www.thei3p.org

Institute for Information Infrastructure Protection

The Development of Security Metrics for Process Control Systems in the Oil and Gas Sector

Cliff Glantz (Pacific Northwest National Laboratory)

cliff.glantz@pnl.gov 509.375.2166

Martin Stoddard (PNNL) Deb Bodeau (MITRE)

Joost Santos (UVA) Lori O'Neil (PNNL)

Annie Mcintyre (SNL) Bayard Gennert (UVa)

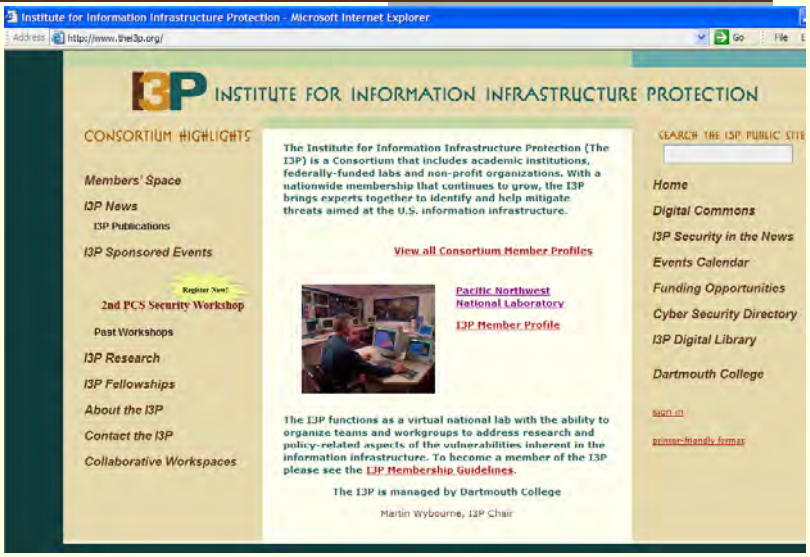
This work was supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate. The I3P is managed by Dartmouth College.

Overview

- Introduction to the I3P and our security metrics task
- The importance of measurements and metrics
- Our team's *Framework for Security Metrics* for process control systems (PCS)
- "Starter-kit" metrics for the Oil and Gas sector

The Institute for Information Infrastructure Protection (I3P)

- The I3P is a consortium of academic institutions, federally-funded laboratories, and non-profit organizations. (See www.theI3P.org)



- The I3P organizes multidisciplinary teams to do technical and policy-related research on issues involving vulnerabilities in information infrastructure.

The I3P SCADA Security Project

- The I3P ***SCADA Security Project*** is investigating ways to enhance PCS security
- Our initial focus is on the oil and gas sector.
- Eleven institutions recognized for their expertise in cyber security and critical infrastructure protection research are participating on this I3P project (including Dartmouth, SNL, PNNL, SRI, MITRE, UVA, NYU, U-Tulsa, MIT-LL, UIUC, and the I3P)
- Six task teams are supporting this project

I3P PCS **Security Metrics** Team

Pacific Northwest National Laboratory
Marty Stoddard – Cliff Glantz – Lori O'Neil -- Wayne Meitzler

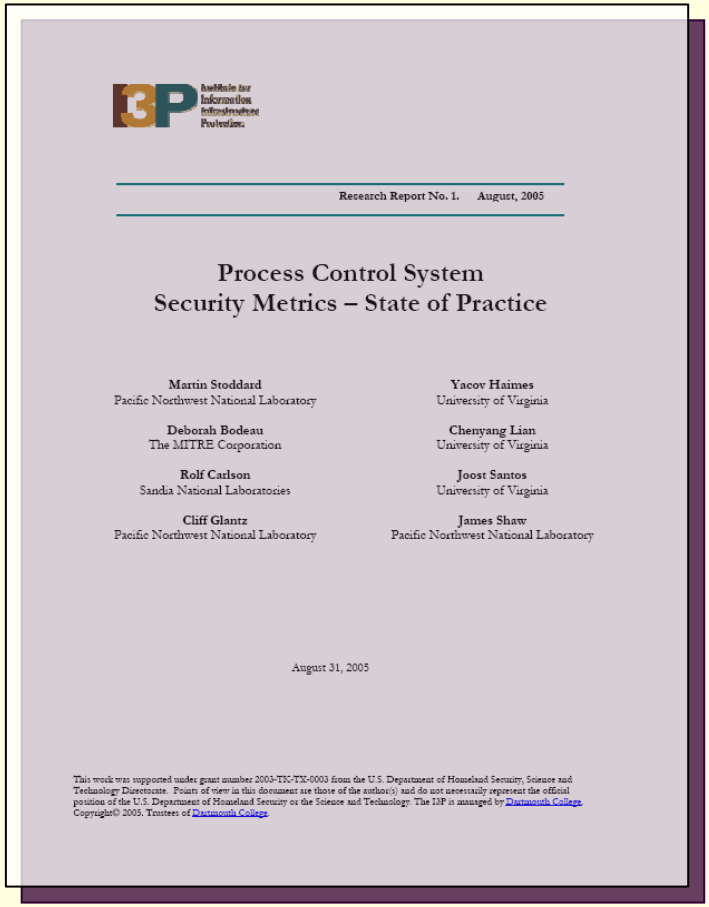
Sandia National Laboratory
Annie McIntyre – Mary Young

University of Virginia
Joost Santos – Bayard Gennert

The MITRE Corporation
Deb Bodeau

Security Metrics Research Plan

- **Phase I:** Survey existing security metrics and provide a high-level view of metrics tools and their application to PCS.
- **Phase II:** Develop detailed requirements for PCS security metrics.
- **Phase III:** Apply what has been learned to both identify existing metrics, and develop new metrics tools, that would be of value for PCS security.



Research Report No. 1. August, 2005

Process Control System
Security Metrics – State of Practice

Martin Stoddard
Pacific Northwest National Laboratory

Yacov Haimes
University of Virginia

Deborah Bodeau
The MITRE Corporation

Chenyang Lian
University of Virginia

Rolf Carlson
Sandia National Laboratories

Joost Santos
University of Virginia

Cliff Glantz
Pacific Northwest National Laboratory

James Shaw
Pacific Northwest National Laboratory

August 31, 2005

This work was supported under grant number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology. The I3P is managed by Dartmouth College.

Copyright© 2005. Trustees of Dartmouth College.

http://www.theI3P.org/about/researchreport1.pdf

The Importance of Measurements

"When you can measure what you are speaking about…. you know something about it; but when you cannot measure it,… your knowledge of it is of a meager and unsatisfactory kind . . ." --Lord Kelvin (1824-1907)

"If you can't measure it, you can't manage it."

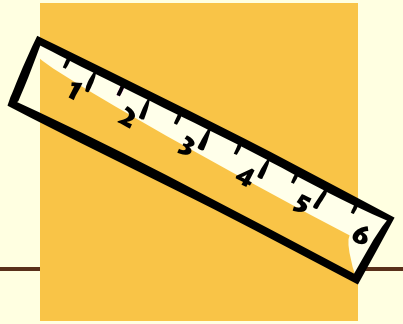
Some questions that decision makers are asking:

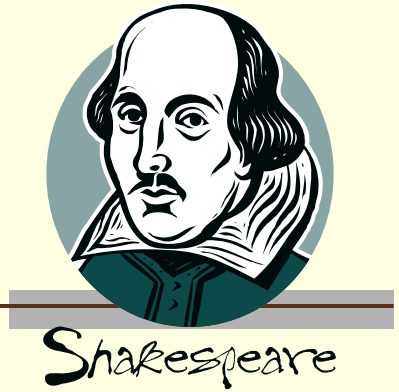
- Is our security posture appropriate and adequate for the risks we face?
- Does our security posture comply with standards and how does it compare with industry practices?
- Is our security posture improving or getting worse?
- What is our return on investment from security?

Measurements

- A measurement can quickly reveal aspects of a system or process that are not inherently obvious.
- This measurement can be in the form of a number, trend line, relative position with respect to a set point, etc.
- However, in many instances measurements by themselves may have little meaning.

What is a Metric?





Definitions:

- metric: "*Of or relating to the meter or the metric system*"
- metrics: "*The use or study of metrical structures in verse*"

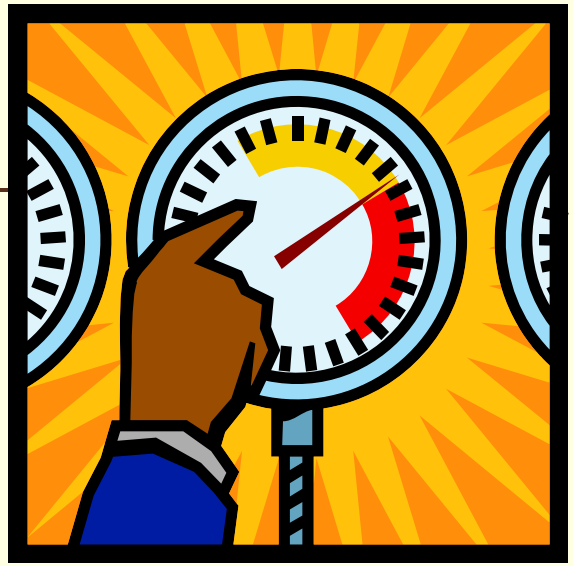
– American Heritage Dictionary

Digging deeper:

- "*a mathematical function defined for a coordinates system that assigns a value to each pair of elements equal to the distance between them, or to a property analogous to distance between points on a line*"

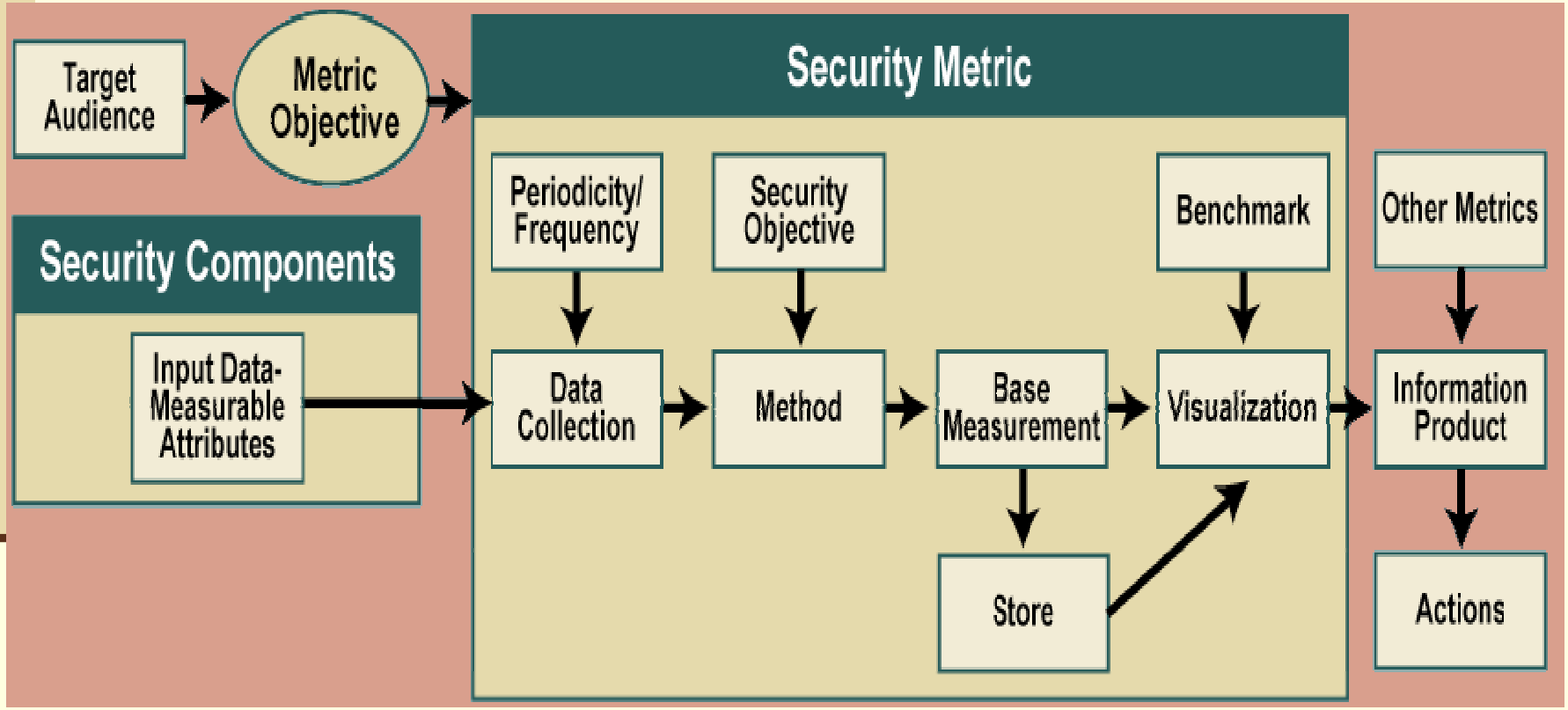
– Encarta Dictionary

Metrics

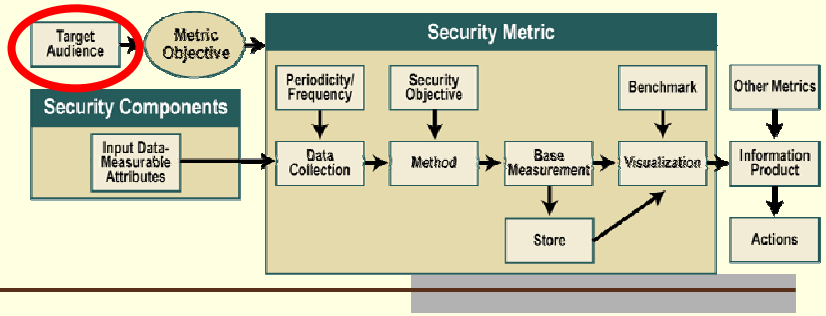


- *Metrics are measurements that are compared to a known scale or benchmark to produce a meaningful result*.
- Metrics are tools that enable stakeholders to make decisions based on qualitative or quantitative assessments rather than best guesses.
- We found that in the oil and gas sector (and other sectors as well) the availability and use of metrics to address PCS security issues is quite limited.

Framework for Metric Development

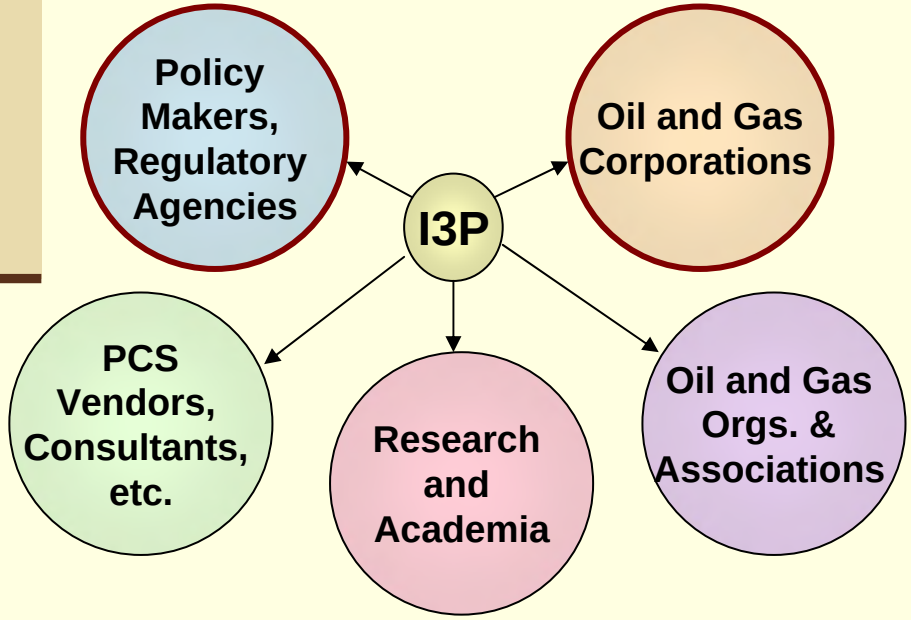


Target Audience

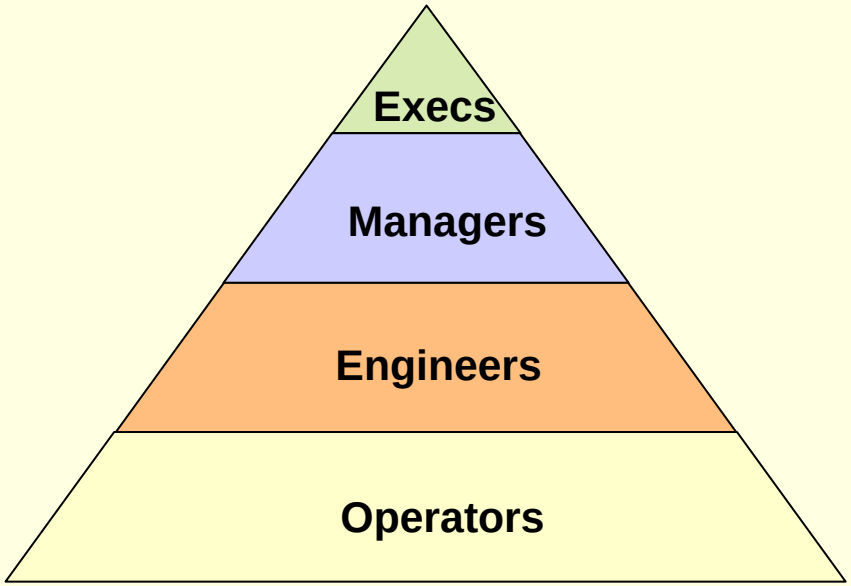


Different metrics are needed for different stakeholders, including:

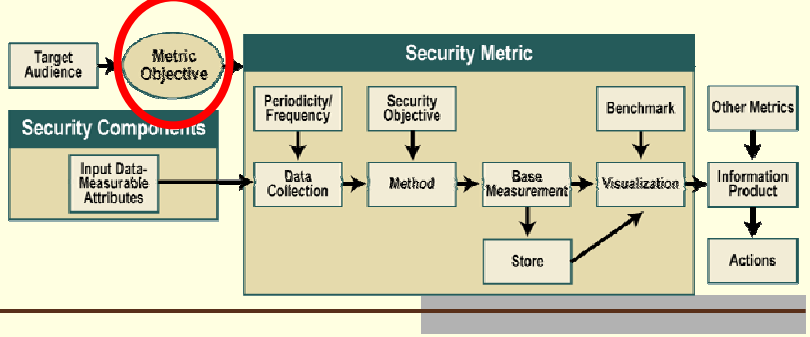
Different organizations or sectors



Different levels within an industry or organization



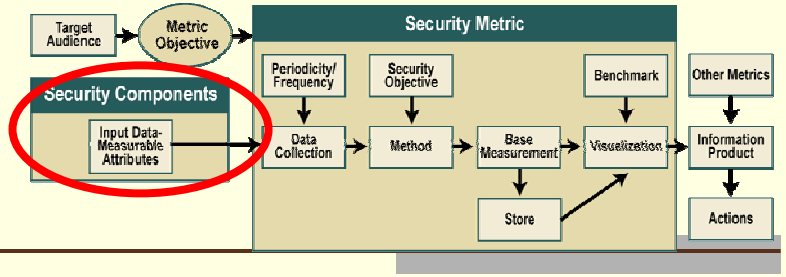
Metric Objectives



Define the objectives for the metrics. This includes determining:

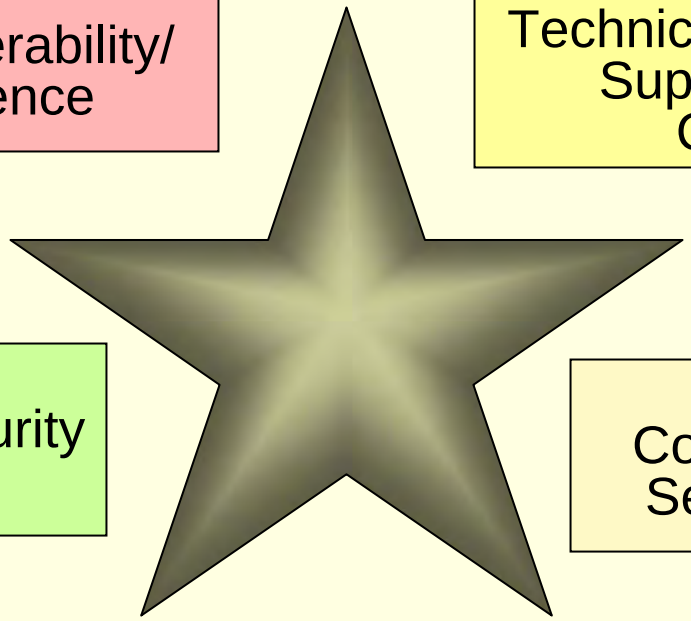
- What is their purpose?
- Who will be applying them?
- Who will be using results?
- When during the PCS lifecycle will they be used?
- What resources and time frame are available for using these metrics?
- Do they cover organizational, operational, or technical areas?

Key Security Components



Risk –
Threat/ Vulnerability/ Consequence

Engineering –
Technical Measurements to Support Design and Configuration

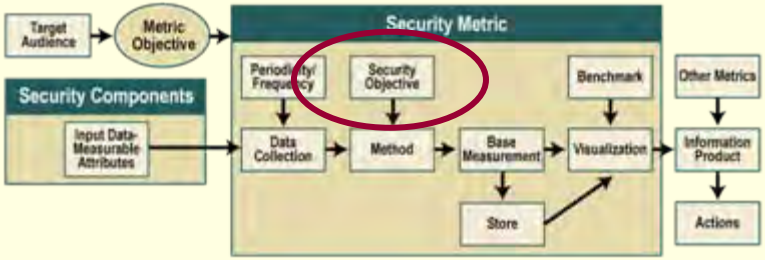


Assurance –
Confidence in Security Solutions

Value –
Costs & Benefits of Security Solutions

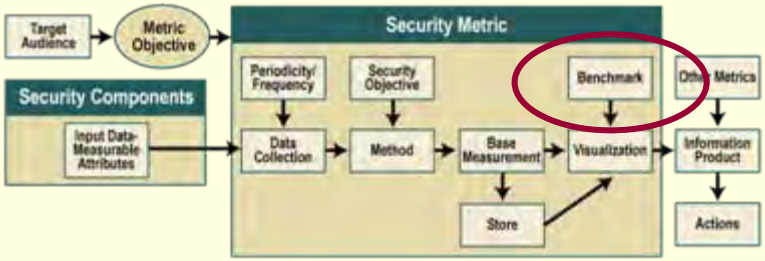
Performance –
How Well Are Objectives Being Met?

Security Objectives



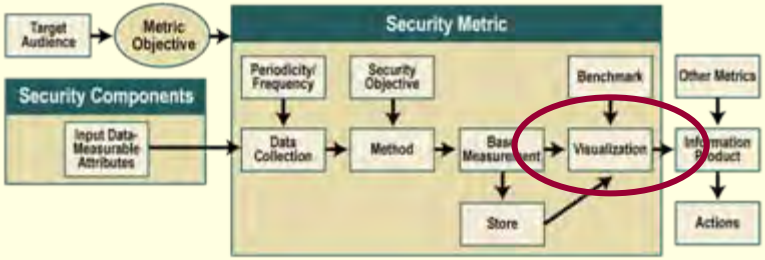
- Security objectives are specific to the organization and control system.
- In general, security objectives focus on preventing, detecting, mitigating, and recovering from attacks on the system.

Benchmarks

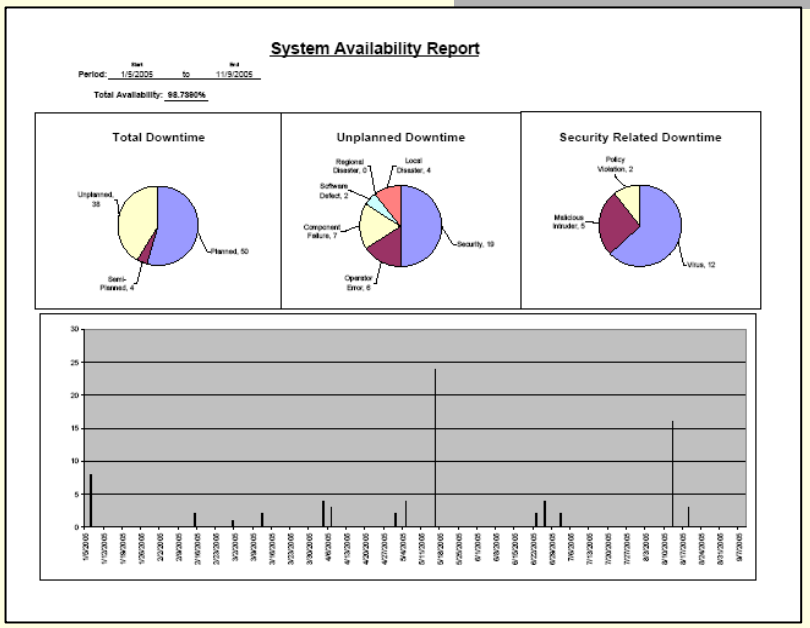


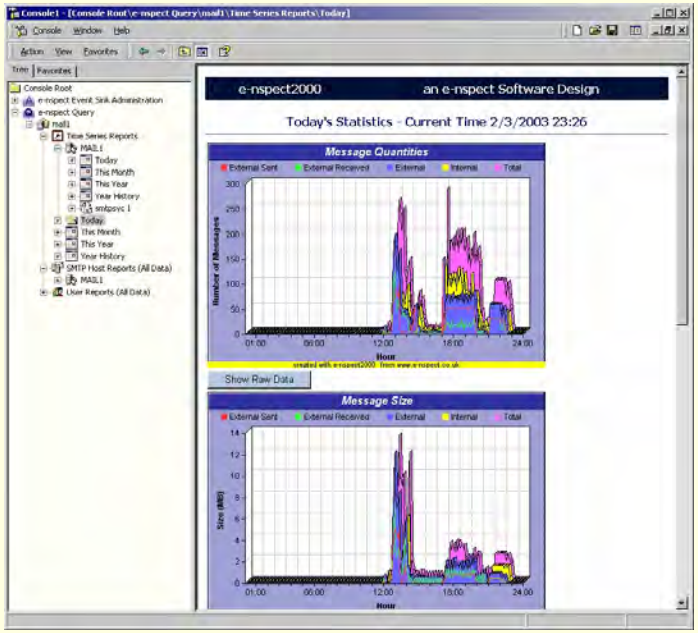
- Benchmarks provide the frame of reference for comparing measurements or assessments.
- Example benchmarks:
  - Industry standards
  - Past performance
  - Corporate goals
  - Expected performance
  - Peer averages

Visualization



- Metrics can be expressed as a number or index or they can be visualized for easy analysis.

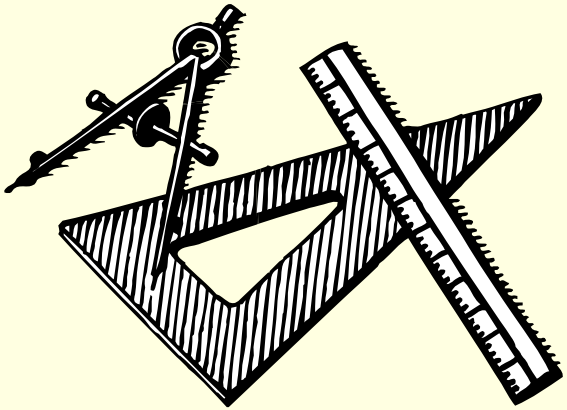




Effect/ Likelihood	Unlikely	Seldom	Occasional	Likely	Frequent
A. Loss of Life/asset (Catastrophic Event)					
B. Loss of operations					
C. Loss of capability					
D. Loss of some capability					
E. Minor or no effect					

Metrics Starter Kit

- Existing or easily developed metrics tools that can be immediately applied
- Simple but meaningful
- Minimal data collection
- Automated where possible
- Actionable



I3P SCADA Security Metrics Starter Kit

Risk

- *Risk Filtering / Prioritization*

Engineering

- *Malicious Code*
- *OS Hardening*
- *Secure Configuration*

Assurance

- *Audit and Compliance (DOE 21-Step Scorecard)*
- *System Information Protection (Cyber OPSEC)*
- *Personnel Security*

Value

- *RiskMAP*

Performance

- *Security Log Audit -- Access Monitoring*
- *Unintentional System Downtime*
- *Network Traffic Report*

For More Information…

- Attend our Risk Metrics Breakout Session at the I3P Workshop on Thursday.
- Check out the products currently on the I3P website (www.theI3P.org) – there are more to come.
- Speak with an I3P Security Metrics team member.