SAND2015-7569PE

Risk-Based Border Security Planning

Eng. Adam D. Williams, Org. 6832

Exceptional service in the national interest

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY | NNSA

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. SAND NO. 2013-9692P

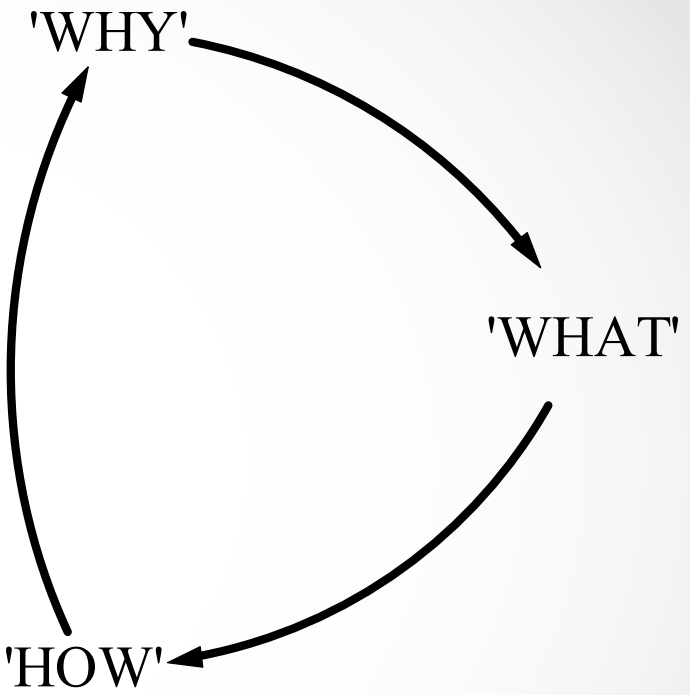
What's the point?

- Based on what has been presented and discussed to this point in the workshop…

- Why do have border security?
  - [discussion question for participants]

Outline

- '**Why**' have border security?
  - Brief review of previous lectures
- '**What**' is border security?
  - Risk-based planning concepts
- '**How**' to do border security?
  - Tools (people, technology, programs)
  - Brief preview of subsequent lectures

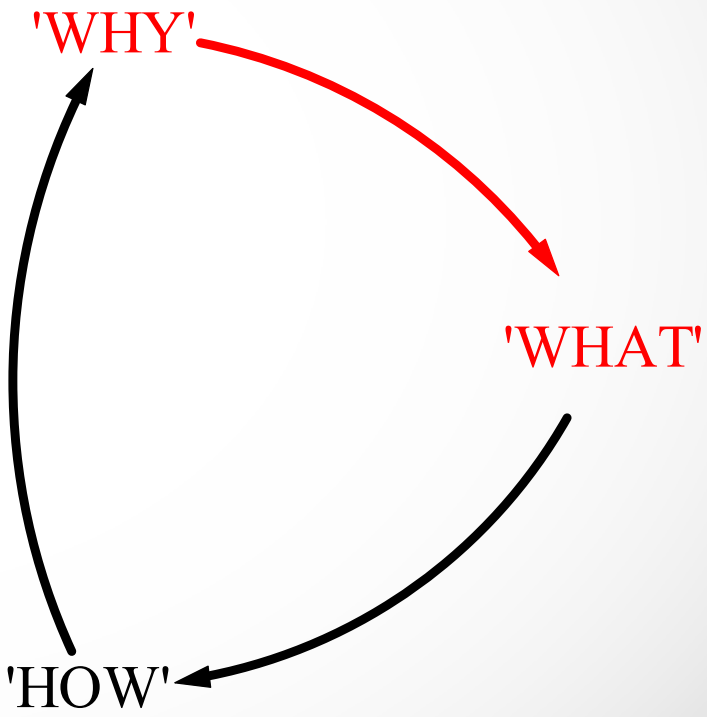


Border Security: WHY?

- ***An increasingly complex problem with increasingly high consequences***
  - from 'Border Security Systems' by Dr. Holly Dockery
- ***Overcome regional tensions & leverage common standard of living goals***
  - from 'Regional Perspectives & Capabilities' by Mr. Al Sharif Nasser Bin Nasser
- ***Capture local benefits & reduced local risks***
  - from 'Border Security Cooperation Concepts and Case Studies' by Dr. Ben Bonin
- ***Mitigate or prevent risks experienced by others***
  - from 'U.S. Perspectives on Border Management' by Mr. Christopher Bertrand

From ‘Why’ to ‘What’

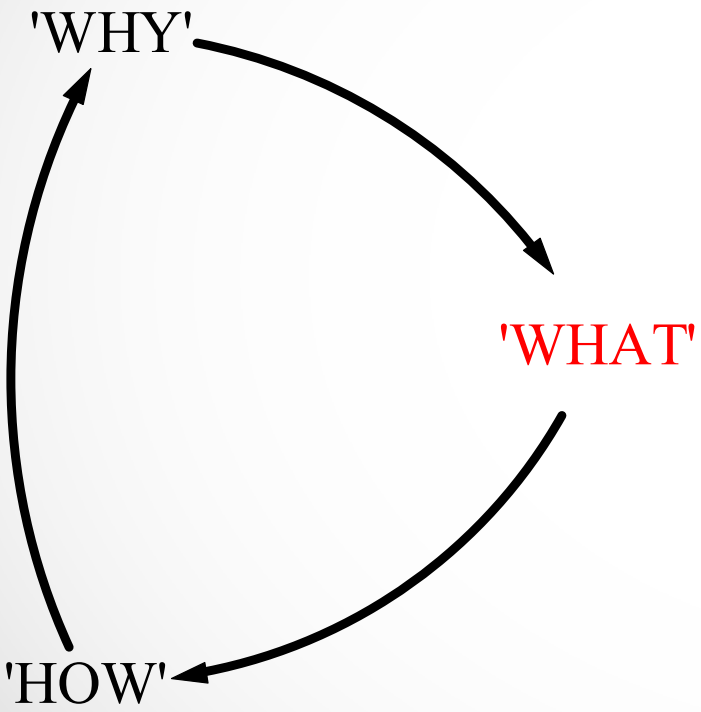
- Now that we know the ‘why’…
- WHAT is border security?
  - [discussion question for participants]



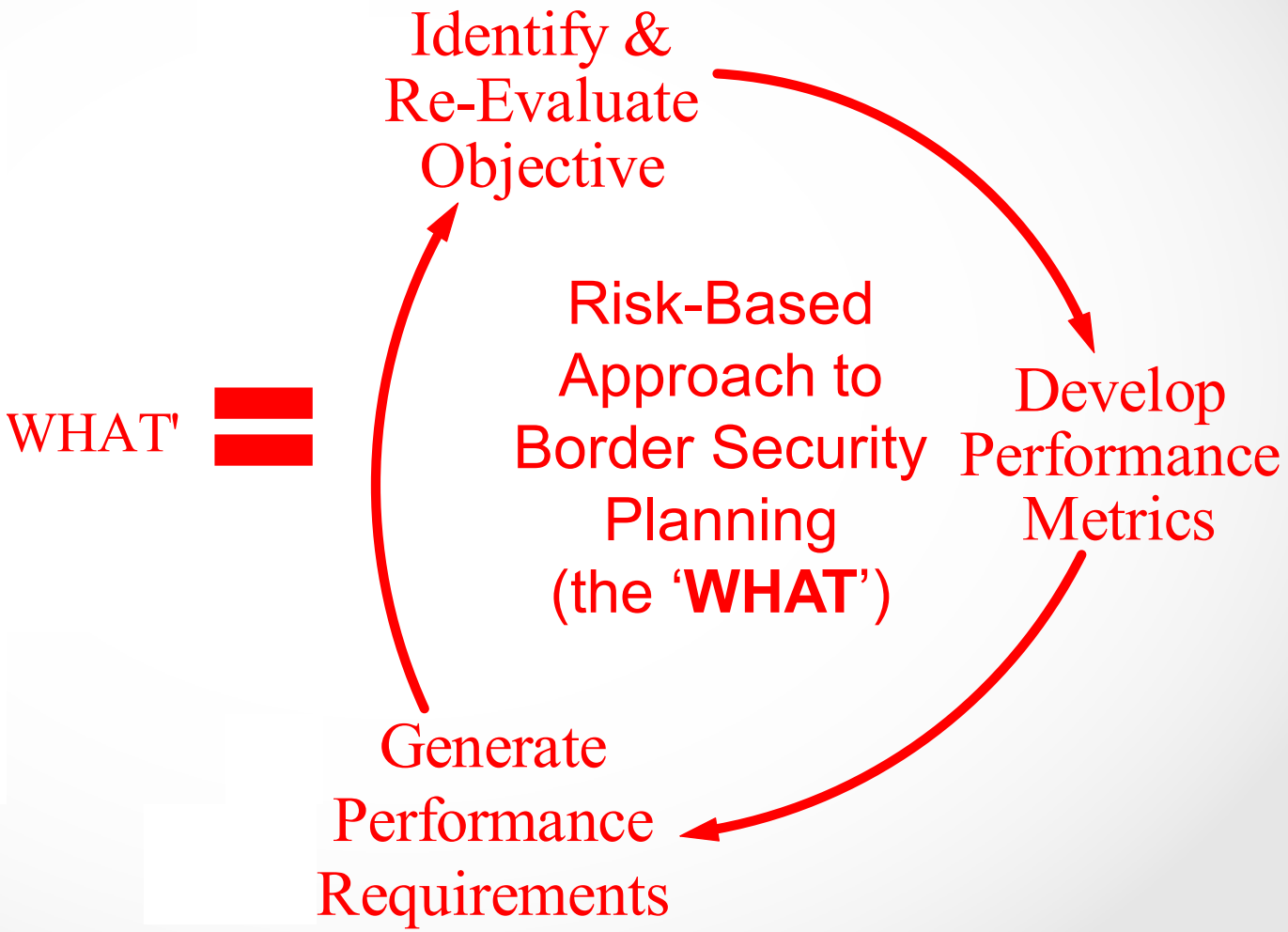
Border Security: WHAT?

- What = **risk-based border security planning**
  - Need to identify objective/mission
    - '***What*** am I trying to do?'
  - Need to develop performance metrics
    - '***What*** is the evidence of what I'm trying to do?'
  - Need to generate performance requirements
    - '***What*** do I need to do?'

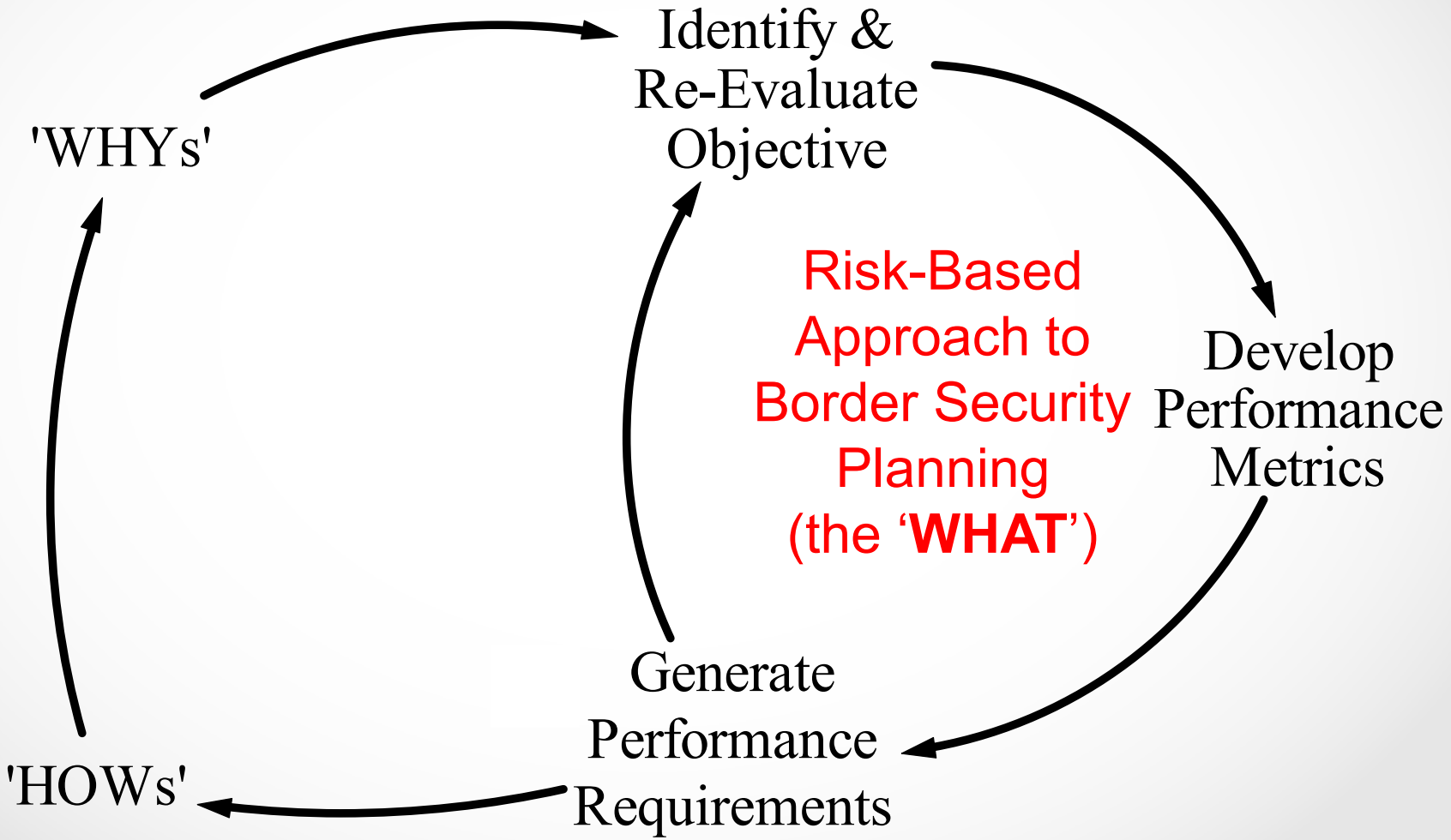
Border Security: WHAT?



Border Security: WHAT?



Border Security: WHAT?



WHAT: Objective(s)

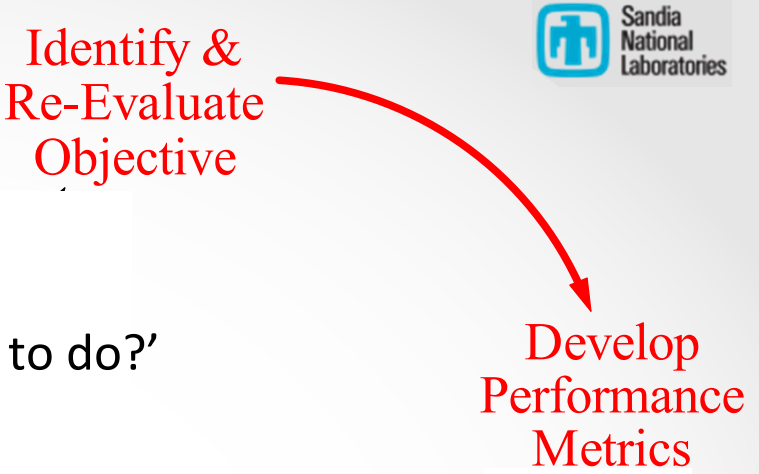
- Identify or re-evaluate the objective
  - '***What*** am I trying to do?'

- The '***whys***' characterizes the '***what***' & help describe the objective
  - ***Why***? = Want **trade** & **tourism**
    - ***What?*** = Allow people and goods to move between countries
  - ***Why***? = Don't want **illicit goods**, **unsavory people** or **violence**
    - ***What?*** = Prevent unsanctioned people or goods to move between countries
  - ***Why***? = Want to **protect people**, **land** and **property**
    - ***What?*** = Reduce the risk of harm to people, land and property around borders

WHAT: Objective(s)

- Example objective:
  - ‘Protecting the sanctioned movement of people, vehicles and goods between neighboring states with the lowest financial cost and minimum risk to people, land or property’
- But, how well am I doing this?

WHAT: Performance Metrics



- Develop performance metrics
  - '***What*** is the evidence of what I'm trying to do?'
- Metrics are **signals** that indicate **how well** the **objective** is being met
  - ALSO become the basis for determining **performance requirements** & **design features** of border security
- Example performance metrics:
  - Threat mitigation (defend against whom?)
  - Risk reduction (prevent what?)
  - Objective assurance (enable what?)

Metrics: Threat Mitigation

- Defending against whom?
  - **Threat** = the existence of an adversary to cause an undesirable consequence
  - **Threat assessment** = characterizing credible motivations, intentions, and capabilities of potential adversaries that could cause undesirable consequences
- What to mitigate?
  - Motivations (what can adversary gain?)
  - Intentions (what can an adversary do?)
  - Capabilities (what tools can adversary bring?)
  - Vulnerabilities (where is adversary's easiest opportunity?)
- **METRIC** = decreasing the severity of potential adversary motivations, intentions, capabilities & opportunities for exploitation

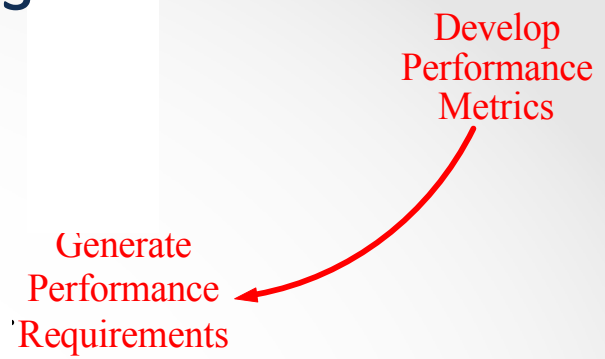
Metrics: Risk Reduction

- Prevent what?
  - **Risk** = the likelihood that a threat will be able to bring about an undesirable consequence
  - **Consequence** = the level of impact on the interests of the public, the state, key interest groups, and the international community
- What to reduce to prevent undesirable consequence? Opportunities at **Ports of Entry** and **Front Borders** for
  - Sabotage
  - Smuggling
  - Infiltration
- **METRIC** = decreasing the possibility that opportunities for sabotage, smuggling and infiltration exist

Metrics: Objective Assurance

- Enable what?
  - **Objective** = the goal, mission or purpose to be achieved
  - **Assurance** = the certainty of desired outcomes occurring
- Desired border outcomes can include:
  - **Port of Entry** = primarily oriented toward facilitating authorized traffic flows
  - **Frontier Border** = primarily oriented toward preventing unauthorized traffic flows
- **METRIC** = increasing the likelihood that intended operations at borders continue

WHAT: Performance Requirements



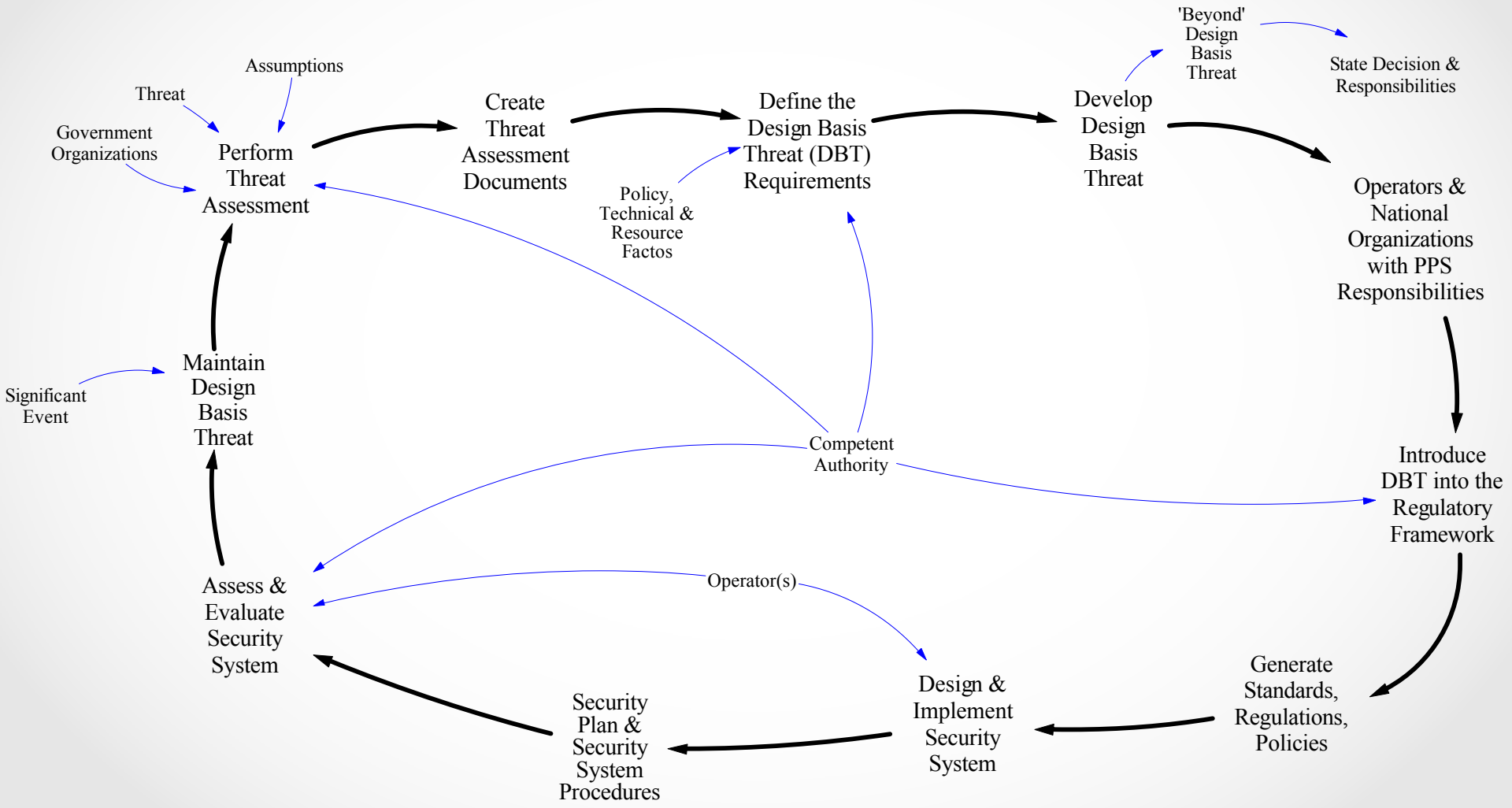
- Generate performance requirements
  - '***What*** do I need to do?'
- Requirements are **standards of behavior** that are **measured** against metrics to indicate **how well** the **objective** is being met
- Example performance requirements:
  - Design basis threat
  - Physical border security systems
  - Border security functions (surveillance/screening, detection/inspection, response, disposition)

Requirements: Design Basis Threat

- Design Basis Threat (DBT)
  - Based on INFCIRC 225/Rev5 & extensive use on physical security for nuclear facilities
  - Attributes of adversaries who might attempt to inflict undesirable consequences on or by exploiting **POE** or **OB**

- Benefits of measuring the **threat mitigation** metric with a DBT:
  - Justifying security decisions/costs
  - Assisting in the design of the border security system
  - Assisting in evaluating the border security system
  - Identifying responsibilities
  - Identifying vulnerabilities/countermeasures

Requirements: Design Basis Threat

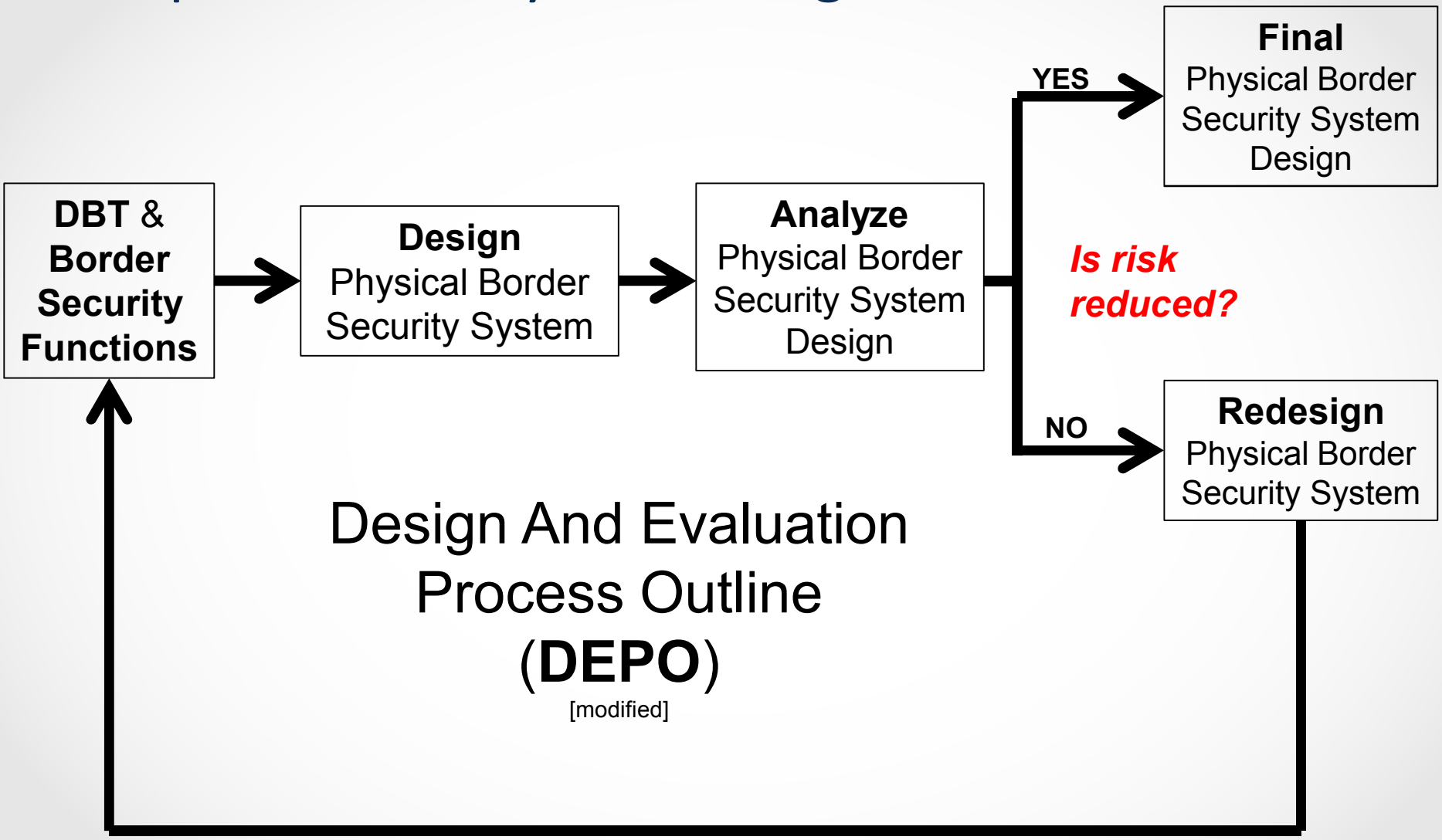


Requirements: System Design

- Physical border security system design
  - Should include technologies **AND** personnel **AND** procedures
  - Should be informed by other performance requirements

- Benefits of measuring the **risk reduction** metric with a physical border security systems:
  - Identifying opportunities of potential adversary exploitation
  - Designing countermeasures/defenses
  - Implementing actions that are under control of border stakeholders
  - Minimizing or eliminating opportunities for sabotage, smuggling and/or infiltration

Requirements: System Design



Design And Evaluation Process Outline (**DEPO**)

[modified]

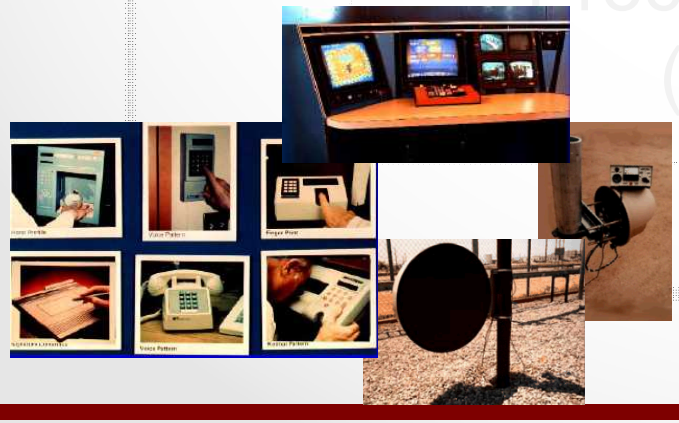
Requirements: System Design

Design
Physical Border Security System

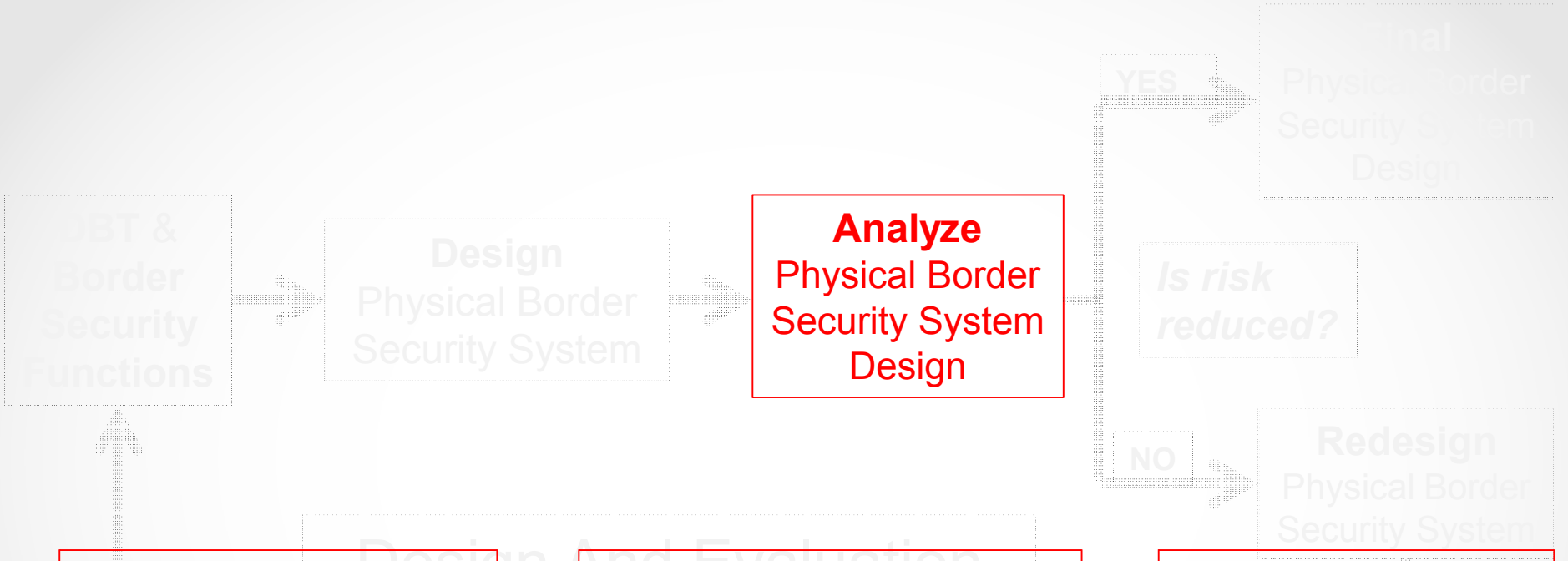
DETECTION

DELAY

RESPONSE



Requirements: System Design



Functional Type Test

- Do the components function as designed?
- Do subsystems complete desired **function**?

Performance Type Test

- Do the subsystems interact as designed?
- Does entire system meet **performance requirements**?

System Type Test

- Does the system perform as designed?
- Does entire system meet **support objective**?

Requirements: Security Functions

- Border security functions
  - Behaviors that occur as part of normal daily activities that have security utility
  - Should not **interfere** with intended **POE** or **OB operations**

- Benefits of measuring the **objective assurance** metric with border security functions:
  - Identifying leverage points of normal activity to support security
  - Minimizing (potential) contradictory operational & security behaviors
  - Emphasizing actions that are under control of border stakeholders
  - Justifying security decisions/costs

Requirements: Security Functions

- **Ports of Entry**
  - Context
    - Fixed entry points
    - Facilitating authorized traffic flows
  - Primary Functions
    - Surveillance/screening
    - Detection/inspection
    - Response
    - Disposition


Detection Portals

Package Scanners


Metal Detectors


Vehicle Inspection Technologies


X-Ray Scanners


Radiation Detectors


Fiber Optic Inspection Tools


Handheld Contraband Detection Equipment

Requirements: Security Functions

- **Frontier Border**
  - Context
    - Non-fixed, continuous entry points
    - Preventing unauthorized traffic flows
  - Primary Functions
    - Surveillance/screening
    - Detection/inspection
    - Response
    - Disposition


Ground Surveillance Radars


Cameras/Sensors


Seismic Sensors


Buried Fiber Optic Sensors

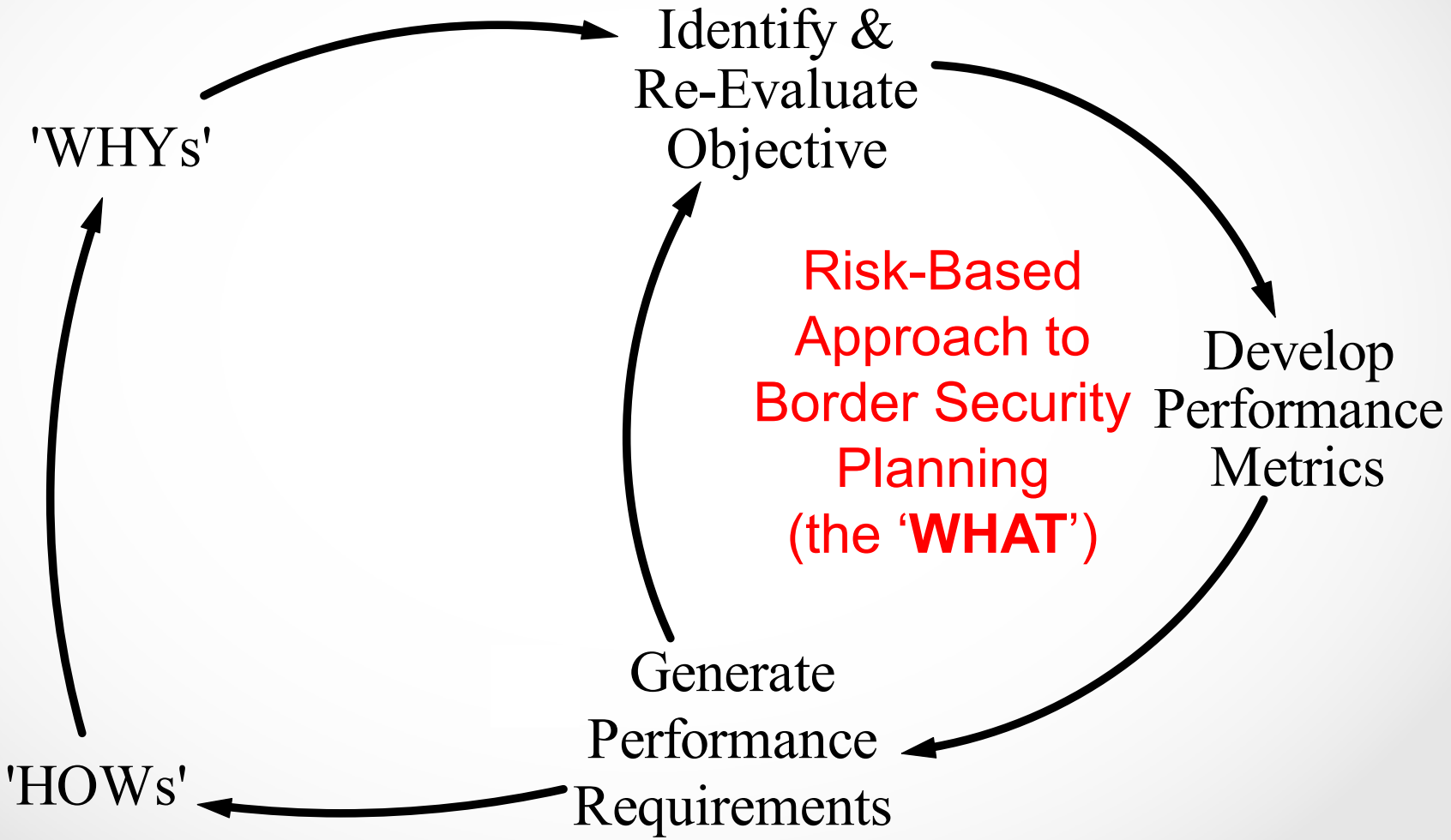

Magnetic Sensors


Mobile Sensor Platforms


Sensor Towers

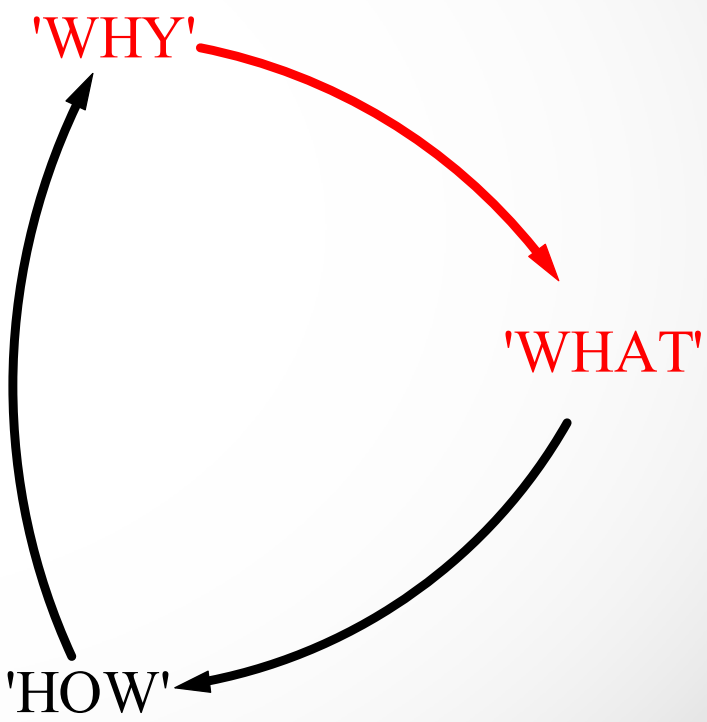

Aerial/Satellite Remote Sensing

Border Security: WHAT?



From ‘What’ to ‘How’

- Now that we know the ‘what’…
- HOW do we do border security?
  - [discussion question for participants]



Border Security: 'HOW?'

- Border security design features = '***how*** do I do it?'
  - The following lectures will introduce some of the specific tools available to 'do' border security

- These include:

  - ***People***: 'The Role of Interagency Collaboration and Personnel Development: Customs, Police, Military, Immigration'
    - by Eng. Alan Runyan-Beeb

  - ***Technology***: 'Augmenting Personnel with Technology'
    - by Eng. Alan Runyan-Beebe & Mr. Al-Sharif Nasser Bin Nasser

  - ***Programs***: 'Nuclear Detection Architectures and Border Security'
    - by Dr. Ben Bonin

Conclusions

- Risk-Based Approach to Border Security Planning
  - Identify **objective** = '***What*** am I trying to do?'
    - Includes **wanted** and **unwanted** actions
  - Develop **performance metrics** = '***What*** is the evidence of what I'm trying to do?'
    - Threat mitigation, risk reduction &/or objective assurance
  - Generate **performance requirements** = '***What*** do I need to do?'
    - Design basis threat, system design &/or border security functions