PNNL CEDS 2012 Overview

SSCP Commercialization

- Transferred technology to SEL & Siemens. Only active in supporting Hallmark. Closed in 2011.

Design Basis Threat / Graded Security Protection

- While DBT was found to be feasible, GSP was found to fit electricity better. OE-30 is picking up follow-on tasks for operational consideration.

Field Device Management

- Framework being readied to demonstrate. New partners Northrup Grumman and Texas Tech University will provide additional functionality.

Secure Coding

- Working with vendors and CMU to apply SCALe to Energy Delivery Systems. Alstom Grid in progress; currently negotiating with GE.

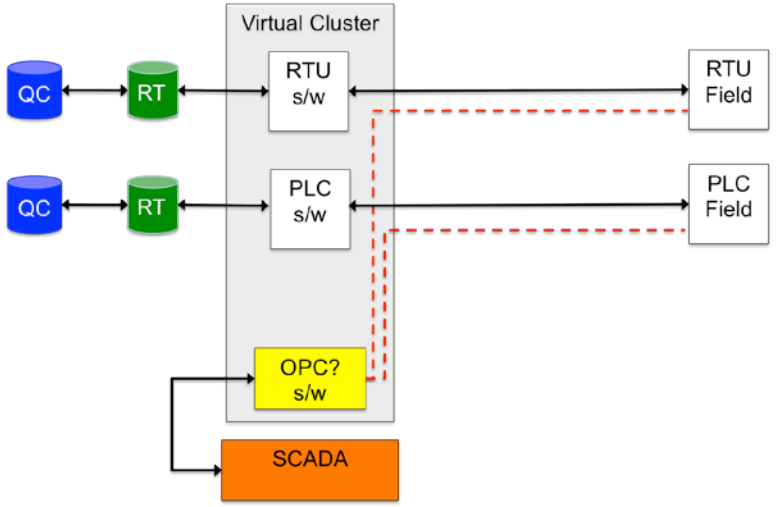
Philip Craig
PNNL

Field Device Management

Cybersecurity for Energy Delivery Systems Peer Review
July 24-26, 2012

Summary: Field Device Management

- **Objective**
  - Utilities are challenged to manage configurations across vendor tools and departments. The challenge is to provide a consistent governance framework. The opportunity is to provide a vendor agnostic approach. This project will leverage enterprise security and virtualization techniques to allow tools to run and store their configurations with high integrity.
- **Technical Approach**
  - Determine commercial capability and best practice mapping to design the framework
  - Capability study, framework document, final report, demonstration



- **Schedule**
  - FY10 Capability study; FY11 Framework document; FY12 Demonstration and final report
- **Performers:** PNNL, Northrup-Grumman, Texas Tech University
- **Partners:** Northrup-Grumman, Texas Tech University

Technical Approach and Feasibility

- **Approach**
  - Current State of the Art (Why is it better?)
    - Current approach is to provide disparate organizational activities supporting each individual organizations requirements/needs.
    - Our new approach provides common framework/platform to meet much tighter and consistent security requirements while also increasing organizational process unity

Technical Approach and Feasibility

- **Approach**
  - Steps to technical approach and schedule
    - Initial requirements gathered that articulate a virtualized approach to multiple software and hardware supported systems and end-point devices (FY10)
    - Formulated framework and platform to integrate requirements (FY11)
    - Working on whitepaper, formal framework document, and construction of small scale functional demonstration (FY12)

Technical Approach and Feasibility

- **Approach**

  Answer the question: how will the end user benefit from the technology?

  – Information systems and control systems are trending towards much higher dependencies and interconnectivity. A successful implementation will push cross-organizational coordination where security expectations are shared and *organizational interconnectivity* must also provide a common security framework for the overall system, and not just for an individual department.

Technical Approach and Feasibility

- **Challenges to Success**
  - Adaptation of technology to very broad and established technical environments
    - Leverages COTS currently used in many engineering, maintenance, and operations environments
    - Utilizes current and common approaches for virtualization techniques that support legacy software/hardware

Progress to Date

- **Major Accomplishments**
  - Validated approach with user community
  - Received additional levels of funded effort from partner organizations
  - Received multiple queries from potential users on *when* this capability would be ready to implement
- **Actual Progress (technical, $, and time) vs Planned Progress**
  - Framework established
  - Platform documentation
  - Demonstration

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - Who will use the technology or knowledge? How will they apply it? How should they not apply it?
    - End users are owner/operators of energy delivery systems, this adaptation well suited for energy. They will be able to read the formal framework and implementation documentation and fully understand the approach and effectiveness of the framework.
    - Users should *not* try to employ this in instances where cross-organizational coordination cannot be achieved (e.g., highly separated duties, or where some critical safety systems may have highly selective security controls.

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - What are your plans to gain industry acceptance?
    - PNNL has been executing communications in many energy engagements, and been working with Northrup-Grumman (partner) in solicitation of potential industry customers
  - How does this solution fit into the existing paradigm of energy delivery systems technologies?
    - Industry is updating/upgrading systems at a much higher rate than historical efforts. Automation is solving many resource problems while providing many new efficiency and resiliency capabilities (e.g., phasors, smart metering, intelligent distribution controls, etc.). This system will provide an environment that would leverage a higher ability to manage these paradigms.

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - How does it leverage and avoid interference with existing capability to protect the reliability of energy delivery systems?
    - The virtualization framework is currently highly leveraged to provide better performance, recovery, and redundancy where critical data and information processing environments are rapidly responding to customer feature requests. Using a common IT platform while deploying specific *virtual enclaves* for multiple organizations *is* itself an *interference* avoidance technique. An environment that is scalable and may be tailored to specific technical requirements will provide higher reliability of those environments thus *adding to* not *interfering with* energy delivery system reliability.

Next Steps

- **Approach for the next year or end of project**
  - Milestones to accomplish
    - Provide formal framework documentation
    - Execute framework demonstration
  - Risks faced
    - No technical risks
    - Resource challenges

Next Steps

- **Project results that may form the basis of future control systems security work or link to other programs/organizations**
  - PNNL partner (Northrup-Grumman) has identified opportunity to integrate their research project (Texas Tech University) into this work.
  - Using the newly formed TTU energy laboratory, TTU, led by Dr. Vittal S. Rao, is leveraging ERCOT, NSF, and other partnerships to expand their energy research and utilize DOE-OE R&D cybersecurity products in them. (Ref. letter next slide underlined important points)

Next Steps

- **Describe potential follow-on work, if any**
  - FY13 AOP, as a mechanism to introduce new commercial and academic partners to the OE R&D program would seek funding for initial gap funding to reach a potential *commercial funding opportunity* in FY14.
  - Timeline
    - FY13 AOP

Next Steps

Dear Philip:

Greetings from Texas Tech University!!

I wish to take this opportunity to thank you for the visit of PNNL and wonderful discussions on Cyber Security of Smart Grids. I really learned a lot from the discussions. At Texas Tech University we have the research infrastructure for conducting research in this emerging area. A team from PNNL, Northrop Grumman and Texas Tech University will be ideally suitable to accomplish significant results in this area.

We are very excited to work with your research group on various aspects of Cyber security of Smart Grid Systems.

(i) As we discussed, at Texas Tech we are in the process of developing excellent hardware/software facilities in smart grid systems under the collaboration of the National Science Foundation and American Electric Power. At the campus level we are also building experimental wind farms along with significant storage of power. Some of this work is done in collaborations with Sandia Labs.

(ii) We are very interested to explore the possibilities of interconnecting of our smart grid laboratory with EIOC of PNNL. During this week we successfully connected our lab with Northrop Grumman lab in Austin. Still we have to conduct experiments using the equipment at different sites. We wish to connect three way connection with PNNL facilities also.

(iii) We are very excited about the possibility of participation in the development proposals under LAB CALL of DOE. Let me know about the status of this effort. We will be ready to contribute any efforts in the development of proposals.

(iv) As mentioned the Texas Tech University is in the process of developing an innovating interdisciplinary Cyber Security education program for protecting critical infrastructure. We cordially invite you to help us to build this program. We will be in touch with you during August 2012 with additional details.

I am personally very excited for the collaborations with PNNL on mutually interested projects and am very confident that we can contribute significantly in this area. I appreciate all your help.

With best personal regards,

Vittal S. Rao Ph.D.

Professor of Electrical and Computer Engineering, Director, Smart Grid Energy Center

Texas Tech University

Sam Clements

PNNL

Secure Coding for Energy Control Systems

Cybersecurity for Energy Delivery Systems Peer Review

July 24-26, 2012

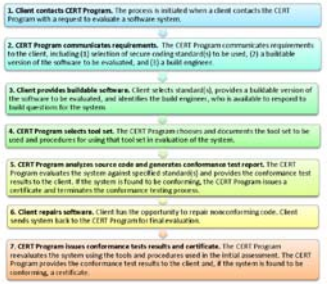
Summary: Secure Coding for Energy Control Systems

- **Objective**
  - EDS vendors do not have uniform support of secure coding practices. The challenge is to improve utility security posture by improving secure coding processes for vendors. CMU's SCALe approach is available. We will work with EDS vendors to evaluate the SCALe and related processes to improve security quality of their products.
- **Technical Approach**
  - Workshop for vendors to understand issues and tools, business case
  - Follow process CMU uses with 2 vendors as they work through the process, communicate pros and cons

Create Secure Coding Standard based on Best Practices
Train Development Staff
Evaluate EDS Source Code with Tools (SCALe)
Correct Defects
Achieve CMU SEI Secure Coding Seal

Pacific Northwest NATIONAL LABORATORY

CERT | Software Engineering Institute Carnegie Mellon



- **Schedule**
  - Key deliverables and dates expected/met
- **Performers:** PNNL, CMU SEI
- **Partners:** ABB, Alstom Grid, GE, Schneider Electric, SEL, Siemens

Technical Approach and Feasibility

- **Approach**
  - Current approaches are ad hoc
  - Vetted approach with widest use of standards
  - Solicit participation from major EMS vendors
  - Engage vendors in a workshop
  - Select one vendor to pilot SCALe process
  - Conduct SCALe assessment and analyze how it may be modified to better fit into business processes
  - Users benefit by using accepted best practice that is well vetted and respected, allowing development of more secure products, thereby increasing security posture.

Technical Approach and Feasibility

- **Challenges to Success**
  - Challenge 1: Scheduling
  - Mitigation: Providing flexibility in the project to allow vendors to participate
  - Challenge 2: Pilot selection and execution
  - Mitigation: Seeking multiple participants knowing that circumstances will inhibit some from participating

Progress to Date

- **Workshop held in April and attended by 4 of 6 vendors**
- **Technical progress is meeting milestones**
- **We are working with CMU SEI to add a second vendor to use SCALe. Alstom Grid started before project started with SCALe, and we are using the experience of this vendor to share with the other vendors to acheive the project goals.**

Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - Who will use the technology or knowledge? How will they apply it? How should they not apply it?
    - EDS Vendors to use, applied to development process in accordance with their existing processes. Must be integrated as a process for success.
  - What are your plans to gain industry acceptance?
    - Pilot assessments will be used to share experiences, feed gaps back to CMU SEI, and product case studies/white papers and outreach to educate vendors and industry
  - How does this solution fit into the existing paradigm of energy delivery systems technologies? How does it leverage and avoid interference with existing capability to protect the reliability of energy delivery systems?
    - Fits well with no technical impacts, only financial development costs.

Next Steps

- **Approach for the next year or end of project**
  - Establish second vendor for assessment
- **Project results that may form the basis of future control systems security work or link to other programs/organizations**
  - Results can be used as DOE National Laboratory process improvement
- **Describe potential follow-on work, if any**
  - Establish a transition partnership with CMU SEI to host SCALe and allow smaller vendors to make use of the process.

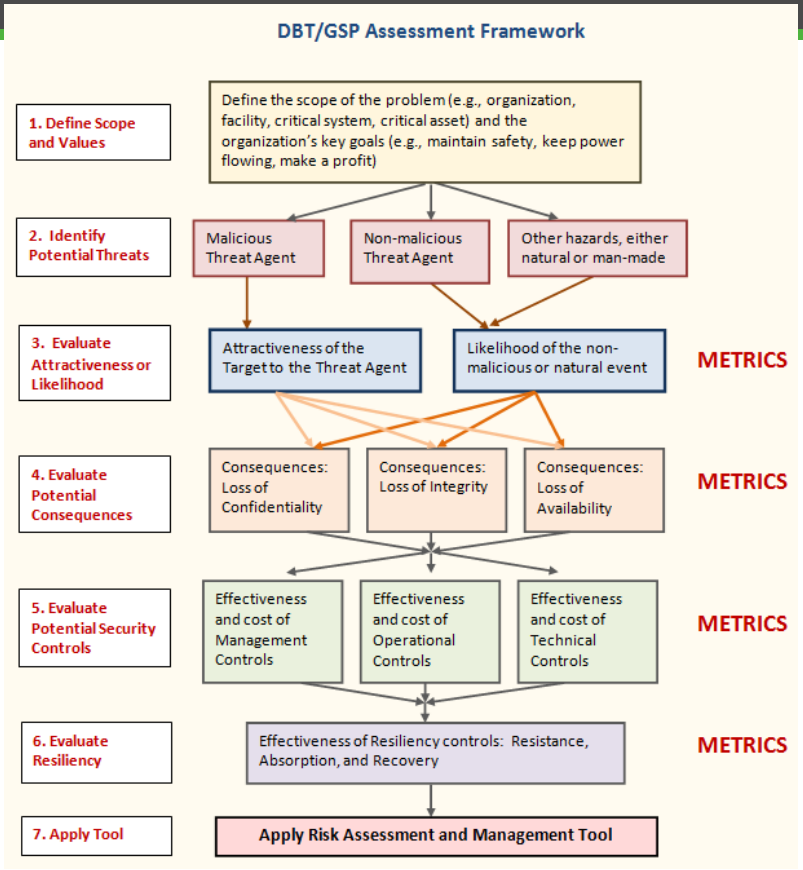
Summary: Design Basis Threat (DBT) / Graded Security Protection (GSP)

Objective

- Use a DBT/GSP set of threats and system information (vulnerabilities, consequences, security controls) to assess the cyber security risk to key energy delivery systems.
- Select cost-effective risk management solutions that reduce threats to acceptable levels

Technical Approach

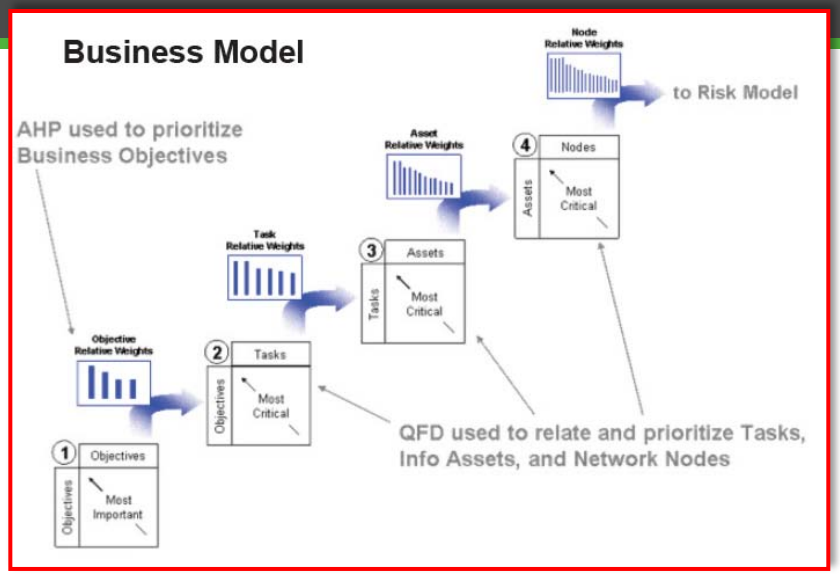
- Compile threat data set
- Select risk management models
- Incorporate DBT/GSP information into the risk management framework.



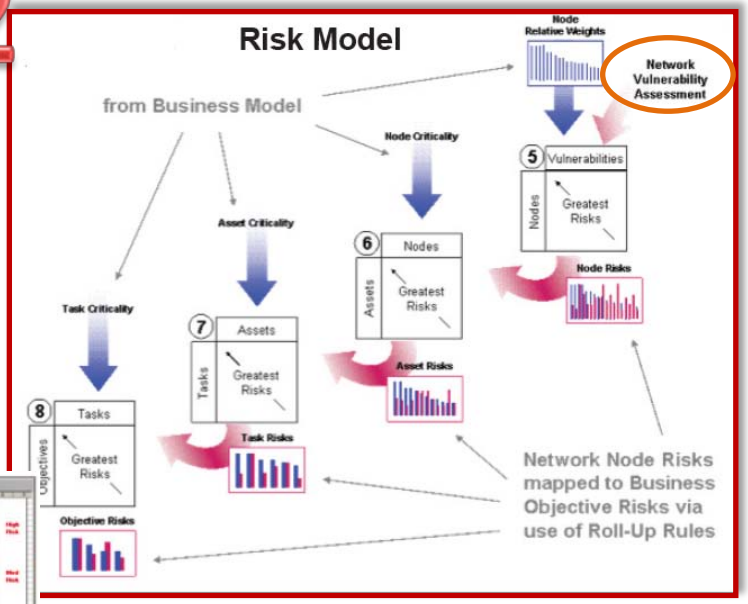
- **Schedule** 8/27 & 9/27 – Complete assessments
- **Performers:** PNNL
- **Partners:** SCL, S.I.T. Benton PUD, MITRE

RiskMAP

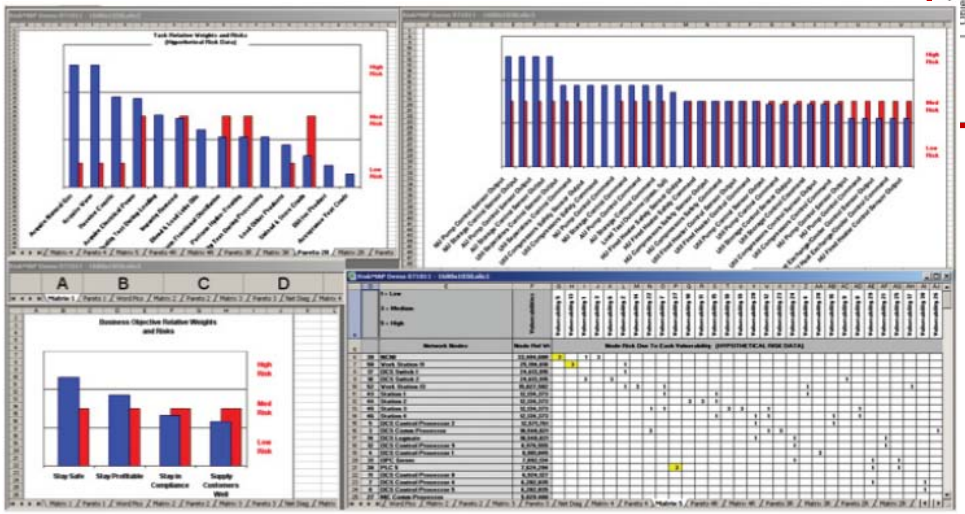
1


Business Model
AHP used to prioritize Business Objectives
Node Relative Weights
to Risk Model
Asset Relative Weights
4 Nodes
Assets
Most Critical
Task Relative Weights
3 Assets
Tasks
Most Critical
Objective Relative Weights
2 Tasks
Objectives
Most Critical
1 Objectives
Objectives
Most Important
QFD used to relate and prioritize Tasks, Info Assets, and Network Nodes

2

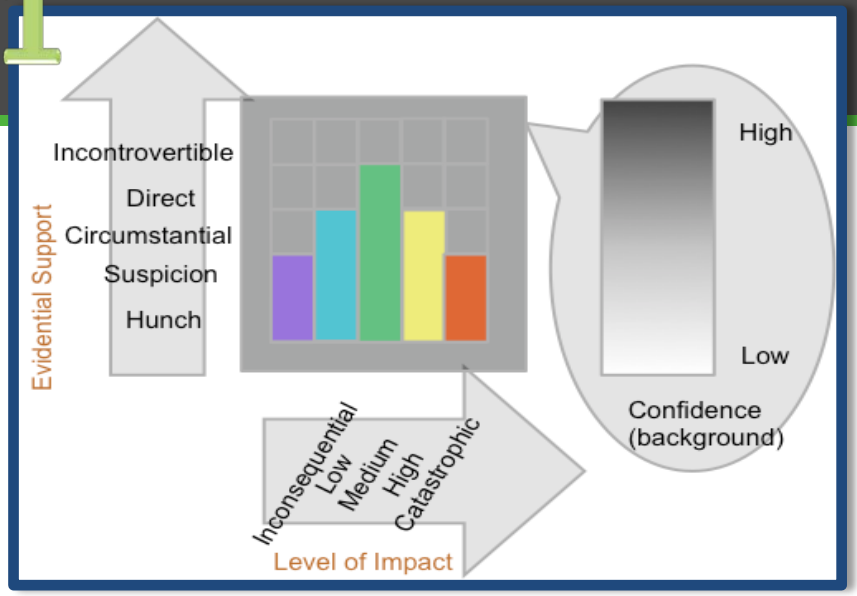

Risk Model
from Business Model
Node Relative Weights
Network Vulnerability Assessment
Node Criticality
5 Vulnerabilities
Nodes
Greatest Risks
Node Risks
Asset Criticality
6 Nodes
Assets
Greatest Risks
Asset Risks
Task Criticality
7 Assets
Tasks
Greatest Risks
Task Risks
8 Tasks
Objectives
Greatest Risks
Objective Risks
Network Node Risks mapped to Business Objective Risks via use of Roll-Up Rules

3

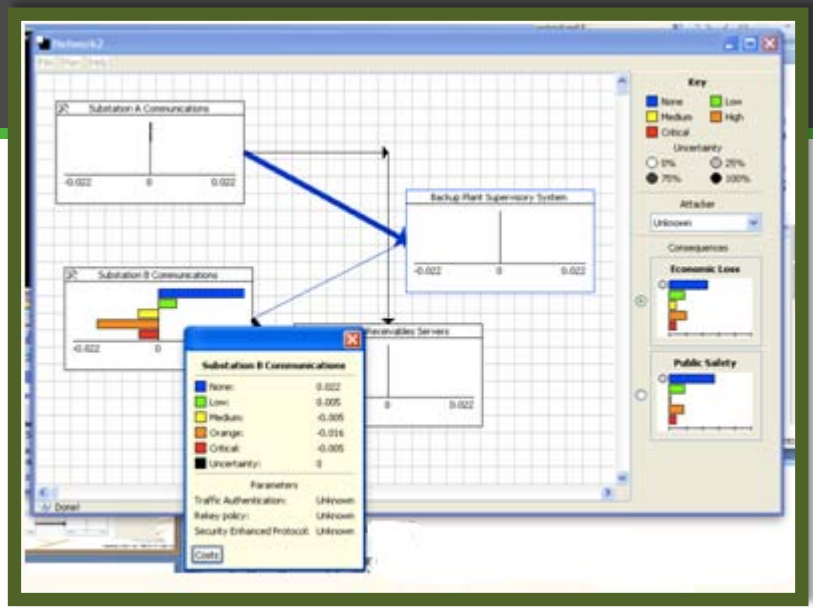

A
B
C
D

CARIM

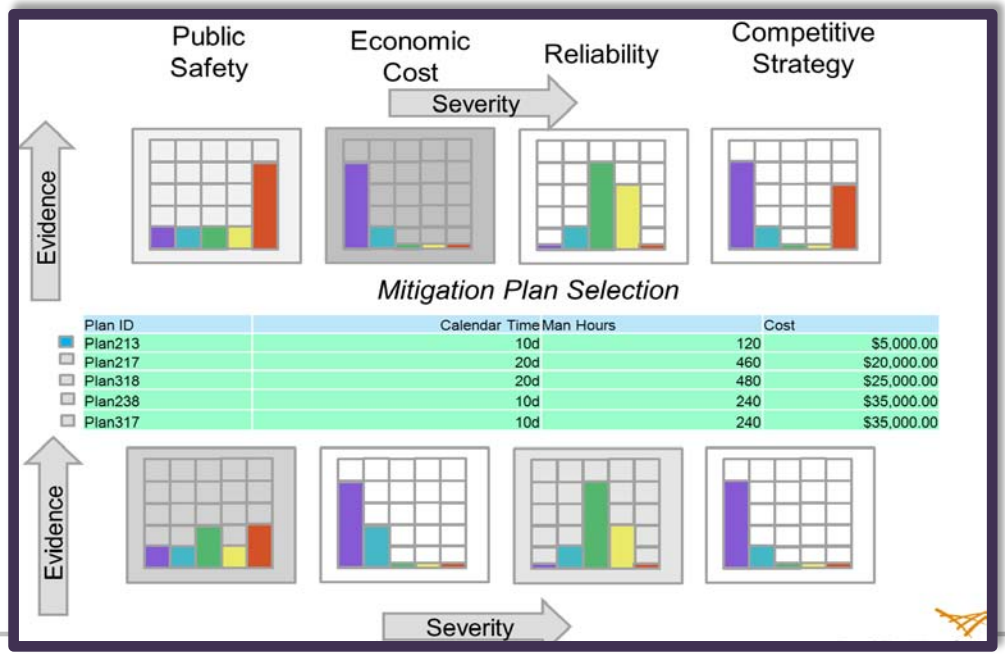
1


Incontrovertible
Direct
Circumstantial
Suspicion
Hunch
Evidential Support
High
Low
Confidence
(background)
Inconsequential
Low
Medium
High
Catastrophic
Level of Impact

2



3


Public Safety
Economic Cost
Reliability
Competitive Strategy
Severity
Evidence
Mitigation Plan Selection
Plan ID | Calendar Time | Man Hours | Cost
Plan213 | 10d | 120 | $5,000.00
Plan217 | 20d | 460 | $20,000.00
Plan318 | 20d | 480 | $25,000.00
Plan238 | 10d | 240 | $35,000.00
Plan317 | 10d | 240 | $35,000.00
Evidence
Severity