The Regulatory Use of System Safety Analysis: A Regulatory Effectiveness Analysis

Prof Dr Jur Vincent M. Brannigan
AJ Clark School of Engineering
University of Maryland at College Park
Firelaw@umd.edu

Abstract

Systems safety analysis largely evolved in well defined closed systems such as nuclear power plants, factory operations, integrated transport systems and military operations. In such systems regulation is based on explicit command and control by a management structure. However introduction of System Safety tools into open regulated environments introduces an entirely new set of problems.

Society regulates safety problems both “directly” through use of control systems of varying effectiveness and “indirectly” though the deterrent effect of penalties and liability exposure. Such regulation creates open networks with enhanced possibilities for failure, both anticipated and unanticipated. In some cases regulation even reduces safety by diffusing responsibility for the safety of the system. The “TITANIC” defense that designers complied with all government regulations is routinely invoked to divert attention from the engineering design process.

Regulatory Effectiveness Analysis and Regulatory Root Cause Analysis are tools that can be used to highlight the specific problems likely to be encountered in introducing System Safety analysis into the regulatory process.

System Safety Analysis

System safety analysis largely developed within "organizations"

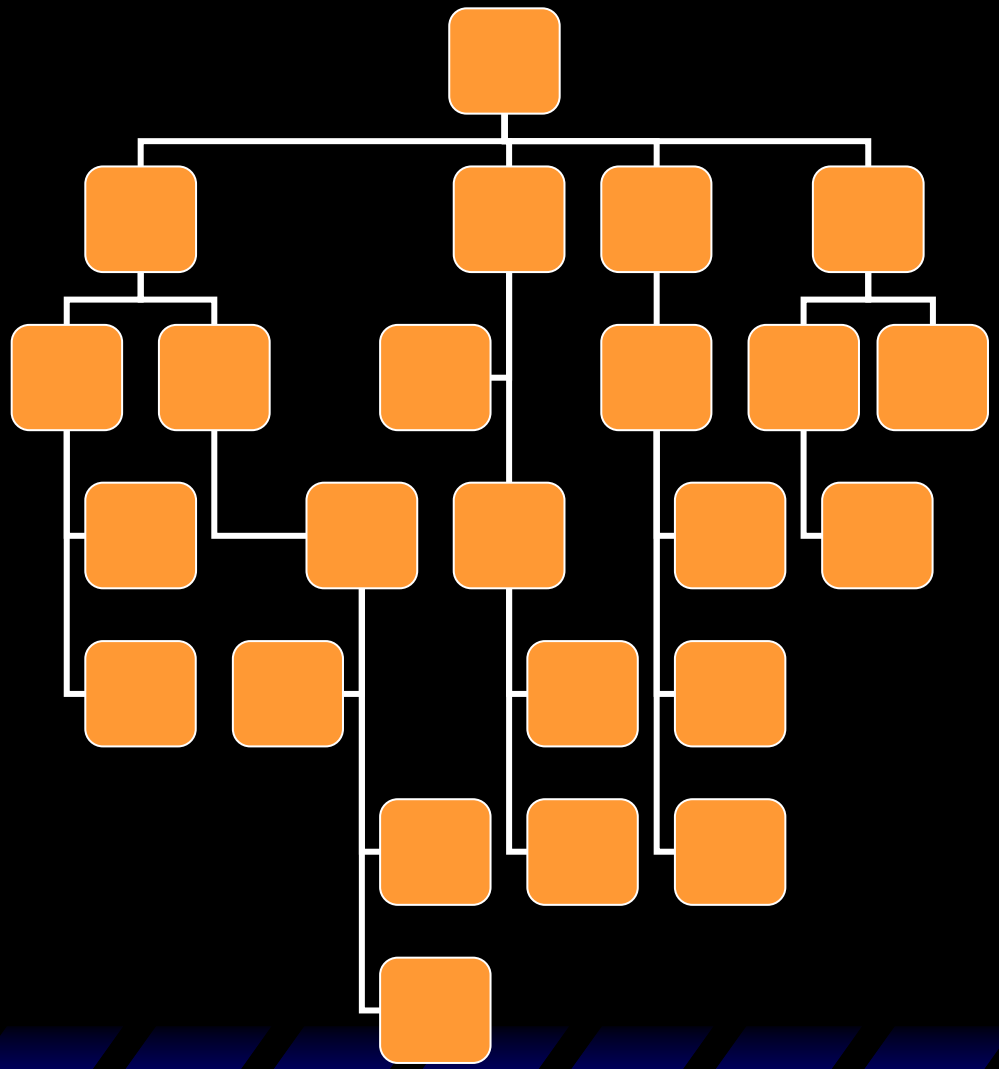
Nuclear power plants

Factories

Integrated transport systems

Military operations

“Organizations” report to a single point



Closed systems

Such organizations are “closed systems” where decisions can be directed by a *command and control* system

Closed systems have problems of complexity but normally management tools can be used to control operations

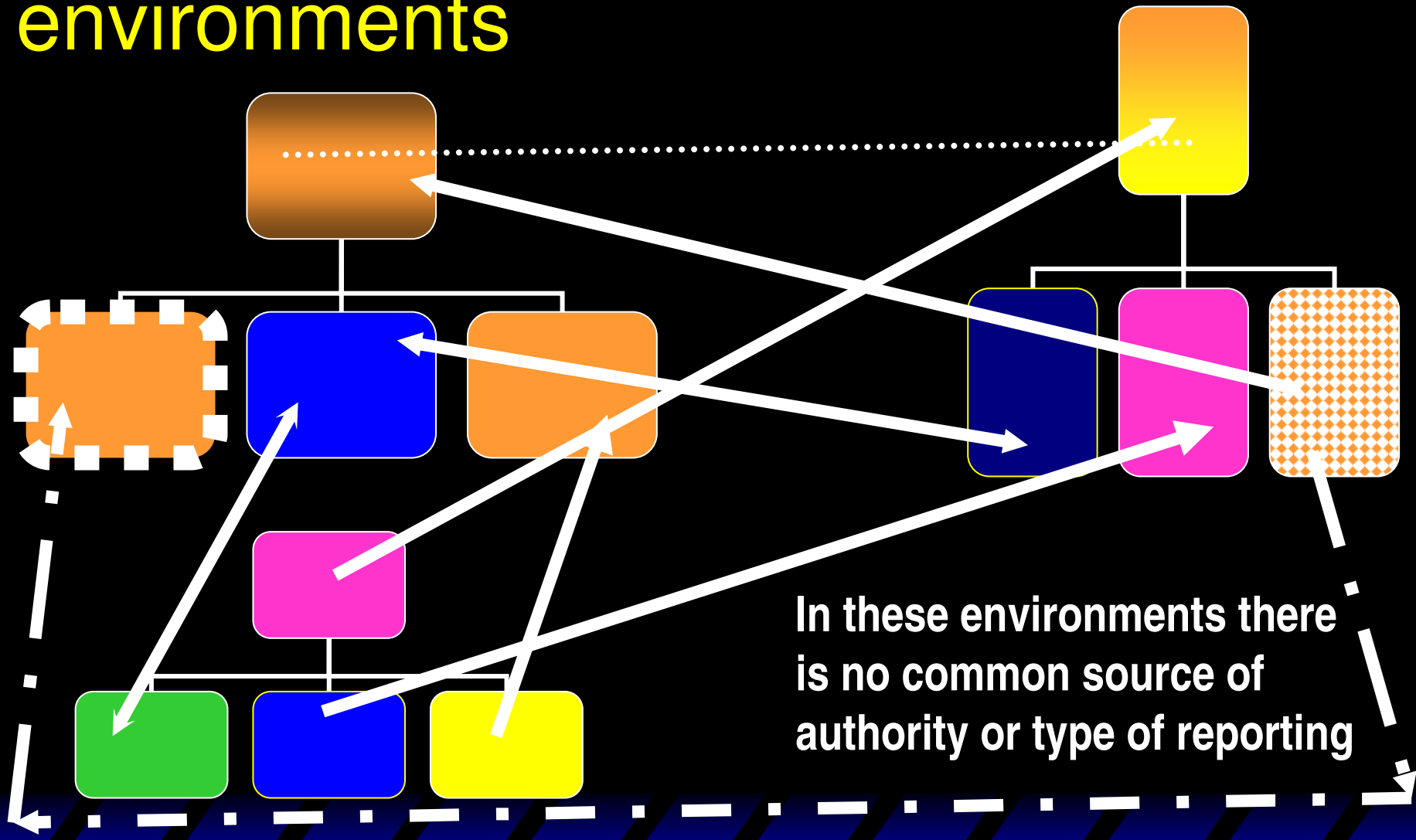
However closed systems are not the only type of hazard

Many modern hazard environments involve sets or collections of interacting systems

The interfaces among these systems are not subject to organizational command and control

The existence of multiple participants not subject to common control raises new hazards and problems

Complex multi organizational environments



Open systems

Open systems do not have any unifying management control. No single person or entity is in "charge"

In general the public regulatory system is used to try to control the risk

However public regulation has a limited set of control systems and also introduces a new entity into the process

Opening a closed system

Some systems which could or should be “closed” are inadvertently “opened” by a management or social error

Regulation can also open a closed system if designers or operators rely on regulatory approval rather than being responsible for the design

Mt Blanc Tunnel was an open system 2 direct regulators and a large number of independent firms

Margarine/flour Fire Mt Blanc tunnel

Operators relied on regulators who had failed to classify margarine on its caloric value

Margarine Classification

From the expert group on tunnel fires:

To study the possibility of classification as dangerous goods of certain liquids or easily liquefied substances with calorific values comparable to that of hydrocarbons

One might easily ask why anyone ever overlooked this key issue

USA is no better

..flash point was selected as the basis for classification of flammable and combustible liquids because it is directly related to a liquid's ability to generate vapor, i.e., its volatility. Since it is the vapor of the liquid, not the liquid itself, that burns, vapor generation becomes the primary factor in determining the fire hazard.

The expression "low flash - high hazard" applies. Liquids having flash points below ambient storage temperatures generally display a rapid rate of flame spread over the surface of the liquid, since it is not necessary for the heat of the fire to expend its energy in heating the liquid to generate more vapor.[[i]]

[i] 29 CFR 1910.106, Flammable and Combustible Liquids

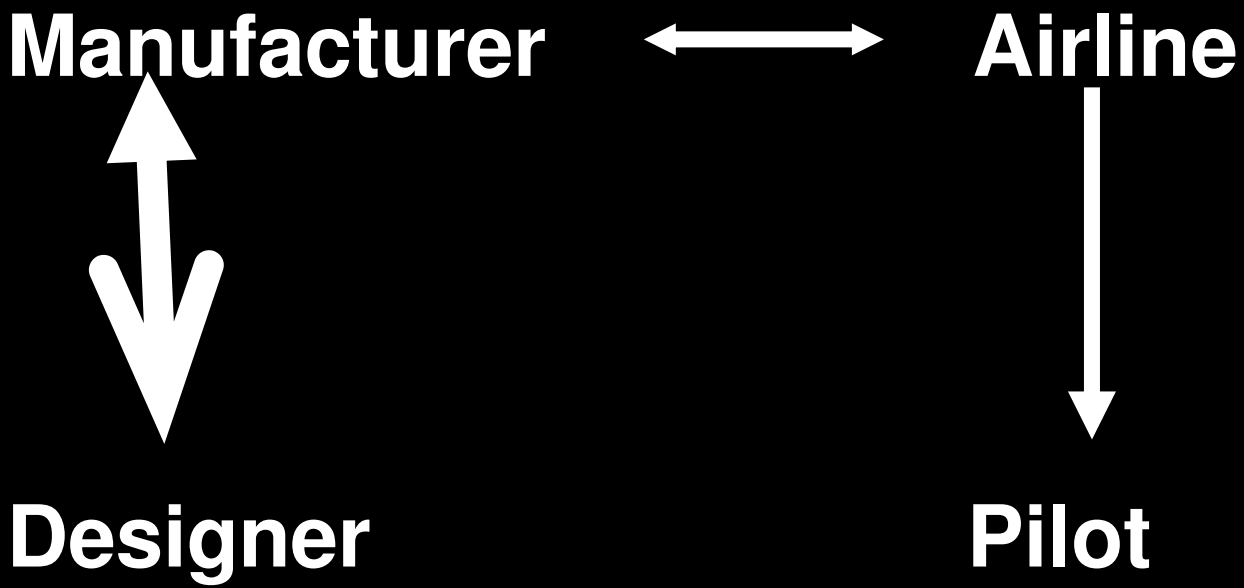
Complex systems

Take a very simple regulated system:

Two organizations

Two levels of operation within each organization

Commercial air transports



Airbus crash

Aircraft Accident Report

In-Flight Separation of Vertical Stabilizer
American Airlines Flight 587
Airbus Industrie A300-605R, N14053
Belle Harbor, New York
November 12, 2001 NTSB Number AAR-04/04
NTIS Number PB2004-910404

Executive Summary: On November 12, 2001,, American Airlines flight 587, an Airbus Industrie A300-605R, N14053, crashed into a residential area of Belle Harbor, New York,.

All 260 people aboard the airplane and 5 people on the ground were killed, and the airplane was destroyed by impact forces and a post crash fire

Airbus Crash 265 dead

National Transportation Safety Board

The airplane's vertical stabilizer and rudder separated in flight

National Transportation Safety Board

probable cause of this accident was the in-flight separation of the vertical stabilizer as a result of the loads beyond ultimate design that were created by the first officer's unnecessary and excessive rudder pedal inputs..

NTSB

Contributing to these rudder pedal inputs were characteristics of the Airbus A300-600 rudder system design and elements of the American Airlines Advanced Aircraft Maneuvering Program

NTSB

This safety recommendation letter addresses an industry-wide safety issue involving omissions in pilot training on transport-category airplanes. Specifically, the National Transportation Safety Board has learned that many pilot training programs do not include information about the structural certification requirements for the rudder and vertical stabilizer on transport-category airplanes

NTSB

Further, the Safety Board has learned that sequential full opposite rudder inputs …may result in structural loads that exceed those addressed by the requirements

NTSB

pilots may have the impression that the rudder limiter systems…… prevent sequential full opposite rudder deflections from damaging the structure.

However, the structural certification requirements ….do not take such maneuvers into account; therefore, such sequential opposite rudder inputs, even when a rudder limiter is in effect, can produce loads higher than those required for certification and that may exceed the structural capabilities of the aircraft.

NTSB

the Board believes that the FAA should require the manufacturers and operators of transport-category airplanes to establish and implement pilot training programs that: (1) explain the structural certification requirements for the rudder and vertical stabilizer on transport-category airplanes

Finger pointing time

How in 2001 could there be such a gaping hole in the design/regulatory system?

Why would any one wait for a regulator to point out the need for cross communication

Regulatory Effectiveness Analysis and Regulatory Root cause analysis are designed to address that question

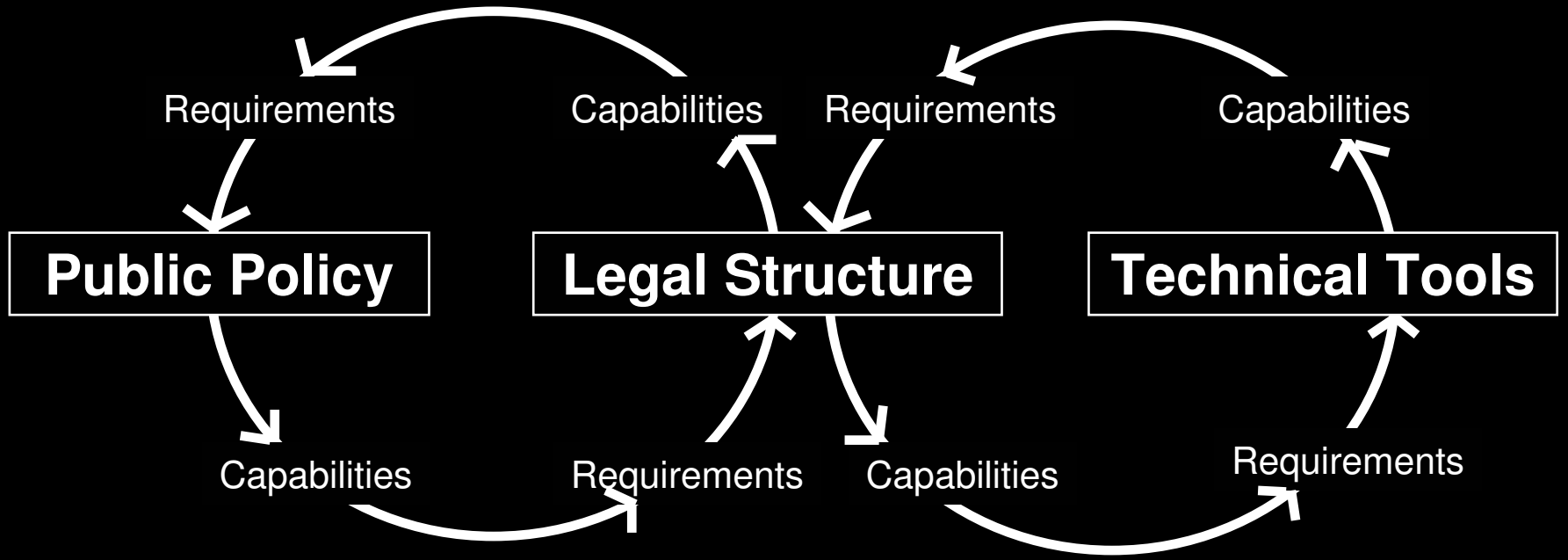
REGULATORY EFFECTIVENESS ANALYSIS (REA)

- REA a method for evaluating the compliance of a proposed technological system with an existing or proposed regulatory program
- REA is designed to measure separately and together the three key components of a technical regulatory system

REGULATORY EFFECTIVENESS ANALYSIS

- Public policies
- Legal Structure
- Technical tools

Regulatory Effectiveness Analysis



PUBLIC POLICIES

Public policy is a narrative statement of the goals to be achieved by the regulatory program.

LEGAL STRUCTURES

- Regulation requires a mechanism to enforce the social will on individuals or firms who would not otherwise comply
- Legal structures are the formal requirements imposed by the society

TECHNICAL TOOLS

Every technology has a distinct and often limited set of technical tools available for regulation

Regulatory Effectiveness Analysis

All three of these components must be properly designed to achieve a working regulatory system

Public policies must be coherent

Legal structures must contain all necessary elements

Technical tools must be available and produce the needed results

Regulatory Effectiveness Analysis

Most importantly, the components interact.

Public policy, legal structures and technical tools have interlocking sets of requirements and capabilities.

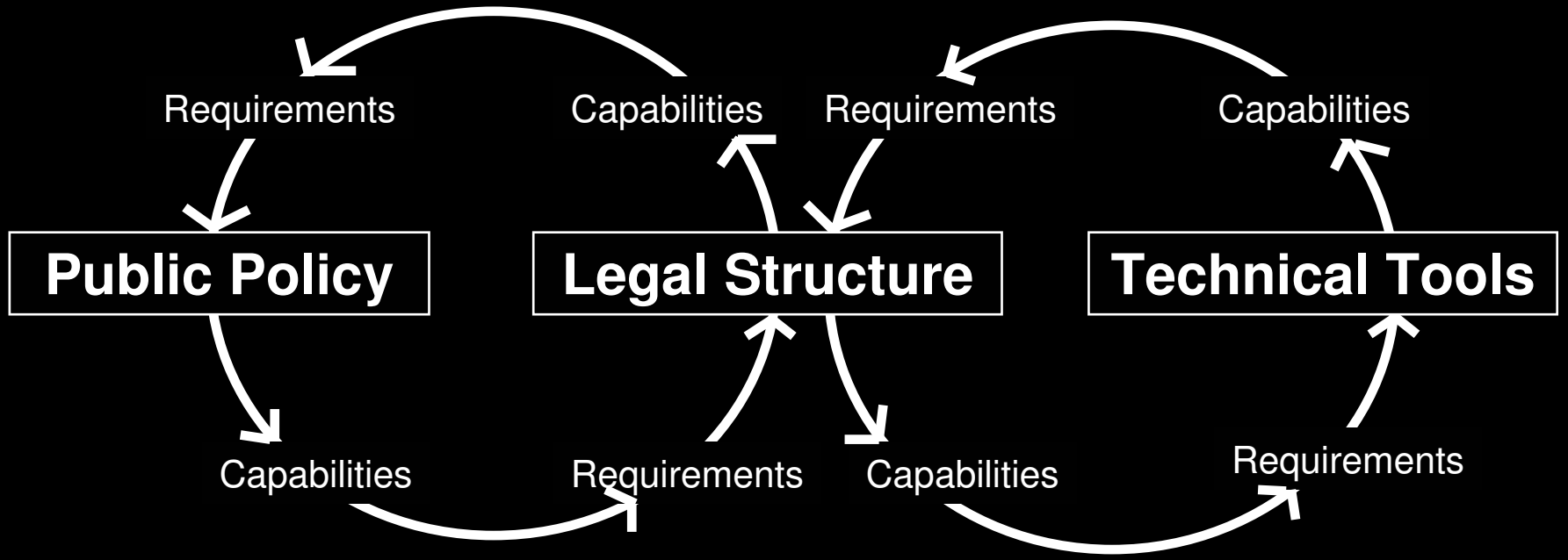
REQUIREMENTS

the preconditions which must be satisfied by other components before a given component can function.

CAPABILITIES

reflect the ability of a component to satisfy a requirement of another component

Regulatory Effectiveness Analysis



Interlocking

In every case each legal structure requires certain capabilities in the technical tool. Similarly, a legal structure has to have capabilities that can satisfy the requirements of the technical tool

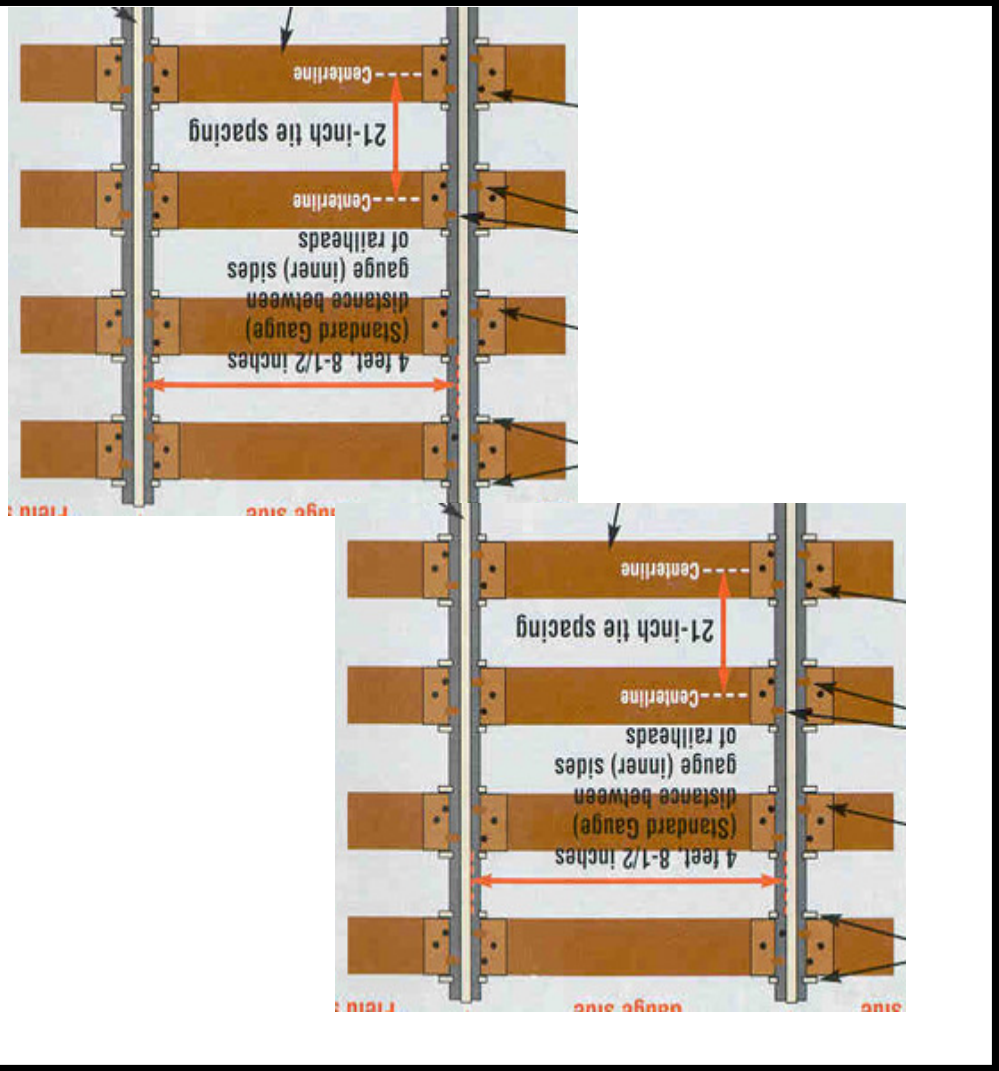
Regulation is therefore “technology specific” , one size does not fit all

Discontinuity

If a component is ill defined or there is no match between policy goals, structure and tools a "discontinuity" exists.

Discontinuity

Individual components may work properly but the system still fails



Legal Structure

Legal structure is normally used to promote safety by interrupting the "chain of causation"

Legal Structure operates using two philosophies and three Methods

The Philosophies are

Prevention &

Deterrence

Prevention uses *direct controls* to interrupt a chain of causation which otherwise leads to injury

Contraception

Deterrence uses the consequence of violation to internalize in the operator a desire to interrupt the chain of causation *(indirect control)*

Paternity suit

Deterrence

Prevention

Two philosophies and Four Legal Methods

- Prevention
  - Information
  - Intervention
- Deterrence
  - Compensation
  - Punishment

Prevention

Intervention - direct action which interrupts a chain of causation

Information – Data required to be provided to a critical decision maker who is in position to interrupt the chain of causation

It is recognized that the use of information when intervention is possible is a specific error under modern safety design principles

Deterrence

Compensation- Payment to the injured party by the responsible party

Punishment Social penalty for the guilty party

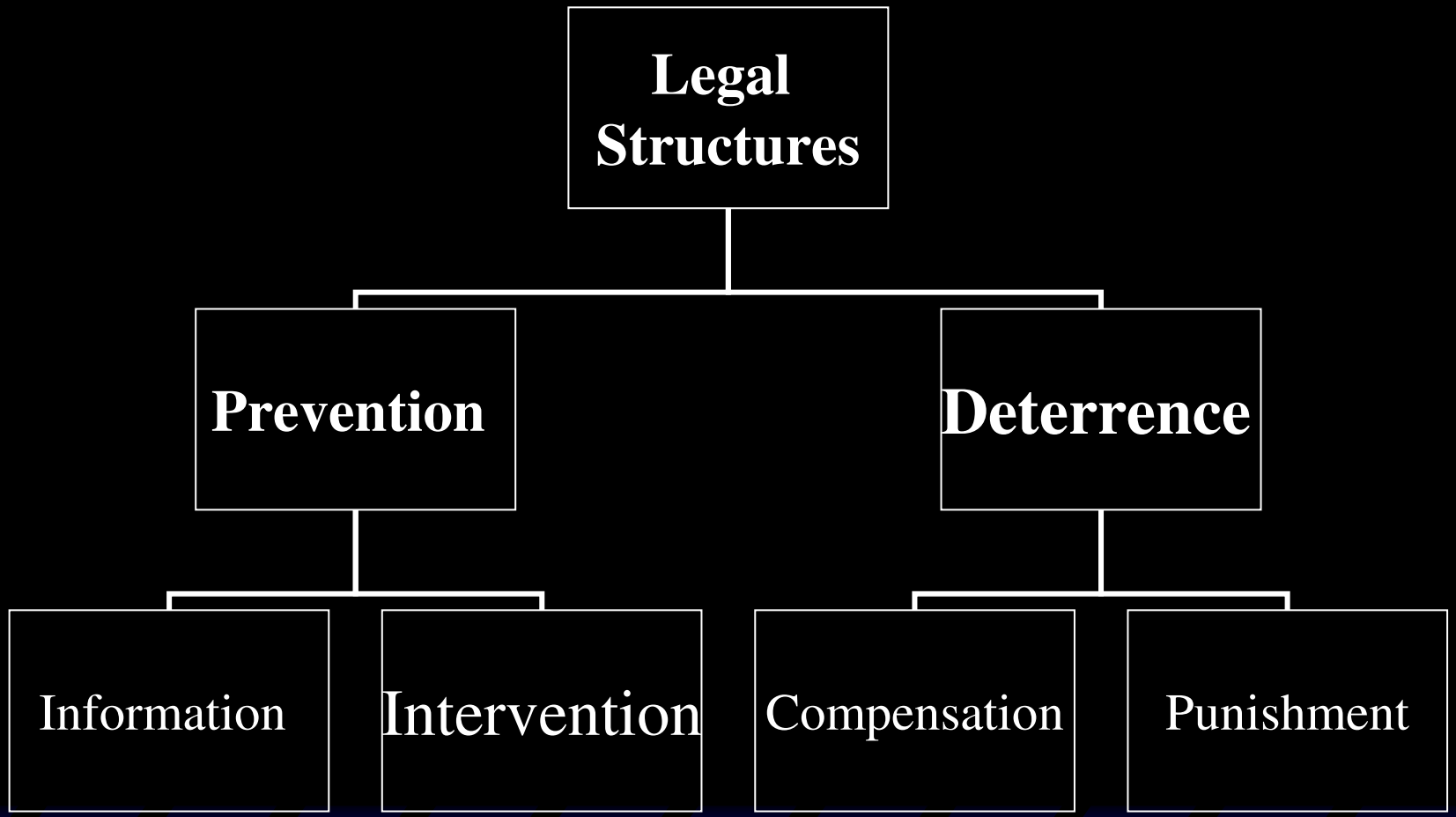
Lawyers often draw an artificial distinction between criminal law and compensation law but they are both deterrence if the responsible party pays the compensation

Combined Methods

Providing information can be required as part of prevention, but it is only effective if adequate deterrence ensures that it will be used

Providing compensation internalizes to the decision maker the need to take precautions if and only if the chain of causation can be established and the responsible party has resources to pay

Legal structures



Regulatory Root Cause Analysis

Regulatory root cause analysis is used at the interface of the legal structures and the technical tool to determine if the precise *philosophies* and *Methods* *provide the needed requirements and capabilities.*

Regulatory Root Cause Analysis

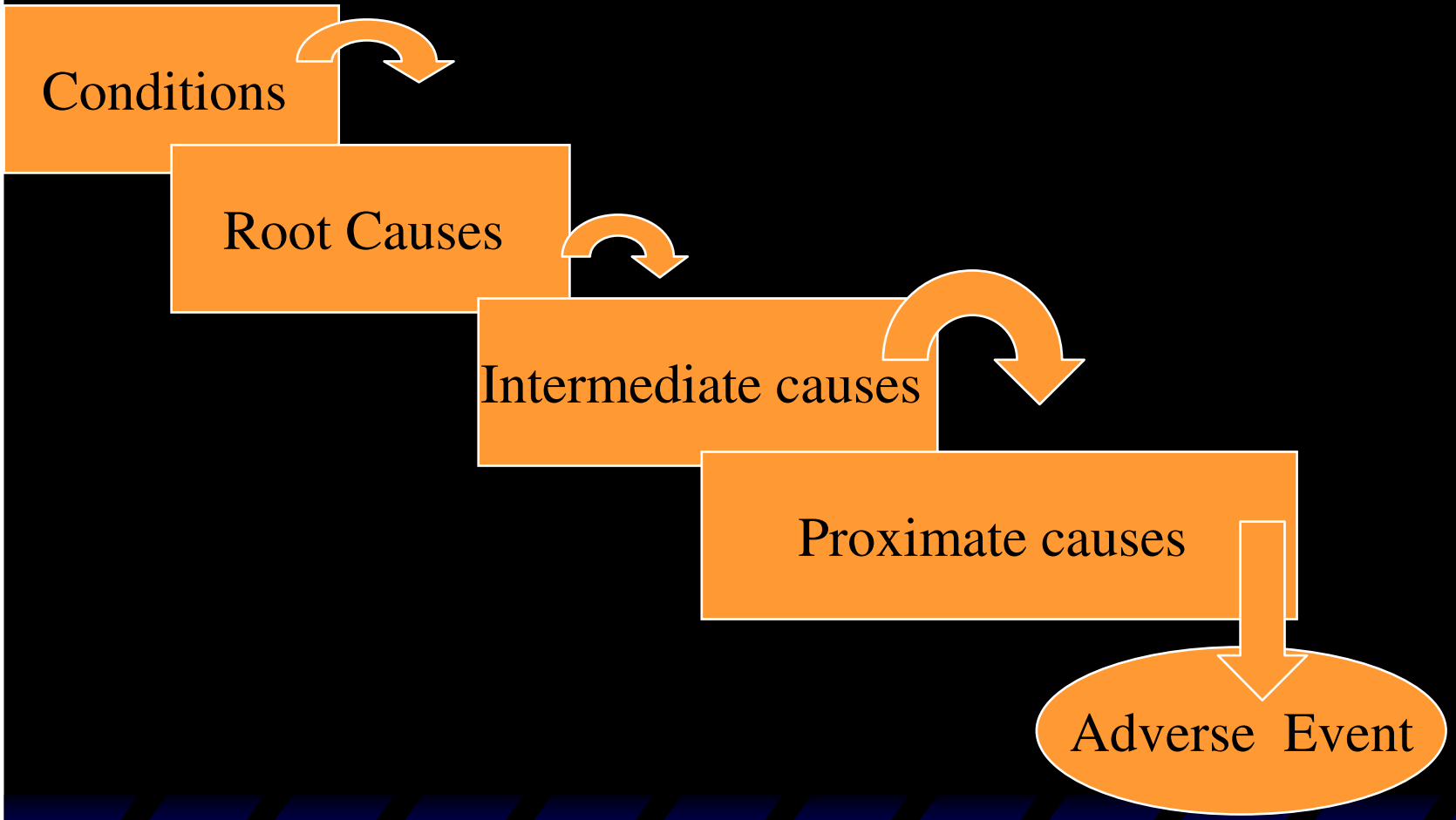
RRCA is an "forward looking" activity that uses the philosophy and tools of Root cause analysis to uncover discontinuities in the regulatory process that result from inappropriate use of philosophies or methods

It is particularly useful in open regulated systems

Regulatory Root Cause Analysis

- Regulatory Root Causes are defined such that when the Regulatory Root Cause is totally eliminated, the adverse event would not have occurred but the desired event would occur
- Inappropriate reliance by designers or operators on regulators is a typical regulatory root cause

Regulatory Root cause analysis (Simplified)



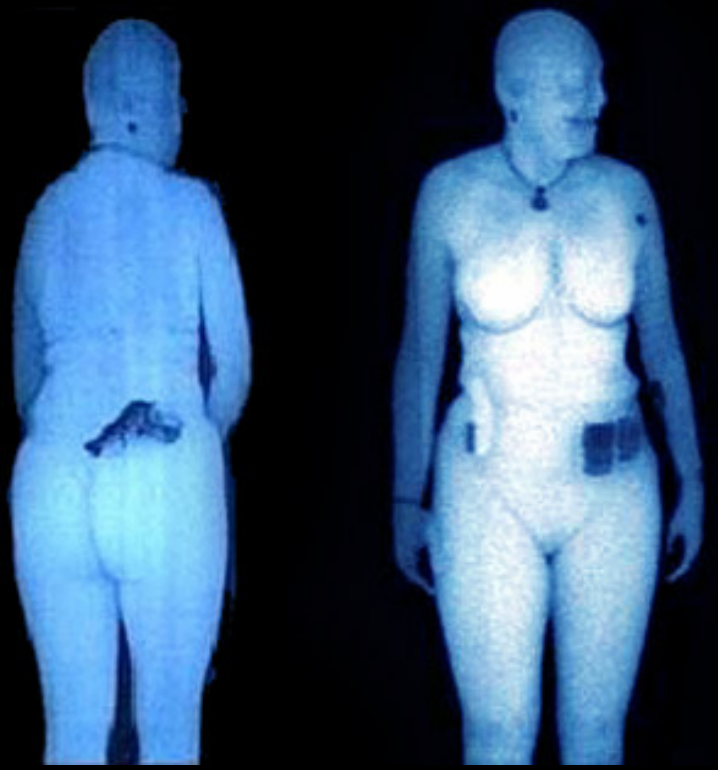
Regulatory Root Cause Analysis

Regulatory root cause analysis is designed to determine which philosophy and method are suited to the actual technical regulatory problem at hand

General solutions are not possible for several reasons

Regulatory Root Cause Analysis

The ability to use prevention or deterrence is *"technology specific"*



New airport screening technology

Relating *cause* to *effect* is technology specific

Cf Deterrence cannot work if the cause of injury cannot be pinpointed

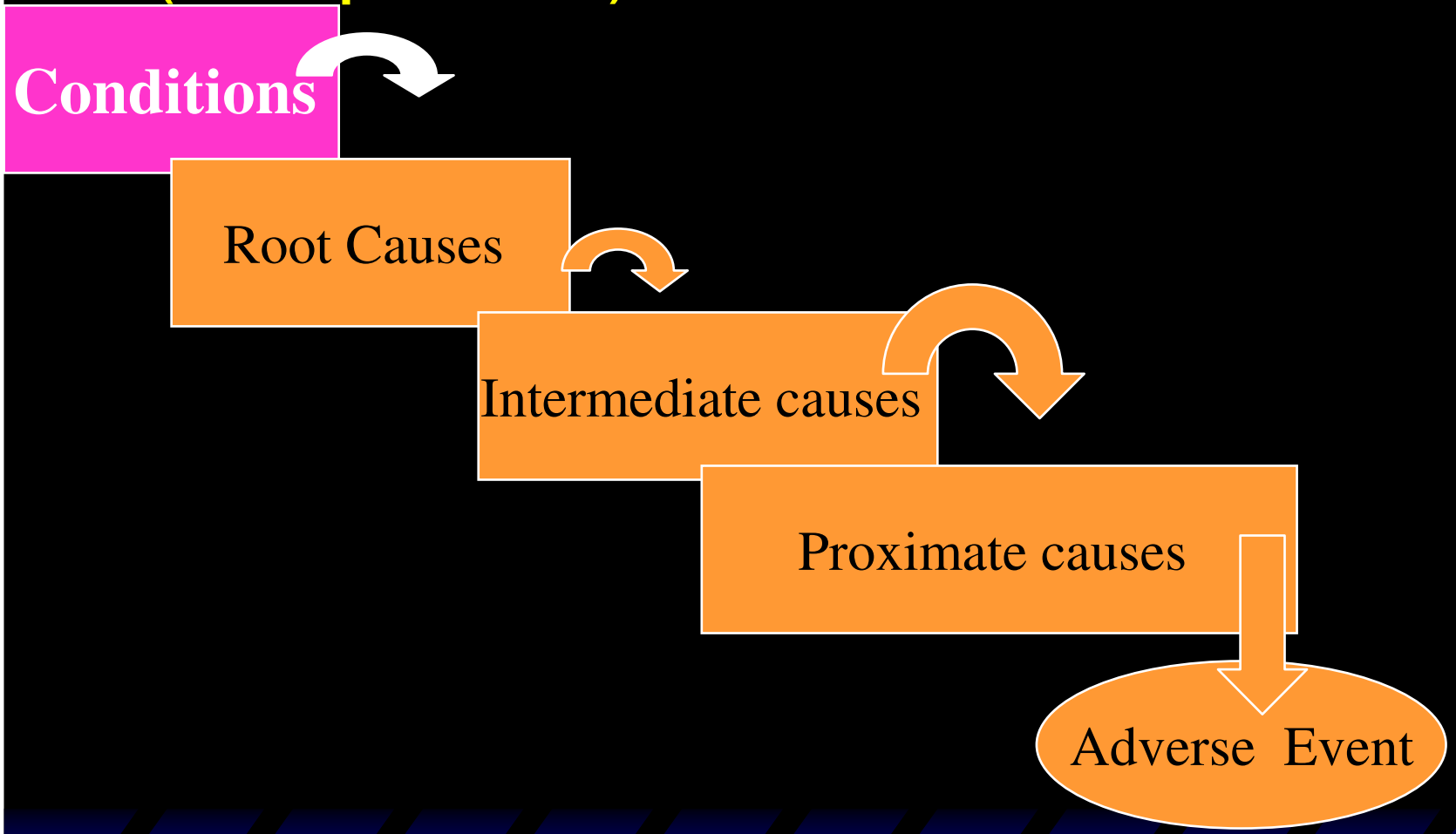
Compare for example trauma with cancer

Regulatory Root Cause Analysis

In a well designed system "preventive" regulation operates "upstream" of deterrent regulation and deterrence is limited to technical environments that do not permit "prevention"

Similarly intervention is used as often as possible instead of relying on the tool of information

Regulatory Root Cause Analysis (Simplified)



Conditions

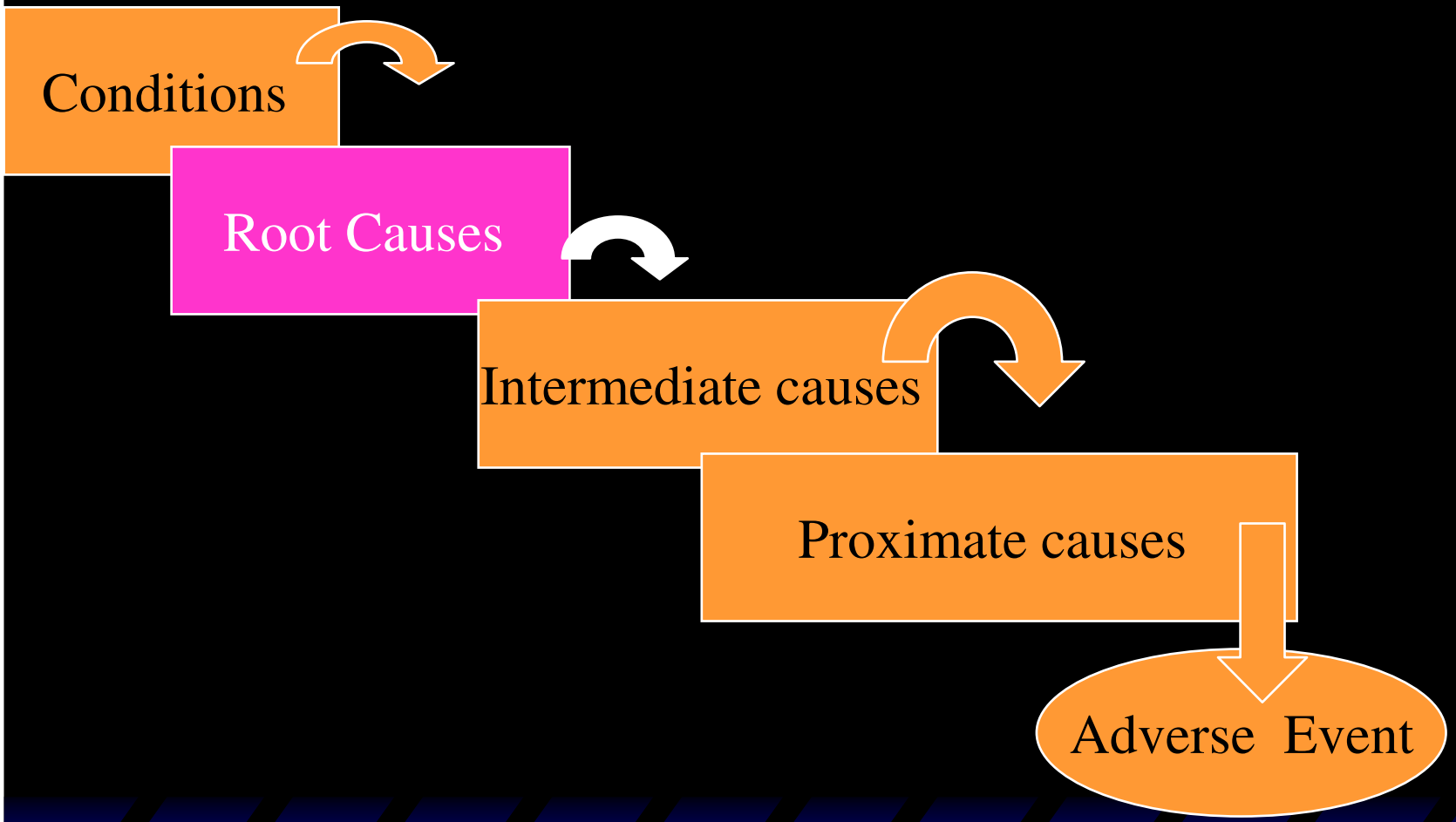
Root cause analysis is always done for a purpose

Root causes reflect choices that create the environment for adverse events.

"Conditions" not involved in choices can be thought of as the first step. Conditions must be *defined* but are not *controlled*

The existing regulatory system may or may not be a condition, depending on the scope of analysis

Regulatory Root cause analysis (Simplified)



Regulatory Root causes

Regulatory Root causes are controllable organizational factors or systemic problems that lead through intermediate and proximate causes to adverse events.

Root causes are often the side effects of otherwise desirable activity

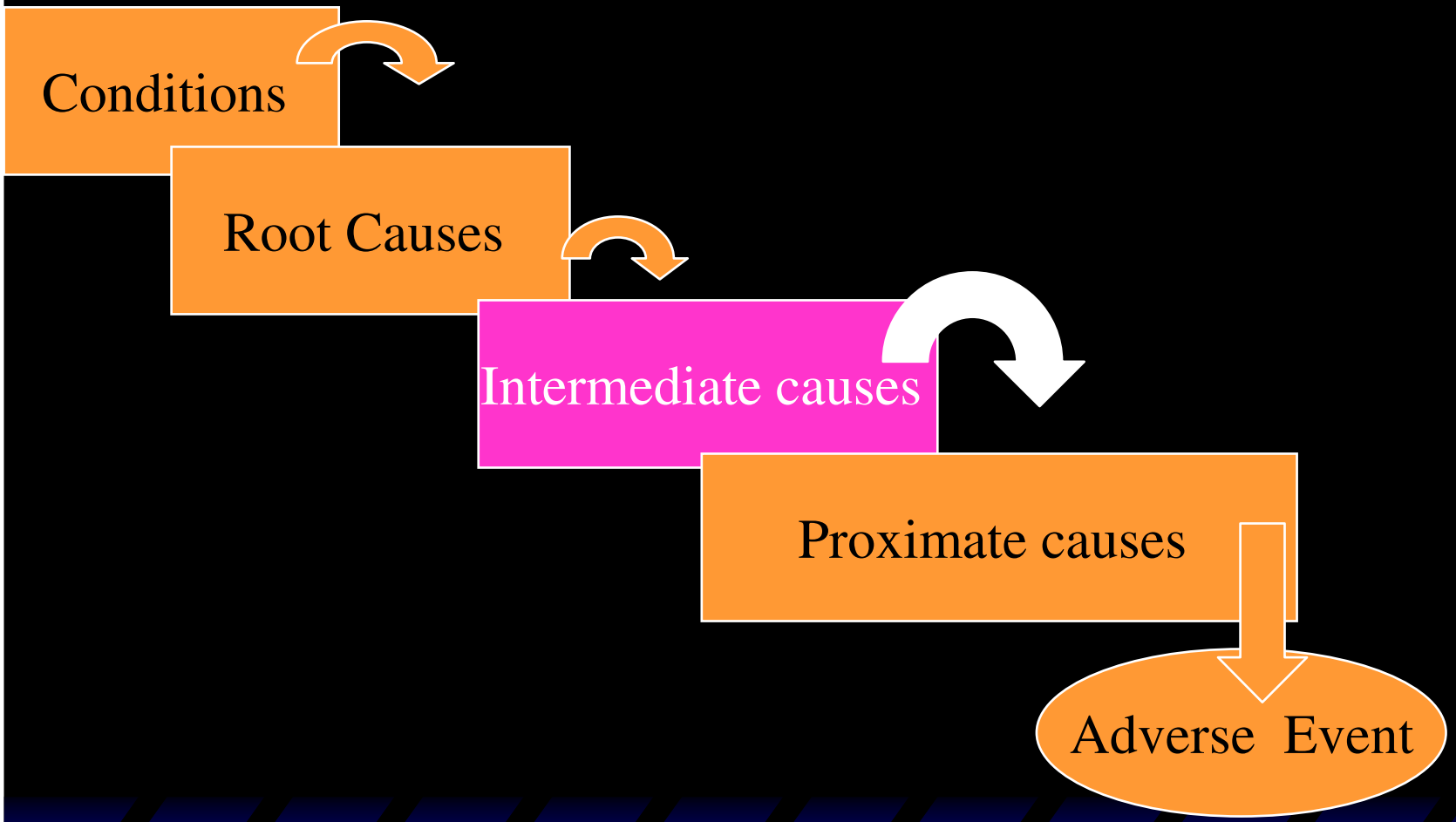
Regulatory Root Cause

In open systems the path of failure from root cause to adverse event may not be *foreseeable* prior to the event

This may be due to complexity, uncertainty or lack of data

However the lack of a known path of injury does not prevent the regulation of safety

Regulatory Root cause analysis (Simplified)



Intermediate causes

Intermediate causes are those between the root and proximate causes

Intermediate causes routinely present as multiple alternative pathways

Elimination of a given intermediate cause may prevent some events but others can occur unless the root cause is eliminated

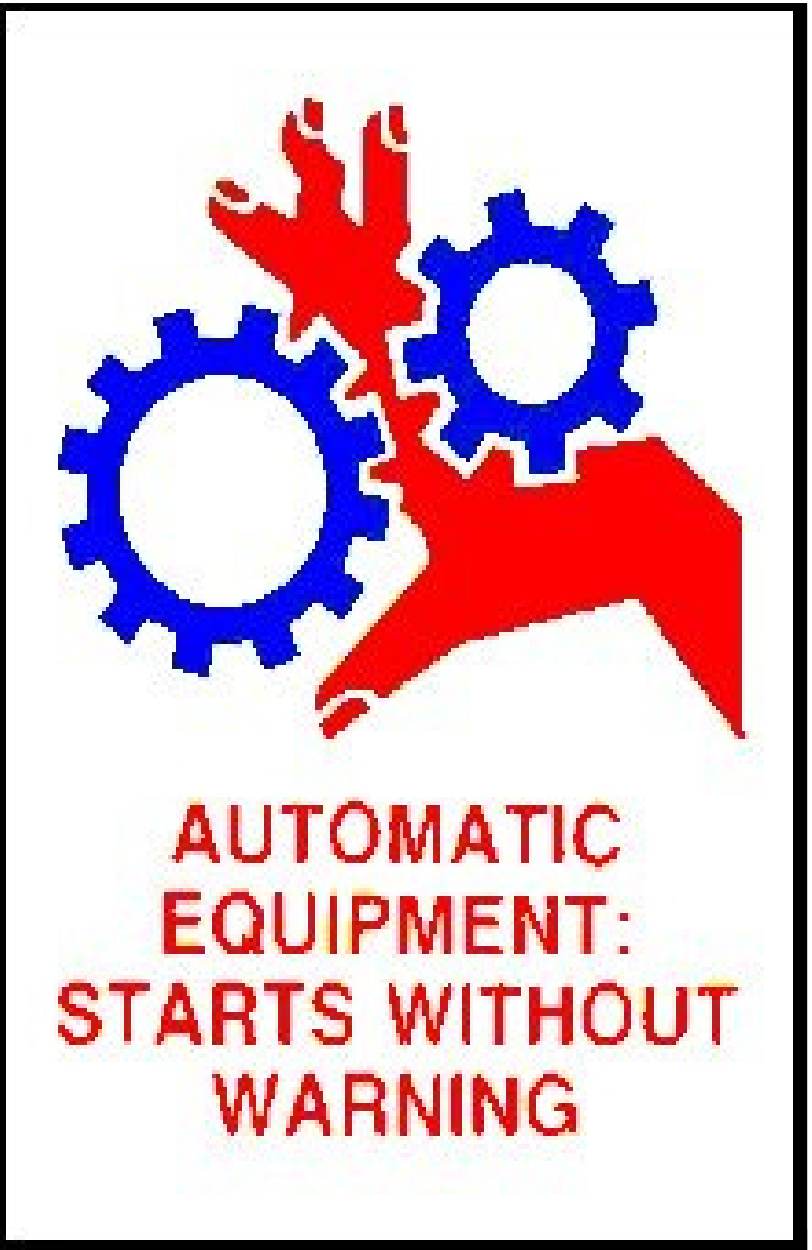
Intermediate Causes

Intermediate causes would often be “root causes” if the analysis was confined to a single organization

Intermediate causes capture the relationship among multiple organizations including regulators

Intermediate Cause

Intermediate cause analysis asks why this machine starts without warning



Intermediate causes

Failure path from intermediate causes to adverse events is often foreseeable but may not be direct.

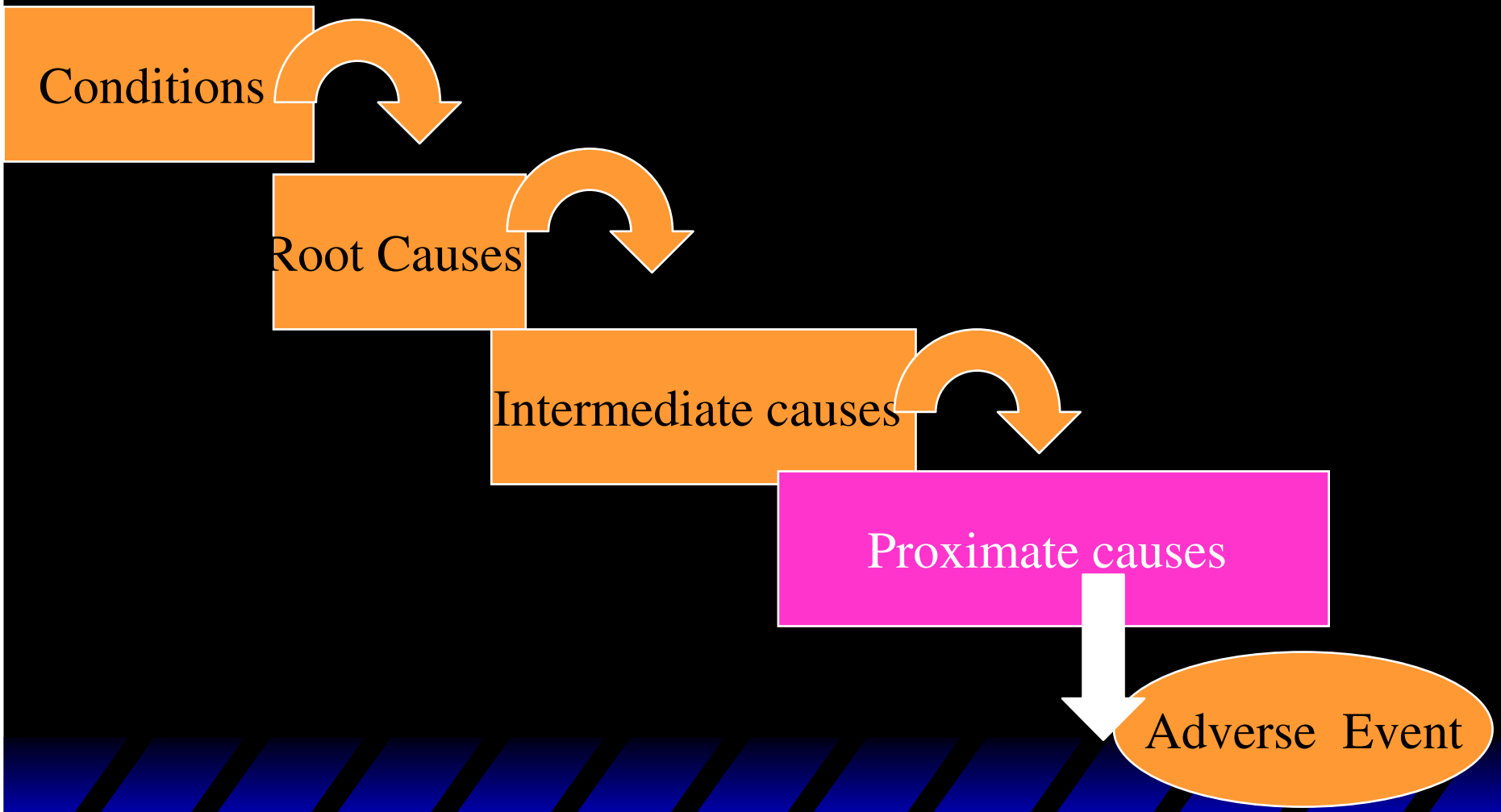
Failure path requiring multiple operator errors is an intermediate cause

Preventive regulation normally acts on intermediate causes

Preventive Regulation

- **Preventive regulation is designed to directly intervene before proximate cause comes into existence**
- **Cf controls on the design or sale of pistols**

Regulatory Root cause analysis (Simplified)



Proximate causes

Proximate causes are those immediately before the Adverse event.

Injury path from proximate cause is direct.

Simple Operator error is a proximate cause

Deterrence

Deterrent regulation acts on proximate causes.

Deterrent regulation “punishes” a defined person “post hoc” for allowing the proximate cause or adverse event to come into existence.

It should only be used when upstream prevention is not available

RRCA-Airbus crash

Air frame certification requirements are
preventive-intervention

Mandatory pilot training is
preventive- information

Pilot licensing and discipline is
Deterrent- punishment

RRCA-Airbus crash

However the failure to integrate these different components led to an obvious set of failures, all of which could have been known before the crash

RRCA-Airbus crash

1) No system was required to feed information from the pilots back to the designers

As a result designers could rely on unchecked outmoded understanding of pilot behavior

RRCA Airbus crash

2) No system was required to feed designer's assumptions to the pilots

As a result pilots inappropriate beliefs about the system went unchecked

RRCA-Airbus crash

3) Assumptions were made that regulations were both comprehensive (covered all relevant issues) and adequate (compliance would generate safety

Pedal action required for avoid hazardous activity was not specified in any design or operating regulation

Conclusion

Certain factors characterize systems with discontinuities

1) Open systems with multiple organizations
2) Organizations that have different technical and safety cultures
3) Rare events with extreme consequences (inappropriate learning)

Conclusion

- Open regulated systems have special potential for catastrophic unplanned interactions of individual systems
- Regulation adds the special problem of untoward reliance on the regulator
- Forward looking analysis can identify some of the worst problems

Conclusion

Open systems subject to regulation require advanced analysis of the assumptions and limitations of the regulatory process and the role of the regulator as a participant in the entire system

The Regulatory Use of System Safety Analysis: A Regulatory Effectiveness Analysis

Prof Dr Jur Vincent M. Brannigan
AJ Clark School of Engineering
University of Maryland at College Park
Firelaw@umd.edu