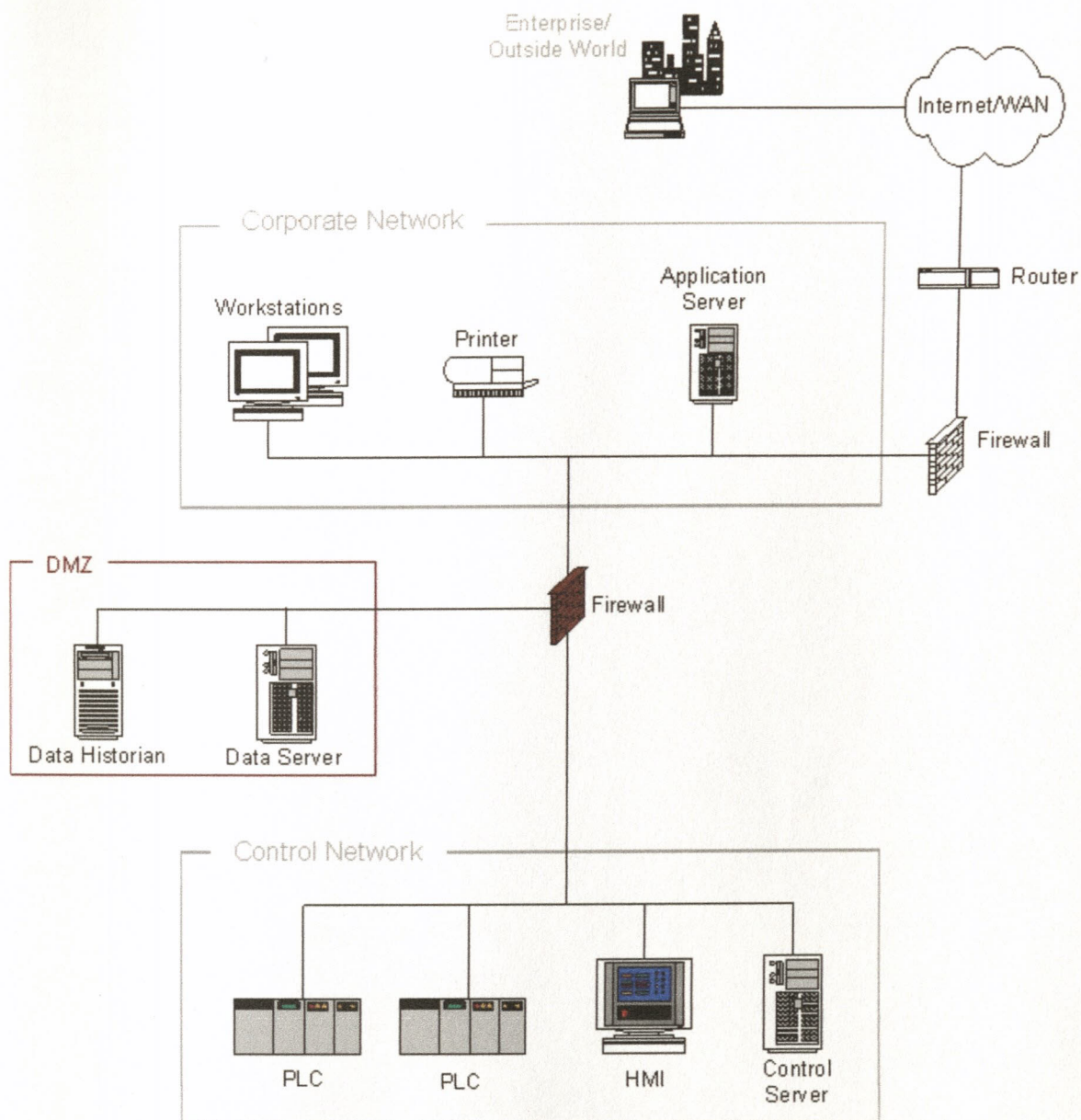


Figure 2 Firewall with DMZ between Corporate Network and Control Network (Falco, Scarfone, and Stouffer 5-7)

Cost-Benefit Analysis

Knowing the art of separating the speculation from the facts, a resulting analysis can be created. A manufacturing site should have a complete and comprehensive list of equipment and software. The list should include purchase price, depreciation schedule,

and life expectancy. With this data one can then calculate downtime cost:

Once the systems have been identified, attempt to quantify their impact relative to the overall business goals. If there are good estimates on the cost of downtime, this information can be used to complete an accurate cost – benefit analysis (Nickolett 4).

Sometimes the sale of an ANDRP can be mainly based on emotion, but often enough the sale must be based on economic factors like return of investment (ROI), loss of revenue, and loss of market share. With economic tools, companies make mutually exclusive decisions based on growing revenue quickly, so while Earnings Before Interest and Taxes (EBIT) is important, all things being equal top line (revenue) growth is more important than a cost reductions that increase EBIT by the same amount.

In benefit and cost analysis, the benefit is prevention of downtime or realization of downtime in present net value and future net value. How much does the company lose in revenue in hours, days, weeks, month, and yes perhaps years. Also, revenue losses might not affect the company as a whole, but areas in production. Loss of the network could affect all of production or just an area; the same for a server. As in the Stuxnet worm, this might only affect a piece of equipment through the Supervisory Control and Data Acquisition (SCADA) system (Falco, Scarfone, and Stouffer 3-20). If it is non-replaceable because it is outdated, then there is re-engineering cost and possible re-validation and long term stability studies before business continuity is possible. Competition will thrive on unpreparedness.

The cost is staffing (internal or external), equipment, and time. In some industries it is not just simply replacing equipment and down loading copies of original software,

but local and federal regulations might come into play. If the system is validated, it must be re-validated and this is an added resource cost that can add weeks or months before product is ready for market. If the system is not like for like (i.e., equipment, software, products, or packaging) then stability tests come into play and this added cost is lost revenue due to years of lost time before product is sellable.

Typically the biggest drivers in project acceptance are expected/anticipated productivity savings as well as ROI. Depending on size/cost of the project, the evaluation method might be based on present net value and incremental benefit cost analysis. So perhaps evaluating the ANDRP project based on a Strengths, Weakness, Opportunities, and Threats (SWOT) analysis and feasibility is the preferred approach. Project selection is never as simple as the one that has the best economic numbers. There are often intangibles that have to be considered, like available resources, consumer preferences (production area might not be worth replacing or repairing), and marketing dynamics. It is not always the “best” numbers project that should be selected, sometimes *do nothing* is an option. Perhaps a budget constraint is a barrier? Then start with minimal cost parts of the project to build upon until capital is available. Ask yourself questions: “is there already a large project in place? Will the present work load conflict with your project? Will this stretch resources and increase stress on the organization?” Know your audience. This might include management from Supply Chain, Finance, Quality Assurance, Compliance, and Engineering. This information will help in aligning with company goals, objectives, and core drivers to effectively sell the ANDRP project.

Challenges and Lessons Learned

In the recent past we have seen the increase of attacks on ICS and as history has proven, even the best DRP will be challenged. There are several examples of lessons learned:

There are three broad categories of ICS incidents including intentional attacks, unintentional consequences or collateral damage from worms, viruses or control system failures, and unintentional internal security consequences, such as inappropriate testing of operational systems or unauthorized system configuration changes. (Falco, Scarfone, and Stouffer 3-19)

Some intentional attacks include Worcester Air Traffic Controller in 1997, where a teenager using a dialup modem took down the airport controller phone and main radio transmitters, plus local home and business phones (Falco, Scarfone, and Stouffer 3-19). Maroochy Shire Sewage in 2000, where a disgruntled employee used remote control to take over ICS and create a major environmental impact releasing raw sewage into a local river (Falco, Scarfone, and Stouffer 3-20). The popular Stuxnet worm in 2010, a Windows Microsoft® computer malware used to specifically target SCADA systems was speculated for damaging equipment at an Iranian nuclear facility.

A few unintentional attacks include an incident in which the CSX Train Signaling System in 2003 was hit with the non-targeted Sobig computer virus (Falco, Scarfone, and Stouffer 3-20). This shut down and disrupted the CSX train transportation system for up to six hours before normal safe operation was resumed. David-Besse nuclear plant in 2003 was hit by a non-targeted worm the Slammer. The Slammer a Microsoft SQL®

worm took down this nuclear plant and five other utilities for many hours (Falco, Scarfone, and Stouffer 3-20). A final example, the Bellingham, Washington gasoline pipeline failure in 1999, caused death and injury in addition to the property damage (Falco, Scarfone, and Stouffer 3-21). This was caused not by a virus or worm; but due to a poorly performing and tested SCADA system.

So whether the disaster is intentional or non-intentional it is difficult to realize all the possibilities that can occur. This is why it is important to do research and stay on top of recent and past events in hopes that lessons learned will not come from your place of business.

3. PROCEDURE – Building a Disaster Recovery Plan

This section contains examples and brief descriptions of an example ANDRP. This is only an example and is not all inclusive. Each manufacturing facility is different and so will their ANDRP be.

Building the Plan

The plan for implementation includes several steps and coordinated meetings with key stake holders.

1. Make a detailed asset inventory list: This includes hardware, software, and dates.
2. With this list start the owners list: this is who and at what level internal and external stake holders will be responsible for.
3. Meet internally to verify asset list and roles of responsibility.
4. Decide internally what will be the varying levels of disasters and assign ratings.
5. Meet with external contract suppliers to share findings and get feedback to complete the ANDRP layout.
6. Once the ANDRP lay out is complete, start compiling cost. This will be cost from contractors based on time and assets. Also there will be cost evaluated for internal backup hardware to keep on site (prioritized by risk, cost, and shelf life)
7. Plan on a meeting to finalize the ANDRP: this will also include discussing what types of mock disaster recreations are deemed important and feasible. Also get cost to involve contractors to do such a mock ANDRP execution.
8. Document mock ANDRP execution and lessons learned.

9. Create Standard Operating Procedures that can be done internally so preventive maintenance will mitigate the extent of disaster. This will increase the effectiveness of ANDRP.

Building the Data List

There are software programs that have utilities that will compile lists of hardware and software on the network and server side. The ICS automation side may include some leg work and hours if not days of compiling a data inventory list. It is important to include manufacture names, software and revision identifiers, and support contracts at a minimum.

Brief Descriptions with Examples

Things to consider

- i. In case of power failure or having to pull the network plug, what should be your device failover states?
- ii. What's the backup power plan in the event of a squirrel or Mylar® party balloon creating havoc in a power distribution center?
- iii. Where will the data backup tapes be stored?
- iv. Are the insurance and support agreements up to date?
- v. If a PLC or HMI dies, where are the backup programs?
- vi. Add more that would be specific to your company.

Create the SWOT analysis

The purpose of establishing an automation and network disaster recovery plan is to map out hardware, its location and critical systems networked dependent. The opportunity is having a set of guidelines in place that cover varying levels of disasters to recover from. The problem is keeping such a document in place and updated yearly.

Complacency is the death of all good processes. In table 1, a SWOT diagram is created with examples for the Strengths, Weakness, Opportunities, and Threats columns.

Table 1 SWOT diagram

Strengths	Weakness
1. Fail over in critical servers and switches 2. Backup tapes stored in secured vault 3. Automation software storage 4. Local third party support	1. Increasing complexity of network 2. Specialized training 3. Dependence on network 4. Limited standardization in automation.
Opportunities	Threats
1. Standard operating procedures 2. Third party support disaster drills	1. Natural disasters 2. Software attacks 3. Dated hardware

Create the disaster ratings list per area

Break the manufacturing plant into logical areas. The bulleted list below shows areas representing equipment, and potential failures / disasters. Disasters have been listed from “1.” being worst case to higher number being more feasibly addressable.

Include alternatives into areas with a list of potential failure possibilities. Keep in mind within these areas there can be different equipment with similar yet unique failure

possibilities.

- *Secure IT/IM room*: is where servers and core switches reside:
 1. Lose the complete floor – Unless another secondary redundant manufacturing liquid plant capability is available, the liquid plant is down indefinitely. The powder plant can still run in stand-alone mode.
 2. One or, worst case scenario, all communication fibers damaged - Have contractor information available to start repairs immediately.
 3. Virus / Hack attack - Disconnect from business side, shut down PC's and isolate virus / hack attack. Have plan and training in place for such an event. Depending on damage extent, minimal damage can be handled by in-house automation technicians; severe damage will require assistance from contractors
 4. Fire or water damage and to what extent - Depending on damage extent, minimal damage can be handled by in-house maintenance; severe damage will require assistance from contractors.
 5. Power Lost - for how long and cause - Depending on damage extent, minimal damage can be handled by in-house maintenance; severe damage will require assistance from contractors.
 6. One or more core switches down and cause - Depending on damage extent, minimal damage can be handled by in-house automation technicians; severe damage will require assistance from contractors.
 7. One or more Servers down and cause - Depending on damage extent, minimal damage can be handled by in-house automation technicians.

If damage is severe, contractors will be required until servers are up and running.

8. Cooling systems down - Depending on damage extent, minimal damage can be handled by in-house maintenance; severe damage will require assistance from contractors.
- *Distribution Switch room*: is where the distribution switches reside and supply only the liquid plant:
 1. Secure room; core switches or severs down and cause - Depending on damage extent, minimal damage can be handled by in-house automation technicians; severe damage will require assistance from contractors.
 2. Fire or water damage and to what extent - Depending on damage extent, minimal damage can be handled by in-house maintenance; severe damage will require assistance from contractors.
 3. Distribution switches down and cause - Depending on damage extent, minimal damage can be handled by in-house automation technicians; severe damage will require assistance from contractors.
 4. One or worst case scenario all communication fibers damaged from core switches - Depending on damage extent, minimal damage can be handled by in-house maintenance; severe damage will require assistance from contractors.
 5. One or more communication fibers damaged to field switches - Depending on damage extent, minimal damage can be handled by in-

house maintenance; severe damage will require assistance from contractors.

6. Virus / hack attack - Disconnect from business side, shut down PC's and isolate virus / hack attack. Have plan and training in place for such an event. Depending on damage extent, minimal damage can be handled by in-house automation technicians; severe damage will require assistance from contractors.
 7. Power loss - Depending on damage extent, minimal damage can be handled by in-house maintenance and automation; severe damage will require assistance from contractors.
- *Liquid Plant*: Several field switches and several hundred PLC controllers, HMI's, PC's and other automation electronic equipment:
 1. Distribution switch room; One or more distribution switches down - Depending on damage extent, minimal damage can be handled by in-house automation technicians; severe damage will require assistance from contractors.
 2. Virus / hack attack - Disconnect from business side, shut down PC's and isolate virus / hack attack. Have plan and training in place for such an event. Depending on damage extent, minimal damage can be handled by in-house automation technicians; severe damage will require assistance from contractors.
 3. One or more access switches down - Depending on damage extent, minimal damage can be handled by in-house automation technicians;

severe damage will require assistance from contractors.

4. Power loss - Depending on damage extent, minimal damage can be handled by in-house maintenance and automation; severe damage will require assistance from contractors.
 5. One or more PLC controllers, HMI's, PC's and other automation electronic equipment down - Depending on damage extent, minimal damage can be handled by in-house maintenance or automation technicians; severe damage will require assistance from contractors.
- *Powder plant*: couple of field switches with several PLC controllers, HMI's, PC's and other automation electronic equipment:
 1. Secure room; core switches or severs down and cause - Depending on damage extent, minimal damage can be handled by in-house automation technicians; severe damage will require assistance from contractors.
 2. Fire or water damage and to what extent - Depending on damage extent, minimal damage can be handled by in-house maintenance; severe damage will require assistance from contractors.
 3. Power loss - Depending on damage extent, minimal damage can be handled by in-house maintenance and automation; severe damage will require assistance from contractors.
 4. Access switches down and cause - Depending on damage extent, minimal damage can be handled by in-house automation technicians; severe damage will require assistance from contractors.

5. One or more PLC controllers, HMI's, PC's and other automation electronic equipment down - Depending on damage extent, minimal damage can be handled by in-house maintenance or automation technicians; severe damage will require assistance from contractors.

Do Nothing Scenarios

Hardware

Do nothing: this is the reactive approach whereas the company waits until a piece of equipment fails and then tries to replace.

1. Not only is there downtime cost but also increased shipping cost in expediting delivery. Also keep in mind that as hardware changes, present software may no longer communicate with the new hardware.
2. Have a reliability program in place to extend equipment life.
3. Have a replacement program in place: With lean manufacturing, on hand parts stock can be limited. Keep an asset list and stay in contact with local suppliers.
4. Not keeping up with new and obsolete hardware might lead to searching and purchasing on EBay.

Software

Do nothing: everything works fine and everyone knows the present software, why rock the boat.

1. Document and backup software; as employee landscape changes, there is hope someone can work with the old software.
2. Recognize software shelf life: All software gets to the point that it is no longer supported by Original Equipment Manufacturer (OEM) suppliers. Older PC's may no longer be able to run new software.
3. Older versions of Microsoft® software may become obsolete and no longer supported. The newer versions of Microsoft® software may not support older versions of automation software.

Training:

Do nothing and learn from the school of hard knocks which can lead to costly downtime

1. Use company history to justify head count and cross train new employees with seasoned employees.
2. Create Standard Operating Procedures (SOP) and mentoring training.
3. Specialized training from OEM suppliers.
4. Degree advancement training from accredited colleges.

4. SUMMARY

In today's manufacturing plants statistical data is required in real time to remote and onsite offices outside of the DMZ firewalls. This real time data can be used to check online efficiency and down time rates. This data can also be historical with trending for finding disruption in plant processes.

Data Choices and Treatment

As in all statistical data the choices and how the data is treated can be overwhelming. To make this more manageable, first, break the process into five steps Define, Collect, Organize, Visualize, and Analyze (DCOVA) (Levine and Stephan 396). DCOVA, not to be confused with, is similar to Six Sigma; Define, Measure, Analyze, Improve, and Control (DMAIC). Second, define the data by what benefit is and what cost is. Remember that benefits versus cost can vary by individuals or institutions; one person's benefit might be another's cost. A single point of view can be adequate, but include more than one point of view, and then several analyses might be necessary.

Collecting and Organizing the data is two steps in one. Before data is collected, decide how to organize the data. A typical model for benefit-cost analysis is creating a parameters table, an incremental-effect model, a table of costs and benefits over time, and a table of possible investment results and a statistical and graphical analysis of net present values and investment risk (Watson 12).

After a comprehensive benefit-cost analysis is completed then other methods should be considered. A risk analysis should be conducted, compare any alternatives, and

then apply sensitivity analysis. A lot of time and calculations are done when creating the sale of an ANDRP to management.

Visualize the data is deciding what graphs and plots will you create for managers who will give you maybe an hour to present the case. We are all aware of the many types of visualization with Bar Charts, Histograms, Percentage Polygons, Scatter Plots, Time Series Plots, Pivot Tables, and Cause-and-Effect diagrams. Sometimes misrepresented data or common errors can occur in visualized data. Nothing is more embarrassing than having your data questioned and then having to reschedule another meeting at a later date.

Finally, analyze your data to reach conclusions and find areas of opportunity. The use of statistical tools that is available in Microsoft Excel® make for ease of application and results. Other methods like redundancy allocation model (Shao 1381), contingent valuation method, and discounting to reach conclusions:

According to the governmental Office of Management and Budget (OMB) guidelines for performing BCA, it is inappropriate to use variations in the discount rate to adjust the calculation for particular project risks. But many analyses can capture uncertainty by adding a factor to the discount rate to compensate for the added risk associated with uncertainty (Ganderton 21).

Contingent valuation method is the use of hypothetical scenarios in surveys to find the willingness and to what amount a respondent will pay for hazard mitigation. So do not confine yourself to narrow types of data and ways to represent them, the stars are the limits in selling you ANDRP.

5. DISCUSSION

Conclusions

Today's challenge is tomorrow's accomplishment. Preparedness for external or internal attacks, intentional or non-intentional disruption, natural or human induced disasters are only as good as the weakest link in the company's ANDRP.

The days of IT/IM, Mechanical, and Electrical Engineers/Technologist must make room for the new player in the 21st century, The Automation Engineer and Technologist. The knowledge base needed to create and maintain an ANDRP will be the multi-disciplined Automation Engineer and Technologist. Universities and businesses must realize the broad knowledge base needed not only in automation; but IT knowledge, business modeling, Statistics, and Safety. As well, those already in the field of Engineering and Technology must broaden and hone their skills for an ever changing and challenging environment in the future of manufacturing.

Note, a successful ANDRP is protecting yourself, your company, your environment, and a being a good steward to the community.

Recommendations

I feel that it would be unprofessional and misleading of me to recommend only a few documents that will fill your needs to conduct an all-inclusive comprehensive knowledge base for a successful ANDRP. Nonetheless, these reference documents are provided:

1. NIST Special Publication 800-82 (Falco, Scarfone, and Stouffer)

2. ANSI ISA 99 (Cosman)
3. Rockwell® Industry Direction Convergence (Fraser and Zimmermann)
4. Cisco® Ethernet to the Factory Solution (Cisco®)

WORKS CITED

- Al-Harbi, Eman., Soha S. Zaghoul. "A SWOT Analysis on Cisco® High Availability Virtualization Clusters Disaster Recovery Plan." Faculty of Computer and Information Science Department of Computer Science. King Saud University. 2013. Print.
- Anderson, Mary B. "Which Costs More: Prevention or Recovery?"
- Byres, Eric "Revealing Network Threats, Fears – How to use ANSI/ISA-99 standards to improve control system security" ISA InTech Magazine Jan/Feb. 2011 Web. 7 Aug. 2013. < www.isa.org/standards-and-publications/isa-publications/intech-magazine>
- Callaway, Erin. "Disaster Recovery Planning – DRP: Is Your Factory Floor Data Safe?" Managing Automation 03 Nov. 2006 Web 11 Aug. 2013. <<http://www.managingautomation.com/maonline/magazine>>
- Cosman E. "Security for Industrial Automation and Controls Systems" American National Standard ANSI/ISA-99.00.01-2007 29 Oct. 2007. Print.
- Falco, Joe., Scarfone, Karen., Stouffer, Keith. "Guide to Industrial Control Systems (ICS) Security" NIST National Institute of Standards and Technology Special Publication 800-82. June 2011. Print.
- Fraser, Julie., Zimmermann, Ray. "Come Together: IT-Controls Engineering Convergence furthers Manufacturers' Success" Rockwell Automation® June 2007. Print.

- Fussel, Ellen. "Preparation is Key to avert Disasters – Controllers, backup prevent lost production" ISA InTech Magazine Oct 2003, Web. 7 Aug. 2013. <<http://www.isa.org/standards-and-publications/isa-publications/intech-magazine>>
- Ganderton, Philip T. "Benefit-Cost Analysis of Disaster Mitigation: A Review." Economics Department, University of New Mexico. n.d. Print.
- Levine, David., Stephan, David. "Teaching Introductory Business Statistics Using the DCOVA Framework." Decision Sciences; Journal of Innovative Education. Sept. 2003. Print.
- Nickolett, Chip. "An Overview of the Disaster Recovery Planning Process – From Start to Finish" White Paper, March 1999. Print
- Peters, Mark. "Implementing the Right High Availability and Disaster Recovery Plan for Your Business." Enterprise Strategy Group, August 2010. Print.
- Salem, Malek B. "Security Challenges and Requirements for Control Systems in the Semiconductor Manufacturing Sector"
- Shao, Benjamin B. M. "Allocating Redundancy to Critical Information Technology Functions for Disaster Recovery." W. P. Carey School of Business, Arizona State University. n.d. Print.
- Watson, Kenneth. "Benefit-Cost Analysis Guide" Treasury Board of Canada Secretariat 1999. Print.
- White Paper (no author) "Cisco Ethernet to the Factory Solution: Securing Today's Global Networks in Industrial Environments" Cisco® White Paper n.d.