http://www.youtube.com/v/jkbABvNUNw0

videoFileNo113342AM.wmv

http://www.foxnews.com/tech/2012/06/25/drones-vulnerable-to-terrorist-hijacking-researchers-say/

The Next Step: A Fully Integrated Global Multi-Modal Security and Safety Management System

International

System Safety Conference 2012

by Robert Fletcher

Global, Integrated, Multi-modal

- Global: applicable throughout the world
- Integrated: all safety hazards and security threats combined
- Multi-modal:
  - all operations (air, sea, land (road & rail))
  - all safety critical industries (nuclear, medical, oil and gas, petrochemical, space, aerospace and aviation, etc.)

Progress Simple Safety to the Complex

- Safety initially the focus of OSH specialists
- **Technical, human, and organizational** factors considered as complexity increased
- System Safety Hazards and Security Threats
- Reactive, Proactive, and Predictive Methods
- Next Step: With Increasing System Complexity, Control Theory Approach Developed
- Beyond: Critical Infrastructure Protection (CIP) approach with combined security & safety

Analysis Approaches

- Heinrich - Hierarchical View of Workplace
- Reason - Cause and Effect chain of events - reactive
- ICAO - Cause and Effect chain of events - proactive
- Leveson - Control Theory
- Critical Infrastructure Institute (CII) – National & Global Critical Infrastructure Protection Analysis
- Example 1:SCADA remote control systems
- Example 2: NASA - Communications System Combined Security and Safety Analysis

A System Perspective

- A system is a collection of interrelated components that work together to achieve some objective. … Dr. Ian Sommerville, UK
- Complexity Science: the Plexus Institute

Complexity Science

- Traditional view
  - World is made up of machine-like entities that can be understood by taking them apart and examining the components
- Modern View from Complexity Science
  - Majority of the world is made up of non-linear, complex adaptive systems that are constantly changing and interacting with each other
- Emergence
  - occurs where the “system” is a collection of individual agents free to act in ways that are not predictable, and where the actions of one agent changes the context for other agents

Greater Complexity in Systems

- Complexity of current “Systems” is no longer *intellectually manageable* *Dr. N. Leveson*
- More complex mental models required
- “Systems Thinking” needs to be expanded
- Threat and Hazard Identification and Risk Assessments (THIRAs) are required

Safety and Security are Emergent Properties

- Since the 9/11 safety & security are seen as closely related

- Safety and Security must be considered in “design and operation” of complex systems

Complex Systems

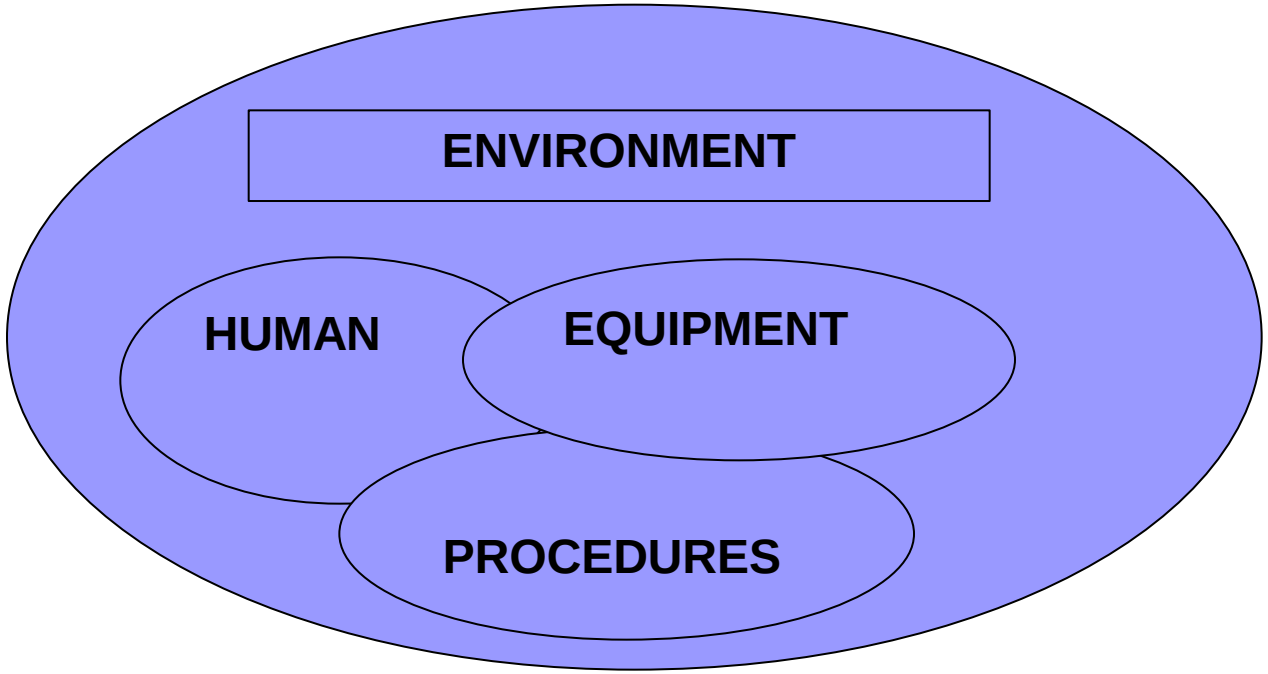
- Are more than simply the sum of the parts
- Include properties that are properties of the whole
- Their properties cannot be attributed to any specific part
- Have emergent properties

Systems with Complex Relationships

- *Mental models* show how "systems thinking" has expanded to enable hazard and threat analyses of increasingly more complex systems

- *Threat and Hazard analysis* has required new and more effective techniques to predict how systems may fail as technology has become more complex

The Basic System Elements



Early Safety Thinking in USA

- Fire in New York city in 1911 in a clothing factory
- Doors were blocked, everyone died
- Formation of the American Society of Safety Engineers (ASSE)

From Individual Safety to Employer & Workplace Safety

- Prior to 1911, the law did not protect the worker
- If a worker willingly accepted a job that was inherently hazardous then the employer shared “no responsibility” for death or injury on the job
- No “system” perspective or responsibility

1931 Heinrich Pyramid - A Mental Model of sorts

- Ratio of every one death to number of injuries and near misses
- Ratio is not effective to predict catastrophes
- Why? - Counting deaths and injuries as an outcome without consideration of what is happening functionally in the total “system” will miss critical “control” information

Heinrich's Pyramid
The Start of "system thinking"

- Practiced by Occupational Safety, Health and Environmental specialists for past 100 years

What is wrong with Heinrich's Pyramid?

- does not involve "systems thinking"
- is reactive, not proactive or predictive
- does not identify deep systemic problems
- captures unsatisfactory workplace conditions not "system" functional problems
- does not identify mitigation for complex systems

Technology Advances

- 1914-18 WW I and 1939–45 WW II
- 1950's, aviation, nuclear power plants, oil and gas, other complex safety critical industries
- new analysis techniques were required to cope with increasING complexity

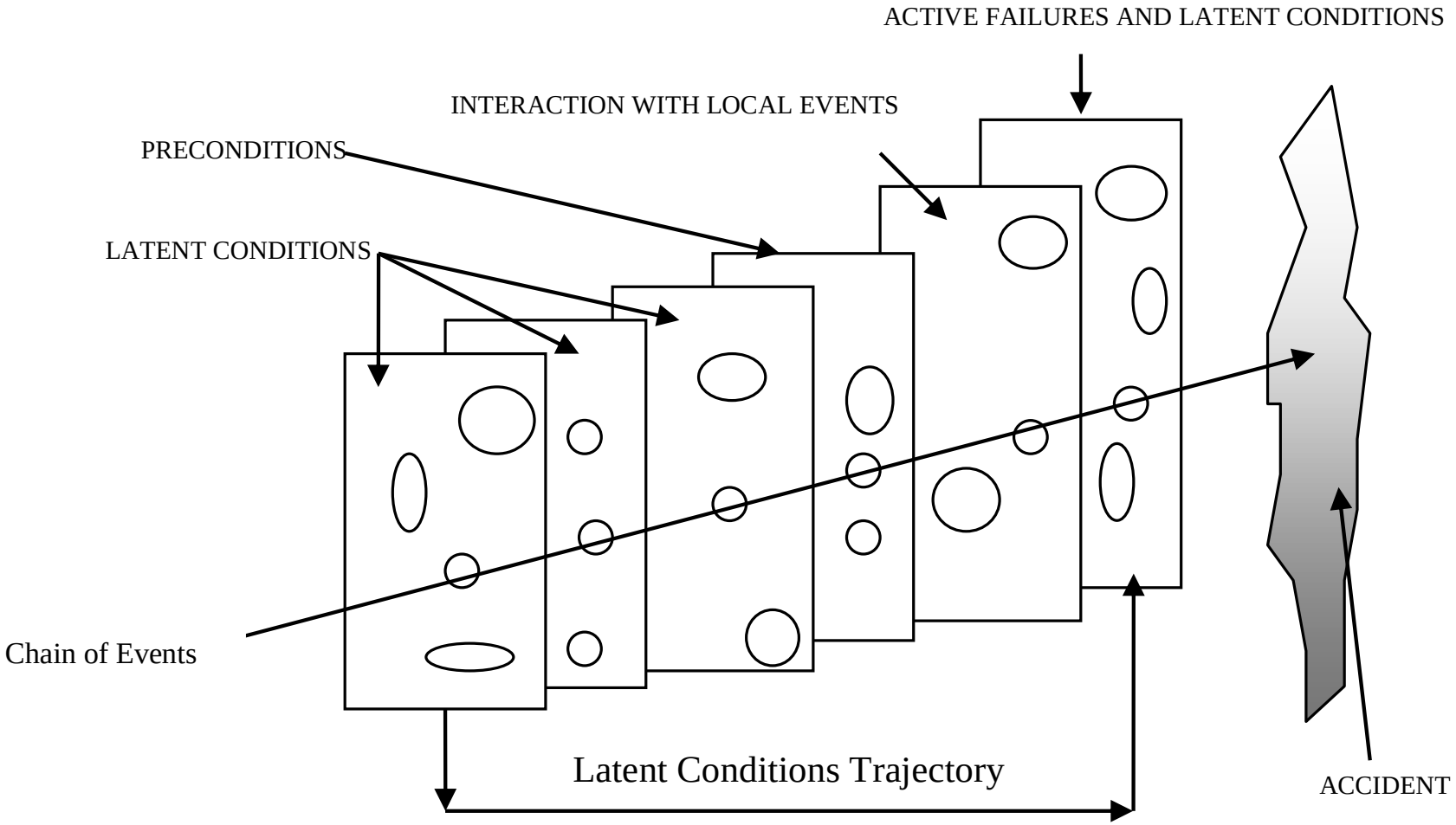
Mental Models – Cause & Effect: Heinrich (Dominos), Reason (Cheese)

- Heinrich's Domino Model in 1931
  - Captures idea that conditions in work places are caused by more than just the worker
  - a scientific approach to describe accident causation
- Dr. James Reason
  - suggested size and placement of holes are random and change over time
  - a linear sequential chain of events model
  - causal factors stem from operator to management

Dr. James Reason's Concept of Accident Causation

- Dr. James Reason's
  - includes all aspects of the hazards within the whole organization responsible for design and operation of a system
- Swiss Cheese model
  - reactive, proactive, and predictive.
  - more hazards are identified and mitigated prior to operating the system

THE ORGANIZATIONAL ACCIDENT



Management Decisions	Working Conditions	People: Errors & Violations	Operator Deficiencies: Training, Regulations, Technology

Model: ICAO Safety Management System

- Based on Reason's Swiss Cheese linear Cause and Effect chain of events thinking
- Considers Whole Organization
- Proactive
- Predictive

System Failures Are Minimized By

- Mandatory and Voluntary reporting
- Safety audits and safety surveys
- Proactive and Predictive thinking
  - safety management is best accomplished by trying to find trouble in advance
  - data captured aggressively - seeks safety information that may be indicative of emerging safety risks from a variety of sources

Example: Target Stores Predictive Analytics

- Target captures types of purchases to determine if a women is pregnant
- pregnancy precedes a whole series of purchases
- Target proactively sends coupons to people to encourage purchases (e.g. father's daughter)
- mature SMSs should have predictive data capture systems

Reactive Identification & Mitigation Inadequate

- Old Way Was Reactive to Unreliable Equipment Failures
- Next Technical Factors during 1950s and 60s saw a dramatic improvement in the quality and reliability of equipment
- Next Human Factors during 1970s and 1980s
  - twenty years of ergonomics, fatigue, psychological factors

Reactive Mitigation Inadequate

- Next Organizational Factors during 1980s and 1990s
- European 4 Part Safety Case Arguments
- Year 2000 and Beyond Focussing on an Integrated “System”
  - Equipment, Human (Complete Organization) and Procedures
  - In Context of ensuring Safety and Security of Operations

Into the 2000s

- Old ways of hazard analysis not adequate
- Based on Cause and Effect Chains
- Can not capture Complexity of a Complete System

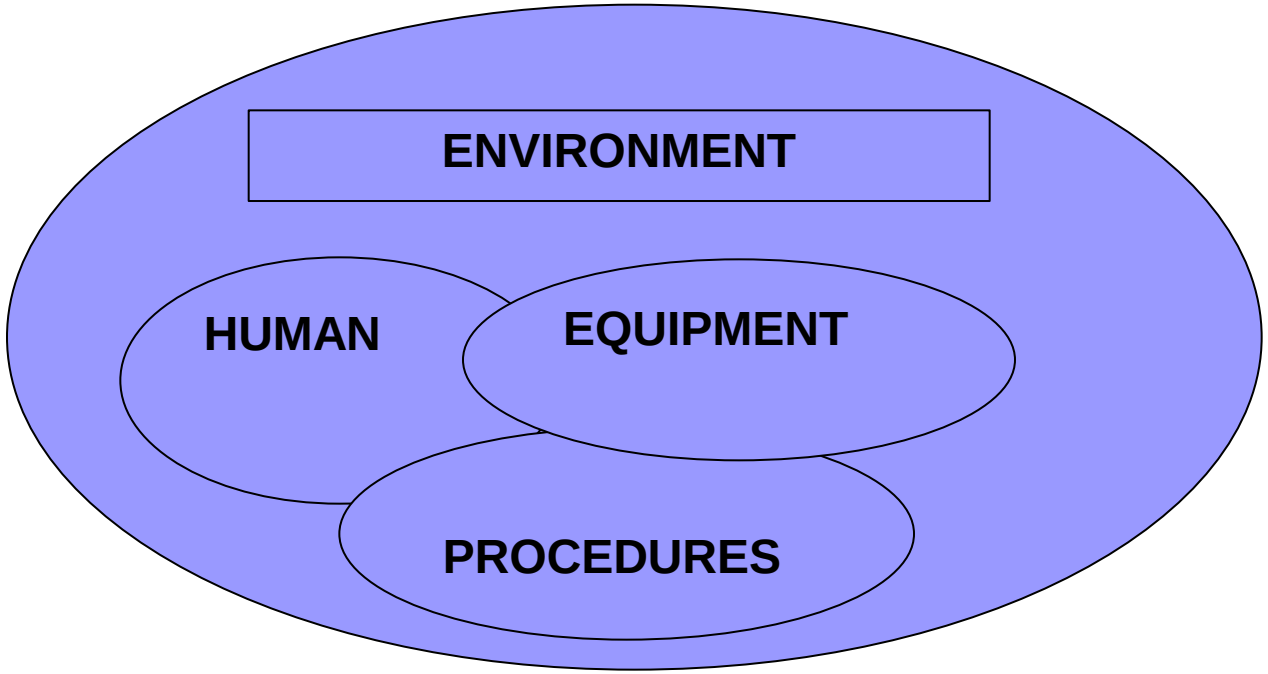
Accidents Continue to Happen

- Space Shuttle: Challenger, Columbia,
- Nuclear Industry: Chernobyl, Three Mile Island, Fukushima
- Aircraft accidents
- Many Hospital Preventable deaths
- Train crashes
- Vehicle accidents: largest killer on the planet
- Mining deaths: multiple

Security Threats Increasing

- Security threats are part of the system complexity
- Proactive thinking identifies risk in the near future
- Predictive thinking identifies risk in the distant future

A System's Basic Elements



What if the System is Analyzed Holistically

- Not by decomposing into cause and effect, chain of events sequences
- See Safety and Security as Emergent Properties of the system to be maintained or controlled
- Consider system from a Control Theory perspective
- Analogies: thermometer, auto-pilot, terrain following radar

The Next Step
System Safety Analysis

- Control Theory concepts used to analyze how, when, where, and why safety is compromised
- Safety hazards and Security threats are merged
- Threats - result of malicious behaviour
- Hazards - result from system losses in environment of well-intentioned behaviour

STAMP/STPA Based on Control Theory (1)

- Dr. Nancy Leveson, MIT
- Book “Engineering a Safer World”, 2011
- Safety as an Emergent Property of a System
- Beyond cause and effect chain of event sequences
- 3 day workshop at MIT, 17-19 Apr.12
- 250 people,19 countries

Dr. Nancy Leveson Challenges Old Assumptions

Old Assumptions	New Assumptions
1. Safety is increased by increasing system or component reliability. If components or systems do not fail, then accidents will not occur	1. High reliability is neither necessary nor sufficient for safety
2. Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chain of events leading to the loss	2. Accidents are complex processes involving the entire socio-technical system. Traditional event-chain models cannot describe this process adequately
3. Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information	3. Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis
4. Most accidents are caused by operator error. Rewarding safe behaviour and punishing unsafe behaviour will eliminate or reduce accidents significantly	4. Operator behaviour is a product of the environment in which it occurs. To reduce operator "error" we must change the environment in which the operator works
5. Highly reliable software is safe	5. Highly reliable software is not necessarily safe. Increasing software reliability or reducing implementation errors will have little impact on safety
6. Major accidents occur from the chance simultaneous occurrence of random events	6. Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk
7. Assigning blame is necessary to learn from and prevent accidents or incidents	7. Blame is the enemy of safety. Focus should be on understanding how the system behaviour as a whole contributed to the loss and not on who or what to blame for it

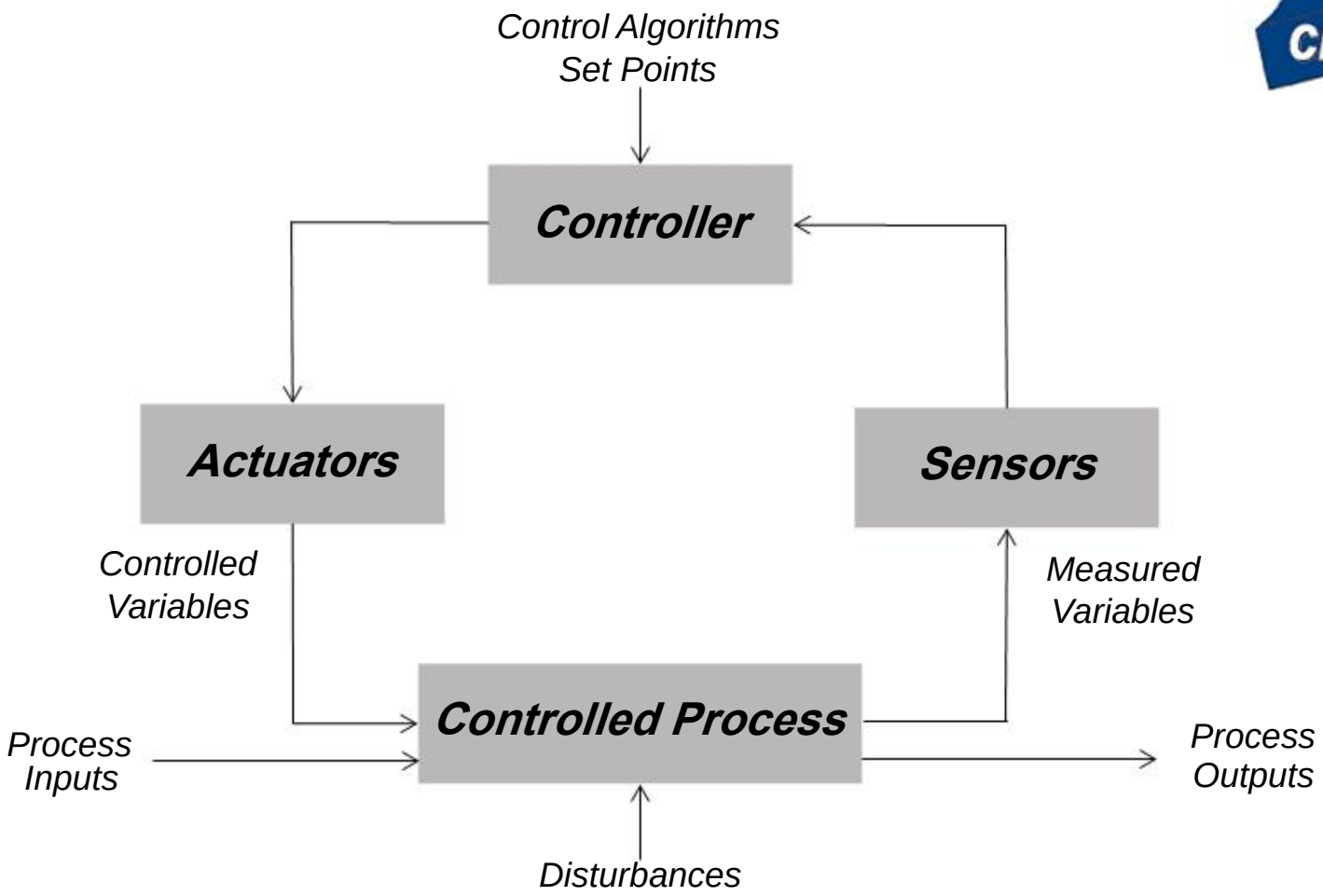
Control Theory with Feedback

- The concept of the feedback loop to control the dynamic behavior of the **system**: this is negative feedback, because the sensed value is subtracted from the desired value to create the error signal, which is amplified by a controller

- a "**system**" is a closed loop function, relating inputs, activation, control(s) and corrective feedback

- Example: Train doors at a subway platform

A Brief Overview of STAMP / STPA



A Standard System Control Loop With Feedback

Beyond the Next Step: Critical Infrastructure Protection

- Consider hazards and threats from a national perspective
- Assess all essential elements required to maintain safe and secure environment within a nation

USA, Homeland Security 18 Critical Sectors

1. Energy
2. Nuclear reactors
3. Dams
4. Banking and Finance
5. Agriculture and Food
6. Transportation systems
7. Government facilities
8. National Monuments and icons
9. Postal and shipping
10. Information technology
11. Communications
12. Health Care and Public Health
13. Water
14. Emergency Services
15. Critical Manufacturing
16. Commercial facilities
17. Defense industrial base
18. Chemical.

Canadian Government
10 Critical Sectors

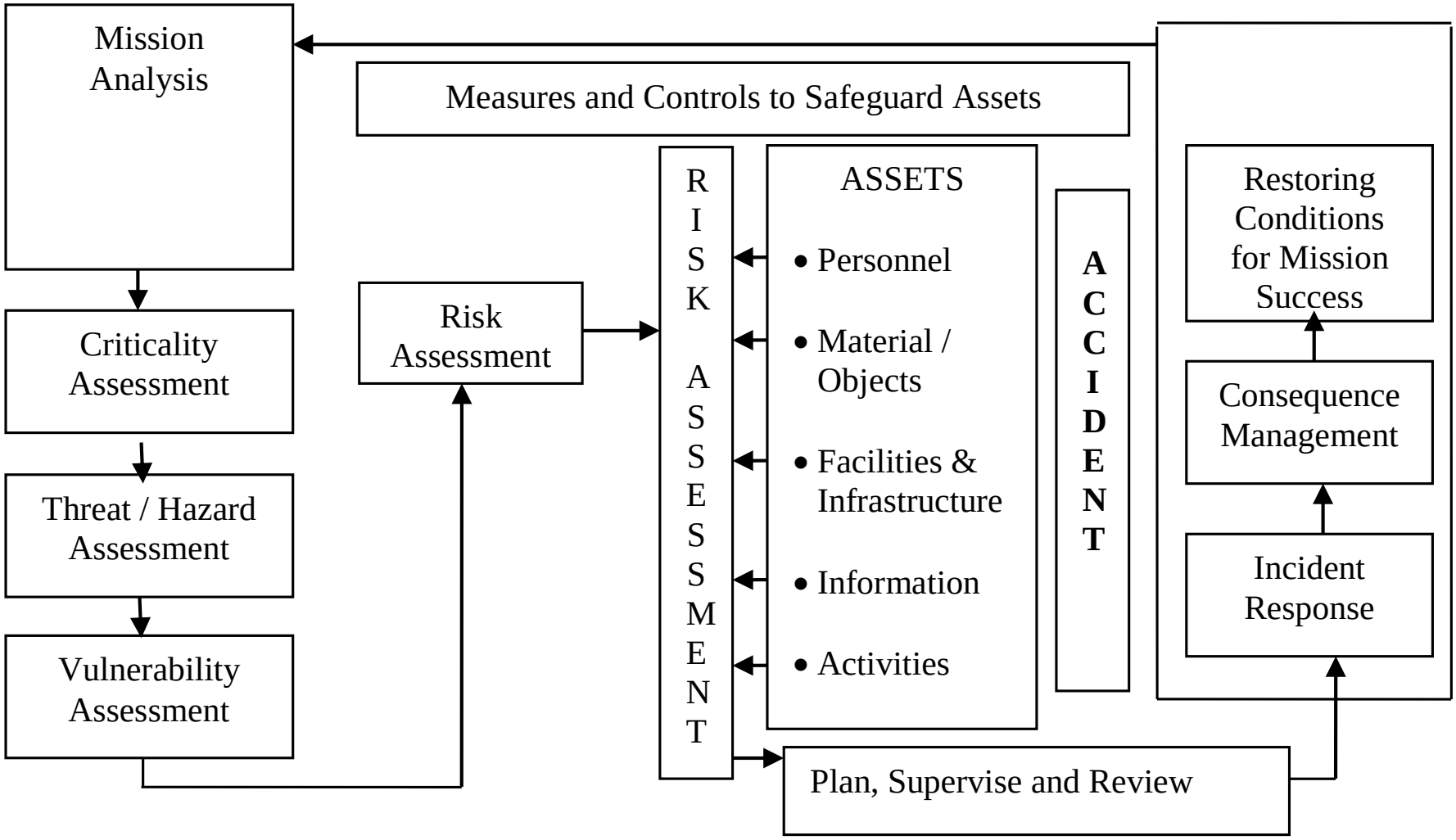
1. Energy and utilities
2. Finance
3. Food
4. Transportation
5. Government
6. Communications and information technology
7. Health care
8. Water
9. Safety
10. Manufacturing

Safety in Critical Infrastructure

- word "***safety***" pertains more to the general *protection of citizens* than from a system safety engineering perspective

- Critical Infrastructure is defined as:
  - infrastructure so vital that its incapacity or destruction would have a debilitating impact on national security, the economy, public health and safety of the general population of a nation

Critical Infrastructure Protection (CIP) Risk Management Model



Analysis Steps in CIP Risk Management Model

1. *Mission Analysis*
2. *Criticality Assessment*
3. *Hazard / Threat Assessment*
4. *Vulnerability Assessment*
5. *Risk Assessment*
6. *Risk Management*
7. *Plan, Supervise & Review*
8. *Incident Response*.
9. *Consequence Management*
10. *Restoring Conditions for Mission Success*

Critical Infrastructure Resilience

- Able to achieve core objectives in face of adversity

- Operational Resilience: ability of an organization to adapt to risk that affects its core operational capacities:
  - business processes
  - systems
  - technology
  - people

Operational Resilience

- Core process of Operational Resilience is **Business Continuity Planning** (BCP)

- BCP identifies what is critical to the operation and the associated tolerances in the event of a disaster

Example: The Drone Proofing Threat / Hazard

- Security Threat: navigation system may be compromised and drone flown into a building or another aircraft

- System Safety Hazard: that people in a building or another aircraft could be killed from an “out-of-control” drone

Example: Cyber security - SCADA (supervisory control and data acquisition) Systems

- "The increasing use of local area networks (LAN) and wide area networks (WAN) to link computer systems is raising the profile of security and access control" … Felix Redmill, UK

- Increased number of connections between SCADA systems, office networks and the internet has made SCADA systems more vulnerable to cyber attacks

SCADA Networks

- Used to control and monitor physical processes in multiple applications
  - transmission of electricity
  - transportation of gas and oil in pipeline
  - water distribution
  - traffic lights

SCADA Systems - Importance

- Losses would impact multiple areas of society
- Blackout of electrical SCADA system would cause financial losses to all customers

SCADA Systems - Security

- **STUXNET** steals design and control files
  - capable of changing control system and hiding changes
- **FLAME**
  - Update to Stuxnet and more potent

Example: NASA L-Band Digital Communications System

- System Safety Engineering (SSE) and Security Engineering (SecE) used in the analysis
  - from a safety perspective; threats that concern security are another potential cause of safety hazards
  - from a security perspective; hazards that concern safety are a potential outcome of security threats

System Safety and Security - Eleven Similarities (1)

Safety and Security are closely related:

1. BOTH deal with risk
2. BOTH involve negative requirements or constraints that may conflict with some important system goals
3. BOTH involve protection against losses
4. BOTH involve global system properties

… Dr. Nancy Leveson

System Safety and Security - Eleven Similarities (2)

5. With BOTH requirements are of supreme importance
6. BOTH require high levels of assurance
7. With BOTH testing alone is insufficient
8. BOTH qualities are regulated by government agencies and license bureaus

… Dr. Nancy Leveson

System Safety and Security - Eleven Similarities (3)

9. BOTH benefit from technologies that are too costly to be applied to the system as a whole, such as formal verification
10. BOTH involve problems that apply to them and not to other more general functional requirements
11. If an accident is defined to include unauthorized withholding of data then Security becomes a subset of Safety … Dr. Nancy Leveson

Conclusion

- Development safety analysis methods;
  - Pyramids, Dominos, and Swiss Cheese Models
  - Next Step: Control Theory approach
  - Next Step+: Critical Infrastructure Protection with Business Continuity Planning (BCP)
  - Examples: **1.** Drone Spoofing, **2.** SCADA Systems, **3.** NASA Communication System - Combined System Safety and Security analysis
- Integrated approach to Threats & Hazards Identification and Risk Assessments (THIRAs)