

The Supervisory Control and Data Acquisition (SCADA) Risk Assessment Capability Maturity Model

Dr. Ronald L. Krutz
Stephen Spoonamore
SARMA – May 2008

CYBRINTH
a **duostech** company

The logo graphic for Cybrinth consists of a stylized orange and yellow swoosh that curves from the right side towards the left, ending in a small orange circle. A larger orange circle is positioned above the swoosh, and a smaller orange circle is positioned below it, both appearing to be part of the swoosh's path.



About Cybrinth

- Risk Assessments and Solutions in Financial Services, Govt and SCADA.
- CCLIF Process of IT Risk Scoring
- Intelligent Algorithms for Risk Detection
- FERC/NERC Compliance Tools in partnership with RiskWatch Inc.
- Clients include: MasterCard, Chubb, CSX, Union Pacific, Dept. of State etc.



Agenda

- State of SCADA and Definitions
- Need for New SCADA Risk Assessment Paradigm
- IT and SCADA Requirements Comparison
- Extant, Relevant Risk Assessment Methodologies
- SCADA Threats and Attack Routes
- Typical Attack Privilege Goals

Agenda (Cont'd)

- The Capability Maturity Model (CMM) Approach
- The SCADA Risk Assessment CMM
- SCADA Risk Assessment CMM Process Areas
- SCADA Risk Assessment CMM Appraisal Steps
- Summary

The State of SCADA

- Mech/IT elements of mixed generations
- Legacy Systems can cover 100 years
- Dominated by Civil Engineers
- IT Risk is “an issue for Billing”
- Security through Obscurity is fading
- IP Addressable devices now common
- Risks of IP devices relatively unknown
- 99.99% uptime is mandatory

SCADA Definition

- “The technology that enables a user to collect data from one or more distant facilities and send limited control instructions to those facilities....”
- “Allows an operator in a location central to a widely distributed process, to
 - Make set point changes on distant process controllers
 - Open or close valves or switches
 - monitor alarms
 - gather measurement information.”

(Boyer, in SCADA, Supervisory Control and Data Acquisition, 3rd edition, ISA Press)



Need for New SCADA Risk Assessment Paradigm

- SCADA SYSTEMS SECURITY AND INFORMATION TECHNOLOGY (IT) SYSTEMS SECURITY ARE NOT THE SAME
- IN SCADA SYSTEMS, THERE IS A TENSION BETWEEN PERFORMANCE AND SECURITY
 - PERFORMANCE DOMINATES
- MOST INFOSEC SECURITY STANDARDS SUCH AS ISO 27001 AND ISO 27002 ARE AIMED AT IT SECURITY
 - FAILOVER NEUTRALITY Etc.
- LACK OF TRAINED PERSONNEL IN SCADA SYSTEM SECURITY

Need for New SCADA Risk Assessment Paradigm (Cont'd)

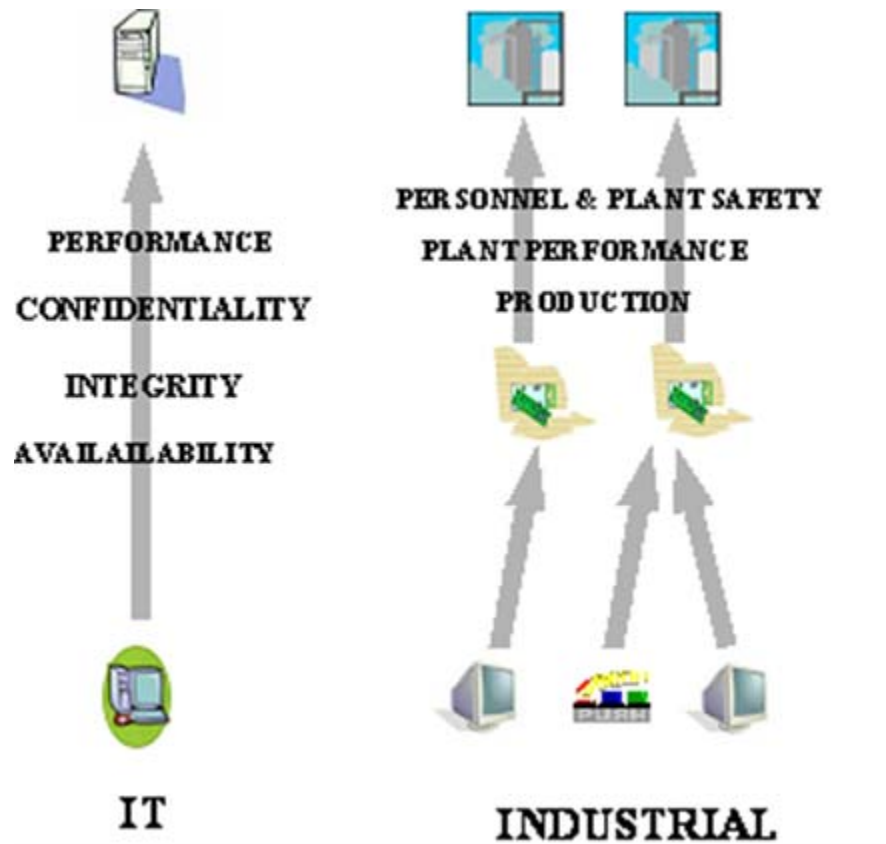
- TRAINING AND CERTIFICATION FOR IT SYSTEMS IS DIFFERENT FROM SCADA SYSTEMS
 - CISSP, CISM, SSCP, ETC. DO NOT ADDRESS CONTROL SYSTEMS SECURITY
- MOST INFRASTRUCTURE EQUIPMENT IS PRIVATE AND NOT GOVERNMENT OWNED
 - LACK OF COMPLETE INFORMATION
 - RELUCTANCE TO REVEAL BREACHES
 - MUST HAVE ECONOMIC INCENTIVE TO INVEST IN SCADA SECURITY AND UPGRADES



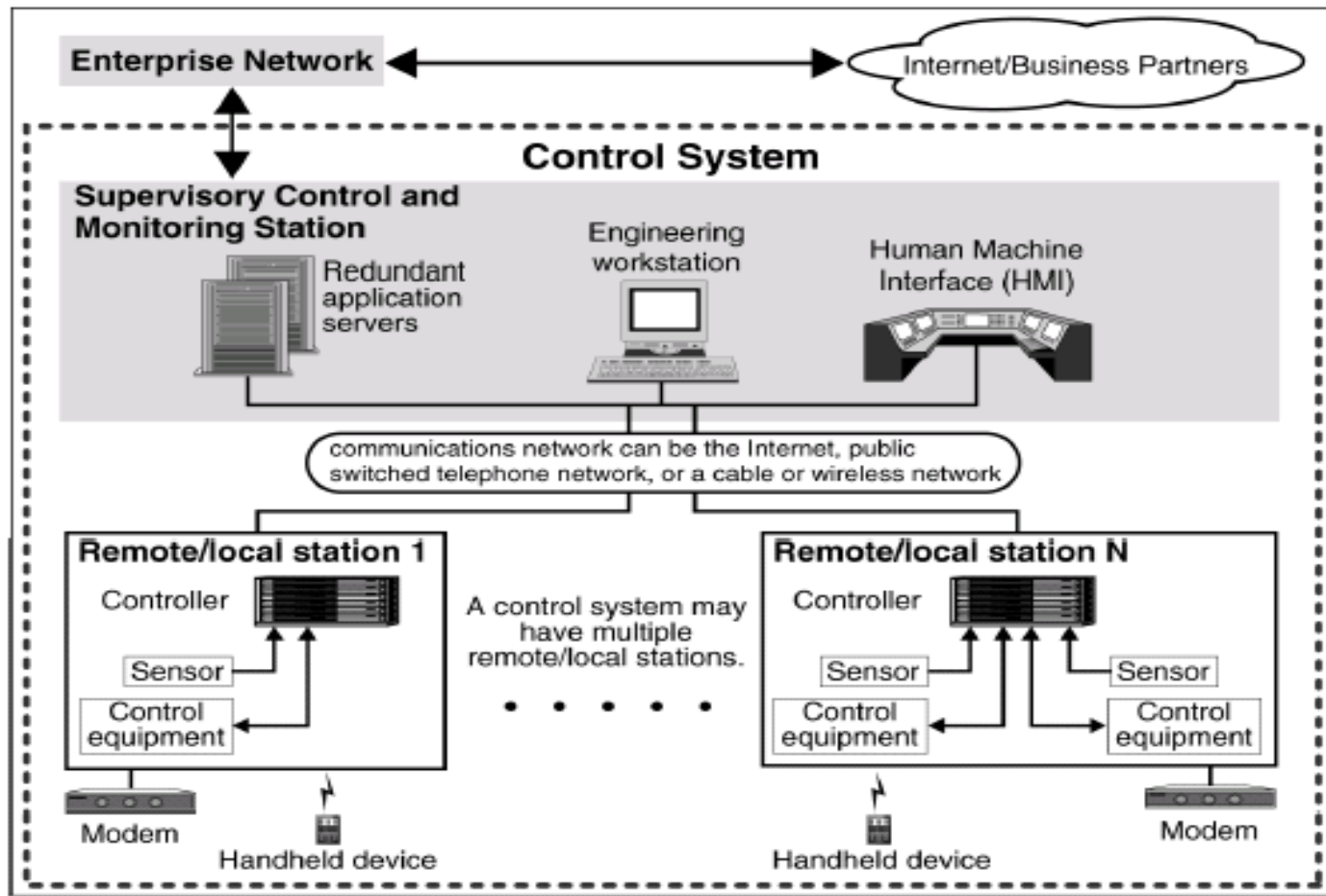
Need for New SCADA Risk Assessment Paradigm (Cont'd)

- MINIMAL UNDERSTANDING OF SCADA THREATS AND VULNERABILITIES
- PERSONNEL TRAINED IN IT CYBERSECURITY MIGHT ACTUALLY DO HARM IF WORKING ON SCADA SYSTEM SECURITY
- SCADA SYSTEMS EXHIBIT A HIGH DEGREE OF INTRA and INTERCONNECTIVITY
 - Cascade Failure Assessments are Critical

IT and SCADA Requirements Comparison



A Typical Modern SCADA System



(Reprinted from GAO-04-140T, "Critical Infrastructure Protection," Challenges in Securing Control Systems, Statement of Robert F. Dacey, Director of Information Security Issues.)

Extant, Relevant Risk Assessment Methods

Petroleum, Gas, and Chemical Industry Guidelines

- American Petroleum Institute (API). April 2005. Security Guidelines for the Petroleum Industry.
- Security Vulnerability Assessment (SVA) Methodology for the Petroleum and Petrochemical Industries
- API RP 70 Security for Offshore Oil & Natural Gas Operations
- API RP 70I Security for International Oil and Natural Gas Operations
- The American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS®) "Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites"
- The Sandia National Laboratories Vulnerability Assessment Methodology for Chemical Facilities (VAM-CF)
- American Gas Association (AGA). August 2004. Cryptographic Protection of SCADA Communications: General Recommendations, Draft 3, AGA Report No. 12

Extant, Relevant Risk Assessment Methods (Cont'd)

Some General Risk Assessment Approaches

- Hierarchical Holographic Modeling (HHM) - Attempts to comprehensively define the sources of risk to SCADA systems and to facilitate the evaluation of subsystem risks
- ISA Technical Report 99.00.01 – Technologies for Protecting Manufacturing and Control Systems
- Interoperability Input-Output Modeling (IIM) - A model that includes intra and interconnectedness with each infrastructure
- Fault Tree Analysis (FTA) - Based on deductive reasoning that begins with an unwanted event and deduces the causes through backward reasoning
- Attack Trees - A form of FTA in which the fault is replaced by the attack goal and the results are the different approaches to effect the attack

SCADA Threats

- Distributed Denial of Service (DDoS) attacks
- Viruses
- Trojan horses
- Human error
- Accidents
- Terrorists
- Disruption of utilities
- Audit Changes – Product Piracy

SCADA Threats (Cont'd)

- Electromagnetic interference (EMI) and Radio Frequency interference (RFI)
- Plant shutdown for maintenance and start-up after maintenance (many harmful events occur as a result of plant maintenance shutdown and start-up)
- Improper application of software patches
- Interdependence with other networks and support elements
- Natural disasters such as earthquakes, tornadoes, volcanoes, fire, thunderstorms, and snow storms

SCADA Attack Routes

- Internet connections
- Business or enterprise network connections
- Connections to other networks that contain vulnerabilities
- “Back door” connections through dial-up modems
- Unsecured wireless connections through the use of “war driving” laptops
- Malformed IP packets, in which packet header information conflicts with actual packet data

SCADA Attack Routes (Cont'd)

- Open computer ports, such as UDP or TCP ports that are unprotected or left open unnecessarily
- Weak authentication in protocols and SCADA elements
- Circumvent security controls during SCADA system development, testing, and maintenance
- Introduced Devices (MIM)
- Email transactions on control network

Typical Attacker Privilege Goals

- Obtain access to the SCADA system
- Compromise the Remote Terminal Units (RTU) or local Programmable Logic Controllers (PLCs)
- Compromise the SCADA Master Control Station
- Disrupt communications between SCADA Master Control Station & RTUs
- Modify control program

SCADA System Attack Concerns

- FUTURE CONCERTED ATTACK ON A SCADA SYSTEM WILL NOT BE SATISFIED WITH ONLY AFFECTING CONTROL PARAMETERS
 - WILL SEEK TO INFLICT LARGE SCALE DAMAGE
 - BURN OUT GENERATORS
 - RELEASE TOXIC SUBSTANCES
 - OPEN FLOOD GATES
 - INITIATE EXPLOSIONS

The Capability Maturity Model (CMM) Approach

- Modern statistical process control emphasizes:
 - Higher quality results can be achieved by emphasizing the *quality of the processes* that produce them and *the maturity of the organizational practices* inherent in those processes
- A framework for evolving SCADA Risk Assessment from an ad hoc, less organized, less effective state to a highly structured and highly effective state

The CMM Approach (Cont'd)

- The Capability Maturity Model (CMM) paradigm:
 - Widely used as a basis for assessing the capability and maturity of organizations in a number of different domains
 - Developed in 1986 at the Carnegie Mellon University Software Engineering Institute (SEI)
 - Initially applied to the domain of Software Engineering as the Software-CMM
 - Has been applied to systems engineering, acquisition, systems security engineering, and other domains

Fundamental CMM Concepts

- Process
 - A sequence of steps performed for a given purpose
 - One of the principal determinants of cost, schedule, and quality
- Process capability
 - An organization's potential
 - The quantifiable range of expected results that can be achieved by following a process
 - Low capability organizations experience wide variations in achieving cost, schedule, functionality, and quality targets

Fundamental CMM Concepts (Cont'd)

- Process maturity
 - The extent to which a specific process is explicitly defined, managed, measured, controlled, and effective
 - Implies a potential for growth in capability
 - The richness of an organization's process
 - The consistency with which it is applied
- Process Area (PA)
 - Composed of Base Practices (BPs)
 - **Mandatory characteristics** that must exist within an implemented SCADA Risk Assessment process before an organization can claim satisfaction in a given PA

The SCADA Risk Assessment CMM

- Has two dimensions, “domain” and “capability”
 - Domain dimension
 - Consists of all the practices (BPs) that collectively define SCADA security risk assessment processes
 - Capability dimension
 - Represents general practices (GPs) that indicate process management and institutionalization capability
 - GPs apply across a wide range of domains
 - GPs represent activities that should be performed as part of doing the BPs
 - GPs are grouped into logical areas called “Common Features” which are organized into five “Capability Levels” which represent increasing organizational capability

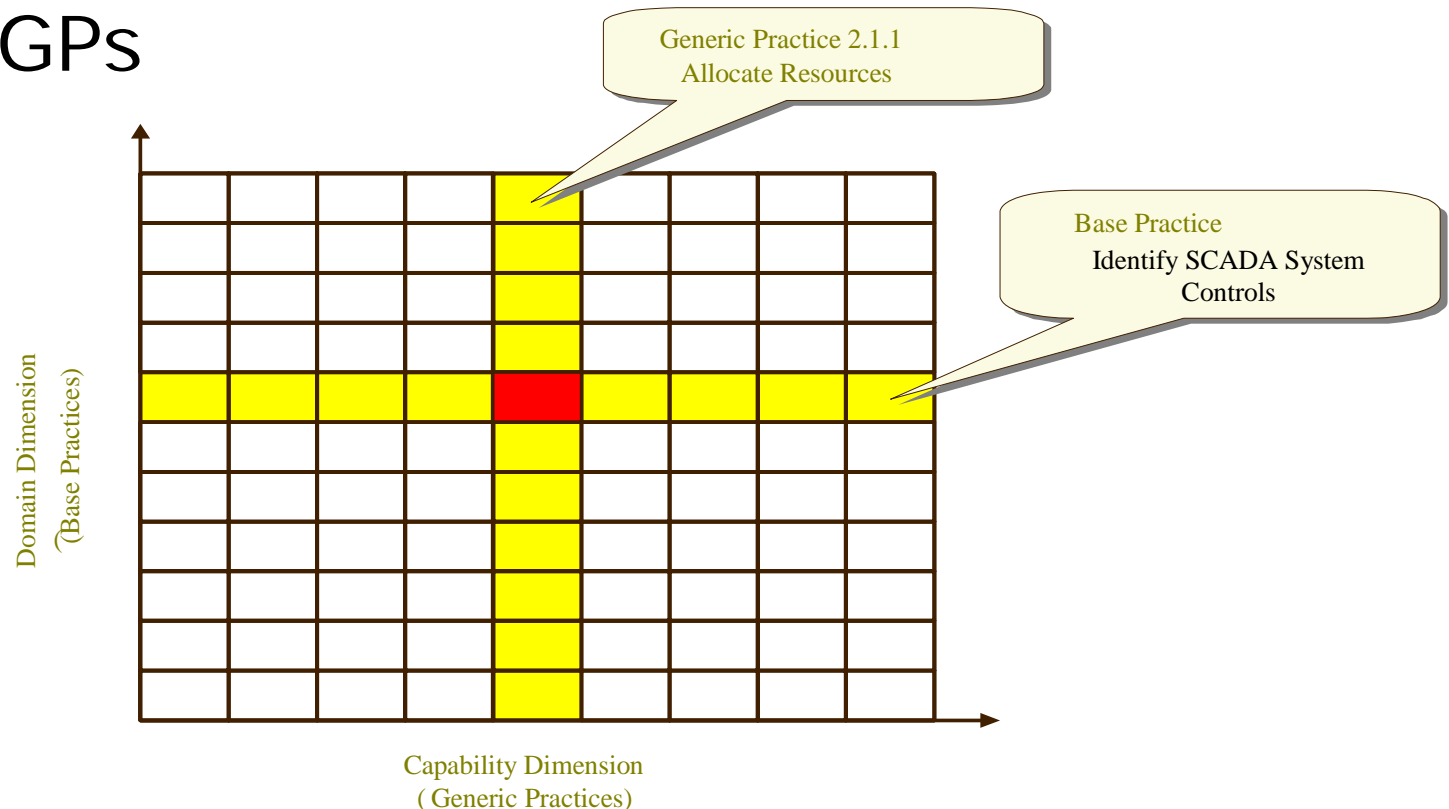
The SCADA Risk Assessment CMM (Cont'd)

○ CMM Common Features

Level	Common Features Comprising GPs
1	<ul style="list-style-type: none">• 1.1 BPs are Performed
2	<ul style="list-style-type: none">• 2.1 Planning Performance• 2.2 Disciplined Performance• 2.3 Verifying Performance• 2.4 Tracking Performance
3	<ul style="list-style-type: none">• 3.1 Defining a Standard Process• 3.2 Perform the Defined Process• 3.3 Coordinate the Process
4	<ul style="list-style-type: none">• 4.1 Establishing Measurable Quality Goals• 4.2 Objectively Managing Performance
5	<ul style="list-style-type: none">• 5.1 Improving Organizational Capability• 5.2 Improving Process Effectiveness

The SCADA Risk Assessment CMM (Cont'd)

- The relationship between BPs and GPs



Process Areas (PA) Evaluated Against Each Common Feature²⁶



SCADA CMM Process Areas

- Derived from published and proven risk assessment sources and methods
- Comprise Basic Practices
- Tailored to SCADA risk assessment
- New Process Areas being developed

SCADA CMM Process Areas (Cont'd)

- PA01 Characterization of the SCADA system
- PA02 Identification of threats to the SCADA system
- PA03 Identification of vulnerabilities in the SCADA system
- PA04 Analysis of the planned or in-place controls for the SCADA system
- PA05 Determination of the probability that a vulnerability in the SCADA system might be exploited by a threat
- PA06 Analysis of the impact of a threat realized against the SCADA system
- PA07 Determination of the level of risk that exists for the SCADA systems
- PA08 Specification of SCADA Risk Assessment controls to be implemented in the risk mitigation process
- PA09 Documentation of the risk assessment process

SCADA CMM Process Areas (Cont'd)

○ Formatting Process / Basic Areas

PA01 – PA Title (in verb-noun form)

Summary Description – An overview of the PAs

Goals – A list indicating the desired results of implementing this PA

BPs List – A list showing the number and name of each BP

PA Notes – Any other notes about this PA

BP.01.01 – BP Title (in verb-noun form)

Descriptive Name – A sentence describing the BP

Description – An overview of this BP

Example Work Products: – A list of examples illustrating some possible output

Notes – Any other notes about this BP

BP.01.02...

SCADA CMM Example Process Area

PA01 – Characterization of the SCADA System

Summary Description

The purpose of PA01 is to define the scope of the SCADA security risk assessment and gather information required for the process

Goal 1: Identify SCADA system boundaries

Goal 2: Establish the scope of the risk assessment

Goal 3: Provide connectivity information

Goal 4: Identify responsible personnel

BPs List

- BP.01.01 – Obtain system information, including hardware, software, and interfaces
- BP.01.02 – Identify SCADA system users and operators
- BP.01.03 – Identify critical SCADA system components and data
- BP.01.04 – Identify SCADA system controls
- BP.01.05 – Identify SCADA physical security environment
- BP.01.06 – Conduct information gathering using questionnaires, interviews, documentation reviews, and scanning



SCADA Risk Assessment Appraisal Steps

- Planning Phase
 - Establishes framework under which the appraisal will be conducted
 - Prepares the logistical aspects for the On-Site phase
- Preparation Phase
 - Prepares appraisal team for On-Site phase
 - Conducts preliminary gathering and analysis of data through a questionnaire, models, mapping
 - Data from the questionnaire is analyzed and supporting evidence is collected
 - Produces a set of exploratory questions for use in the interviews of SCADA personnel

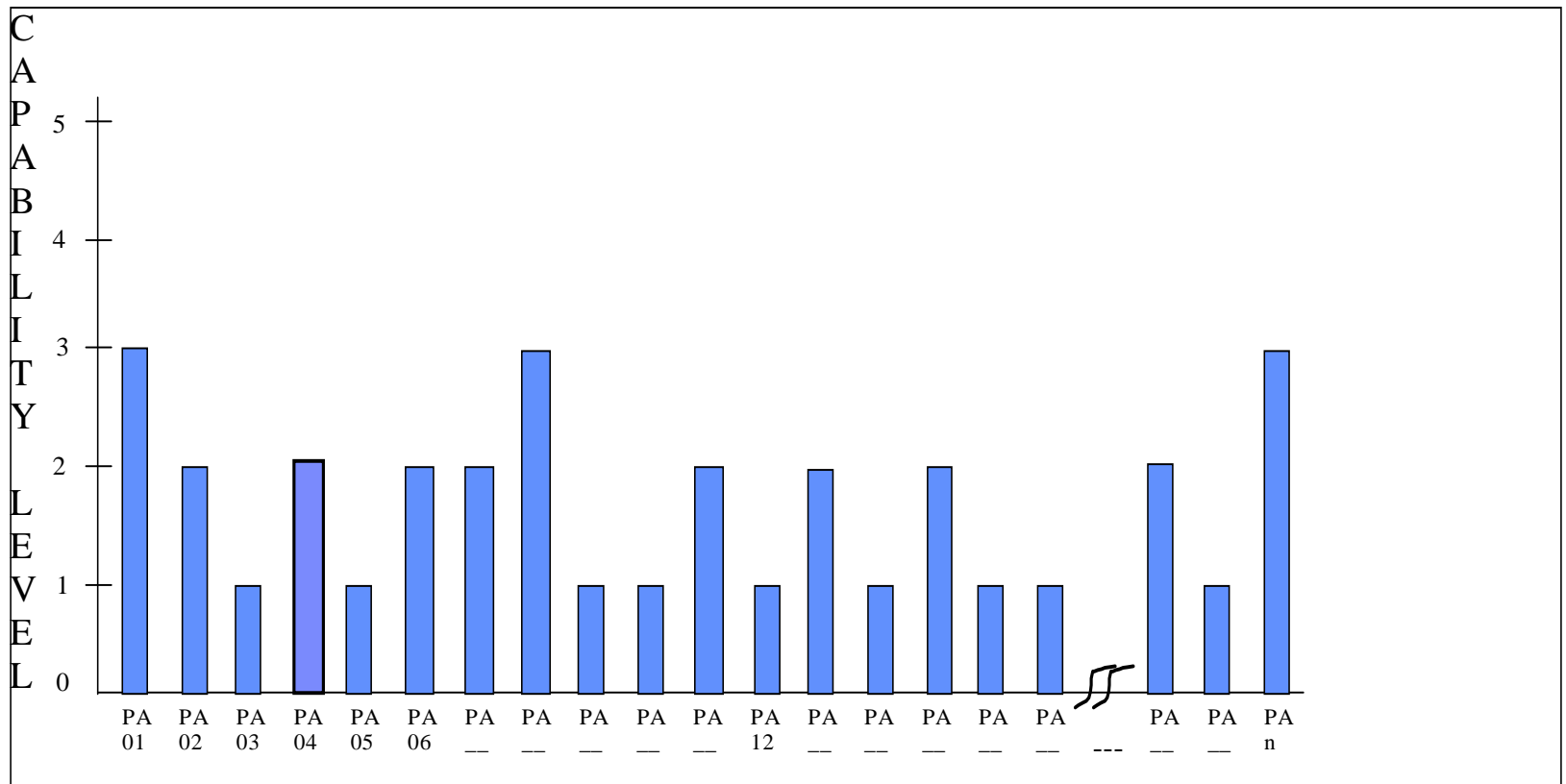
SCADA Risk Assessment Appraisal Steps (Cont'd)

- On-Site Phase
 - Test the preliminary data analysis
 - Provide practitioners at the appraised entity with data validation process
 - Briefing of the appraisal process and schedule made to upper management
 - SCADA personnel and practitioners are interviewed
 - Appraisal results are collated
 - Preliminary findings are proposed and follow-up questions are presented
 - Rating developed to capture appraisal results and presented during wrap-up meeting

SCADA Risk Assessment Appraisal Steps (Cont'd)

- Post-Appraisal Phase
 - Finalizes data analysis begun at the end of the On-Site phase
 - Presents team findings to the sponsor
 - Provides opportunity for practitioners to provide comments on the appraisal process for future improvements
 - Findings report is developed and presented to the sponsor

SCADA Risk Assessment Appraisal Results Example Bar Chart



SCADA Risk Assessment Appraisal Results Example Table

PA Title	Rating
PA01 -	3
PA02 -	2
PA03 -	1
XXXXX	2
XXXXX	3
XXXXX	1
XXXXX	1
XXXXX	2
PA09 : Documentation of the Risk Assessment Process _____	1

Summary

- The SCADA Risk Assessment CMM provides a structure to the field of SCADA Risk Assessment through the use of the CMM paradigm
- Additional PAs under consideration
- Subset of the SCADA Risk Assessment CMM PAs can be selected according to the size of the SCADA-related organization and the services provided
- Allows Isolation of Mission Critical PAs

Thank You

- Stephen Spoonamore
 - CEO of Cybrinth Inc.
 - spoonamore@cybrinth.com
- CCLIF Analysis