Integrated Security Management Systems (SMS):

New International Standards and Organizational Principles for Integrated Management Systems

US Department of Energy
ISM Workshop, Idaho Falls
August, 2008

Michael J. Penders, Esq.
Environmental Security International
www.esisecurity.com

- Environmental Security International

"The only security of all is in a free press. The force of public opinion cannot be resisted when permitted freely to be expressed. The agitation it produces must be submitted to. It is necessary to keep the waters pure."

-Thomas Jefferson to Lafayette, 1823

Reducing Vulnerabilities and Risks with Integrated Management Systems: Performance Measures, Accountability, and Deterrence

- Integrated Security Management requires the capacity to detect, prevent, and limit consequences from deliberate or negligent acts within or outside a facility.
- Focused on acts that would use supply chain, hazardous materials, wastes, or infrastructure as a weapon or means of delivering an attack.

Public Right to Know and Community Security

- EPCRA and the public information as a driver for safer and secure communities.
- Terrorists Right to Know?
- Structuring Communications internally and to external stakeholder and Emergency Responders. (NATO/OECD Policy on Communication.)
- Strategic Environmental and Security Management Systems.

Process for Integrated Risk Assessment and Management System Design

- Planning for many release and likely attack scenarios that pose threats to critical assets; not just worst case
- New paradigms for risk analysis and planning
- Measuring Benefits of Integrating Environmental, Health, Safety, Emergency Response, IT and Physical Security Management Systems…
- After a Security Vulnerability Assessment (SVA) and gap analyses of EHS rates risks to critical assets
- Facilitating Senior Management Decisions

Homeland Defense and Elements of Integrated Management and National Security

- Nationally, Internationally, at Ports, and at Facilities: “We don’t know what we know.”
- Stove piping of agencies and information
- Speed and synthesis: keys to comprehension and security.
- Integrating environmental, energy, and security monitoring into operational controls, with defenses for IT systems

National and International Security: Towards a Systems Approach

- 9/11 Commission Report: FAA and SAC
- A Few Brave Men with Cell Phones
- Integrating Trade, Customs, and Compliance Data
- Communications and Emergency Response
- Hurricanes and Homeland Security
- Regional and Facility Security Management
- Supply Chain Security Management

Integrating Elements of Security into Environmental Management Systems and Vice Versa

- Access to Reliable Information by Decision Makers, Emergency Responders, Security
- Data Mining, Operational Controls, Remote Sensing
- Planning, Communications, Training
- Standards for ER; Incident Command
- Demonstrated Performance at Military Bases

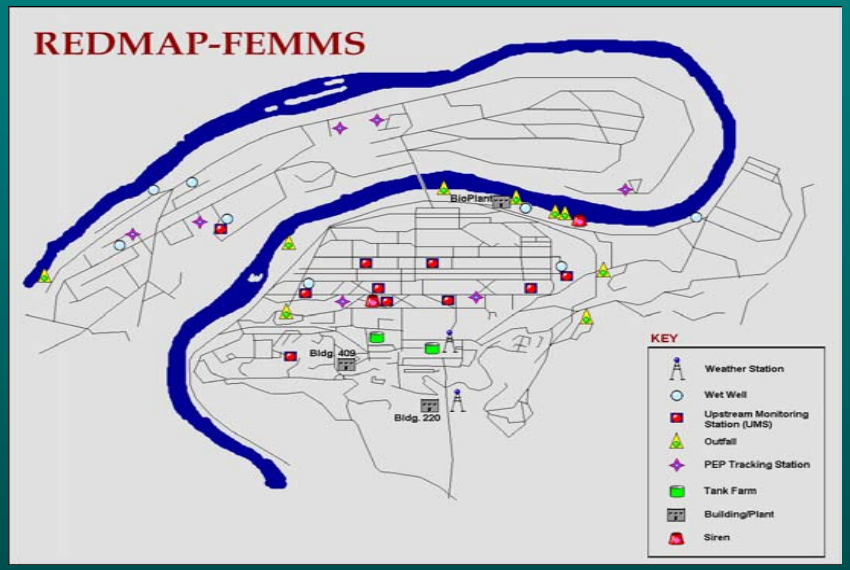

Radford Army Ammunition Plant
Environment Development and
Management Program
REDMAP
40 square mile industrial facility
located on the New River, near
Blacksburg, Virginia, producing
explosives and propellants

EWA Environmental Technologies

Ammonia Plume Dispersion Model/Emergency Response System

Meteorological Station

Upstream Effluent Quality Monitoring Stations



Selective Catalytic Reduction/NOx

Sulfuric Acid Concentration Monitoring Process

Outfall and River Temperature Monitoring

Propellant Explosive Pyrotechnic Tracking and Material Management System

Biological Wastewater Treatment Control and Monitoring

Integrated Security Management Systems for Critical Infrastructure: Achieving Efficiencies, Measurable Cost and Resource Savings

- Integration of Environmental Management, Security, and Information Assessment
- Vulnerability Assessment and EHS gap analysis: New Incentives for P2; E3
- Blue Plains…
- Lockheed…

Critical Elements of Vulnerability Assessment and Management Systems Review

- Facility and Process Reviews
- Physical Security: Perimeter; access controls; vehicles and materials delivery management; hazardous materials management; facilities design; critical infrastructure; personnel; subcontractors; *Energy Supply*
- SCADA, Information, and Cyber Security
- Energy; EHS; Emergency Response, Disaster Recovery, Business Continuity

Strategic Risk Management Systems

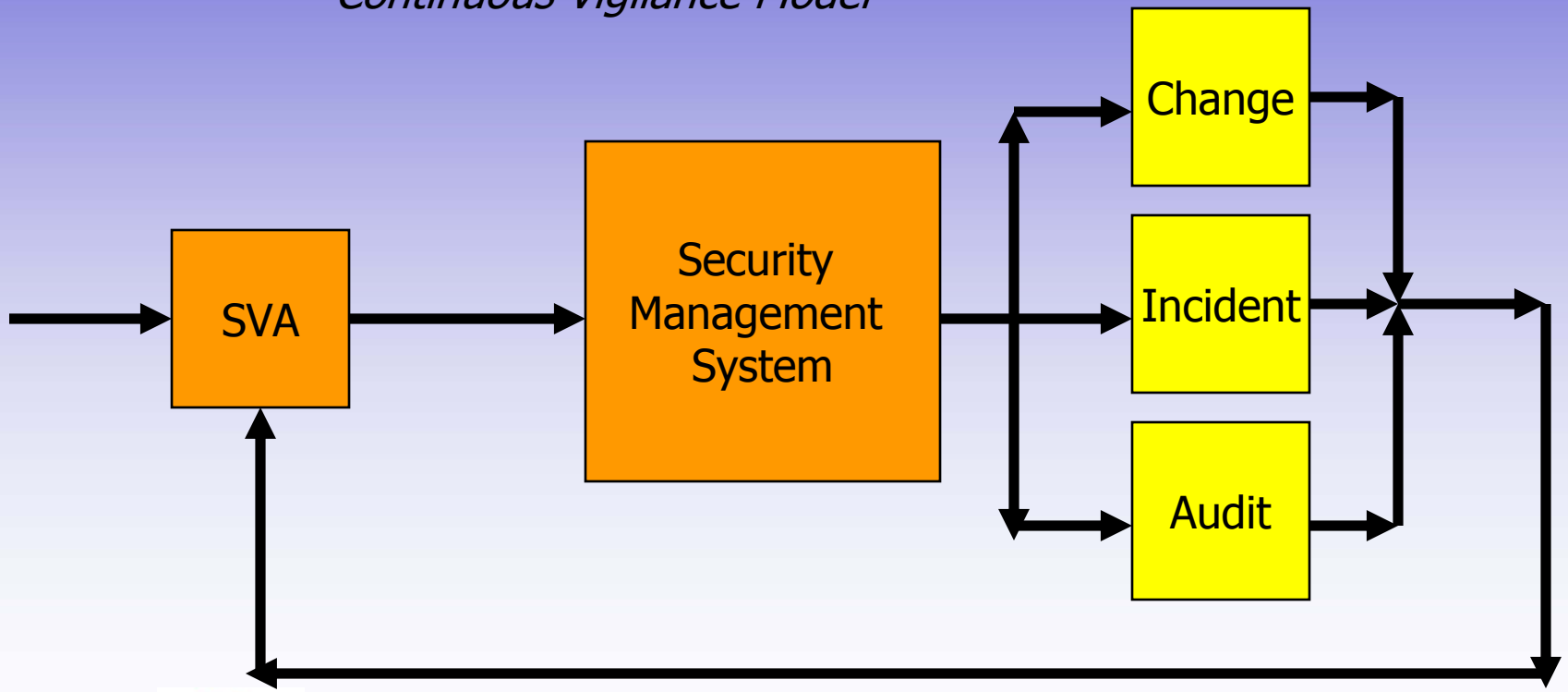
- Pollution Prevention and Strategic Sustainability
- Co-Generation, Redundancy, Defenses
- Management Controls and Real Time Monitoring
- Towards an Integrated Systems Approach
- Assuming worst case scenarios and that the enemy knows; design systems accordingly

New Standard and Incentives for Integrated Security Management

- The new international standard for Security Management Systems (SMS): ISO 28000
- US/Israeli Pilot Projects at Critical Infrastructure
- Petro-Chemical; Refineries; LNG; Nuclear
- ISO 14001+++ ISO 22000; ISO 27000
- Performance Measures for Integrated Systems: Speed, Synthesis, Risk Reduction
- Insurance/Financial/Regulatory Consideration

Security Planning Model

Continuous Vigilance Model



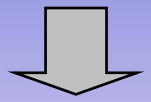
Security Management System Model Elements

- **Leadership commitment**
- **Security vulnerability assessment**
- **Legal and other requirements**
- **Threat and hazard deterrence and mitigation**
- **Implementation and operation**
- **Resources, roles, responsibility and authority**
- **Competence, training and awareness**
- **Continuous improvement**
- **Monitoring and measurement**
- **System evaluation**
- **Nonconformity, corrective action and preventive action**
- **Control of record**
- **Internal audit**
- **Management review**
- **Communications and warning**
- **Documentation**
- **Control of documents**
- **Operations and procedure**
- **Emergency preparedness and response**

SVA Methodology

Step 1: Asset Characterization

Step 2: Threat Assessment



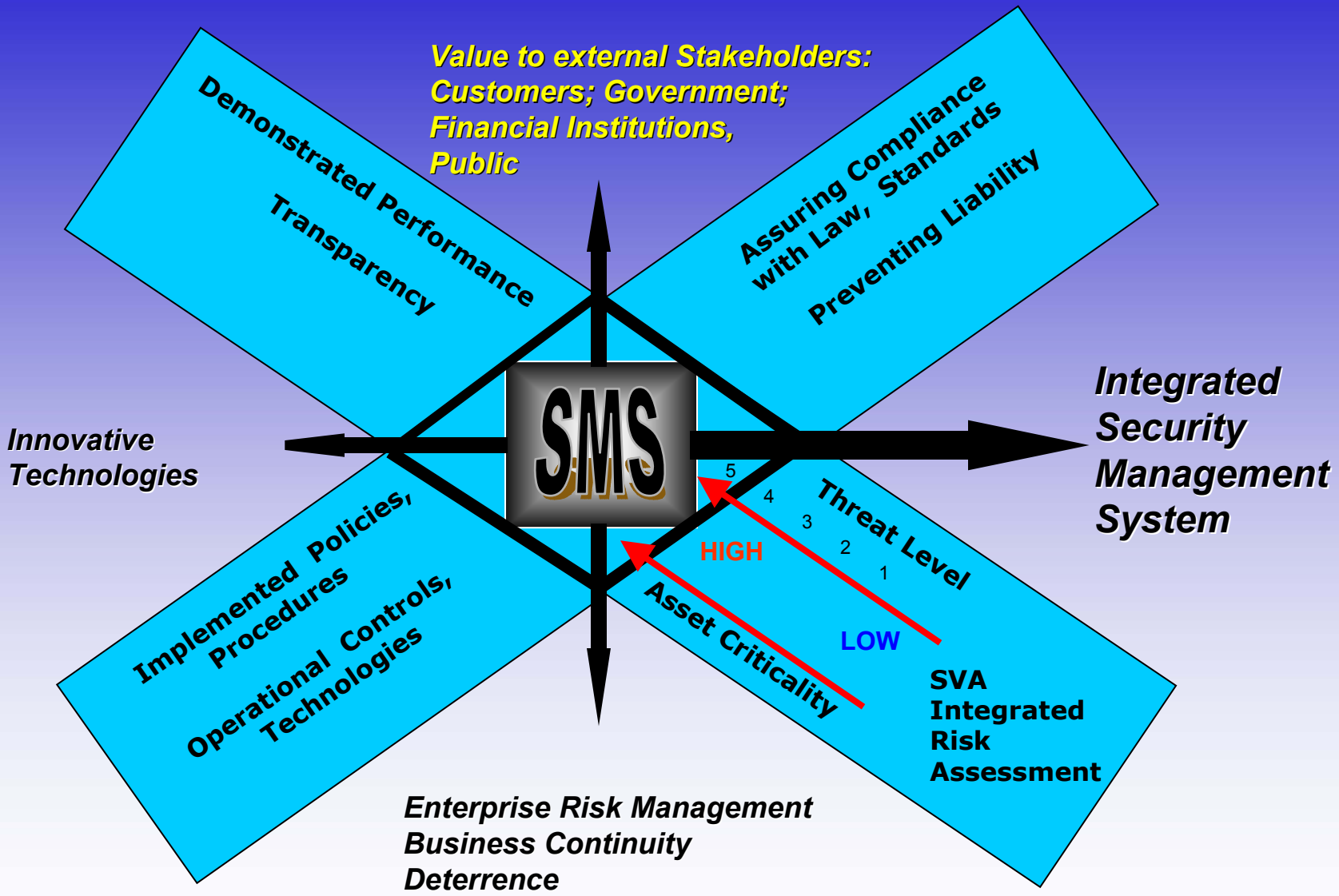
Step 3: Vulnerability Analysis

Step 4: Risk Assessment

Step 5: Countermeasures Analysis


POLICY
Gap Analyses – SVA; MGMT Commitment – Define Program Intent
PLANNING
High Risk Areas – Gaps to SMS standard - Regulatory Issues:
Define policies, procedures, critical control points, technical solutions/countermeasures
– as substantive elements of Integrated SMS--
IMPLEMENTATION
Assign Responsibility/Accountability – Communication & Training Across Functions –
SMS Integration
MEASURE & EVALUATE
Operational Controls – Tests/Audits/Drills that Measure Performance
Communication/Reporting/Documentation –
Performance Indices
REVIEW & IMPROVE
Problem Reports – Management Review – Problem Resolution

Security Management System



For more information or questions:

Michael Penders

mpenders@esisecurity.com

(703) 330-3752

www.esisecurity.com

ANSI

American National Standards Institute

Management Systems Standards Update

Michael J. Penders Esq.
President
Environmental Security International
www.esisecurity.com

Foci of Emerging Issues group on Management System Standards

- ISO Strategic Advisory Group on Management System Standards
- ANAB accreditations related to MSS
- ISO TC 223 on Societal Security
- ISO TC 8 Ships and marine technology ISO 28000 Supply Chain Security Management Systems
- New ISO Project Committee to Develop Energy Management Standard *Secretariat Jointly Held by U.S. and Brazil*
- ISO TMB WG on risk management
- OECD Guidance for the Integrated Management of SHE&Q

ANSI-ASQ National Accreditation Board

U.S. accreditation body for management systems. ANAB accredits certification bodies (CBs) for:

- ISO 9001 quality management systems (QMS)
- ISO 14001 environmental management systems (EMS)
- ISO 27001 information security management systems (ISMS)
- ISO 22000 food safety management systems (FSMS)
- ANSI/AIHA Z10 occupational health and safety management systems (OHSMS)

Under Study: Safety Management; Emergency Preparedness; Energy Management

ANSI-ASQ National Accreditation Board

The Department of Homeland Security (DHS) intends to enter into negotiations on a sole source basis with ANSI-ASQ National Accreditation Board (ANAB), … The contractor will operate the Private Sector Preparedness Voluntary Accreditation and Certification Program to assess whether a private sector entity complies with voluntary preparedness standards http://www.gtwassociates.com/alerts/DHStoANSIsoliciation.htm

ISO TC 223 on Societal Security

- ISO/TC 223/Working Group (WG) 1 took IWA 5 and evolved it into ISO/PAS 22399 - *Guideline for incident preparedness and operational continuity management* (published Nov. 2007)
- ISO/TC 223 is now looking into the possibility of turning the Publicly Available Specification (PAS) 22399 into an ISO standard, as well as a starting a separate new work item proposal on a management system standard for preparedness and continuity
- US experts interested in participating in the international work need to join the US Technical Advisory Group (TAG) to ISO/TC 223 – contact David Trebisacci (dtrebisacci@nfpa.org). There is a working group meeting in a few weeks in Milan, Italy, and the next TC 223 plenary meeting is in May in Seoul, Korea.

ISO TC 8 Ships and marine technology ISO 18000 Supply chain security management systems

- ISO 28000, *Supply chain security management systems*
  - Published – similar risk based approach as ISO 14001
- ISO 28001, *Best practices for implementing supply chain security, assessments and plans*
  - Published – conducting security vulnerability assessments
  - consistent with WCO Framework of Standards
  - Assist industry in meeting Authorized Economic Operators (AEO's) criteria set by WCO
  - *Note: Only a National Customs Agency can designate & certify AEO*'s
- ISO 28003, *Auditing & Certification*
  - Published - guidance for accreditation & certification bodies
- ISO 28004, *Guide for implementing ISO 28000*
  - Published – assist users in implementing ISO 28000
- ISO 28005, *Electronic port clearance*
  - Under development - computer-to-computer data transmission
  - All reporting related to ship's clearance in or out of a port

ISO Project Committee to Develop Energy Management Standard *Secretariat U.S. and Brazil*

The new standard will provide all types of organizations and companies with a practical and widely recognized approach to increase energy efficiency, reduce costs, and improve their environmental performance.

Following the successful examples of the ISO 9000 series on quality management and the ISO 14000 series on environmental management, PC 242, *Energy management*, will consider the development of a standard that contains relevant terms and definitions and provides management system requirements together with technical guidance for use, implementation, and metrics.

ISO 9000 series on quality management and the ISO 14000 series on environmental management, PC 242, *Energy management*, will consider the development of a standard that contains relevant terms and definitions and provides management system requirements together with technical guidance for use, implementation, and metrics.

The secretariat of PC 242 will be held jointly by the American National Standards Institute (ANSI) and the Associação Brasileira de Normas Técnicas (ABNT), the national member bodies for the United States and Brazil, respectively

ISO Technical Management Board Working Group (ISO/TMB/RM) on Risk Management

ANSI has approved American Society of Safety Engineers (ASSE) as administrator for the U.S. Technical Advisory Group (TAG) for the ISO Technical Management Board Working Group (ISO/TMB/RM) on Risk Management.

The ISO ISO/TMB/RM last met December 3 – December 7 in China to review *N47 Committee Draft of ISO 31000 "Risk management — Guidelines on principles and implementation of risk management"* . The United States has not previously participated in the work.

Other drafts prepared by the ISO/TMB/RM include:

N29 Working Draft 3 of AWI 25700 "Risk Management – Guidelines on principles and implementation of risk management"
N30 Working Draft 1 of "Risk management – Vocabulary – Guidelines for use in standards"

Draft OECD Guidance for the Integrated Management of SHE&Q

The "Draft OECD Guidance for the Integrated Management of SHE&Q" dated December 2005 is an interim document developed by Korea and a small group of experts from other member countries. The draft will become a final document when it will be approved by the OECD member countries (via the WGCA and higher bodies of the Chemicals Group). Once "declassified", the document can be published (planned 2008) and will be then publicly available. But before that, there has been and there will be a number of meetings of the Expert Group and other revisions of the document. In addition, currently there is a pilot programme to test the December 2005 version of the guidance.