# Current Research in Process Control Security Metrics

**June 2006**
**Ann Miller**
**University of Missouri – Rolla**

# Current Approaches and Issues

- **Based on results of audits, analyses, and assessments**
  - **Typically, use whatever is easiest to "count"**
  - **However, many times, much of the information cannot be accurately collected.**
  - **This results in many "guestimated" numbers.**
- **Based on risk avoidance**
  - **Downtime relatively easy to track**
  - **How to quantify possible IP loss?**
  - **How to quantify PR loss, even if no actual damage or loss of data?**
  - **Again, more unsubstantiated estimates.**

# Other Issues

- **Lack of a "single number"**
- **Lack of worthwhile ROI metrics for trade-off decisions.**
- **Most metrics do not consider state-dependence**
  - **Systems have differing security capabilities and/or characteristics depending on state, not just time.**
- **Lack of system-of-systems metric**
  - **Composability/interoperability issues for security**
    - **Even if system A has "quantifiable security level" *alpha* and system B has level *beta*, and the connection mechanism has level *gamma*, what is the level of A + B?**
  - **Of course, most SoS composed of many more than 2 systems**

PROCESS CONTROL SYSTEMS FORUM

# Research Metrics Approaches

- **Substitution**
  - **Substitute actual, “close” values when you don’t have your own actual values**
- **Four-phase spiral approach**
  - **Iterate on the particular phase of the four-phase model (next slide) as more information is available or improved accuracy is needed**
  - **Experimentation with iteration as models developed**
- **Learn from other areas**
  - **Assurance cases for safety adapted for security**

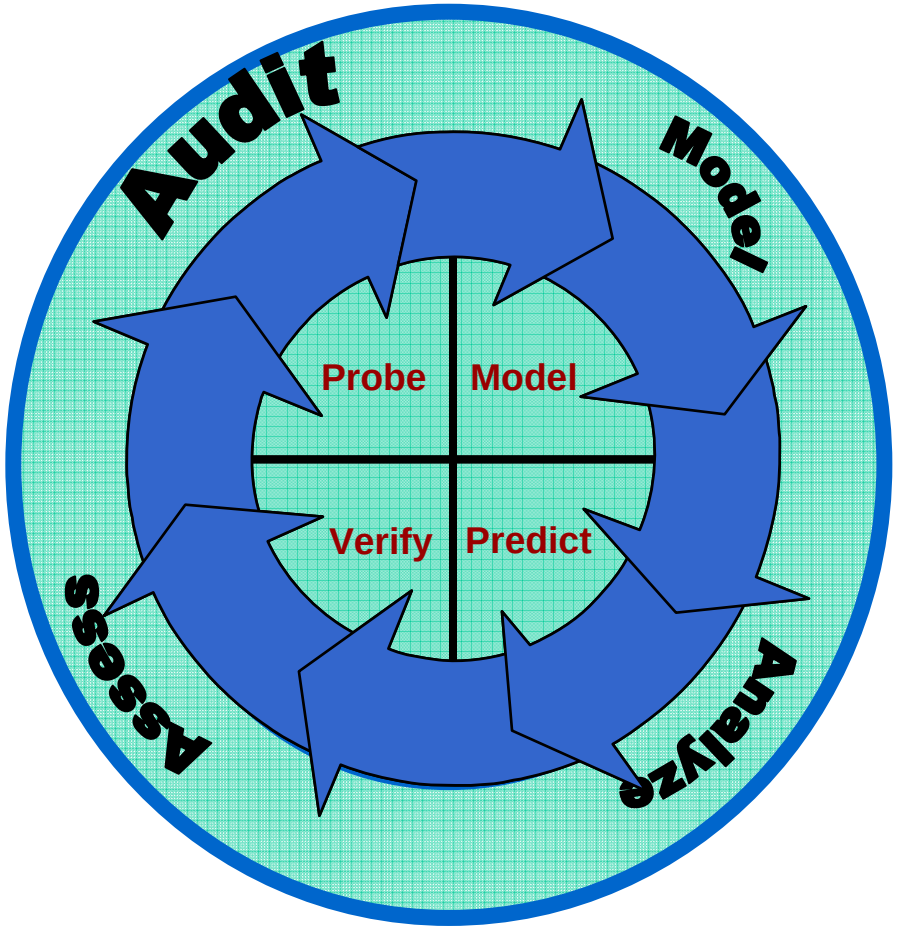
# Substitution Approach

- **Probabilistic risk assessment, yet important data missing for the fault tree (Erickson)**
  - **Basic events:**
    - **Several databases and handbooks exist to help with the estimation of failure probabilities (Bellcore; DOD; Gertman and Blackman; RAC).**
    - **Within some specific communities of interest, failure data for systems and components are available, including summaries of licensee event reports (for oil and gas: SINTEF).**
  - **Operator error: Data exist on the frequency of human error in common tasks found in an industrial environment (Henley and Kumamoto; Shooman).**
  - **Communications links, routers, etc.: much material available on web, from vendors and other trustworthy sources.**

# Spiral Approach Based on 4-Phase Model

**Audit**

- Passive and active network discovery
- COTS components
- Reachability




**Model**

- Mathematically based model of system, network, or program
- Architecture
- Network
- System-of-Systems

**Analyze**

- First round:
  - •Fault-tree analysis with environmental and run-time assumptions
- Protocol+Vulnerability analysis

**Assess**

- First round:
  - •List of exploitable weaknesses
  - •Determine type of attacks
- Threat-based
- Threat+Vulnerability-based

PROCESS CONTROL SYSTEMS FORUM

# Extension: 4 Phase Model in Conjunction with Experimentation as Iterations

Improve

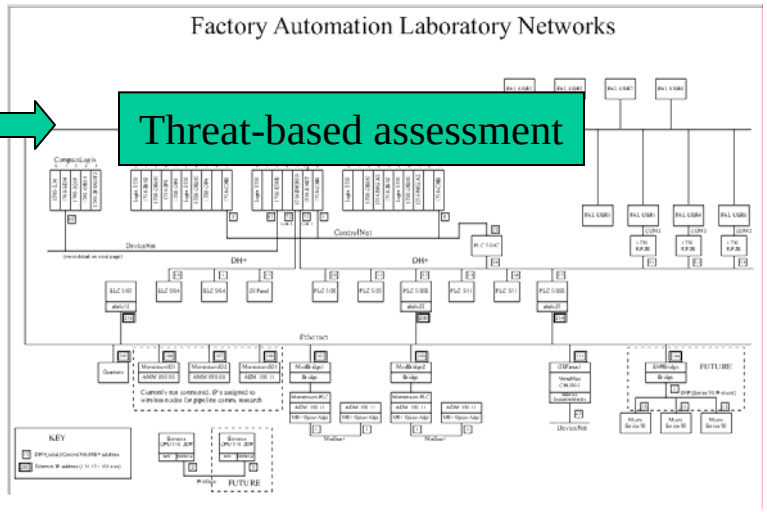
- **Determine network topology and host configurations**
- **Passive & active network discovery/reachability**
- **Differentiate between internal and external views**

**Off-the-shelf tools: Nessus, Ethereal, Snort, Netcat, TCPDump, Hping2, Dsniff**

Model ↓ ↑ Experiment

**Mathematical analysis**

Threat-based assessment




Experiment ↓ ↑ Model

Protocol Analysis
Infrastructure Analysis

PROCESS CONTROL SYSTEMS FORUM

# Learn from Another Area

- **Adapt assurance case for security from safety cases**
- **Joint EU-US Workshops (Bloomfield) to determine best ways to provide compelling arguments and convincing evidence**
  - **Confidentiality, availability, integrity**
  - **People, processes, environment, technology**
  - **Other**
- **Advantage: a substantive body of knowledge on which to build**
- **Disadvantage: not a single number**

# Assurance Case for Safety

- **Definition: A documented body of evidence that provides a demonstrable and valid argument that a system is adequately safe for a given application and environment over its lifetime.**
- **Reality: Large documents with complex internal interdependencies and numerous analyses throughout the lifecycle of the product.**
  - **Rest on explicit and implicit assumptions**
  - **Product and process issues**
  - **Analyses depend on suitability of models**

PROCESS CONTROL SYSTEMS FORUM

# Types of Claims in *Safety Cases*

- **Different attributes of system and of sub-systems, including:**
  - **Reliability**
  - **Availability**
  - **Security**
  - **Functional correctness**
  - **Accuracy**
  - **Time response**
  - **Robustness to overload**

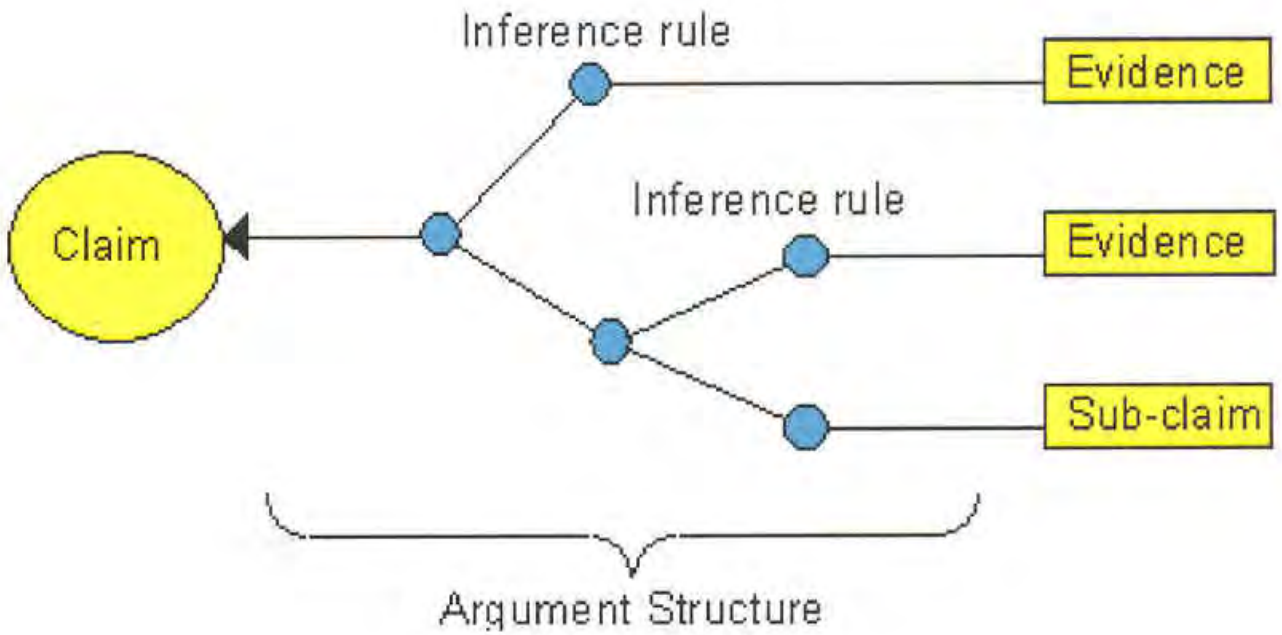
# Assurance Case

- **The motivation for an assurance case is to:**
  - **Provide an assurance viewpoint with focus and rationale - for efficient analysis and evaluation**
  - **Provide a reviewable approach - so that all stakeholders can be involved**
  - **Demonstrate discharge duty to public and shareholders**
  - **Allow inter-working between standards and innovation**
- **The emphasis should be on the behavior of product, not merely the process used to develop it.**

# Assurance Case

- **To implement an assurance case, we need to:**
  - **Make an explicit set of claims about the system**
  - **Produce the supporting evidence**
  - **Provide a set of safety arguments that link the claims to the evidence**
  - **Make clear the assumptions and judgments underlying the arguments**
  - **Allow different perspectives and levels of detail.**

# Assurance Case



# Research in Process Control Security Metrics

- **Critical need because these are critical systems**
- **Teaming between government, industry and academia can achieve more than any one group independently**
  - **Issues include non-attribution and anonymity in data collection and dissemination**

# References: 1 of 2


- **Bellcore. *Reliability Prediction for Electronic Equipment*, Report TR-NWT-000332, Issue 4, September. 1992**
- **Billinton, R. and R.N. Allan. *Reliability Evaluation of Engineering Systems: Concepts and Techniques*, 2nd Ed., New York: Plenum Press, 1992.**
- **Bloomfield, R., S. Guerra, M. Masera, A. Miller, C. Weinstock. "International Working Group on Assurance Cases (for Security)", *IEEE Security and Privacy*, Vol. 4, No. 3 , pp. 66-68, May/June 2006.**
- **DOD (U.S. Department of Defense). *Reliability Prediction of Electronic Equipment*, Mil-Handbook-217F. New York: Griffiss Air Force Base. December, 1991.**

# References: 2 of 2


- **Erickson K., S. Dunn-Norman, A. Miller, E. K. Stanek, Final report to U. S. Department of Interior, Minerals Management Service: *"Survey of SCADA System Technology and Reliability in the Oil and Gas Industry"*, November 2000.**
- **Gertman and Blackman. 1994. *Human Reliability and Safety Analysis Handbook*, New York: Wiley.**
- **Henley, E.J. and H. Kumamoto. 1992. *Probabilistic Risk Assessment*, New York: IEEE Press.**
- **RAC (Reliability Analysis Center). 1995. *Nonelectronic Parts Reliability Data 1995*, Rome, N. Y.: Reliability Analysis Center.**
- **Shooman, Martin L., *Probabilistic Reliability: An Engineering Approach*, McGraw-Hill, New York, 1968.**
- **SINTEF, 1997, *OREDA - Offshore Reliability Data*, 3rd Edition, SINTEF Industrial Management, Trondheim, Norway.**