Security Risk formula for control systems

- Should include Threats, Vulnerabilities, Consequences, Cost, and Probability/Likelihood
- Threats, Vulnerabilities and Consequences should be broken down by types and each type should be given a score of severity ranking
- If cost of consequences can be determined then cost should be assigned if that consequence occurs
- Probability and likelihood should include separate scores for each type of threat and each type of consequence. However Vulnerabilities occur at all times due to supply chain, code, human actions etc. probability/likelihood cannot always directly be applied to types of vulnerabilities

Threats

- Need to be broken down by types then given a score so they can be quantified injections into the Risk formula
- Natural Threats can include – Hurricane, Fires, Earthquakes
- Human non electronic threats include – active shooter, chemical, biological, nuclear, radiological and explosives, physical sabotage, kidnapping, phycological manipulation (social engineering) etc.
- Human electronic threats include – EMP, GEOINT, OSINT, electronic social engineering (e.g. phishing), malware (e.g. ransomware), SIGINT, code manipulation, protocol manipulation, spoofing, etc.
- Insider threats – accidental (e.g. mistakes) or intentional (e.g. blackmail, disgruntled contractor/employee), third party partners (e.g. suppliers)
- External threats – nation stations, freelancers/mercenaries, commodity attackers or script kiddies, criminals, terrorists, hacktivists
- Each type of threat needs a severity score assigned to them

Vulnerabilities

- They are weaknesses in people, process, technology, supply chain etc.
- Major categories include hardware, firmware, software, networks, systems, applications, logic/code (e.g. LD, FBD, SFC/CFC, IL, ST), OS, memory stack, input/output validation/manipulation, protocols, etc.
- Vulnerabilities can be found in workstations, devices, chips, circuit boards, API, functional features and logic, code, bootloaders, operating systems, access control systems and procedures
- Each type of vulnerability needs to be cataloged and scored based on ease of exploitability (e.g. local host, local network, remote execution, physical access, hardware tampering etc.) the more exploitable the more severe the score should be
- Two vulnerabilities can have different exploitability factors which will change their score severity (e.g. two exact same PLCs being used differently in architecture may have different exploitability factors/paths thus their vulnerability/severity scores will be different)
- For control systems tools such as IVSS (http://securingics.com/IVSS/IVSS.html) should be used as a replacement for CVSS (https://www.first.org/cvss/calculator/3.0) particularly at PERA levels 0, 1,2 and 3. For PERA levels 4 or 5 using CVSS as is custom for most corporate IT security vulnerability tools is still feasible but for control systems particularly lower levels of PERA it would be wise to leverage IVSS instead.

Consequences

- Should include hazards and impacts to life, safety, environment, property and society – including cascading impacts in supply chain
- Should take injects from types of threats and vulnerabilities that can create or initiate or cause hazards, impacts and consequences to occur
- Where possible should include existing identified and quantified hazards and impacts
- Probability here can usually be quantified from a normal safety perspective but does not adequately account for the human threat actors who attack people, process, technology to exploit vulnerabilities – any security probability/likelihood calculated for consequences must account for each type of threat and vulnerability
- Common Consequences from a control systems and critical infrastructure attacker objective perspective include loss of view, loss of control, manipulation, loss of integrity, denial of service, loss of product, contamination of product, sabotage, espionage, loss of life, environmental damage, supply chain disruption, degradation of services, loss of trust, damage to brand reputation etc.

Probability/Likelihood

- In security most of this is considered to be a moving target and not as creditable as threats, vulnerabilities and consequences which are all tangible and can be concretely identified like elements on the periodic table
- Probability/Likelihood from a traditional engineering and safety perspective can still be leveraged for those traditional consequences but should be done so with caution when engaging in determining security especially human attacker based quantification
- For human attacker based determinization probability/Likelihood must take injects from types of threats and types of vulnerabilities and the exploitability severity scoring/ranking otherwise from a security perspective probability/likelihood would be a subjective arbitrary moving target to security professionals

Costs

- Costs should be where possible associated with various types of consequences
- If possible sometimes vulnerabilities have a known costs as well or their cost can be inferred by the consequences those vulnerabilities are discovered to be linked to directly
- Some threats particularly the natural threats (e.g. earthquake, fire, hurricane, flooding) may have a cost associated with a consequence due to historical data
- However assigning costs to human threat types and vulnerabilities directly without being linked directly to a consequence should be frowned upon and seen as too subjective and arbitrary. Threat types and vulnerability types must be directly linked to a specific consequence and inherit the known cost of the consequence in order to be objective and accurate
- This approach will allow the technical ground truth to be rolled into a prioritized list of costs for executives and decision makers who do not understand what exists under the hood but who need to make decisions that directly contain, mitigation, soften those details under the hood should those threat types, exploit those vulnerability types to create those linked consequences
- Cost should also not just be financial bottom line to business budget or profits, they should include or account for increase in insurance premiums, regulatory fines, damage to brand value and stock prices, environmental cleanup, class action lawsuits from communities/people hurt etc. These are the true total costs should a threat type exploit a vulnerability type to create various consequences