MIT ESD Sandia National Laboratories
Massachusetts Institute of Technology
Engineering Systems Division

SAND2014-15707PE

Beyond 'Gates, Guards & Guns':

Applying a Systems, Control & Organizational Theory-Based Methodology for Security at Nuclear Facilities

Adam D. Williams*

July 2014

26th International Summer Symposium on Science & World Affairs
Hosted by the Union of Concerned Scientists | | Princeton, NJ

*SAND2014-XXXX

Outline

What's Wrong?

What We Have Now

What's Missing?

What's Needed?

What New?

What's Gained?

The **views expressed herein are those of the author** and do **NOT** reflect the official policy, position or recommendation of Sandia National Laboratories, the National Nuclear Security Administration, the Lockheed Martin Corporation, the U.S. Department of Energy or the U.S. Government.

What's Wrong?

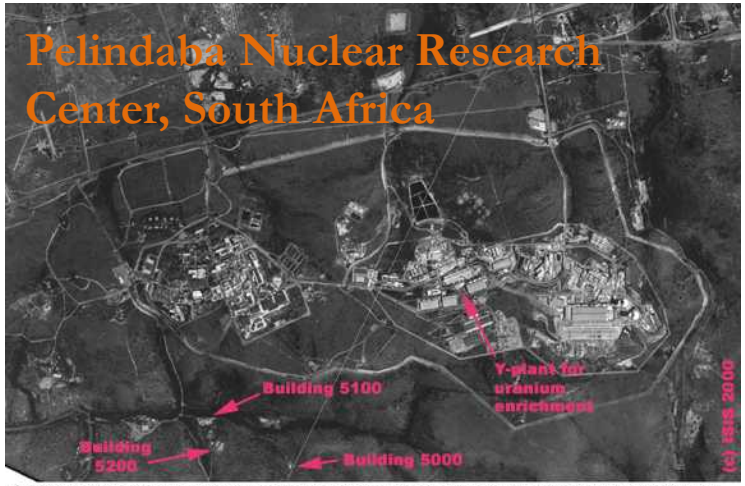
Global **attention**:

- Nuclear Security Summits
- IAEA Security Division
- Terrorist groups/rogue nations

Resource **attention**:

- >$1B spent in U.S.

Operational **attention**?

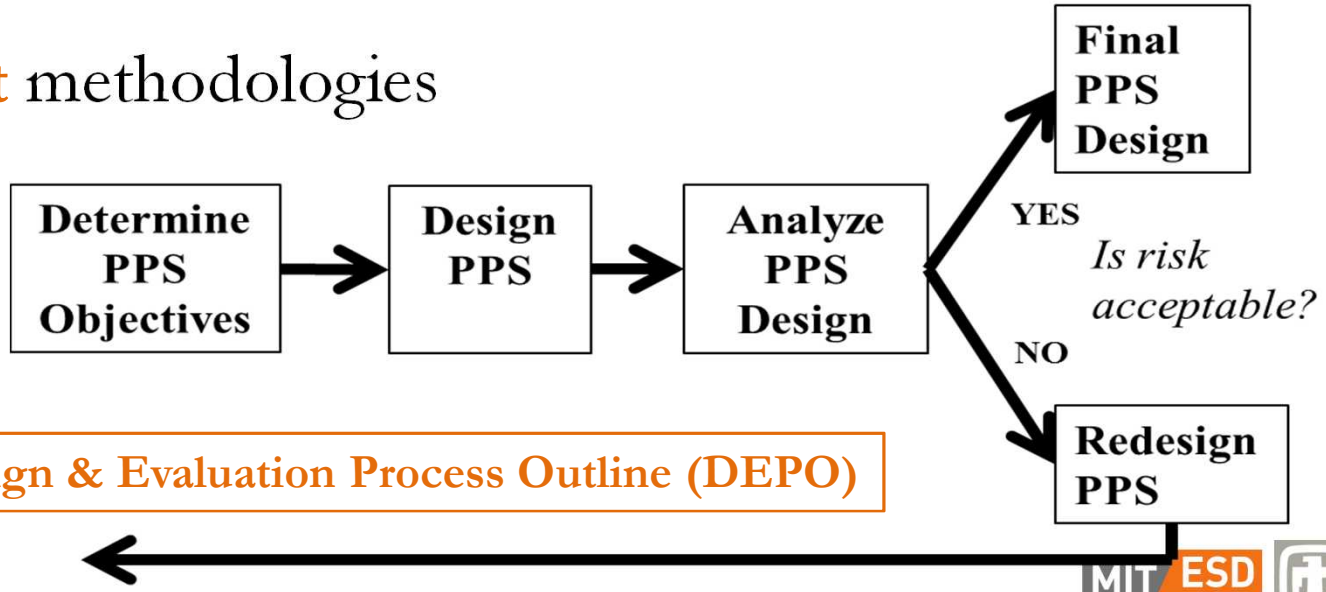


Significant former nuclear weapons related facilities at the Pelindaba-Valindaba Complex, near Pretoria, South Africa. December 1991 KVR-1000 image from www.terraserver.com.

'Every dollar that a facility manager spends on protection is a dollar *not* spent on revenue-generating production' [Bunn 2007]

Today's Approaches Emphasize:

- '**bottom-up**' causality
- '**chain-of-event**' models
- **Probability** (independence & randomness) theory
- **Reliability** (component redundancy & balanced layers) thinking
- **Path dependent** methodologies



Design & Evaluation Process Outline (DEPO)

Today's Security is Challenged By:

- The '**insider**' problem
- **Legacy effects**
- **Complacency**
- Need to define '**security culture**'
- The **long time intervals** between security incidents

Security = protecting the most vulnerable path(???)

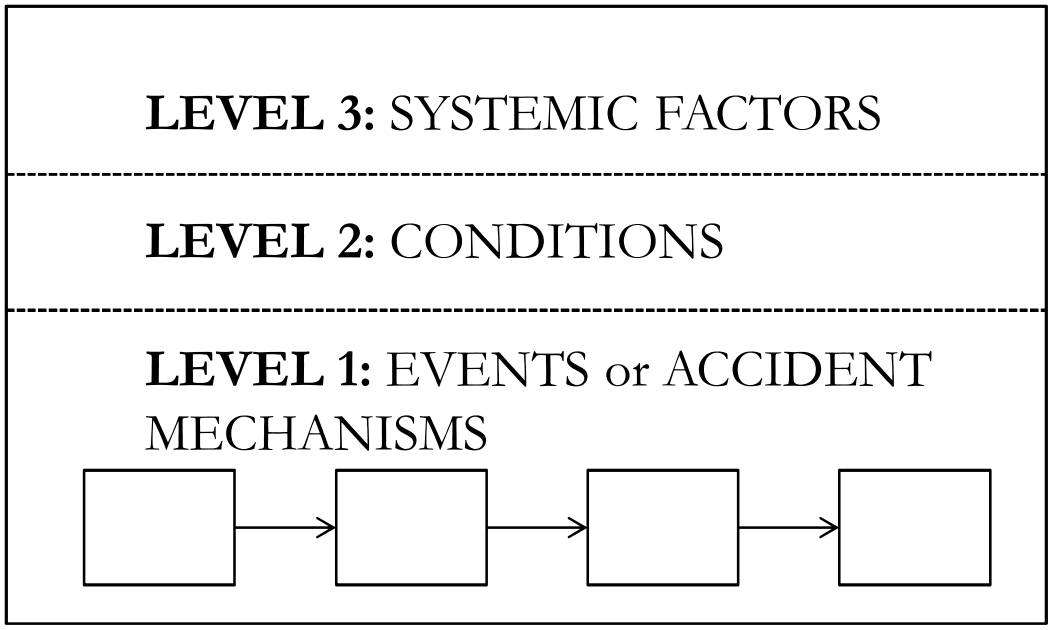
Today's Security is Missing:

- Nuclear facility = **complex, socio-technical system**
- **Security** of system ≠ **reliability** of components
- **Dynamic** & **interactive** complexity
- Rigorous **inclusion** of **organizational/social** aspects

$$\text{Security} = f\left(\begin{array}{c}\textit{System Theory}\\ \textit{Control Theory}\\ \textit{Organization Theory}\end{array}\right)$$

Today's Security Needs: SYSTEM THEORY

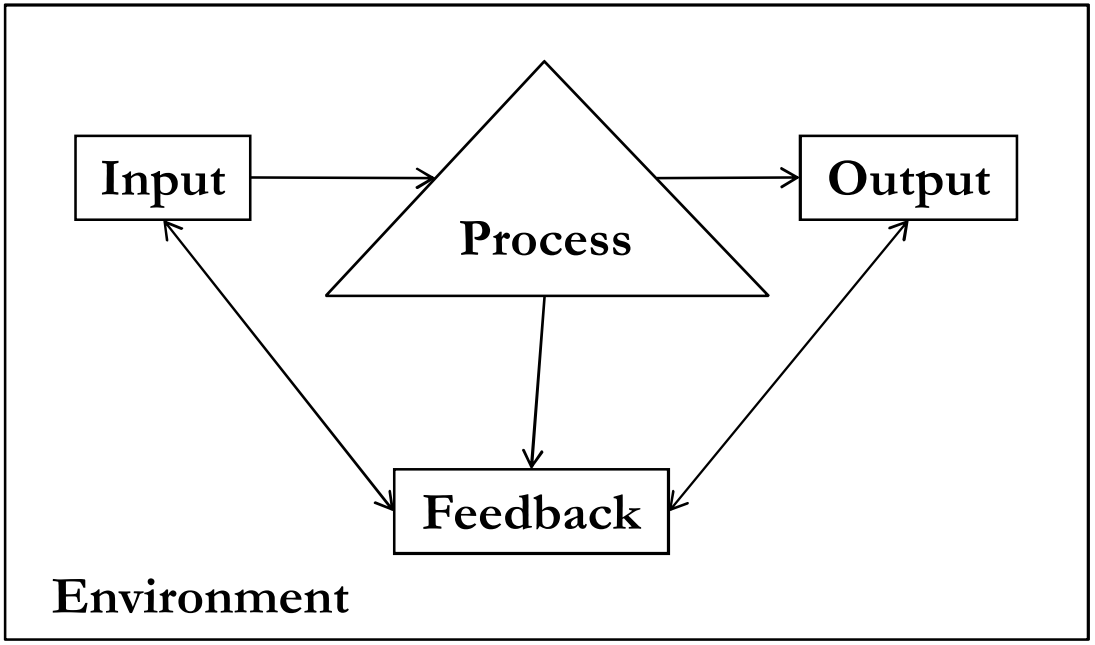
- **Hierarchy**: relationship between levels of complexity
- **Emergence**: irreducible phenomenon



Security = emergent across hierarchical levels

Today's Security Needs: CONTOL THEORY

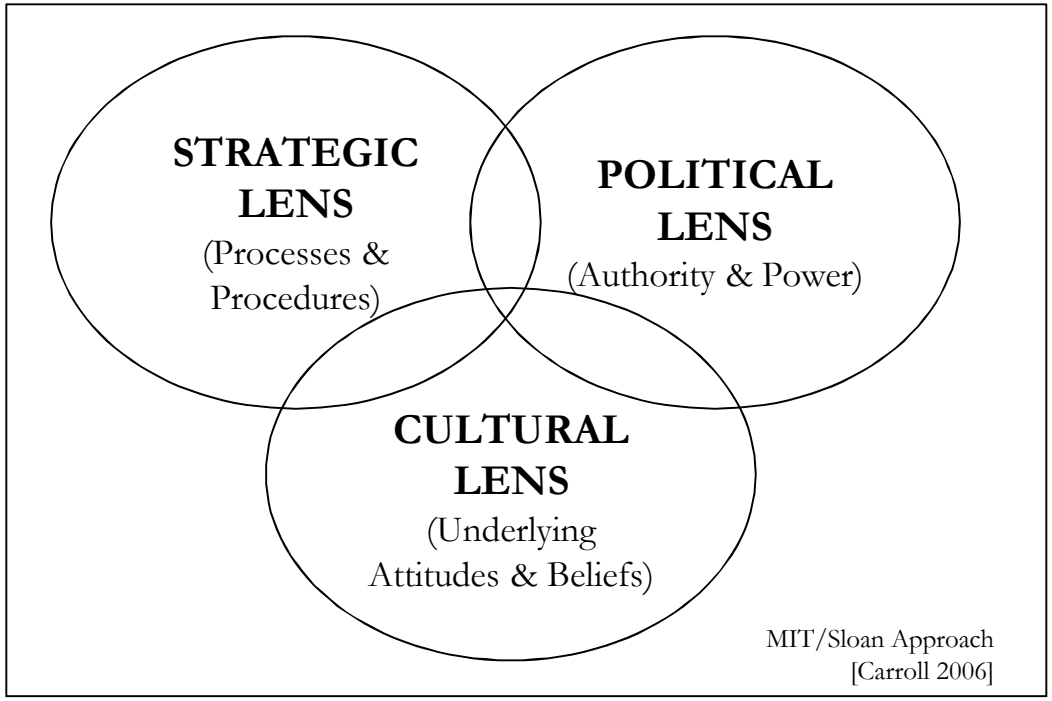
- **Control**: constraints on behavior across levels
- **Communication**: information travel around control loop



Security = communication of control actions

Today's Security Needs: ORGANIZATION THEORY

- **Structuration Theory**: structure emerges from recurrent human action
- **System Dynamics**: non-linear feedback & dynamic complexity



Security = recurrent human actions over time

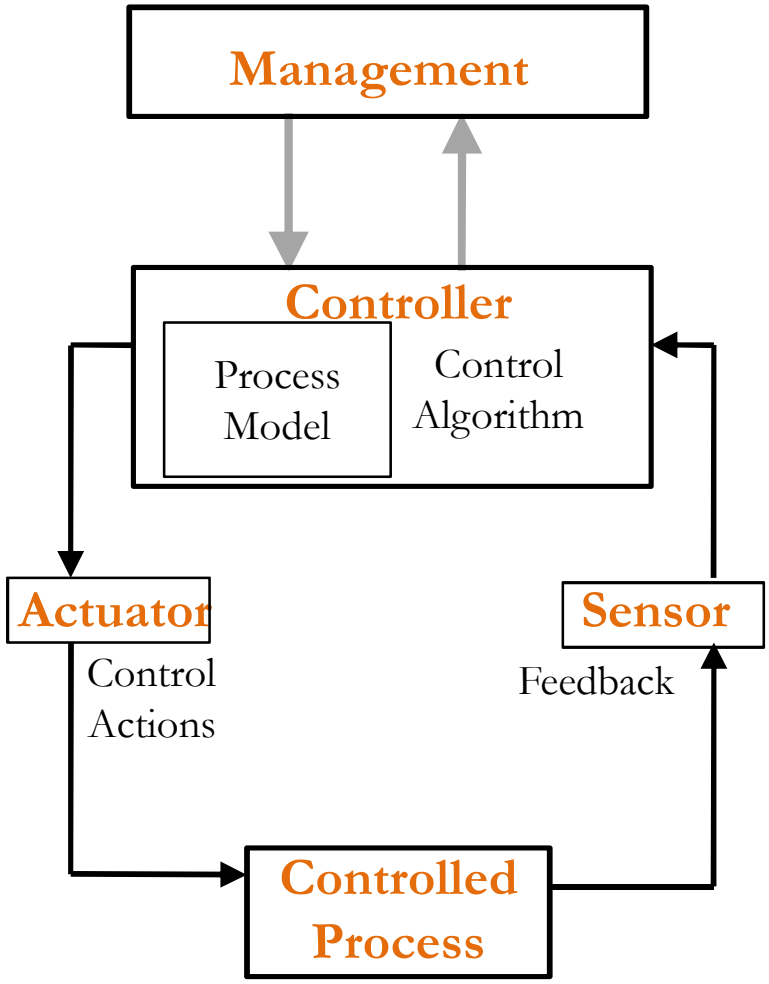
Today's Security Via: STAMP

- **System Theoretic Accident Model & Process** (**STAMP**)
- '**top-down**' causality model for vulnerabilities
- Based on **systems** & **control** theory
- Identify vulnerabilities to **eliminate/minimize insecure system states** (e.g., redesign)
- Includes **organizational considerations** in analysis

Security = eliminating migration of facility into vulnerable or insecure states

Today's Security Via: STAMP

- Define Mission
- Identify Losses
- Identify Vulnerable States
- Derive Security Requirements
- Define Security Control Actions
- Find Security Control Action Violations
- Derive Adversary Actions



STAMP Basic Control Structure

[Leveson, 2012; Thomas 2012]

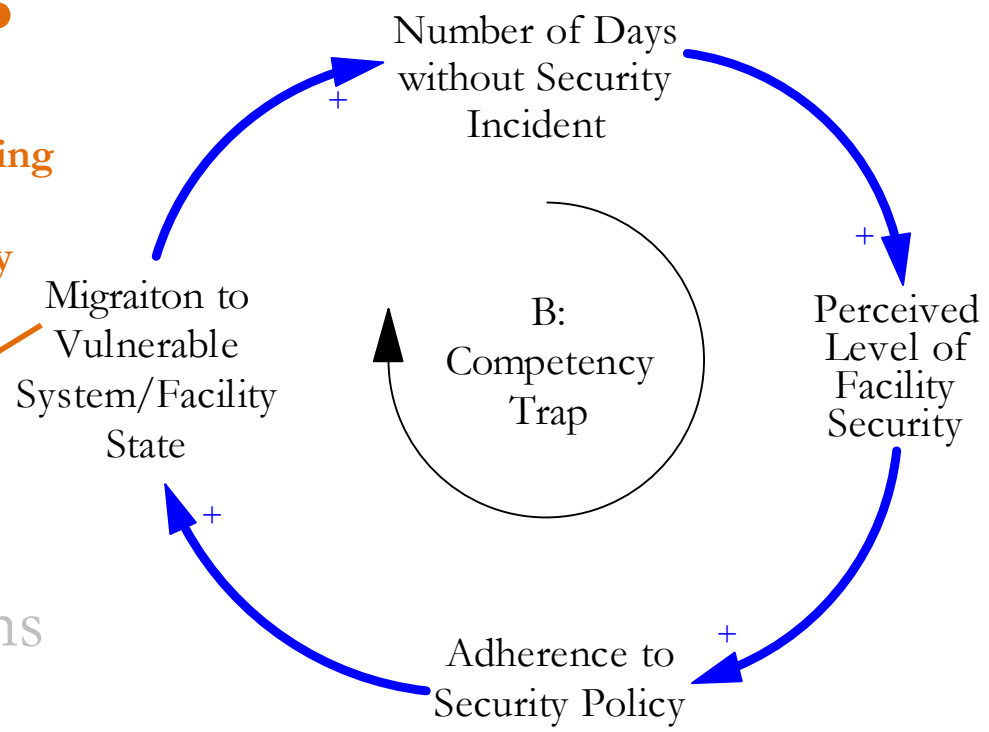
Today's Security Via: STAMP

- Define Mission
- Identify Losses

Detection trap; funding & incentives issues; frequency of security policy changes

- **Identify Vulnerable States**
- Derive Security Requirements
- Define Security Control Actions
- Find Security Control Action Violations
- **Derive Adversary Actions**

'Insider' actions; collusion/coercion; disaffected employee



Today's Security Via: STAMP

- **Higher # vulnerabilities** identified
- **Physical/cyber interaction** vulnerabilities identified
- **Safety/Security/ Safeguards interaction** vulnerabilities identified

Current Approaches	System Attribute	STAMP Approach
Protection of nuclear materials against most vulnerable paths	**Definition of Security**	Maintaining a system state that can protect nuclear materials from loss
Reliability engineering, probability theory	**Basis for Analytical Framework**	Systems theory, system dynamics
Included as initial design condition	**Treatment of Organizational Culture**	Included as an ongoing system attribute
Combinatorial	**Type of Complexity**	Dynamic Interactive

Today's Security Via: STAMP

- Security = **emergent property of a nuclear facility**
- Accounts for dynamic complexity → **dynamic equilibrium**
- **Traceability** between security improvements & vulnerable states
- **Organizational issues** related to vulnerable facility states
- Framework for identifying **component interaction effects**
- Paradigm shift: **preventing security failures** → **enforcing security constraints**

Questions???

"No problem can be solved from the same level of consciousness that created it"

-Albert Einstein