Risk Analysis for

Industrial Control Systems

Abstract

You have been asked to perform a risk analysis of an Industrial Control System (ICS). How do you do this? What is different in analyzing the risks to an ICS as compared to any other system used by the business? How do you report this so that your findings can actually make a difference? Industrial control systems can be evaluated for risk using a standard methodology. This methodology must be tuned to the specific concerns of your ICS environment. Once you have tuned this methodology to reflect your environment, the assessor will be able to reliably and consistently produce ICS Threat Risk Assessments (TRAs) that can be understood by decision makers. This information will enable them to provide a reasonable level of safety to people as well as guide the business for best results.

# 1. Introduction

Risk has been generally understood and analyzed since the 17th century (Bernstein, 1998). Measuring risk has long been a staple of the insurance industry. In the past few years risk has interested the business world in general. This is expanding to all areas of the business including ICS. Many organizations, such as those in healthcare (Office for Civil Rights, 2014) or energy transmission (NERC, 2015) are even required by law to incorporate risk analysis into their decision making process.

Risk is not just “what could go wrong”, although looking at what could go wrong is part of risk analysis. There is inherent risk in operating any business. People, assets and information must be protected, but you can’t protect everything completely. The business has to prioritize. Identifying the highest areas of risk, documenting and communicating them will let business leaders decide on the appropriate technical and procedural controls that can reduce the risk.

The following document will help a Risk Assessor develop an appropriate (TRA) process. Although this paper will focus on understanding and then tuning the standard methodology for use with ICS systems, the methodology itself is common to most threat risk assessment processes.

# 2. What is so different about ICS risk analysis?

Information Security often starts using risk analysis when implementing ISO 27001. In section 2.2 of ISO 27001, the reader is told to “identify all information assets in the organization… and assign a value to each asset in terms of the worst-case impact the loss of confidentiality, integrity or availability (CIA) of the asset may have on the organization” (International Organization for Standardization , 2013). For information, this makes sense. Each element of the CIA triad may be the most important depending on the nature and use case of the information. Although the information is important to the business, no-one can get hurt. Business risk calculations are all about money (Peavier, 2014). Money is important, but it won’t physically hurt anyone. If something goes wrong with an Industrial Control System, it is possible people can be hurt or killed. To take this into account, some assessors have said that ICS risk priority uses Availability, Integrity and Confidentiality in that order. Justin Searle’s ICS 410 class (Searle, 2014) challenged this to say that Integrity is just as important as Availability. This needs to be taken a step further: For ICS confidentiality should be removed from the equation and be replaced with Safety: SAI.

# 3. What is the Goal of Having an ICS Risk Assessment Process?

ICS risk assessments should provide the opportunity to minimize harm while alerting the business to risks that had not been considered before. It should also provide information as to the impact and probability of loss. This will let the business make properly informed decisions. Ultimately, management is the final decision maker and holds the responsibility. Responsible managers have access to information and considerations that the assessor does not. Management may accept your recommendations, implement alternate controls or do nothing at all. If the assessor has clearly documented and communicated their findings, they have done their job.

Occasionally, management will only want a threat/risk assessment process for compliance. They aren’t thinking about how it can be useful; they just want to show the auditor that they have a process. If you are in this situation, don’t try to force management to do more. Implement a basic system and used it to create awareness. Eventually you can evolve it into a more comprehensive system. A good example is the binary.io [work card](http://binary.protect.io/workcard.pdf) (Sapiro, 2013). It is very quick and simple to use. Its simplicity comes at the cost of being thorough. Using the work card can make others aware of the benefits of threat risk analysis without a lot of effort.

There are many other systems out there. You can be guaranteed that at least one person will ask why you aren’t using their favorite. Fortunately, most systems can be mapped to the standard methodology. Knowing this standard methodology will help you explain your decisions.

# 4. Why don’t we just use method X?

Threat/risk assessment systems and methodologies can be distilled down to three categories:

1. Developed by xxx government. It is used by everyone in their jurisdiction. Use of this system is generally mandated or legislated. If you live in that jurisdiction, you will use that system. Most of these systems use the standard methodology but have been adjusted for concerns specific to the economic, geographic or political focus of the government that had it created. Examples include CRAMM (Yazar, 2002), the All Hazards Risk Assessment Methodology (Public Safety Canada, 2014), MAGERIT (MINISTERIO DE ADMINISTRACIONES PÚBLICAS, 2012), and the Dutch A&K Analysis system (European Union Agency for Network and Information Security, 2015).
2. Developed for yyy industry. This system is used by companies in that industry. These generally take the standard methodology and identify common threats, vulnerabilities, asset valuations or outcomes within that particular industry. For example, the Airlines Risk Management Solution (ARMS Working Group, 2013) covers common problems with aircraft and how they should be handled. At its core, though, it still uses the same principles that will be explained here. FAIR (Jones, 2005), HIPAA Risk (Office for Civil Rights, 2014) and NIST 800-30 (JOINT TASK FORCE TRANSFORMATION INITIATIVE, 2012) also follow this methodology. These systems work well until they encounter a situation that is not covered! At that point the assessor must go back to the standard methodology to properly modify the system to accommodate the change.
3. Just use Risk = (whatever you read about on the internet today). These are usually someone’s idea of the day and they are looking at a very specific problem that they are dealing with at that time. Unless the assessor is dealing with the same problem that author is, these need to be considered with a grain of salt.

In order to understand the standard risk assessment methodology, we need to break it down into basic components.

# 5. What is Risk and How Do We Define It?

Risk is practically defined (Jones, 2005) as “the probable frequency and probable magnitude of future loss”. We need something more quantifiable for evaluating ICS systems so we will use

Risk = function of (Asset value, Vulnerability impact, Threat frequency or probability)

Different industries may use different terms for each area. This is acceptable as long as they are not used to change the intent.

## 5.1 The Function

The actual function varies because of the intangible value of human life. As such it is very difficult to express mathematically. Mathematical models can also be difficult to use and are only required when a wide range of values are needed. As a practical alternative, we will use matrixes to provide the function. They are easy to use and easily modified to provide the level of detail that works best for your organization. Assigning death and injury is relatively easy. Each just has their own column in the matrix. Matrixes are covered in more detail in section 7.1.1.

## 5.2 Asset Value

Asset value is relative to the asset owner and may be defined in many ways including annualized loss, one-time loss, replacement cost, CIA, loss of reputation and number of deaths. The value of the asset is decided by the business unless that is superseded by regulation. For ICS systems, this means making sure that people do not get hurt or killed is paramount. Next we look at the cost to the business if the asset isn’t functioning properly. Finally, we look at the cash value of the asset. Quite often management will only look at the financial value of an asset. If it appears they do, confirm that they are expecting you bring forward any chance of death or injury.

## 5.3 Vulnerability and impact

A vulnerability is “This means the item in question can be damaged or have a loss in value. When evaluating a vulnerability, look at the control weakness (also called prevention) as compared to the impact. Impact is also known as severity or detection, response and recovery. In simple terms, “how bad would it be?” Sometimes a vulnerability can be fixed within a system itself. Other times outside protection, also called a compensating control, needs to be put in place.

5.4 Threat and Frequency or Probability

A threat is “someone or something that could cause trouble, harm, etc.”[[1]](#footnote-1) This includes natural disasters, human error and malicious intent. Threat can also be looked at in terms of “what could go wrong” and “what are the chances”. For our calculations, threat is a function of its frequency (or likelihood) vs. its impact (also known as gravity). We compare the two determine the threat level.

**Nothing is invulnerable, but it may have no value.**

**If something has no value, there can be no risk to it.**

**Something that is vulnerable is safe if nothing is going to hurt it.**

**If there is no threat, there is no risk!**

# 6. Threat and Risk Assessment (TRA) Process

So what is this standard methodology? It consists of the following steps.

## 6.1 Informal TRA

This is also called a cursory or high level TRA. Its main purpose is to quickly determine if a full TRA is needed. Quite often, this will be done during the discovery phase of a project to help determine if the project being evaluated is worthwhile to take on. For an ICS system, you would look at possible injury and if the operation was routine or not. If the probability of injury is low and the operation is routine, a TRA is not needed. If a TRA has never been performed on this operation before, you may want to perform one so that you have a benchmark going forward.

A good example would be an expansion to a rail loading facility. Although there is the possibility for loss of life or damage to cargo if things went wrong, the assessor may decide that only an informal TRA is necessary because the company building the terminal is using the same blueprints and process that they have use to construct 15 identical terminals that are already in use. A full TRA would have been performed for the first loading facility that was built.

## 6.2 The Threat Risk Assessment

The process used when conducting a risk assessment is the same regardless of the type of assessment. The depth of analysis may be significantly different. The process is comprised of the following four main steps:

**Threat Risk Assessment Process**



Initiation

Gather Information

Analyze Risk

Report Risk

These terms may be interchanged with ITIL (Glenfis AG) and ISO 27001 terms of plan, check, act, do (International Organization for Standardization , 2013). Use which one is most appropriate for your business. The recommendation is to use the same wording as management.

During the entire process, the Information Risk assessor will consult and communicate with all stakeholders including the business unit owners, users, technical contacts, Information Systems (IS) staff, Operational Technology (OT) staff, management, and any third-parties.

## 6.2.1 Initiation

1. Obtain Management Commitment. Make sure there is a business owner who will be ultimately responsible. This is a key component. Most assessments will fail without management commitment.
2. Determine what laws, contracts and standards that you have to comply with. With the exception of NERC/CIP 5 (NERC, 2015), legislations are generally very vague. This works in your favor if you really understand your subject. If you don’t, you will have to be thorough with your analysis which will force you to understand your subject.
3. Determine the Scope of the Assessment – this is generally defined as all systems that encompass or interact with the system being evaluated. The scope may be narrowed to the subset that will actually be changing.

Example: A chemical mixing system needs to have a control valve replaced. A full TRA should look at the complete mixing system, but a narrowed scope would only look at the Human Machine Interface (HMI) and Safety Instrumentation System (SIS) that directly interact with the new valve.

1. Select the TRA Team – This will be the risk assessor plus all business, OT and IS members on the project team. Legal, Human Resources and Occupational Health and Safety (OHS) may also be required. If the risk assessor feels that they need to bring any staff member onto the team, they bring them onto the team.

## Gather Information – Asset Identification and Valuation

1. Identify Assets – This is done by reviewing the implementation plan and diagrams as well as interviewing business owners, administrators, users and operators to define the boundaries of the system. The assessor should not be confined to what the project teams hands her. If she feels that she needs information directly from a particular business user or any other individual that has relevant experience, she needs to be free to go and get it.

Example: The project team gives the assessor architectural drawings and manufacturer’s specification sheets for the installation of a new transfer pump. This may be enough, but if the assessor decides that they want to talk to the lead maintenance hand that has repaired the old pump for 10 years, they go and talk to them. The lead hand may provide information on the reasons for the failures that will help the assessor determine if the new pump will be a greater safety hazard.

1. Assess Injuries and Assign Asset Values –Quite often the values used will be driven by fines for non-compliance or penalties for breach of contract. Material assets may be viewed as having a one-time replacement cost or an annualized replacement cost. Determining which of these two methods to use often involves meetings with the accounting and insurance departments. Please note that the value of human life is considered to be higher than any material, financial or data values.

There will be situations where the Risk Assessment ends with the Asset Valuation. If the asset is considered to be of low value or that any possible incidents will not cause any harm, it may be decided that it is not worth the time and effort to complete the TRA.

## 6.2.3 Analyze Risk – Vulnerability Assessment

Vulnerability Assessment is quite often overlooked. Although it may be accurate to do so in some cases, the assessor is missing valuable information by not considering the specific vulnerabilities. It is technically correct to say “children are vulnerable to the impact of a car”, but making this kind of vulnerability statement misses the point. Saying “children don’t understand what will happen if they are hit by a car” opens the door to many more scenarios and mitigations. Vulnerability assessments can also provide a shortcut when determining how best to mitigate risks. For example, if the vulnerability is “no lock on door”, the obvious remediation is “install lock on door”.

## 6.2.4 Analyze Risk– Threat Assessment

Who or what would actually threaten this system? There may be active threats such as a disgruntled employee or passive threats such as not performing routine maintenance. Quite often recognizing threats is driven by experience and keeping up with news and information feeds. If the assessor doesn’t have the experience, they should rely on interviews with the appropriate staff members who do. Manufacturers specifications may say that a part will only fail once every 10 years, but the mechanic who actually performs the maintenance will have the logs books to show that the part usually only lasts 6 years.

## 6.2.5 Analyze Risk – Calculation of Risk

Once we understand both the treats and the vulnerabilities, we can use them to calculate risk. We look at the frequency or **likelihood** of each threat. We then compare that to the **impact** of the vulnerability and what preventions are in place to protect the asset.

## 6.2.6 Report Risk– Recommendations

Recommendations always need to be worded in terms of impact to the business. Although some consequences, such as loss of life may appear obvious, it never hurts to show awareness of the impact loss of life would have on the business. Quite often senior management might not be aware of the scale of the impact. They may be thinking “someone could get hurt” when the reality is “many people will die”.

Management may decide to accept the risk and not do anything about your findings. That is their prerogative. If they choose do this, document it and have them sign off on their decision.

Warning to business leaders: Don’t make the “[Ford mistake](http://en.wikipedia.org/wiki/Firestone_and_Ford_tire_controversy) (Corona&Komendanchik, 2008)” of deciding that it would be cheaper to pay out the costs of people dying from a flaw as opposed to fixing the flaw.

## 6.2.7 Repeat

Risk assessments are a point in time evaluation. They should be repeated on a regular basis. Frequency of the evaluation will depend on the initial threat rating, rate of change and value of a system. Things like media attention or changes in legislation may also influence this.

6.2.8 Act

Remediation of findings doesn’t always fall to the assessor in ICS environments. However, it will be the responsibility of the assessor to document any remediation. Quite often spreadsheets are used for this function, but tools such as Simple Risk (Sokol, 2014) are highly recommended as they make tracking the remediation of multiple risks much easier.

# 7. How do I customize this for my organization?

The above steps are general. They need to be focused specifically on the ICS environment that they will be used for. If you find that you are always evaluating the same types of systems, many of these steps can be streamlined or you will find that the basic information never changes. The laws that your company has to comply with won’t change that often. Your threat, vulnerability and risks matrixes should rarely change.

We will demonstrate this by going through each step as it would be used by a fictitious organization – Downhole Inc. Downhole is a low volume, high precision manufacturing firm that makes downhole measurement, fracking and wireline tools for drilling rigs. Downhole is preparing to release a new multipurpose tool that combines features of their current pulse tool with sensor that uses an explosive shock to measure surrounding rock formations. The TRA process that is developed will initially focus on the changes needed to modify their production facility to handle the required equipment and storage. The TRA process will be developed by the IT guy who supports the manufacturing floor as well as the wireline trucks..

7.1 Preparation

### 7.1.1 Management Commitment

As one of the most critical parts of TRAs, management commitment needs to be developed as part of the corporate culture. Start by getting management buy in to perform TRAs on high value systems. These will be the easiest systems to get support for because of their value. As management and staff become more comfortable with the process, they will accept TRAs on other assets. At this stage they usually start requesting assessments on their own. Ideally, the mandate for TRAs will be “everything in the organization is evaluated for risk”. This takes time.

For organizations that have a considerable safety focus such as oil and gas or construction companies, this can be developed as an extension of the OHS requirements that already exist.

Compliance is also a common reason for starting a TRA program. It is a requirement for many pieces of legislation including [HIPPA](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf) (Office for Civil Rights, 2014), [PCI](https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v1.pdf) (PCI Security Standards Council, 2015), [NERC](https://www.esisac.com/Public%20Library/Documents/Security%20Guidelines/Vulnerability%20and%20Risk%20Assessment,%20Version%201.0.pdf) (NERC, 2015) and [CSA z246.1](http://www.ccohs.ca/oshanswers/hsprograms/risk_assessment.html) (CSA Group, 2013).

#### What you need to do:

1. Get backing – preferably in writing - from:
   1. The project sponsor.
   2. The person who authorizes payments.
   3. The project manager.
   4. CxO (Chief Executive, Financial or Information Officer) or Vice President.
2. List the laws, standards and contracts that you have to comply with.
3. Determine matrix size and document why you chose this size.

Most threat, vulnerability and risk matrixes are based on a 5 square by 5 square (5x5) matrix, but the best size for your needs depends on a few different factors. Smaller matrixes are easier to work with. This is why university risk courses always start with a 2x2 matrix. Executives in your company may already have a matrix that they use. There is a good chance that it is a 5x5 matrix as this is what most external auditors and consultants will look for. 5x5 is also a good compromise between detail and simplicity. You may have to use a specific matrix for compliance reasons. If none of these reasons apply, you might want to consider a non-standard or larger size that makes more sense for the systems you are working with.

Here is the list of choices in the order that you should choose them.

1. If you require a specific matrix for compliance or regulatory reasons, use that matrix.
2. If senior management already has a specific matrix that they uses, use that matrix.
3. If this is the first time that both you and your organization are going to perform a risk analysis, start with a 2x2 matrix. You can move to a larger matrix later once you understand how it will help you and your organization.
4. Use a 5x5 matrix. This will make communications with outside sources easier.
5. Use a custom or non-square size. Make sure that you can explain and document why you chose this. Also make sure that management is OK with this option before you select it.

This is an example of a typical risk matrix:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Threat**  **(Likelihood)** | Very High | Medium | Medium | High | Very High | Very High |
| High | Low | Medium | Medium | High | Very High |
| Medium | Low | Low | Medium | Medium | High |
| Low | Very Low | Low | Low | Medium | Medium |
| Very Low | Very Low | Very Low | Low | Low | Low |
|  | | Very Low | Low | Medium | High | Very High |
| **Vulnerability (impact)** | | | | |

Similar matrixes are used to calculate both the impact of vulnerabilities and the likelihood of treats occurring.

**Downhole Inc.**

Downhole’s management team has concerns with many possible risks with the new tool. This includes regulatory concerns around storing and transporting explosives, integration of the new CNC lathe that will turn the new casings and of course, staff safety. As the CEO of Downhole started his career working on drilling rig, there is a very strong focus on safety. He mandates that both the production and use of the new tool must happen in such a way that there will be 0 lost time incidents.

Downhole already has a list of rig safety regulations required by province and state. They know what they have to do getting to the site and while on site. The IT guy thinks this should be good enough.

Downhole does not currently have a corporate risk management process. None of the staff involved have done this before. The IT guy decides to use a 2x2 matrix to keep things simple.

### 7.1.2 Scope

Many operating environments do not change after they are initially commissioned. IT and business environments may change rapidly, but usually only individual sections. This makes it possible to map out the business functions and their interdependencies. When the need arises to perform a TRA on one area, it should be possible to look at the maps and quickly see what other systems may be related or impacted. This is a business version of “know your network”.

#### What you need to do:

1. Identify all parts of the system in question. Document them and their relationships.
2. List out items or systems that affect the identified system. Document the relationships.
3. Talk to the business owner, the people who work with the system and the people who maintain the system. They will provide information on function and system relationships that only comes with experience. Document this.
4. List the items or systems that are affected by they identified system. Document these relationships as well.
5. Now that you understand the system, decide which parts or sub-systems actually need to be evaluated. Confirm this with the business owner and document it.

**Downhole Inc.**

The IT guy assumes that everything in their plant will need to be considered. He figures that it would be best to talk to the manufacturing supervisor to be sure, though. As he expected, the manufacturing supervisor is very excited to be getting three new, state of the art CNC lathes. He know exactly where they will sit on the floor and has already arranged for power and cooling. He has been waiting to talk to the IT guy about the control software. All of his current tools run Modbus over token ring while the new lathe only supports a proprietary program over Ethernet. There is no login screen. He is very worried about the office staff being able to access his lathes! What is the IT guy going to do about this? The IT guy makes a note and promises that he will bring it up in his TRA. The manufacturing supervisor is surprised in a different area, though. He knew they were working on a new tool, but no one mentioned to him that it was going to use an explosive charge! He doesn’t know if he has an areas that will be safe to store explosives in. Realizing that there may be some regulations in play that they weren’t aware of, the IT guy asks the manufacturing supervisor to see if there are any city bylaws that they need to consider. The manufacturing supervisor also wants to know if the explosives going to be loaded on the floor or in the field? The IT guys decides to call on the engineer who is designing the tool and the field manager who takes care of the truck operators.

The engineer says that it doesn’t matter where the devices get loaded to him. The field manager does care, though. If they are loaded in the shop, he will need larger explosive containers on his trucks. His team will not be able to troubleshoot if something goes wrong, either. On the downside, his team will need more training. The field manager also realizes that there may be DOT or Transport Canada regulations that they may need to consider. He promises to find out and let everyone know. The IT guy writes all of this down as well.

After talking with the OHS person about what is already happening, IT guy realizes that his scope should only look at things that are changing. Currently, the manufacturing floor operates daily. Field crews already drive out to rigs to make measurements or perform tests. The key changes are three new lathes that can be controlled over the network and the incorporation of explosives in a down hole tool – that is also controlled by software.

### 7.1.3 Team

Like ITIL’s Change Advisory Board (CAB), a TRA team will consist of core members with subject matter experts brought in as needed. The business owner must be included. The people who maintain the system should be next on the list. Third should be representative(s) of the day to day users of the system. Team members required after that will change, but you may need advisors from legal, Corporate Risk, IT, OT, human resources and OHS on a regular basis.

#### What you need to do:

One time TRA: At a minimum, engage the business owner. As you discuss the system with them, make notes of other parties that might be stakeholders or have needed information.

If you are setting up a framework for regularly performing TRAs for a business, first reach out to the various departments that will be regular stakeholders. Let them know why you are setting this up and what your expectations will be from them. Each time you go through the process with them, you will get better and more accurate information from them as they grow in their understanding of what is needed. It will also get faster.

**Downhole Inc.**

IT guy realizes that part of his team has already been defined for this TRA. The engineer, the manufacturing supervisor and the field manager all need to be on the team. Because there is the potential for people to get hurt, IT guy wants the OHS rep as well as legal counsel on the team as well. He goes to both individuals, explains what he is doing and why he needs their input. Both agree to be on the team.

### 7.2 Asset Identification and Valuation

### 7.2.1 Identify Assets

Sometime this is simple and obvious, sometimes it’s not. While the definition “it’s a truck” may be accurate for a half ton that isn’t carrying anything, it will be less accurate for a tanker. In that case a truck needs to be broken down into “tractor unit, tank unit, cargo, pump, flow computer with collar, and onboard video recording unit” to give an accurate representation of what it really is. Ideally, the list of assets will be generated from the scope document generated above.

#### What you need to do:

1. List the physical assets that make up the systems listed in the scope. Make sure to include control systems and automated safety systems.
2. List the people that affect the assets.
3. List the processes that affect the scope including any that need to be developed.
4. Identify intangible assets such as the information used or generated by the system.

**Downhole Inc.**

IT guy starts listing the assets:

Everything on the manufacturing floor

Three new lathes

Control system for the new lathes

Twenty four wireline trucks that will move and control the new tool

Control software for the new tool

Manufacturing floor staff

Note: If explosive charges are loaded in the field, this changes to only the lathe operators.

Field staff

Manufacturing process for making the new tool.

Field process for using the new tool. This would include securing the site before deployment.

Data produced by the new tool. Note: This is what the customer is really paying for!

### 7.2.2 Assign Asset Values

Defining Asset Values is an area that is usually easy to bring the business into. Both business people and operational people understand what they have and they are generally happy to tell you about it. This is a very good place to build trust.

#### What you need to do:

Determine:

1. Could multiple people be killed? Are there possible long term deaths?
2. Could an individual be killed?
3. Could multiple people be injured? How badly?
4. Could an individual be hurt? How badly?
5. Could material damage be done?
   1. How much would the damage cost to repair?
   2. Damage values need to include lost production, materials and labor.
   3. Include environmental damage clean up and restoration costs.
6. Could there be damage to company reputation and possibly the company’s stock prices?
7. Would there be any fines or contractual payouts?
8. Could altering an information system cause this damage to happen?

**Downhole Inc.**

IT guys goes through his asset list. Yes, many people could be killed or injured if things go wrong and there was an explosion. Valuable equipment could be damaged. If the charges are loaded on the manufacturing floor, the entire plant the entire facility and the surrounding area could be damaged. If they are loaded on site, only the truck, crew and the client’s rig are at risk. An explosion would also cause a loss of customers because the company would be viewed as unsafe. The new lathes could be damaged beyond repair if they are attached to the corporate network and someone sends the wrong command at the wrong time.

## 7.3 Vulnerability Assessment

Now that we know what we have, we need to look at what they can affect. Some industries have standard definitions for the common vulnerabilities that are found. A straight IT shop will be familiar with CVE numbers and scoring. Production lines are often graded on percentage of product with a defect. A pipeline inspector will looks for rust, maintenance logs, and maximum recorded pressure readings to help determine if a pipeline has any vulnerabilities. A risk assessor will use this type of information and combine it with either public information on how often these lead to incidents or an inspector’s (expert) opinion of how often they encounter each type of problem to determine the probability of each vulnerability leading to an incident.

The impact of a vulnerability being realized can change over time. For example, moving oil by railcar was considered very safe in 2010. After the events in [Lac Megantic](http://www.cbc.ca/news/canada/montreal/lac-m%C3%A9gantic-train-disaster-voted-top-news-story-of-2013-1.2476212) (CBC News, 2013) and [West Virginia](http://www.cnn.com/2015/02/16/us/west-virginia-train-derailment/index.html) (Kevin Conlon and Dana Ford, CNN, 2015), the world sees moving oil by rail as being far more dangerous.

#### What you need to do:

1. Make a five column chart. Label the headers as follows: Vulnerability Name, Weakness, Impact, Vulnerability Rating and Mitigations.
2. For each component of the system, list potential vulnerabilities.
3. For each vulnerability, look at existing things that would make it more difficult or easier for the vulnerability to be exploited. Give each one a rating that corresponds to the Vulnerability Weakness values on the matrix you selected.
4. List the impact if that vulnerability is exploited. Give each of these a rating that corresponds to the control weakness side of the matrix that you selected.
5. For each vulnerability, list anything that can be done to mitigate the vulnerability.
6. Use the matrix to determine the vulnerability weakness.

If someone could get hurt, use this for you vulnerability matrix:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Reliability** | Very Unreliable | Medium | Medium | High | Very High | Very High |
| Unreliable | Low | Medium | Medium | High | Very High |
| Average | Low | Low | Medium | Medium | High |
| Reliable | Very Low | Low | Low | Medium | Medium |
| Very Reliable | Very Low | Very Low | Low | Low | Low |
|  | | No injuries | One person hurt | Many people hurt | One person killed | Many people killed |
| **Safety Impact** | | | | |

If no injuries are possible, use this for your vulnerability matrix:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ease of Damage** | Fragile | Medium | Medium | High | Very High | Very High |
| Weak | Low | Medium | Medium | High | Very High |
| Average | Low | Low | Medium | Medium | High |
| Sturdy | Very Low | Low | Low | Medium | Medium |
| Durable | Very Low | Very Low | Low | Low | Low |
|  | | Very Low | Low | Medium | High | Very High |
| **Asset Value** | | | | |

As with the risk matrix described in 7.1.1, adjust these to suite your needs. Follow the same rules. Generally, this matrix will be the same size as your risk matrix

The outcome of this matrix is your vulnerability ranking or impact.

**Downhole Inc.**

After talking with the OHS person, IT guy decides to on

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vulnerability Name | Weakness | Impact | Vulnerability Rating | Mitigations |
|  |  |  |  |  |

## 7.4 Threat Assessment

Threats are not always malicious. Quite often, they are things that can ‘just happen’. Bad weather, a user entering a value wrong and a valve wearing out are all examples of threats. What makes threat identification practical for a business is developing a list of the non-routine threats that have a reasonable probability of occurring. Routine threats should be handled as part of the day to day business processes.

If you have a list of every possible threat that could affect any type of asset, you are probably working in the back room of an insurance underwriting company. Most of us don’t have – and don’t need – that level of detail. You build list of common threats in your industry as well as specific threats to your organization. Manufacturer’s defect and service bulletins are great starting points. So is the news. One of the most valuable sources of this information are the veteran employees of a company who have the historical knowledge of their equipment, When they say“ Don’t do \_\_\_\_ on that piece of equipment or it will take 3 people a week to get it going again!”, you need to listen to them.

List out the threats that are directly applicable. Don’t waste your time or managements time with obvious or alarmist statements like “a meteor might hit the earth” or “someone might make a mistake”. These types of statement will make you look incompetent. However, a statement like “The user may click on the wrong button because the buttons are close together, the same color and have very small text” is a very valid threat. Sometimes you need to point out the obvious.

#### What you need to do:

This part can be fun - you get to think like a bad guy. Feel free to ask a penetration tester for help.

1. Make a list of everything that everyone on the project team thinks could go wrong.
2. Determine how often events based on these threats have actually happened in the past.
3. Compile the documentation to back up this list. If you don’t have the supporting documentation, management will view this list as an opinion. That increases the chance that they will not take it seriously.
4. Use current news feeds, manufacturers notices, industry SIRTs and government notices to estimate the probability or frequency of each item occurring in the future.
5. Perform an estimate of how difficult it would be for the event to happen. For natural events this may take the form of “these seven things have to go wrong all at the same time so it is not very probable.” Malicious events are usually characterized by “This type of access, this this skill level and this level of resources to perform the action.”
6. Use the matrix to determine the threat level.

Unless you know that you are being actively attacked, use this threat matrix:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Frequency of Failure** | Very Unreliable | Medium | Medium | High | Very High | Very High |
| Unreliable | Low | Medium | Medium | High | Very High |
| Average | Low | Low | Medium | Medium | High |
| Reliable | Very Low | Low | Low | Medium | Medium |
| Very Reliable | Very Low | Very Low | Low | Low | Low |
|  | | Very High | High | Medium | Low | Very Low |
| **Quality of Build** | | | | |

If you know you face an active threat, use this matrix:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Probability of Attack** | Very High | Medium | Medium | High | Very High | Critical |
| High | Low | Medium | Medium | High | Very High |
| Medium | Low | Low | Medium | Medium | High |
| Low | Very Low | Low | Low | Medium | Medium |
| Very Low | Negligible | Very Low | Low | Low | Low |
|  | | Very Low | Low | Medium | High | Very High |
| **Skill and Resources of Attacker** | | | | |

The result is the likelihood of the threat occurring.

**Downhole Inc.**

## 7.5 Calculation of Risk

Now that we know the likelihood of threat and the impact of the vulnerability, determining the risk is very straightforward. On the matrix that you agreed to with senior management, plot your likelihood results on left-hand side. Plot your impact along the bottom. Where they meet on the matrix is your risk.

#### What you need to do:

1. Plot each combination of threat and vulnerability on your matrix.
2. Compare this value to the assets value.
3. Do a gut check on each result. For example, could a script kiddie really take out the North Eastern power grid? Possibly, but this is where you need to be sure of your justifications.
4. Document your results and their justifications.

**Downhole Inc.**

## 7.6 Recommendations

Now that we understand the actual risks we need to put them in appropriate terms for management and provide recommendations to mitigate them. The management write up tends to be the most difficult part. This is because different levels of management talk in different terms. There isn’t a one size fits all solution, but you have to do your best to create one. Do not get bogged down in technical terms or details. Have them ready in supporting documents, but do not include them in your main report.

Be careful with your wording. Most people don’t understand the difference between a threat, vulnerability and a risk. They will use them interchangeably and incorrectly. The higher up the management chain you go, the more likely people will be to use the terms correctly.

Learn which level of management can make a difference in terms of remediating the findings. Quite often this comes down to budget. A field supervisor can usually authorize small expenditures. You may need a VP for remediation’s that take considerable resources. You may need to go to the CEO if the is a high probability that someone will get killed and no-one else will take you seriously.

#### What you need to do:

1. Write a report that summarizes the threats, vulnerability and resulting risks. Include recommendations for remediation. If you are good at writing reports or have a good template, use them. If not use the attached template.

D**ownhole Inc.**

8. Conclusion

ICS risk assessment is not that different than any other type of risk assessment except for a greater focus on safety and reliability. To help get this focus, the assessor should not just try to pick out likelihoods and impacts but break these down into their components of “the likelihood of a threat” and “the impact on a vulnerability”. The standard risk assessment process follows known calculation formats and uses standard terminology to help accurately communicate with management. The risk assessor should use legislated standards or the standards already used by management if already present. If they are not present, use terminology presented here. It will be understood by anyone who regularly works with risk.

Properly prepared and presented, threat risk assessments will help decision makers by giving them a proper understanding of the risks that their organization faces.

# References

ARMS Working Group. (2013, December 3). *ARMS Methodology for Risk Assessment*. Retrieved from SKYbary: http://www.skybrary.aero/index.php/ARMS\_Methodology\_for\_Risk\_Assessment

Bernstein, P. L. (1998). *Against the Gods: The Remarkable Story of Risk.* New York: John Wiey & Sons, Inc.

CBC News. (2013, July). *TIMELINE: Lac-Mégantic rail disaster*. Retrieved from CBC: http://www.cbc.ca/news2/interactives/timeline-lac-megantic/

Corona&Komendanchik. (2008, April). *Bridgestone/Firestone Recall: A Case Study in Public Relations.* Retrieved from Louisiana State University: http://dcomm.cxc.lsu.edu/portfolios/09spr/dcoron1/BridgestoneFirestoneCaseStudy.pdf

CSA Group. (2013, March). *Security Management for petroeum and natural gas industry systems.* Retrieved from Canadian Centre for Occupational Heath and Safety: http://shop.csa.ca/en/canada/petroleum-and-natural-gas-industry-systems/cancsa-z2461-13/invt/27029812013

European Union Agency for Network and Information Security. (2015). *Afhankelijkheids- en kwetsbaarheidsanalyse (A&K analysis)*. Retrieved from European Union Agency for Network and Information Security : https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m\_dutch\_ak\_analysis.html

Glenfis AG. (n.d.). *From Knowledge > ISO 20000 > Service Management System > Plan, Do, Check & Act .* Retrieved from os.itil.org: http://os.itil.org/en/vomkennen/iso20000/managementsystem/plandocheckact.php

International Organization for Standardization . (2013). Information technology — Security techniques — Information security management systems — Requirements. Geneva, Switzerland.

JOINT TASK FORCE TRANSFORMATION INITIATIVE. (2012, September). *Guide for Conducting Risk Assessments.* Retrieved from National Institute of Standards and Technology: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\_30\_r1.pdf

Jones, J. A. (2005). *An Introduction to Factor Analysis of Information Risk (FAIR).* Retrieved from Risk Management Insight: http://www.riskmanagementinsight.com/media/documents/FAIR\_Introduction.pdf

Kevin Conlon and Dana Ford, CNN. (2015, February). *Explosion and oil spill after train derails in West Virginia*. Retrieved from CNN: http://www.cnn.com/2015/02/16/us/west-virginia-train-derailment/index.html

Knight, K. W. (2012, 05). *7th International Conference Brazil May 2012 Presentation.* Retrieved from Inmetro: http://www.inmetro.gov.br/download/wac/painel\_1/7th\_inter\_conf\_brazil\_2012\_may\_2012\_presentation.pdf

MINISTERIO DE ADMINISTRACIONES PÚBLICAS. (2012, November 13). *MAGERIT – version 2 Methodology for Information Systems Risk Analysis and Management*. Retrieved from Portal de Administración Electrónica : http://administracionelectronica.gob.es/ctt/magerit#.VhQCiDZREcQ

NERC. (2015). *Reliability Risk Management*. Retrieved from North American Electric Reliability Corporation: http://www.nerc.com/pa/rrm/Pages/Default.aspx

Office for Civil Rights. (2014). *Guidance on Risk Analysis Requirements under the HIPAA Security Rule.* Office for Civil Rights.

PCI Security Standards Council. (2015, April). *Requirements and Security Assessment Procedures.* Retrieved from PCI Security Standards Council: https://www.pcisecuritystandards.org/documents/PCI\_DSS\_v3-1.pdf

Peavier, R. (2014, December 4). *Business Risk Ratios - How to Calculate Business Risk*. Retrieved from about money: http://bizfinance.about.com/od/pricingyourproduct/a/business-risk-ratios-how-to-calculate-business-risk.htm

Public Safety Canada. (2014, 03 04). *All Hazards Risk Assessment Methodology Guidelines 2012-2013.* Retrieved from Public Safety Canada: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ll-hzrds-ssssmnt/index-eng.aspx

Royal Canadian Mounted Police. (2007, October 23). *Harmonized Threat and Risk Assessment (TRA) Methodology.* Retrieved from Government of Canada: https://www.cse-cst.gc.ca/en/system/files/pdf\_documents/tra-emr-1-e.pdf

Sapiro, B. (2013). *Binary Risk Assessment*. Retrieved from Binary IO: https://binary.protect.io/

Searle, J. (2014). *ICS 410 book 2.* SANS Institute.

Sokol, J. (2014, 01 01). *Simple Risk*. Retrieved from Simple Risk: https://www.simplerisk.it/

Yazar, Z. (2002). *A Qualitative Risk Analysis and Management Tool CRAMM.* Retrieved from SANS: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83

1. Merriam-Webster, <http://www.merriam-webster.com/dictionary/threat> [↑](#footnote-ref-1)