MIT ESD

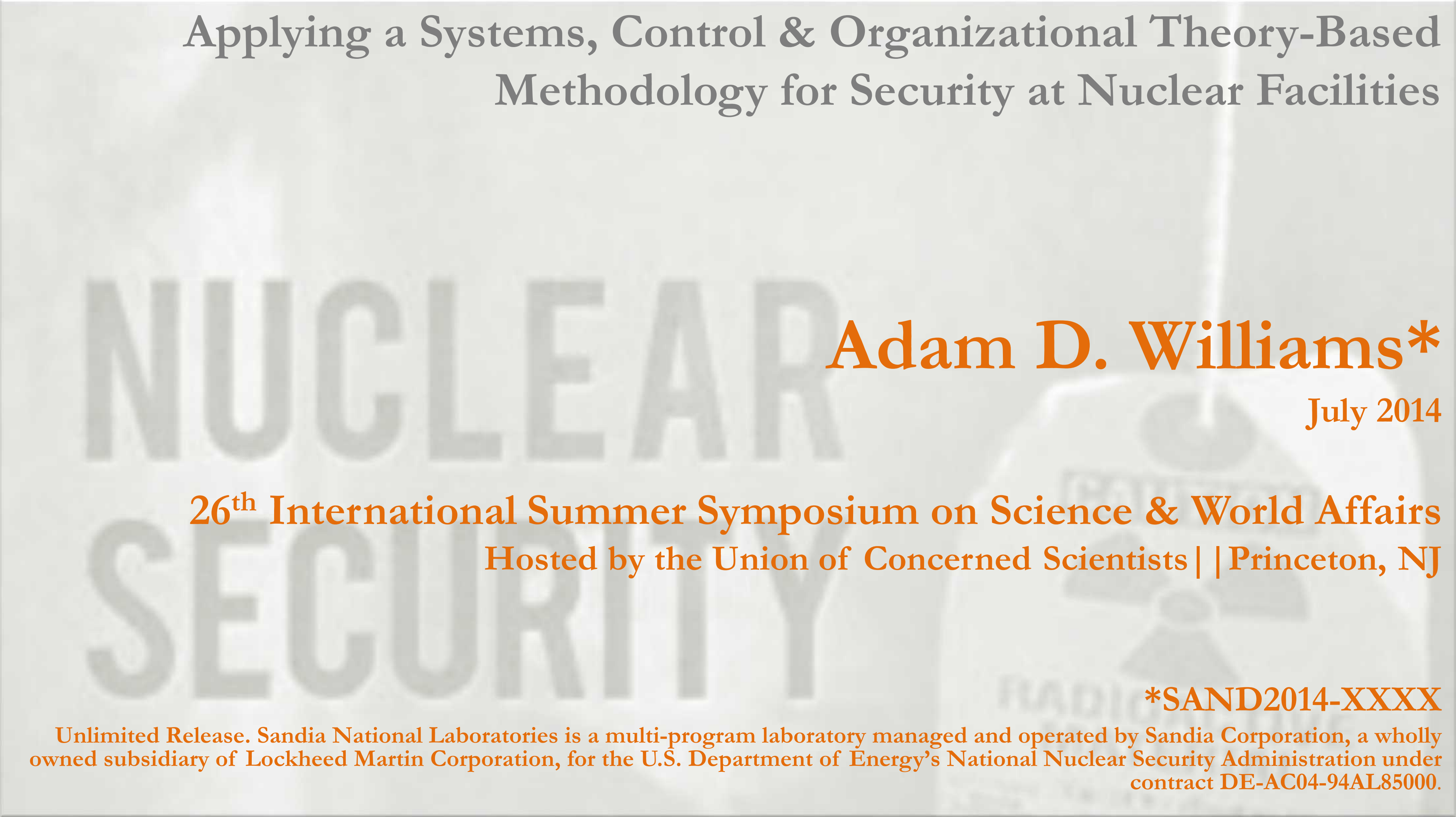
Sandia National Laboratories

Massachusetts Institute of Technology
Engineering Systems Division

SAND2014-15708PE

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

Unlimited Release. Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy’s National Nuclear Security Administration under contract DE-AC04-94AL85000.

Motivation

Courtesy: Google Maps

July 28, 2012:

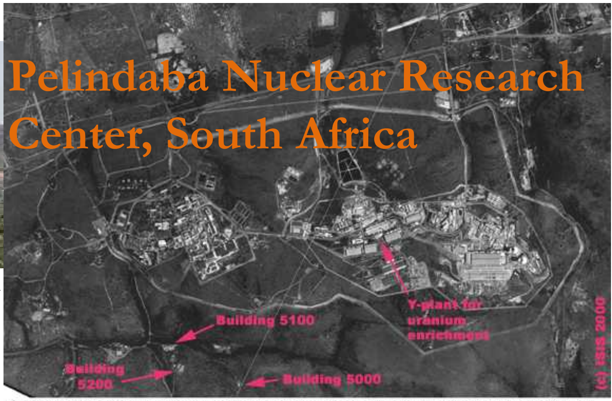
- 3 protestors successfully breach several layers of security elements
- Deface & vandalize buildings [DOE 2012]

BOTH of these events were considered 'wins' by their respective security systems

November 8, 2007:

- Facility is attacked by armed gunmen
- Second group attacked a different section of perimeter [Bunn 2008]

Courtesy: Wikipedia


Pelindaba Nuclear Research Center, South Africa
Building 5100
Y-plant for uranium enrichment
Building 5200
Building 5000
(c) ISIS 2000

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

Courtesy: ISIS

Courtesy: NRC

Copyright: A. Williams

Force-on-Force Inspections at U.S. Nuclear Power Plants

- Tightly controlled, simulated exercises & 'plant defenders know that a mock attack will take place sometime during a specific period of a few hours'
- 23 inspections conducted in 2012 [Holt 2014]
  - 11 facilities with security 'performance deficiencies'

Outline

Motivation

Current Approaches

A New Approach

An Example

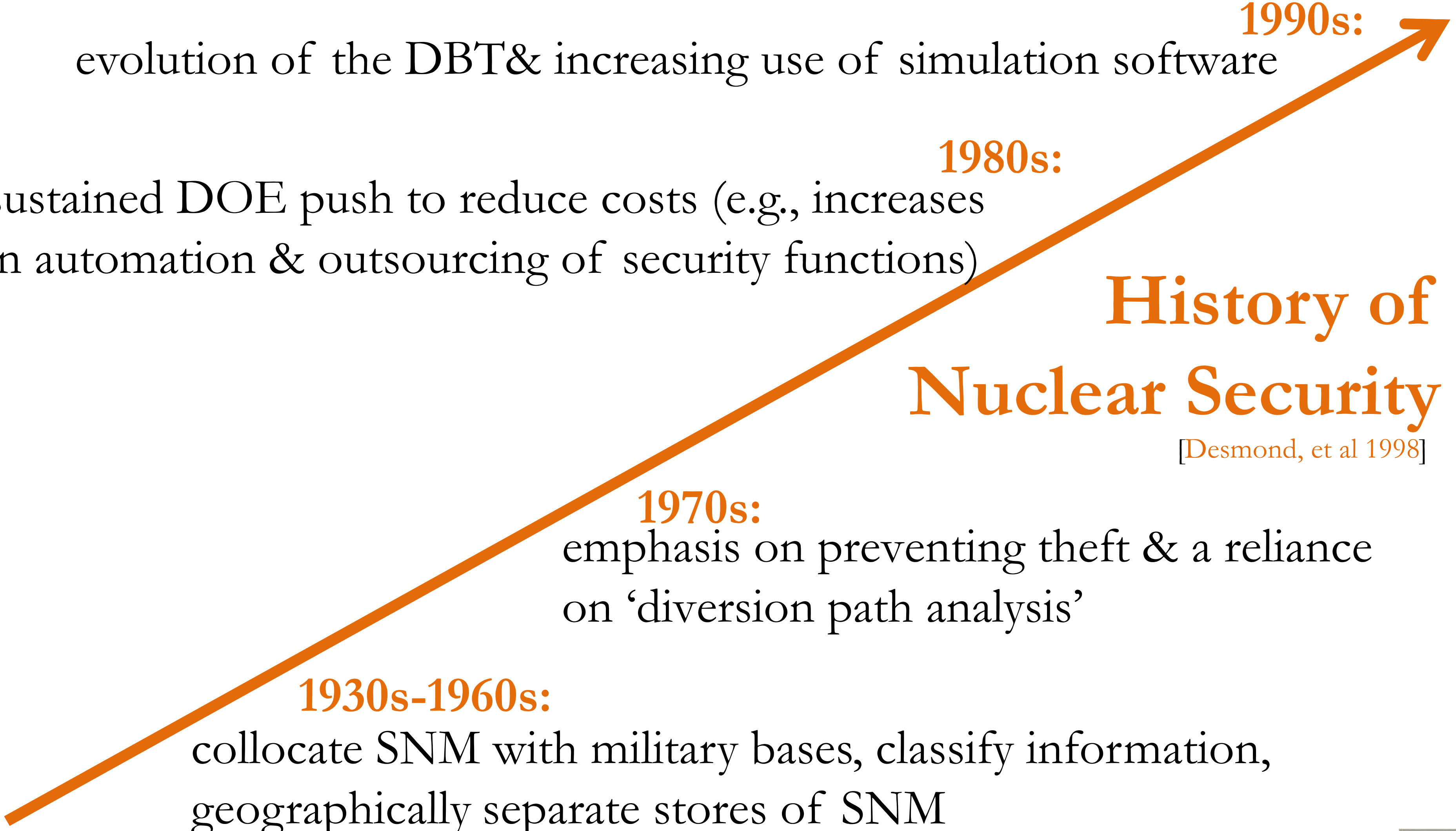
Path Forward

Summary

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.

History of Nuclear Security

[Desmond, et al 1998]



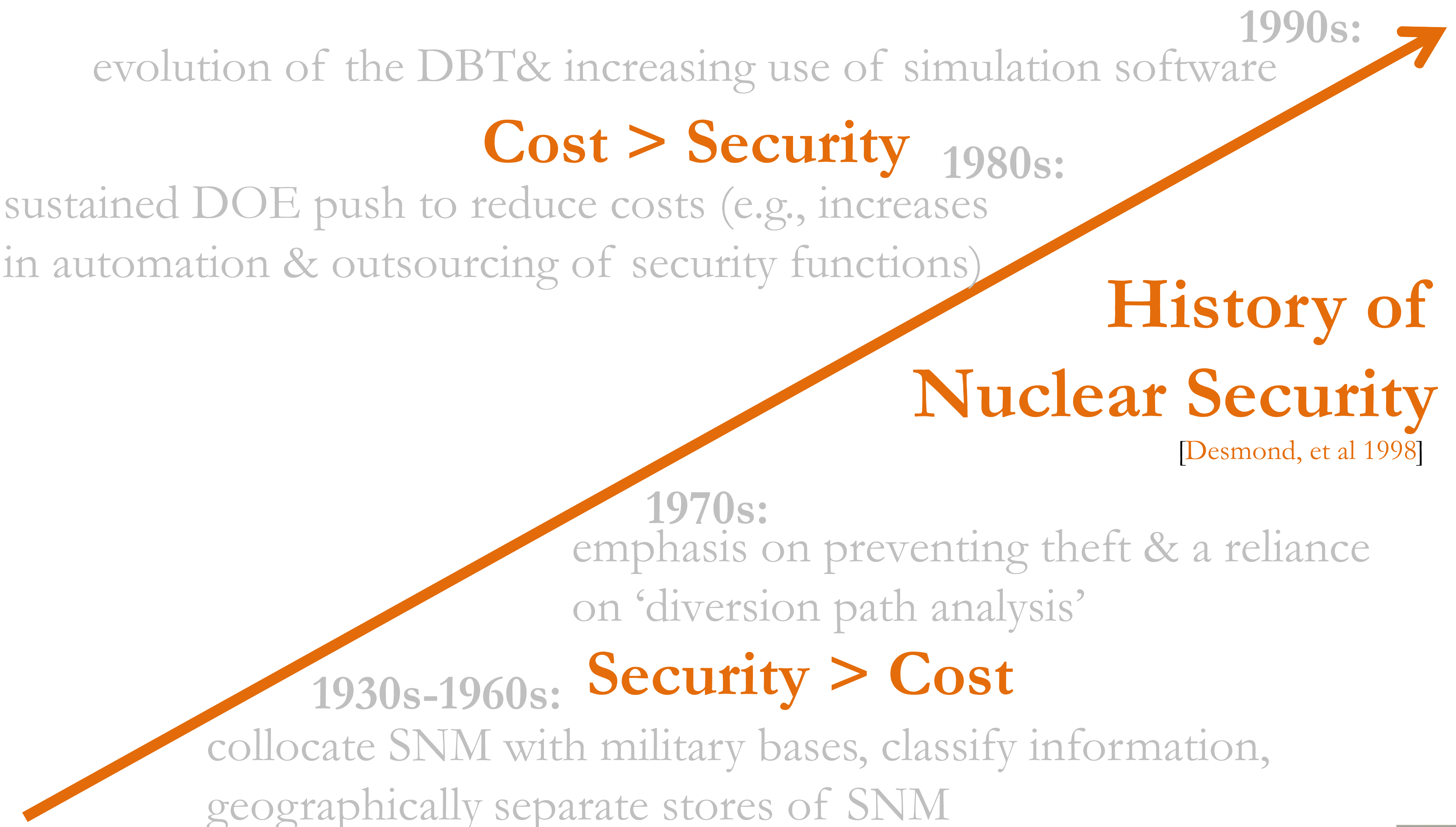
1930s-1960s:
collocate SNM with military bases, classify information, geographically separate stores of SNM

1970s:
emphasis on preventing theft & a reliance on ‘diversion path analysis’

1980s:
sustained DOE push to reduce costs (e.g., increases in automation & outsourcing of security functions)

1990s:
evolution of the DBT& increasing use of simulation software

Motivation



1990s:
evolution of the DBT& increasing use of simulation software

Cost > Security

1980s:
sustained DOE push to reduce costs (e.g., increases in automation & outsourcing of security functions)

History of Nuclear Security

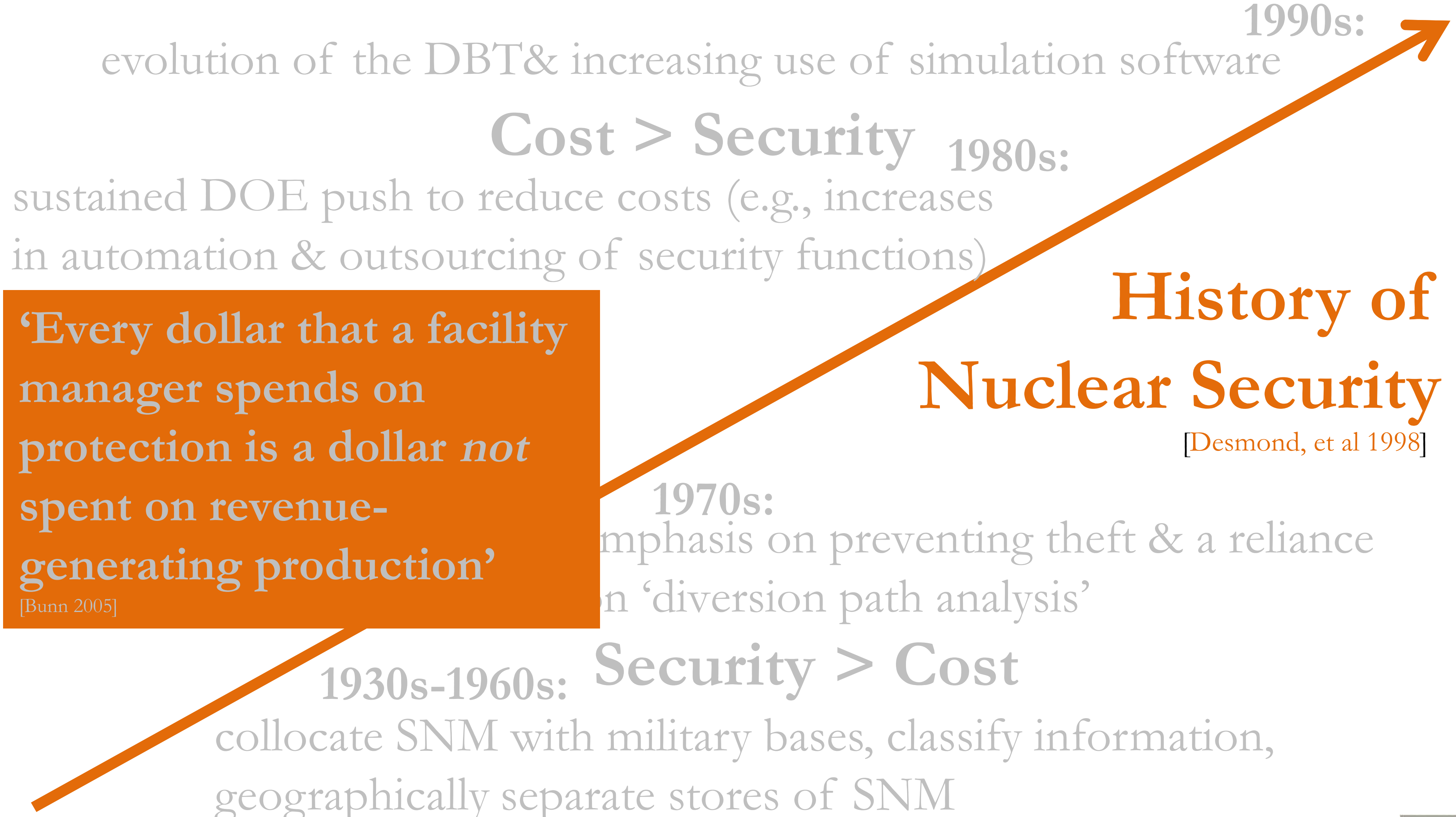
[Desmond, et al 1998]

1970s:
emphasis on preventing theft & a reliance on 'diversion path analysis'

1930s-1960s: **Security > Cost**

collocate SNM with military bases, classify information, geographically separate stores of SNM

Motivation



1990s:

evolution of the DBT& increasing use of simulation software

Cost > Security

1980s:

sustained DOE push to reduce costs (e.g., increases in automation & outsourcing of security functions)

History of Nuclear Security

[Desmond, et al 1998]

> **'Every dollar that a facility manager spends on protection is a dollar *not* spent on revenue-generating production'**
>
> [Bunn 2005]

1970s:

mphasis on preventing theft & a reliance n 'diversion path analysis'

Security > Cost

1930s-1960s:

collocate SNM with military bases, classify information, geographically separate stores of SNM

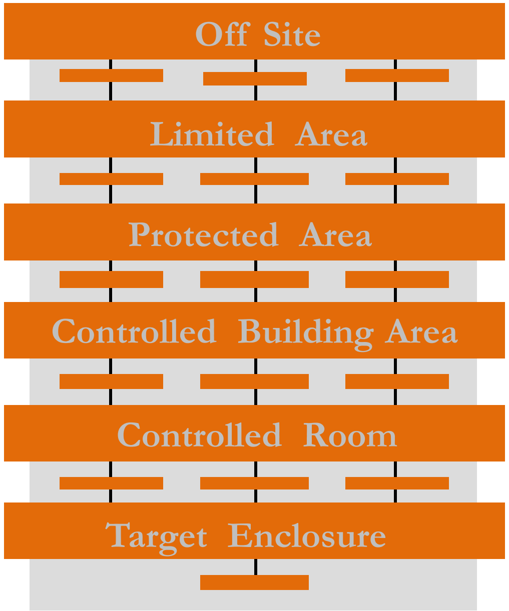
What is **nuclear security**?

- Consistent **definitions**:
  - International Atomic Energy Agency (INFCIRC/225); US/Nuclear Regulatory Commission (CFR73.1)
    - Prevent, detect & respond to theft or sabotage of nuclear materials
- Consistent **logical arguments**:
  - Design security systems to mitigate an expected adversary threat (under conservative assumptions)
    - If mitigate ‘worst-case path,’ can mitigate all least-worse paths
- Inconsistent **results**?

Current Approaches

Design Evaluation Process Outline (DEPO)

- ‘**bottom-up**’ causality understanding of vulnerabilities [Garcia 2005]
- Based on **probability** (independence & randomness) theory and **reliability** (component redundancy & balanced layers) thinking
- Identify vulnerabilities for redesign toward meeting **regulated system effectiveness**



Adversary Sequence Diagram

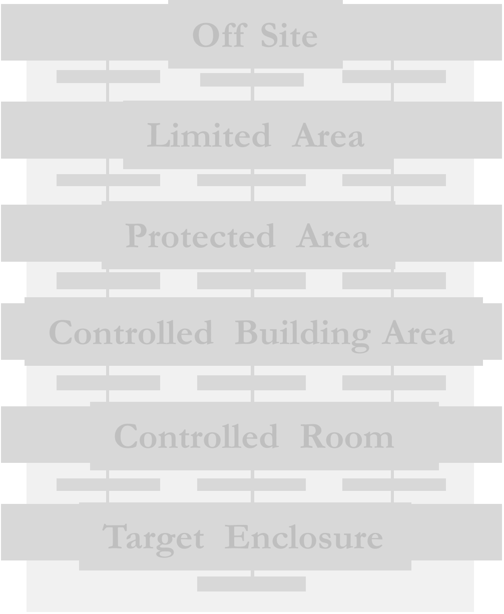
[Garcia 2005]

- Translate 3D facility into **2D model of layers & components**
- Assign **worst case P_D & t_D** to each element (based on **adversary capabilities**)
- Calculate ‘**most vulnerable path(s)**’
- Change **components/ parameters** to meet **regulated P_E**

Current Approaches

Design Evaluation Process Outline (DEPO)

- ‘**bottom-up**’ causality understanding of vulnerabilities [Garcia 2005]
- Based on **probability** (independence & randomness) theory and **reliability** (component redundancy & balanced layers) thinking
- Identify vulnerabilities for redesign toward meeting **regulated system effectiveness**



Adversary Sequence Diagram

[Garcia 2005]

- Translate 3D facility into **2D model of layers & components**
- Assign **worst case P_D & t_D** to each element (based on **adversary capabilities**)
- Calculate ‘**most vulnerable path(s)**’
- Change **components/ parameters** to meet **regulated P_E**

New Approaches

- **Extensions** of/**advancements** on DEPO…
  - Advanced stochastic methods [Lord & Nunes-Vaz 2013; Duran 2012]
  - Nuclear security culture [IAEA 2008; WINS 2011]
  - ‘Security-by-Design’ [Snell, et. al. 2013]

Current Approaches

Design Evaluation Process Outline (DEPO)

What's Missing?

- Considering a **nuclear facility as a complex, socio-technical system**
  - Need to move away from military security models [Personal Correspondence with Nuclear Security Expert]
  - DBT & Adversary specific countermeasures [Garcia 2005; Duran 2012]

- **Security** of system **≠ reliability** of components in series
  - 'Gates, guards & guns' [Desmond, et. al 1998; Garcia 2005]
  - Lessons learned from nuclear safety [Sagan 1995, 2004; Kuperman & Kirkham 2013]

- **Dynamic** & **interactive** complexity
  - The reality of the 'insider threat' [Bunn & Sagan 2014]
  - Evolving technologies & threats [Personal Correspondence with Nuclear Security Expert; NSGEG 2013]
  - Vulnerabilities from redundancy [Sagan 2004]

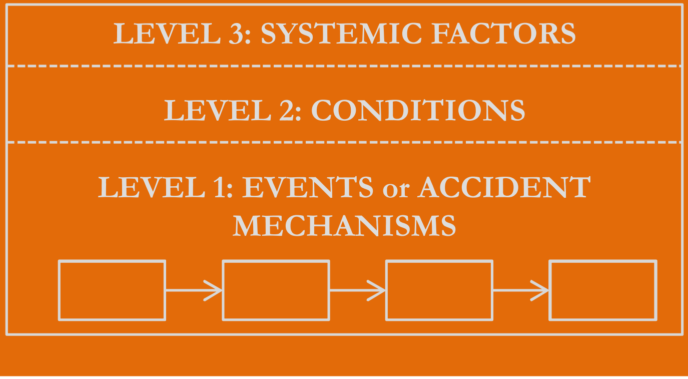
- **Rigorous inclusion** of **organizational**/social aspects
  - Motivation/incentives issues for facility staff members (e.g., boredom) [Bunn 2005; Charlton & Hertz 1989]
  - National prestige of nuclear facilities [Nuclear Security Summit Communiques 2010, 2012]
  - Sovereignty & secrecy [CPPNM 1980; Amend. 2005; IAEA 2006, 2011]

Current Approaches

Design Evaluation Process Outline (DEPO)

What's Needed?

Systems Theory

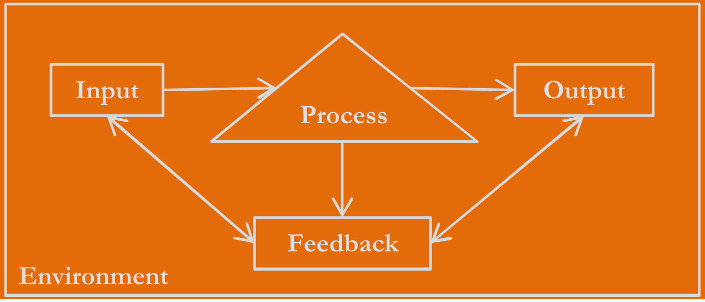


LEVEL 3: SYSTEMIC FACTORS

LEVEL 2: CONDITIONS

LEVEL 1: EVENTS or ACCIDENT MECHANISMS

Control Theory



Input

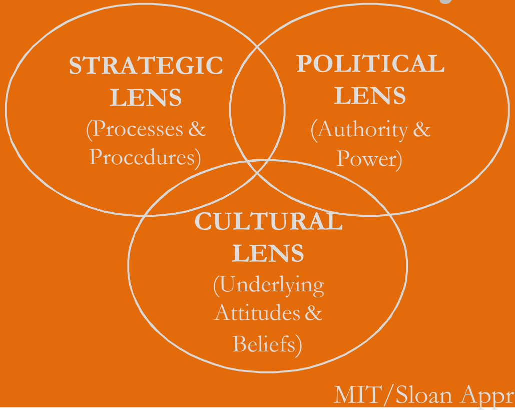
Process

Output

Feedback

Environment

Organization Theory



STRATEGIC LENS (Processes & Procedures)

POLITICAL LENS (Authority & Power)

CULTURAL LENS (Underlying Attitudes & Beliefs)

MIT/Sloan Approach [Carroll 2006]

Current Approaches

System Theoretic Accident Model & Process (STAMP)

What's Needed?

Systems Theory

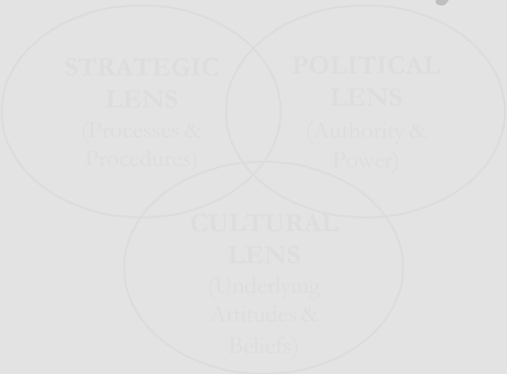
LEVEL 3: SYSTEMIC FACTORS
LEVEL 2: CONDITIONS
LEVEL 1: EVENTS or ACCIDENT MECHANISMS

– **Systems** & **control** theory-based causality model for complex, socio-technical systems [Leveson 2012]

–'**top-down**' model for hazards & losses used across complex technical domains [Leveson 2012; Stringfellow, et. al. 2010; Alemzadeh, et. al. 2013]

Control Theory

Organization Theory

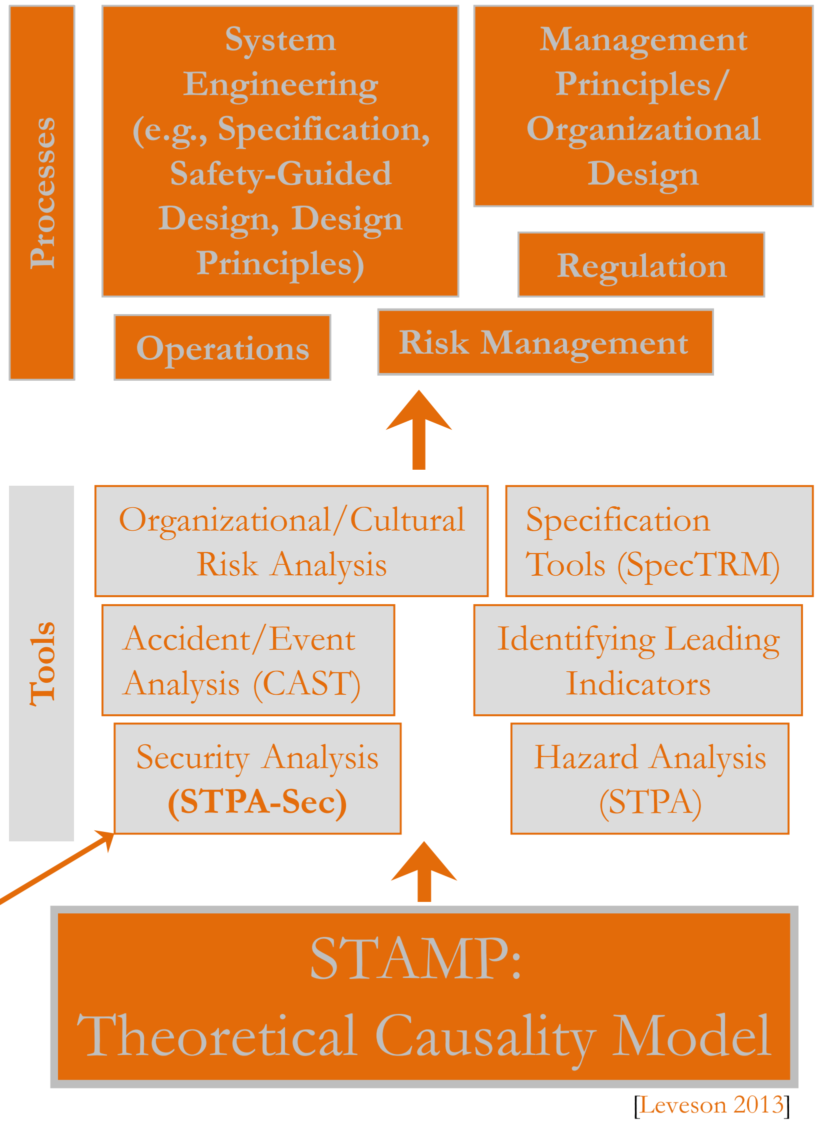

STRATEGIC LENS (Processes & Procedures)
POLITICAL LENS (Authority & Power)
CULTURAL LENS (Underlying Attitudes & Beliefs)

MIT/Sloan Approach [Carroll 2006]

A New Approach

System Theoretic Accident Model & Process (STAMP)

- ‘**top-down**’ causality model for vulnerabilities [Leveson 2012]
- Based on **systems** (emergence & hierarchy) and **control** (communications & constraints) theory
- Identify vulnerabilities to **eliminate/minimize vulnerable system states** (e.g., redesign)
- Safety (and thus security) is considered an **emergent system property**



Processes

System Engineering (e.g., Specification, Safety-Guided Design, Design Principles)

Management Principles/ Organizational Design

Regulation

Operations

Risk Management

Tools

Organizational/Cultural Risk Analysis

Specification Tools (SpecTRM)

Accident/Event Analysis (CAST)

Identifying Leading Indicators

Security Analysis **(STPA-Sec)**

Hazard Analysis (STPA)

STAMP: Theoretical Causality Model

[Leveson 2013]

Recent work argues that the **theoretical basis** of **STAMP** is **highly applicable** to the **security domain**

[Laracy & Leveson 2011; Williams 2013; Leveson & Young 2013]

A New Approach

System Theoretic Accident Model & Process (STAMP)

System Theoretic Process Analysis (STPA)

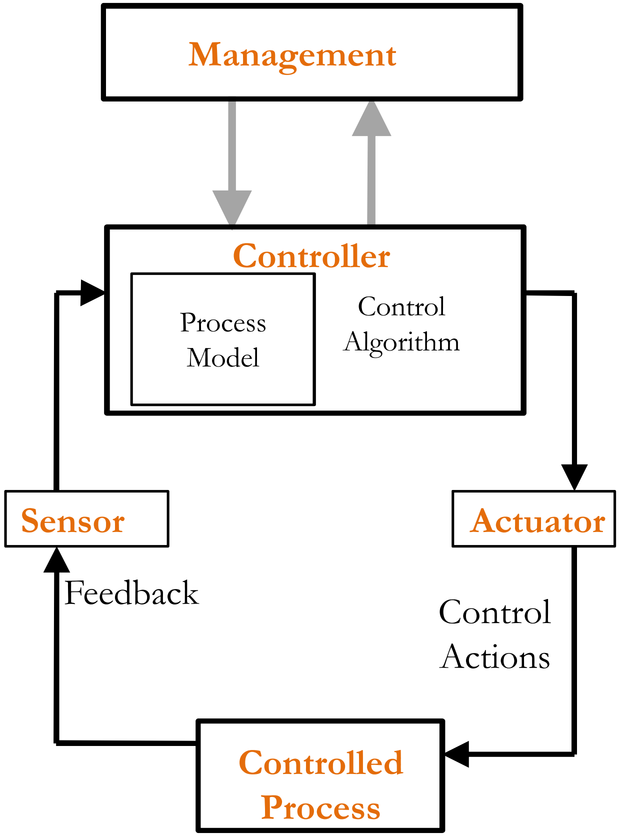
•Identify **high level vulnerabilities**

•Identify **vulnerable control actions** and **security constraints**

•Identify **scenarios that lead** to **violation** of security constraints

• **Redesign** system to **eliminate** or **minimize** such violations

STPA-SEC is an extension of STPA being developed for **cyber** and **physical** complex systems [Young 2014 (forthcoming diss.); Williams 2013]



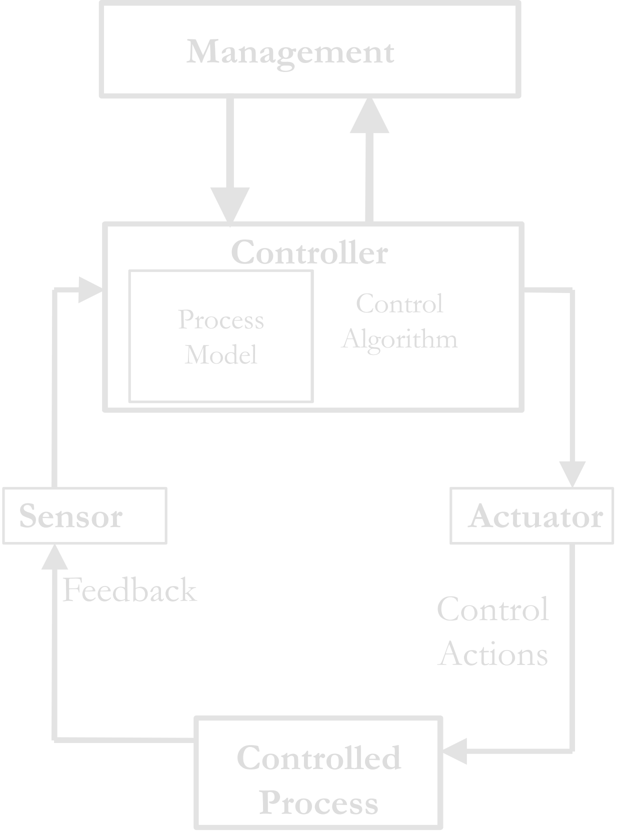
STPA Basic Control Structure

[Leveson, 2012; Thomas 2012]

System Theoretic Accident Model & Process (STAMP)

How can STAMP/STPA-Sec be extended to account for:

- The 'insider' threat [Bunn & Saga 2014; Johnston (n.d.); IAEA 2008]
- The 'competence trap' (e.g., complacency) [DOE 2012; Charlton & Hertz 1989; Henderson & Clark 1990]
- The 'detection trap' [Anderson, et al 2004]
- The presence of 'security theater' [Johnston (n.d.)]
- Such legacy effects as [Bunn 2005, 2013; Johnston (n.d.)]:
  - Relationship with funding organization
  - Security policy change frequency/process
  - Incentives for adherence to security policies



STPA Basic Control Structure

[Leveson, 2012; Thomas 2012]

NUCLEAR SECURITY

A New Approach

System Theoretic Accident Model & Process (STAMP)

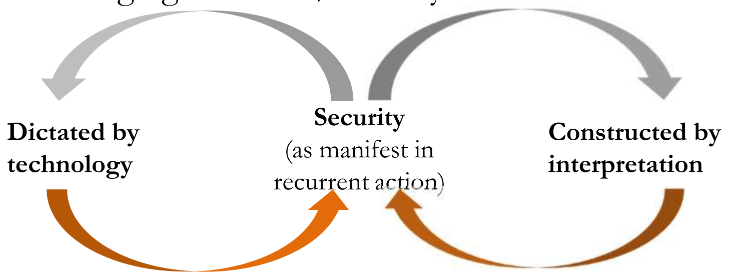
How can STAMP/STPA-Sec be extended to account for:

- The ‘insider’ threat [Bunn & Saga 2014; Johnston (n.d.); IAEA 2008]
- The ‘competence trap’ (e.g., complacency) [DOE 2012; Charlton & Hertz 1989; Henderson & Clark 1990]
- The ‘detection trap’ [Anderson, et al 2004]
- The presence of ‘security theater’ [Johnston (n.d.)]
- Such legacy effects as [Bunn 2005, 2013; Johnston (n.d.)]:
  - Relationship with funding organization
  - Security policy change frequency/process
  - Incentives for adherence to security policies

If security as an ‘**emergent property**’, then these issues can be captured with:

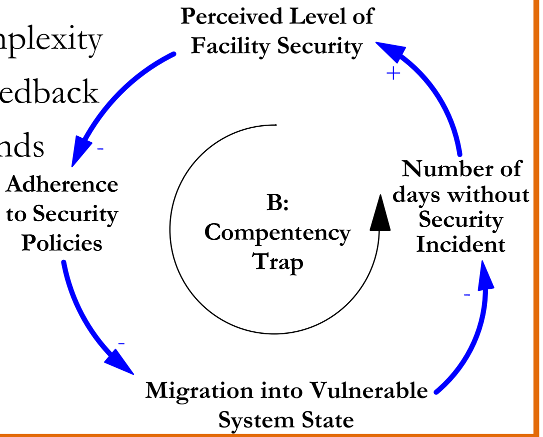
– **Structuration Theory** of organizations [Giddens 1984; Orlikowski 2000]

- Recurrent human action
- Emerging structure/security


Dictated by technology
Security
(as manifest in recurrent action)
Constructed by interpretation

– **System Dynamics** modeling [Sterman 2000]

- Dynamic complexity
- Non-linear feedback
- Emerging trends


Perceived Level of Facility Security
+
-
Adherence to Security Policies
B: Compentency Trap
Number of days without Security Incident
-
-
Migration into Vulnerable System State

MIT ESD

A New Approach

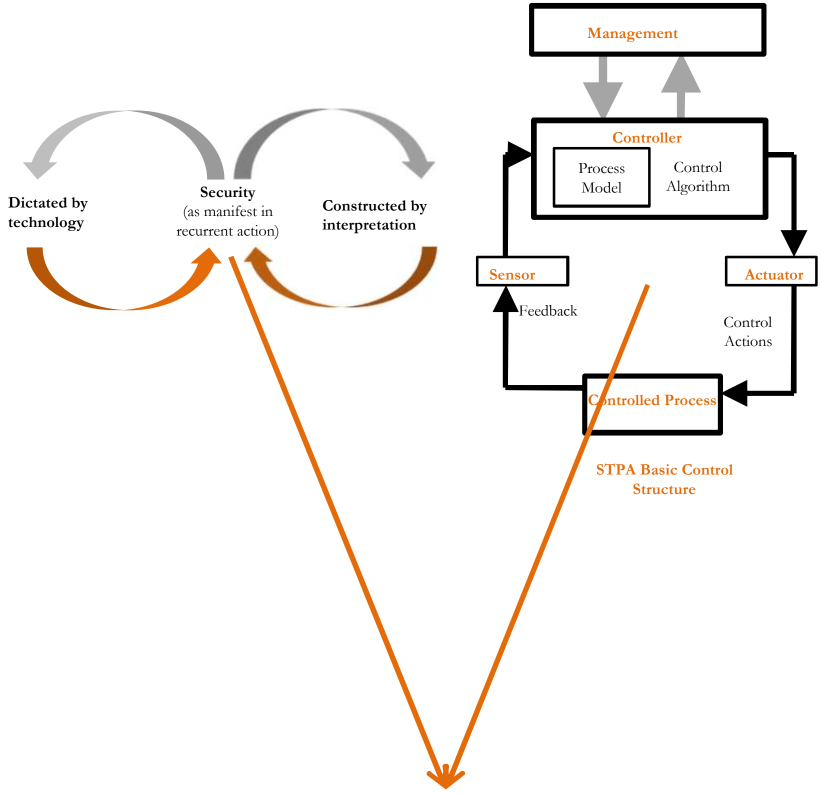
System Theoretic Accident Model & Process (STAMP)

SUMMARY

•Facilities that hold nuclear materials are '**complex, socio-technical systems**'

•Security is an '**emergent property**' of complex systems

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



STPA Basic Control Structure

Emergent property of '**system security**' for **nuclear facilities**

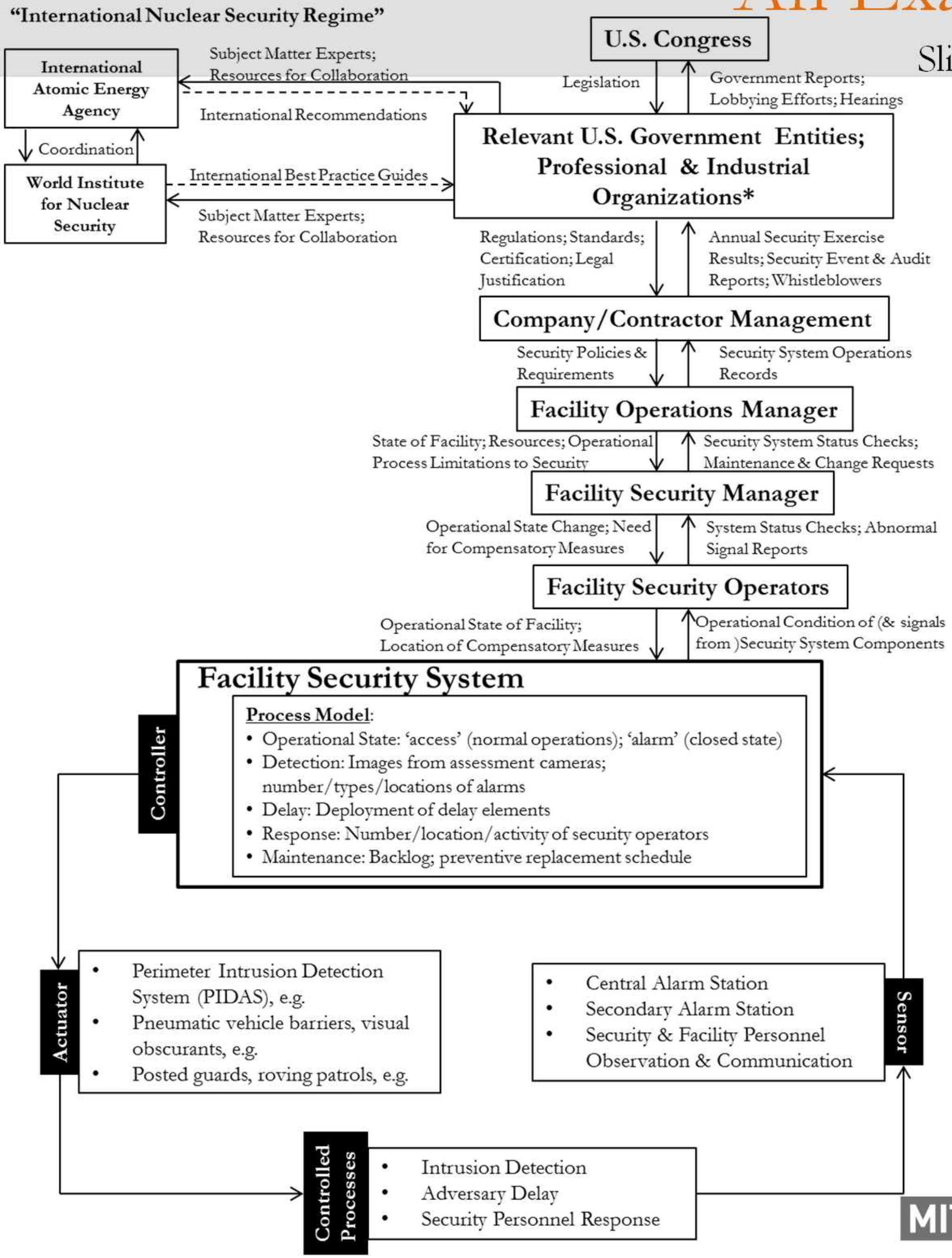
STPA-SEC WITH EXTENSION: AN EXAMPLE

A Generic U.S. Nuclear Power Plant

Courtesy: Wikipedia

An Example

Hierarchical Control Structure



"International Nuclear Security Regime"

International Atomic Energy Agency

World Institute for Nuclear Security

Coordination

Subject Matter Experts; Resources for Collaboration

International Recommendations

International Best Practice Guides

Subject Matter Experts; Resources for Collaboration

U.S. Congress

Legislation

Government Reports; Lobbying Efforts; Hearings

Relevant U.S. Government Entities; Professional & Industrial Organizations*

Regulations; Standards; Certification; Legal Justification

Annual Security Exercise Results; Security Event & Audit Reports; Whistleblowers

Company/Contractor Management

Security Policies & Requirements

Security System Operations Records

Facility Operations Manager

State of Facility; Resources; Operational Process Limitations to Security

Security System Status Checks; Maintenance & Change Requests

Facility Security Manager

Operational State Change; Need for Compensatory Measures

System Status Checks; Abnormal Signal Reports

Facility Security Operators

Operational State of Facility; Location of Compensatory Measures

Operational Condition of (& signals from)Security System Components

Facility Security System

Controller

Process Model:

- Operational State: 'access' (normal operations); 'alarm' (closed state)
- Detection: Images from assessment cameras; number/types/locations of alarms
- Delay: Deployment of delay elements
- Response: Number/location/activity of security operators
- Maintenance: Backlog; preventive replacement schedule

Actuator

- Perimeter Intrusion Detection System (PIDAS), e.g.
- Pneumatic vehicle barriers, visual obscurants, e.g.
- Posted guards, roving patrols, e.g.

Sensor

- Central Alarm Station
- Secondary Alarm Station
- Security & Facility Personnel Observation & Communication

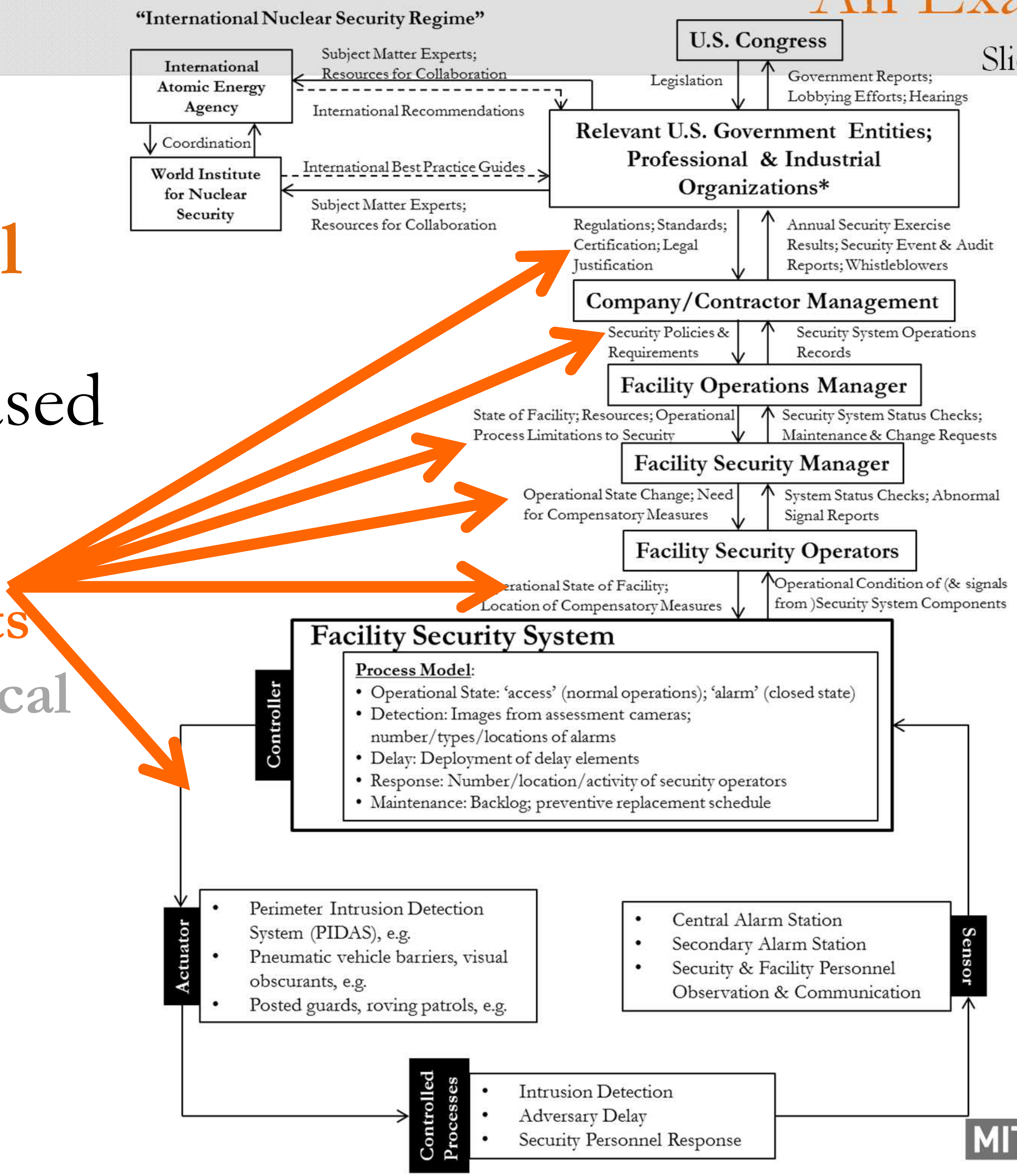
Controlled Processes

- Intrusion Detection
- Adversary Delay
- Security Personnel Response

An Example

Hierarchical Control Structure based on:

- Security constraints
- Hierarchical levels of control
- Process models



"International Nuclear Security Regime"

International Atomic Energy Agency

Subject Matter Experts; Resources for Collaboration

International Recommendations

Coordination

World Institute for Nuclear Security

International Best Practice Guides

Subject Matter Experts; Resources for Collaboration

U.S. Congress

Legislation

Government Reports; Lobbying Efforts; Hearings

Relevant U.S. Government Entities; Professional & Industrial Organizations*

Regulations; Standards; Certification; Legal Justification

Annual Security Exercise Results; Security Event & Audit Reports; Whistleblowers

Company/Contractor Management

Security Policies & Requirements

Security System Operations Records

Facility Operations Manager

State of Facility; Resources; Operational Process Limitations to Security

Security System Status Checks; Maintenance & Change Requests

Facility Security Manager

Operational State Change; Need for Compensatory Measures

System Status Checks; Abnormal Signal Reports

Facility Security Operators

...erational State of Facility; Location of Compensatory Measures

Operational Condition of (& signals from)Security System Components

Facility Security System

Controller

Process Model:

- Operational State: 'access' (normal operations); 'alarm' (closed state)
- Detection: Images from assessment cameras; number/types/locations of alarms
- Delay: Deployment of delay elements
- Response: Number/location/activity of security operators
- Maintenance: Backlog; preventive replacement schedule

Actuator

- Perimeter Intrusion Detection System (PIDAS), e.g.
- Pneumatic vehicle barriers, visual obscurants, e.g.
- Posted guards, roving patrols, e.g.

Sensor

- Central Alarm Station
- Secondary Alarm Station
- Security & Facility Personnel Observation & Communication

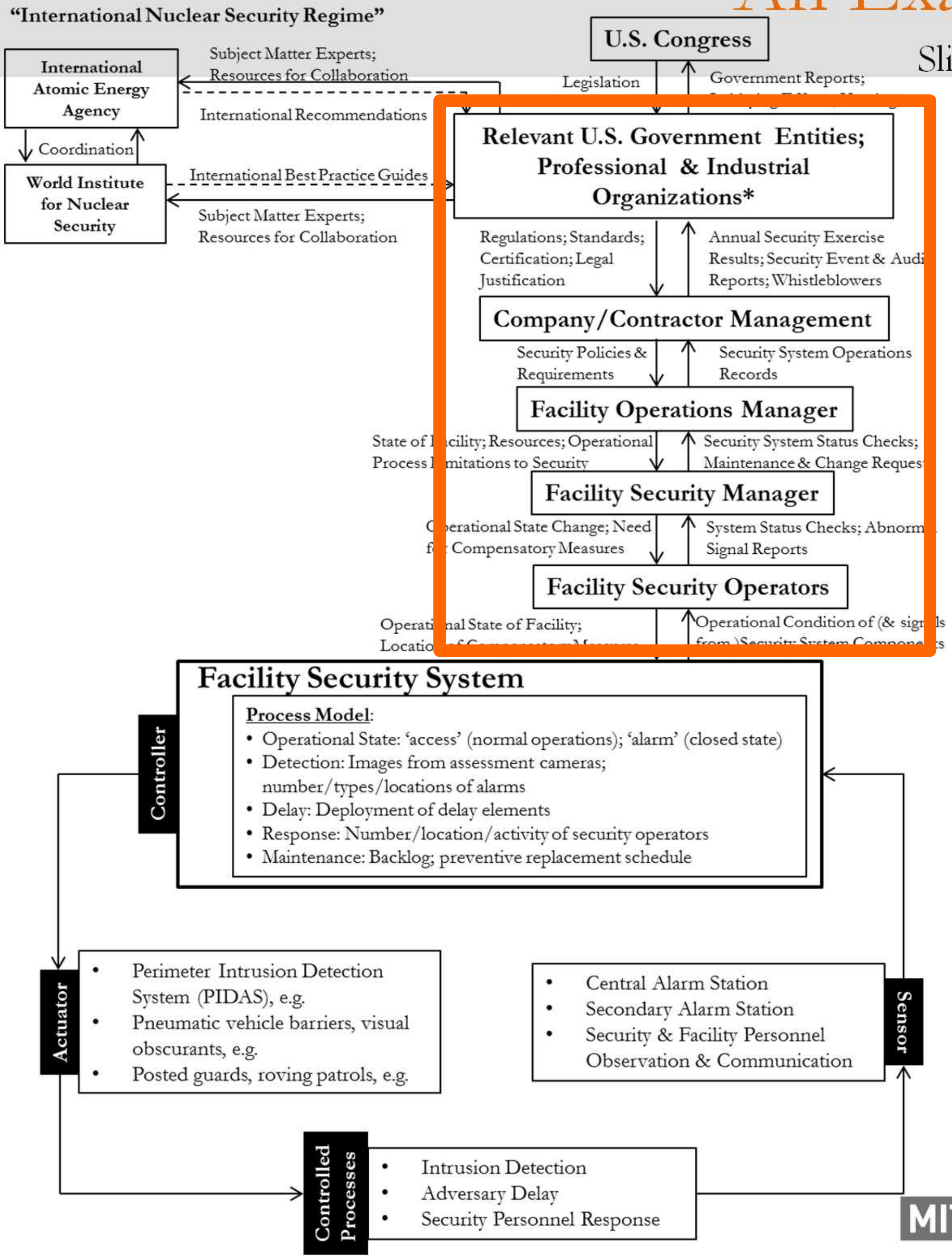
Controlled Processes

- Intrusion Detection
- Adversary Delay
- Security Personnel Response

An Example

Hierarchical Control Structure based on:

- – Security constraints
- – **Hierarchical levels of control**
- – Process models


"International Nuclear Security Regime"
International Atomic Energy Agency
Subject Matter Experts; Resources for Collaboration
International Recommendations
Coordination
World Institute for Nuclear Security
International Best Practice Guides
Subject Matter Experts; Resources for Collaboration
U.S. Congress
Legislation
Government Reports;
Relevant U.S. Government Entities; Professional & Industrial Organizations*
Regulations; Standards; Certification; Legal Justification
Annual Security Exercise Results; Security Event & Audi
Reports; Whistleblowers
Company/Contractor Management
Security Policies & Requirements
Security System Operations Records
Facility Operations Manager
State of I cility; Resources; Operational Process I mitations to Security
Security System Status Checks; Maintenance & Change Reques
Facility Security Manager
C erational State Change; Need f Compensatory Measures
System Status Checks; Abnorm
Signal Reports
Facility Security Operators
Operati nal State of Facility;
Locatio
Operational Condition of (& sig ls
from)Security System Compone s
Facility Security System
Controller
Process Model:
• Operational State: 'access' (normal operations); 'alarm' (closed state)
• Detection: Images from assessment cameras; number/types/locations of alarms
• Delay: Deployment of delay elements
• Response: Number/location/activity of security operators
• Maintenance: Backlog; preventive replacement schedule
Actuator
• Perimeter Intrusion Detection System (PIDAS), e.g.
• Pneumatic vehicle barriers, visual obscurants, e.g.
• Posted guards, roving patrols, e.g.
Sensor
• Central Alarm Station
• Secondary Alarm Station
• Security & Facility Personnel Observation & Communication
Controlled Processes
• Intrusion Detection
• Adversary Delay
• Security Personnel Response

Copyright: A. Williams

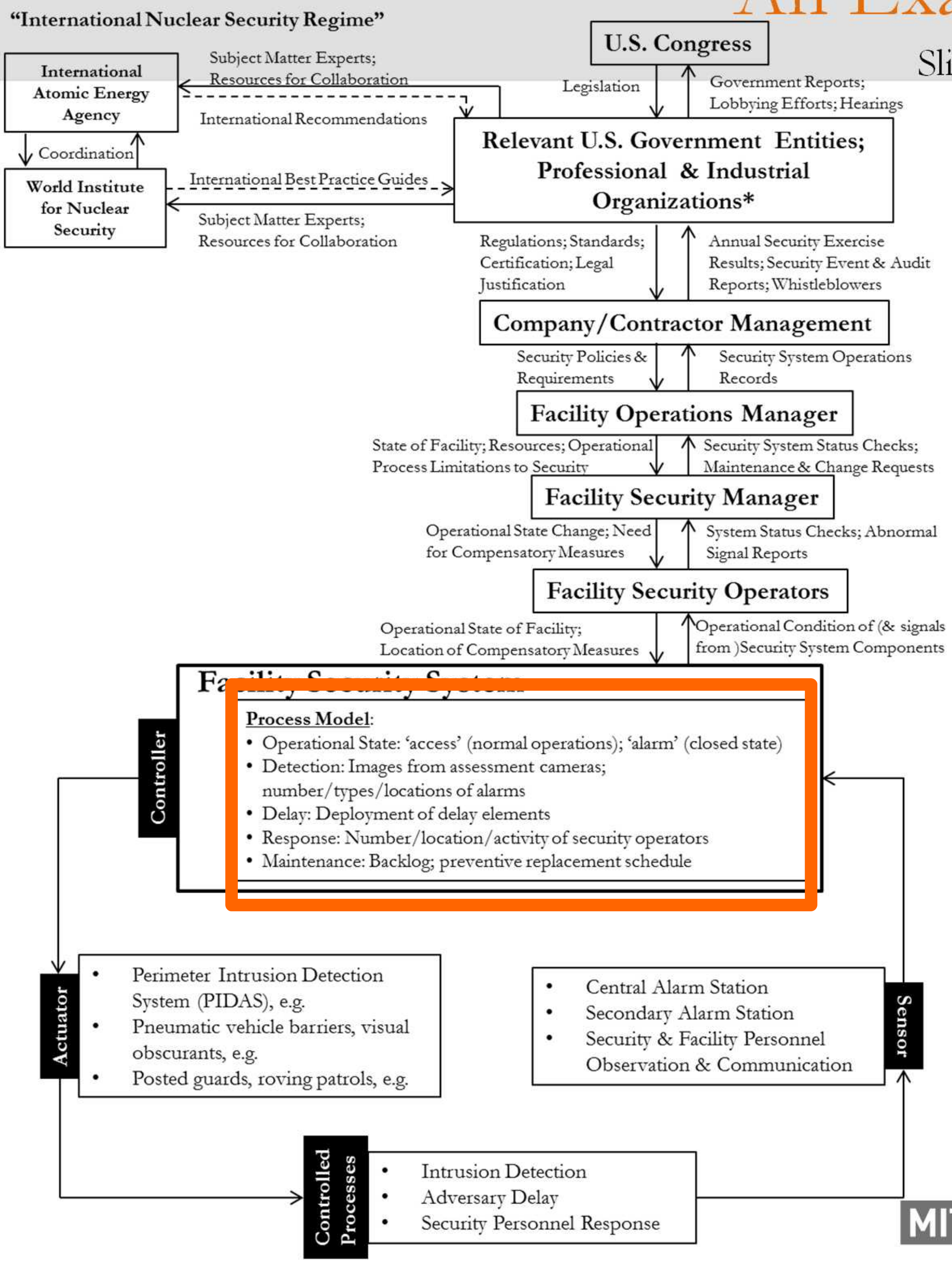
NUCLEAR SECURITY

An Example

Slide 23 of 36

Hierarchical Control Structure based on:

- – Security constraints
- – Hierarchical levels of control
- – **Process models**



"International Nuclear Security Regime"

International Atomic Energy Agency

Subject Matter Experts; Resources for Collaboration

International Recommendations

Coordination

World Institute for Nuclear Security

International Best Practice Guides

Subject Matter Experts; Resources for Collaboration

U.S. Congress

Legislation

Government Reports; Lobbying Efforts; Hearings

Relevant U.S. Government Entities; Professional & Industrial Organizations*

Regulations; Standards; Certification; Legal Justification

Annual Security Exercise Results; Security Event & Audit Reports; Whistleblowers

Company/Contractor Management

Security Policies & Requirements

Security System Operations Records

Facility Operations Manager

State of Facility; Resources; Operational Process Limitations to Security

Security System Status Checks; Maintenance & Change Requests

Facility Security Manager

Operational State Change; Need for Compensatory Measures

System Status Checks; Abnormal Signal Reports

Facility Security Operators

Operational State of Facility; Location of Compensatory Measures

Operational Condition of (& signals from)Security System Components

Facility Security System

Controller

Process Model:

- Operational State: 'access' (normal operations); 'alarm' (closed state)
- Detection: Images from assessment cameras; number/types/locations of alarms
- Delay: Deployment of delay elements
- Response: Number/location/activity of security operators
- Maintenance: Backlog; preventive replacement schedule

Actuator

- Perimeter Intrusion Detection System (PIDAS), e.g.
- Pneumatic vehicle barriers, visual obscurants, e.g.
- Posted guards, roving patrols, e.g.

Sensor

- Central Alarm Station
- Secondary Alarm Station
- Security & Facility Personnel Observation & Communication

Controlled Processes

- Intrusion Detection
- Adversary Delay
- Security Personnel Response

An Example

Identify Facility Mission

– Nuclear power plant = generate electricity/revenue

Identify Unacceptable Losses

– L1: Human serious injury or loss of life (sabotage)

– L2: Significant damage to the plant (sabotage) infrastructure/surrounding area

– L3: Theft of nuclear material

– L4: Significant loss of revenue

Identify Vulnerable States & Determine High Level Security Control Actions

Vulnerable States	Related Losses	Security Requirement (System Constraint)
(V1) Malevolent access to special nuclear material, their containment structures or their control systems by an adversary group	L1, L2, L3, L4	Malevolent individuals or groups must not access special nuclear material, their containment structures or their control systems by an adversary group
(V2) Unauthorized access special nuclear material, their containment structures or their control systems	L1, L2, L3, L4	Unauthorized individuals must not access special nuclear material, their containment structures or their control systems
(V3) Uncoordinated implementation of security procedures	L1, L2, L3	All security procedures must be coordinated between operational and security personnel
(V4) Unverified nuclear material within the facility	L3, L4	All nuclear materials within a facility must be known and

From High Level to More Specific Security Control Actions

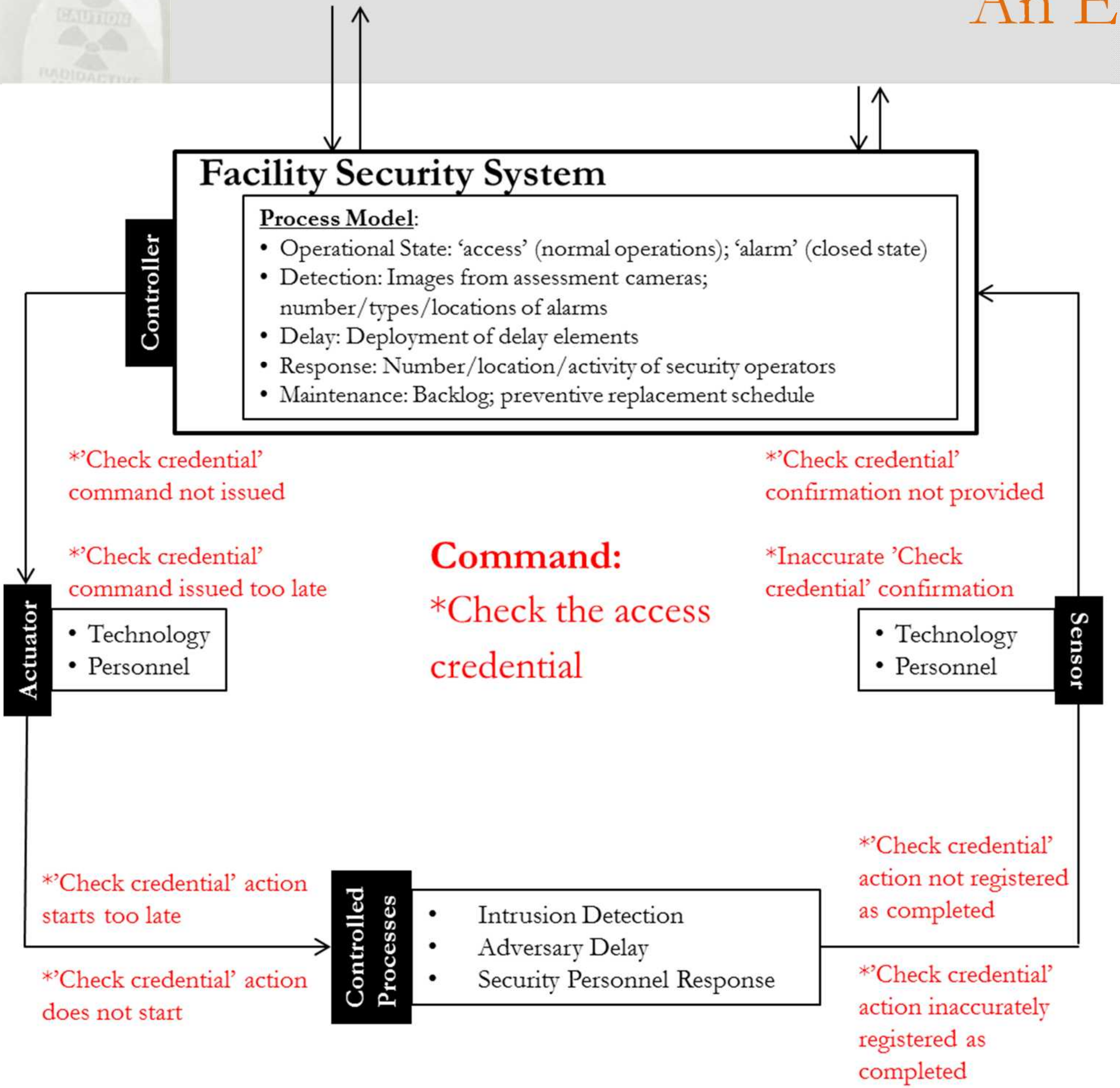
Vulnerable States	Related Losses	Security Requirement (System Constraint)	Example Security Control Actions
(V1) Malevolent access to special nuclear material, their containment structures or their control systems by an adversary group	L1, L2, L3, L4	Malevolent individuals or groups must not access special nuclear material, their containment structures or their control systems by an adversary group	Post response force members strategically to protect special nuclear material, their containment structures or their control systems by an adversary group
(V2) Unauthorized access special nuclear material, their containment structures or their control systems	L1, L2, L3, L4	Unauthorized individuals must not access special nuclear material, their containment structures or their control systems	Check the access credential of any individual trying to access special nuclear material, their containment structures or their control systems
(V3) Uncoordinated implementation of security procedures	L1, L2, L3	All security procedures must be coordinated between operational and security personnel	Security personnel clearly communicate any new procedure to operational personnel
(V4) Unverified nuclear material within the facility	L3, L4	All nuclear materials within a facility must be known and	Count the irradiated (used) fuel rods in dry cask storage for

From Security Control Actions to STPA

Step 1 (identify insecure control actions)

Example Security Control Actions	Command Needed & Not Provided	Command Not Needed & Provided	Command Given Too Early/Late or in Wrong Order	Command Stopped Too Soon/Engaged Too Long
Check the access credential of any individual trying to access special nuclear material, their containment structures or their control systems	*Unauthorized individual accesses nuclear material areas, systems or controls [V1, V2, V3]	*Already credentialed person is re-checked (e.g., different agency or badge) [V1, V2, V3]	*Check credential after individual near nuclear material areas, systems or controls (e.g., too late/wrong order) [V1, V2, V3]	Check the access credential of any individual trying to access special nuclear material, their containment structures or their control systems

An Example



Facility Security System

Controller

Process Model:

- Operational State: 'access' (normal operations); 'alarm' (closed state)
- Detection: Images from assessment cameras; number/types/locations of alarms
- Delay: Deployment of delay elements
- Response: Number/location/activity of security operators
- Maintenance: Backlog; preventive replacement schedule

*'Check credential' command not issued

*'Check credential' command issued too late

Actuator

- Technology
- Personnel

Command:

*Check the access credential

*'Check credential' confirmation not provided

*Inaccurate 'Check credential' confirmation

Sensor

- Technology
- Personnel

*'Check credential' action starts too late

*'Check credential' action does not start

Controlled Processes

- Intrusion Detection
- Adversary Delay
- Security Personnel Response

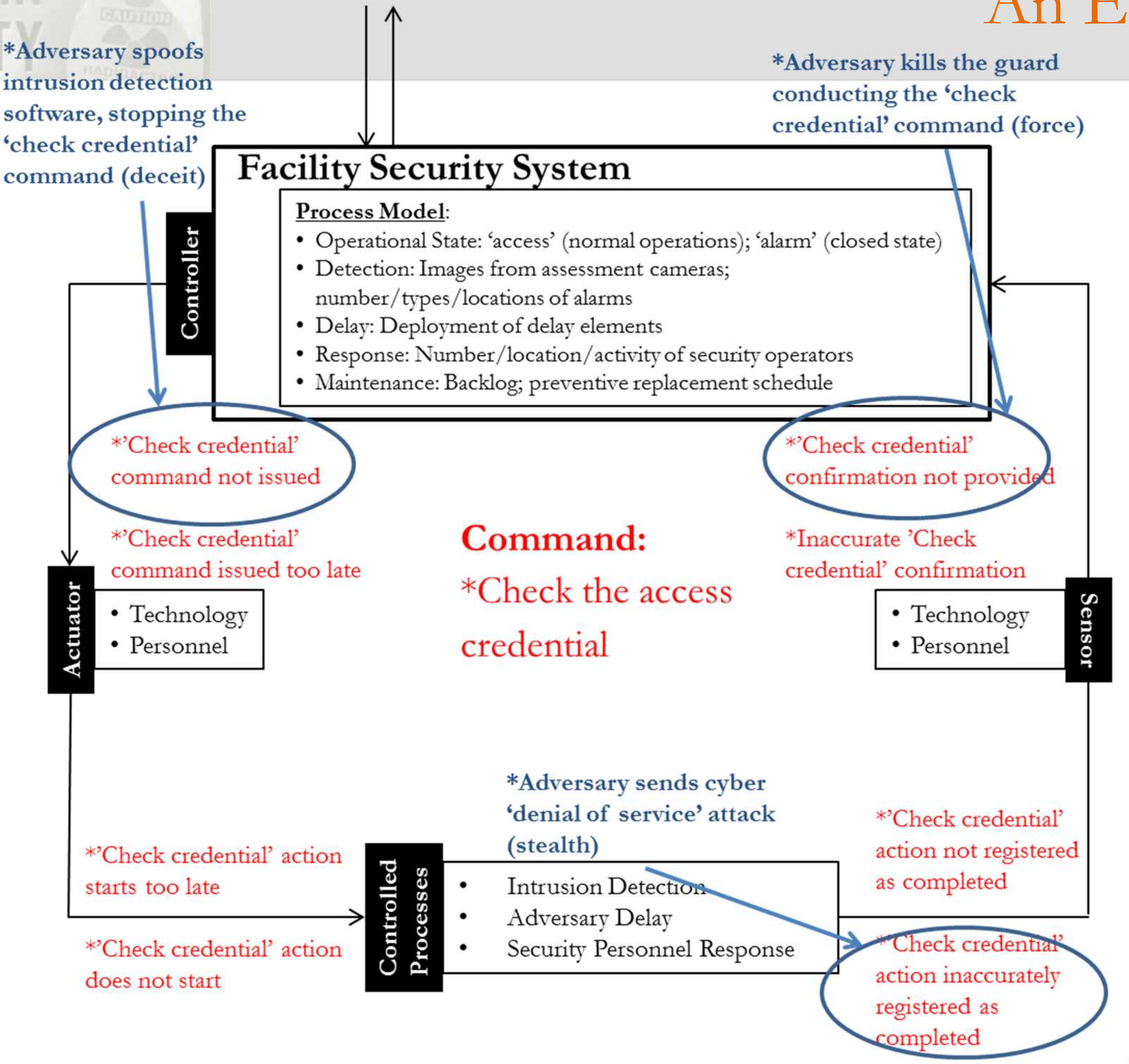
*'Check credential' action not registered as completed

*'Check credential' action inaccurately registered as completed

From Security Control Action Violations to STPA Step 2 (identify adversary actions)

Security Control Action Violations	Stealth	Deceit	Force
*Response force members do not arrive to strategic post [V1, V2, V3]	*Response force members do not arrive to strategic post [V1, V2, V3]	*Response force members do not arrive to strategic post [V1, V2, V3]	*Response force members do not arrive to strategic post [V1, V2, V3]
*Response force members do not arrive to strategic post [V1, V2, V3]	*Response force members do not arrive to strategic post [V1, V2, V3]	*Response force members do not arrive to strategic post [V1, V2, V3]	*Response force members do not arrive to strategic post [V1, V2, V3]
*Unauthorized individual accesses nuclear material areas, systems or controls [V1, V2, V3]	*Cutting hole in a fence without triggering any related alarm to access the nuclear material areas, systems or controls	*Using a forged badge to access the nuclear material areas, systems or controls	*Using a vehicle to drive through/over barriers to the nuclear material areas, systems or controls

An Example



*Adversary spoofs intrusion detection software, stopping the 'check credential' command (deceit)

*Adversary kills the guard conducting the 'check credential' command (force)

Facility Security System

Process Model:

- Operational State: 'access' (normal operations); 'alarm' (closed state)
- Detection: Images from assessment cameras; number/types/locations of alarms
- Delay: Deployment of delay elements
- Response: Number/location/activity of security operators
- Maintenance: Backlog; preventive replacement schedule

*'Check credential' command not issued

*'Check credential' confirmation not provided

*'Check credential' command issued too late

*Inaccurate 'Check credential' confirmation

Command:

*Check the access credential

- Technology
- Personnel

- Technology
- Personnel

*Adversary sends cyber 'denial of service' attack (stealth)

*'Check credential' action starts too late

*'Check credential' action does not start

- Intrusion Detection
- Adversary Delay
- Security Personnel Response

*'Check credential' action not registered as completed

*'Check credential' action inaccurately registered as completed

An Example

Define Mission

Identify Losses

Identify Vulnerable States

Derive Security Requirements

Define Security Control Actions

Find Security Control Action Violations

Derive Adversary Actions

Where does the system dynamics model of organizational issues fit?

An Example

Define Mission

Identify Losses

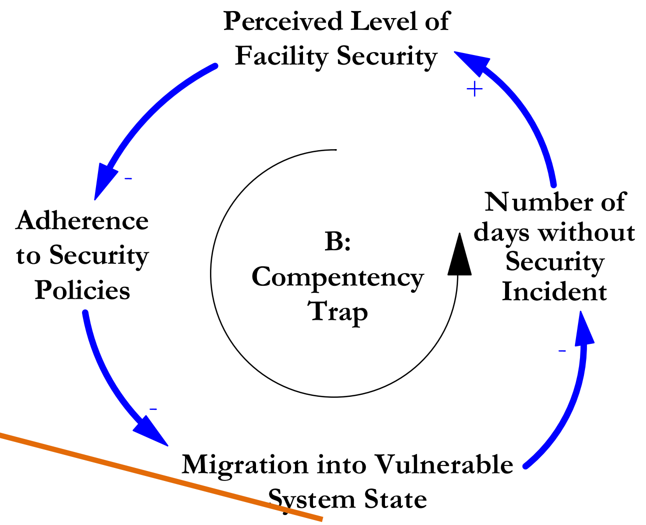
Identify Vulnerable States

Derive Security Requirements

Define Security Control Actions

Find Security Control Action Violations

Derive Adversary Actions


Perceived Level of Facility Security
+
-
Adherence to Security Policies
B: Compentency Trap
Number of days without Security Incident
-
-
Migration into Vulnerable System State

Competence trap; detection trap; funding issues; incentives issues; frequency of security policy changes

'Insider' actions; collusion/coercion; disaffected employee

Path Forward

- **Finish literature review**
  - Systems, control, organization theory
- **Case study to develop SD model**
  - Hypothetical case study culled from ‘real’ cases
- **Conduct interviews to calibrate SD model**
  - Expected interviews at one nuclear power/research/defense facility
- **Analytical comparison across 3 types of nuclear facilities**
  - Current ‘state-of-the-art’
  - STPA-Sec
  - STPA-Sec w/Extension

Path Forward

Theoretical Contributions

– Empirical support for **a paradigm shift** in unclear security from preventing failures to enforcing security constraints

– Development of an **SD model** for an **organization theory-based extension** of STPA-Sec

Methodological Contributions

– **Validation** of relevance **organization theory-based extension** of STPA-Sec

– **Process** incorporating the insights gained from the extension into STPA-Sec analysis of nuclear facilities

Practical Contributions

– Empirical support for new approach to nuclear security: interview data to supporting that STPA-Sec w/ Extension can identify **more robust, & adaptable vulnerabilities** than current state-of-the-art

Summary

Motivation

- Security breaches (Y-12, Pelindaba)
- NRC FoF exercise results

Current Approaches

- Founded on probability & reliability theory (e.g., DEPO)
- 'Bottom-up' consideration of security as meeting regulated effectiveness

A New Approach

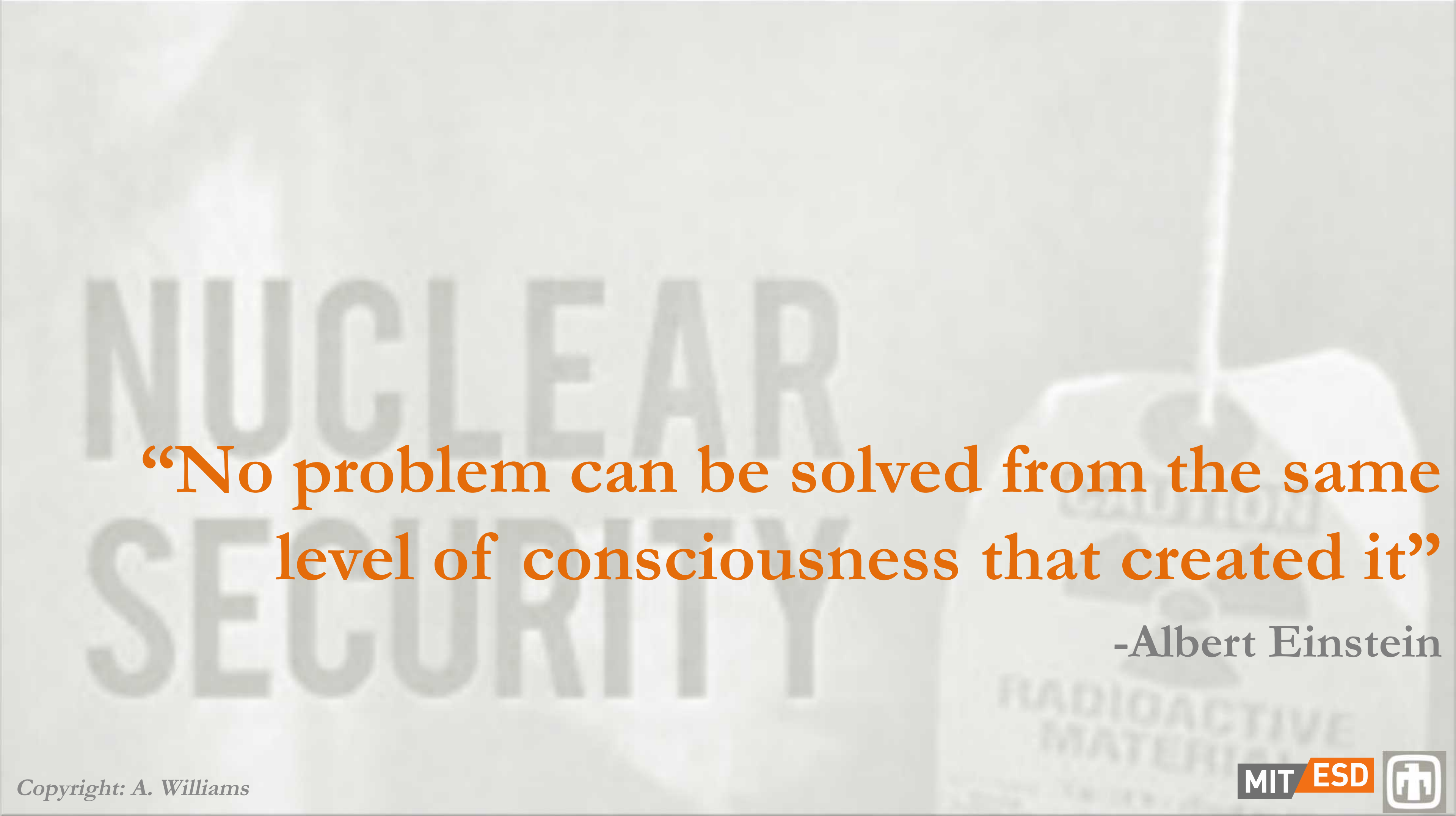
- Founded on systems, control (and organization) theory
- 'Top-down' consideration of security as an 'emergent property'

An Example

Path Forward

- PhD research plan
- Post-graduate research (?)

Questions???



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

-Albert Einstein