SAND2008-1818C

A Concept of Operations to Ensure System-Level Survivability and Recovery

Ben Cook
Sandia National Laboratories

4th Annual I3P PCS Security Workshop
March 6, 2008

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

System Survivability

- What is system-level survivability and why is it important?

- What can you do today to make your operations more resilient to a cyber disruption?

- What is ROBUST and how will it help your company in the future?

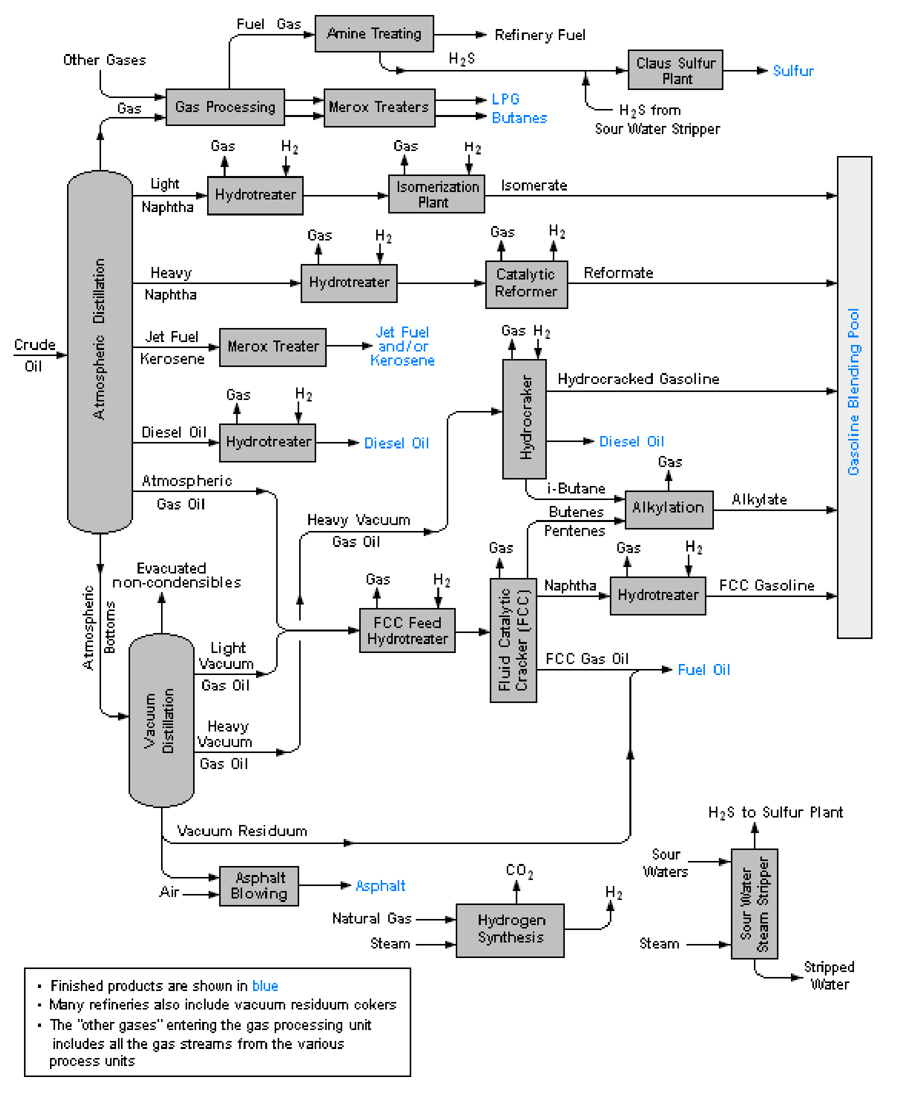
What is Survivability?

- Capability of a system to fulfill its mission in a timely manner, even in the presence of a *natural* or *man-made* disturbance
  - What should be engineered to survive a cyber disruption: your PCS or your operations?
- Survivability is more than fault tolerance and security
  - Withstand both natural failures and attacks

Why is Survivability Important?

- Cyber disruptions are inevitable risks that must be managed
  - Threats are evolving, vulnerabilities are difficult to determine and eliminate, consequences from disruptions can be severe
- To be effective, systems approach required rather than an *ad hoc* application of point solutions and procedures

Putting Survivability in Context



- Finished products are shown in blue
- Many refineries also include vacuum residuum cokers
- The "other gases" entering the gas processing unit includes all the gas streams from the various process units

Refinery Operations

Basic Objectives

- Safety
- Compliance
- Production and Profit
  - Produce Finished Products
    - Market Driven
    - Depends on Feedstocks
    - Meet Specifications
  - Minimize Side Products
    - Disposal Costs
    - Impacts Profits

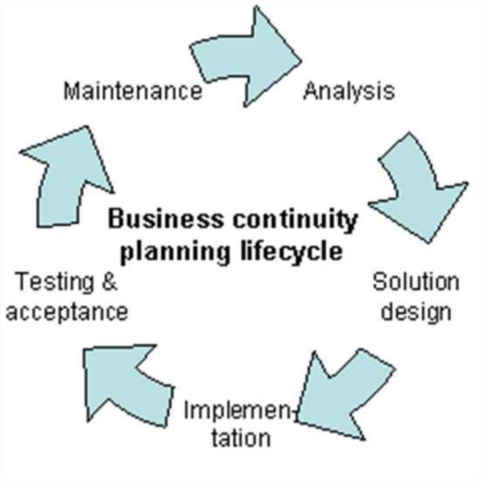
Achieving Survivability

- How can the operational and business impacts of a cyber disruption be minimized?
  - What are the operationally essential control systems functions/services that must be maintained?
  - What steps should be taken – e.g. security measures – to harden these functions against disruptions?
  - What are the indicators and warnings of a potential disruption of these services?
  - Given a certain disruption, what response is most likely to contain the disruption and minimize impacts?

Survivability Not Just Technology

- Work within existing risk management and business continuity methodologies to frame your approach and design a solution
  - Assess risk exposure
  - Design and deploy defenses
  - Build resilience
  - Test and train

Perform vulnerability evaluation and business impact assessment



Develop mitigation and contingency strategies, design and develop BCP

Keep plan updated and assure effectiveness through drills

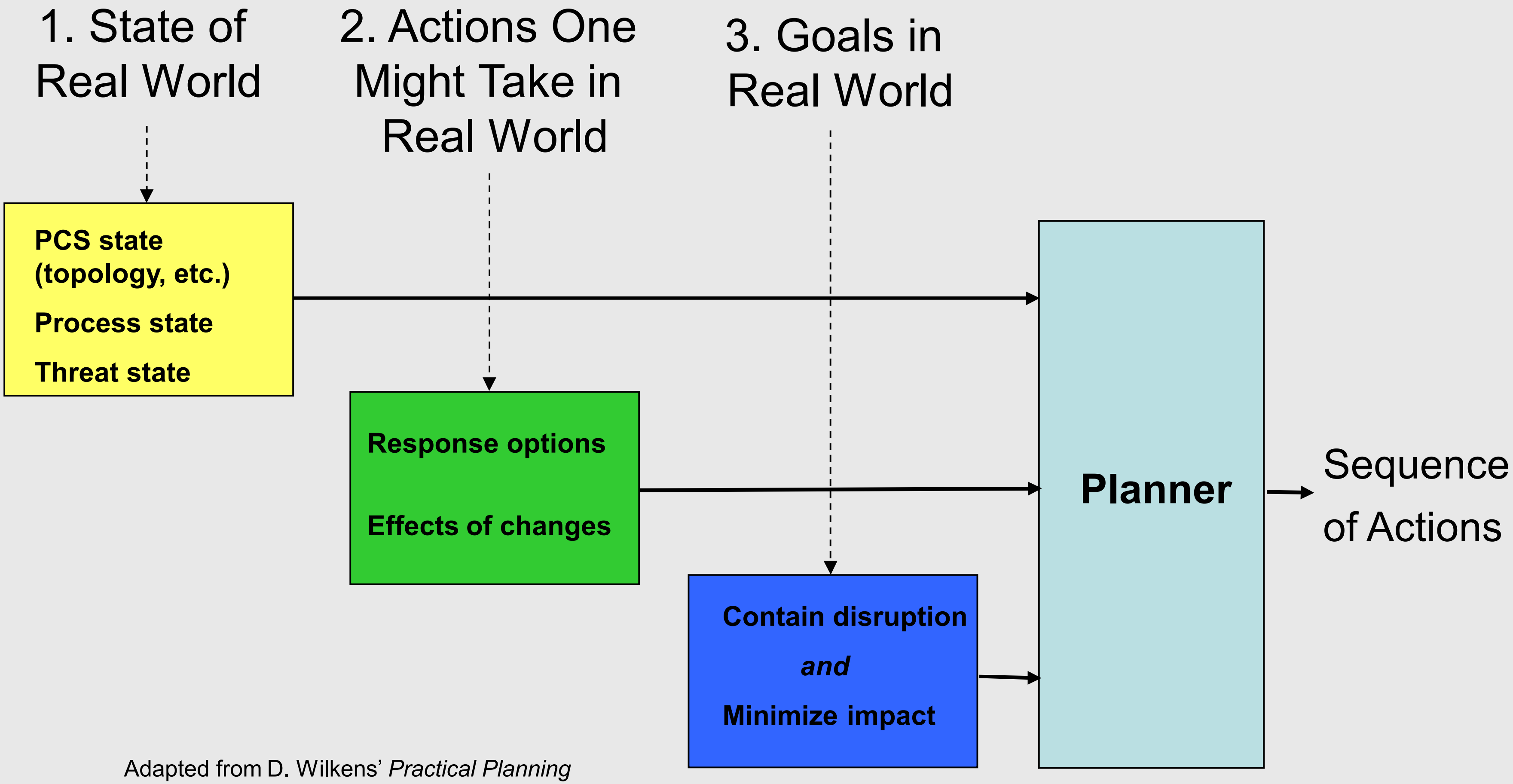
Implement plan, generate awareness, train responders

The Future of Survivability: ROBUST

- Formalizing methodology and codifying it in an response planning tool called ROBUST[1]
- Implementing ROBUST prototype and validating it with disruption scenarios on Sandia test bed
- Developing knowledgebase and hands-on demonstration for next workshop

[1] Resilient Operations Back-Up STrategizer

Response as a Planning Problem



1. State of Real World

2. Actions One Might Take in Real World

3. Goals in Real World

PCS state (topology, etc.)

Process state

Threat state

Response options

Effects of changes

Contain disruption

and

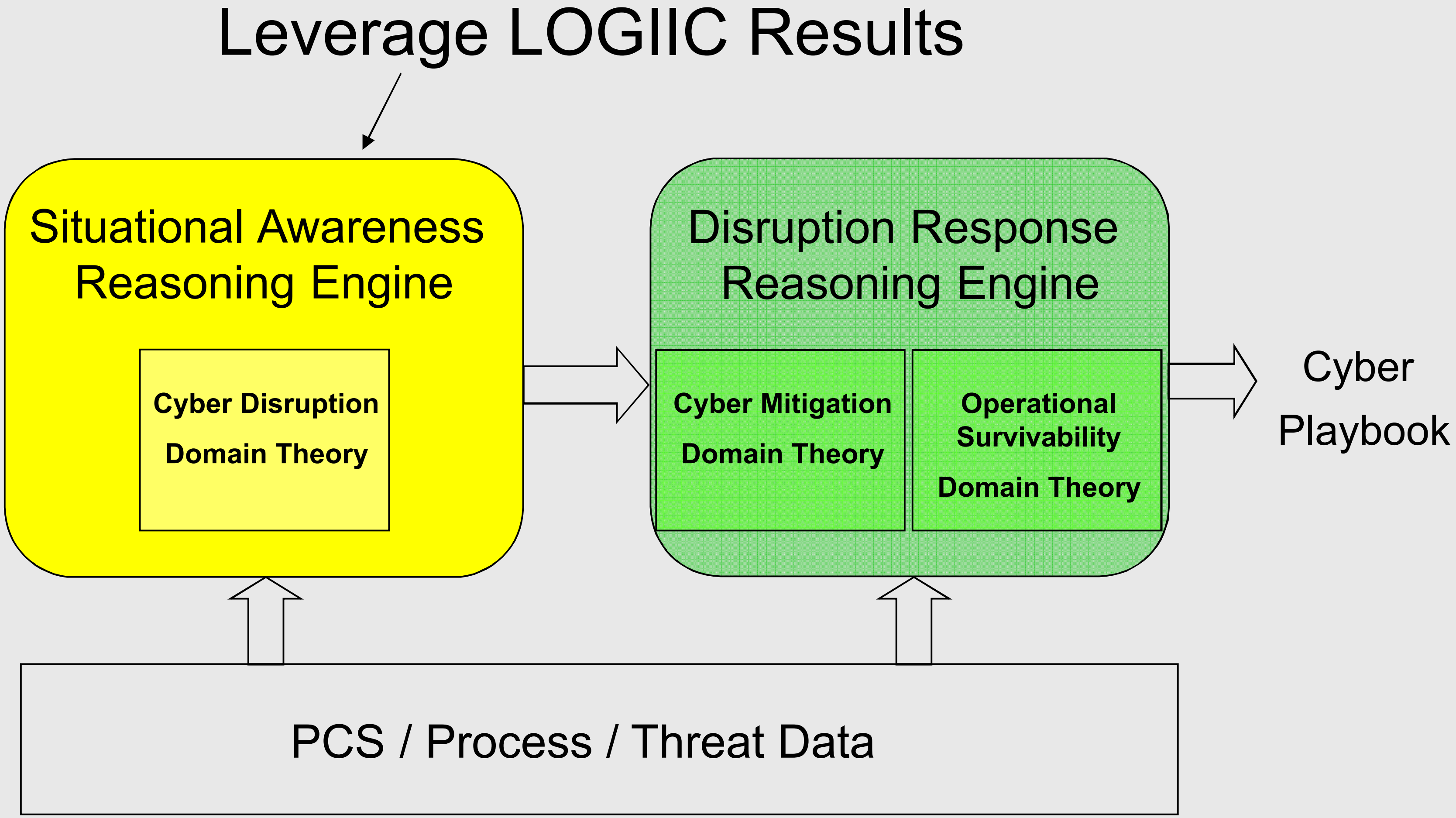
Minimize impact

Planner

Sequence of Actions

Adapted from D. Wilkens' *Practical Planning*

ROBUST Analysis Framework


Leverage LOGIIC Results

Situational Awareness Reasoning Engine

Cyber Disruption Domain Theory

Disruption Response Reasoning Engine

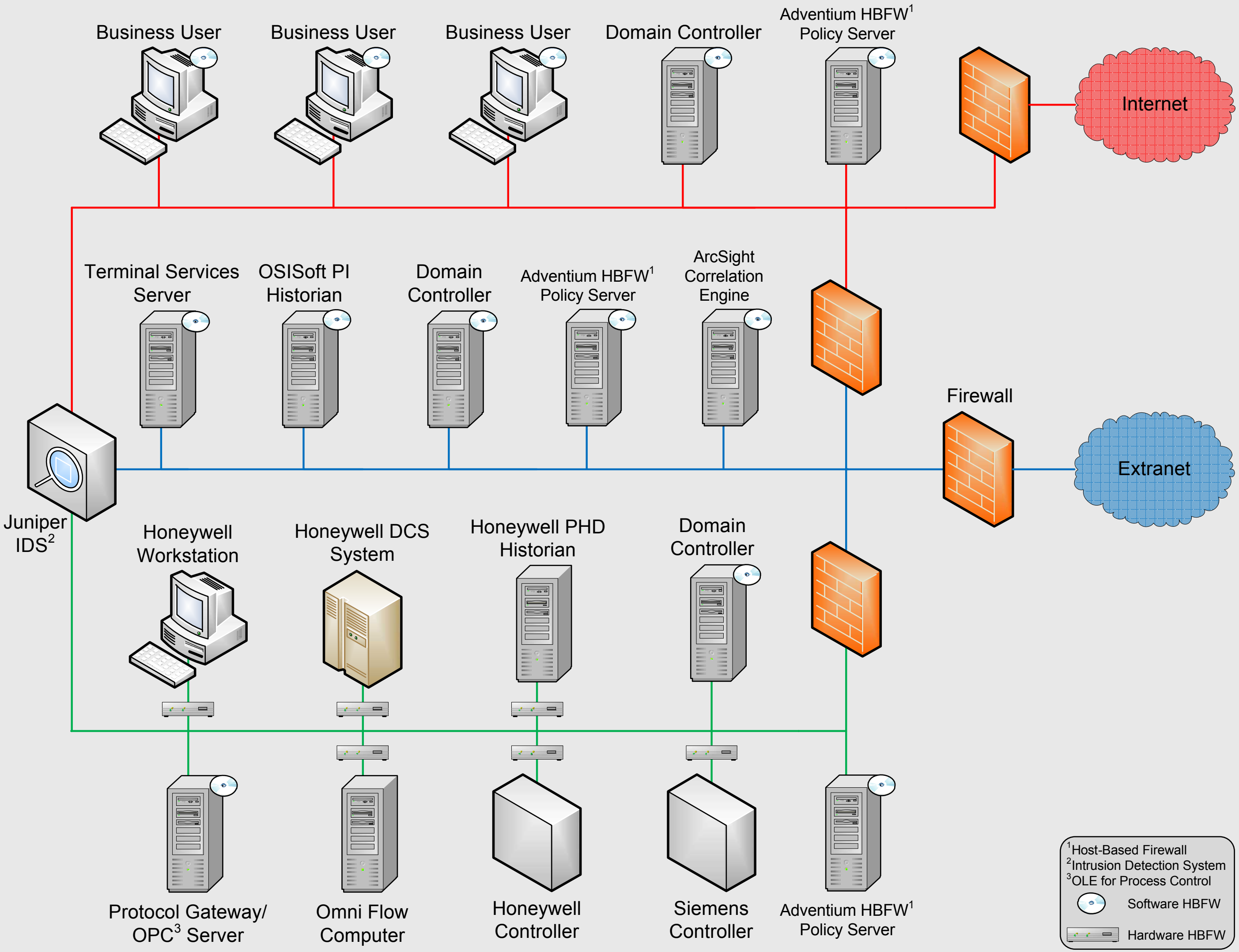
Cyber Mitigation Domain Theory

Operational Survivability Domain Theory

Cyber Playbook

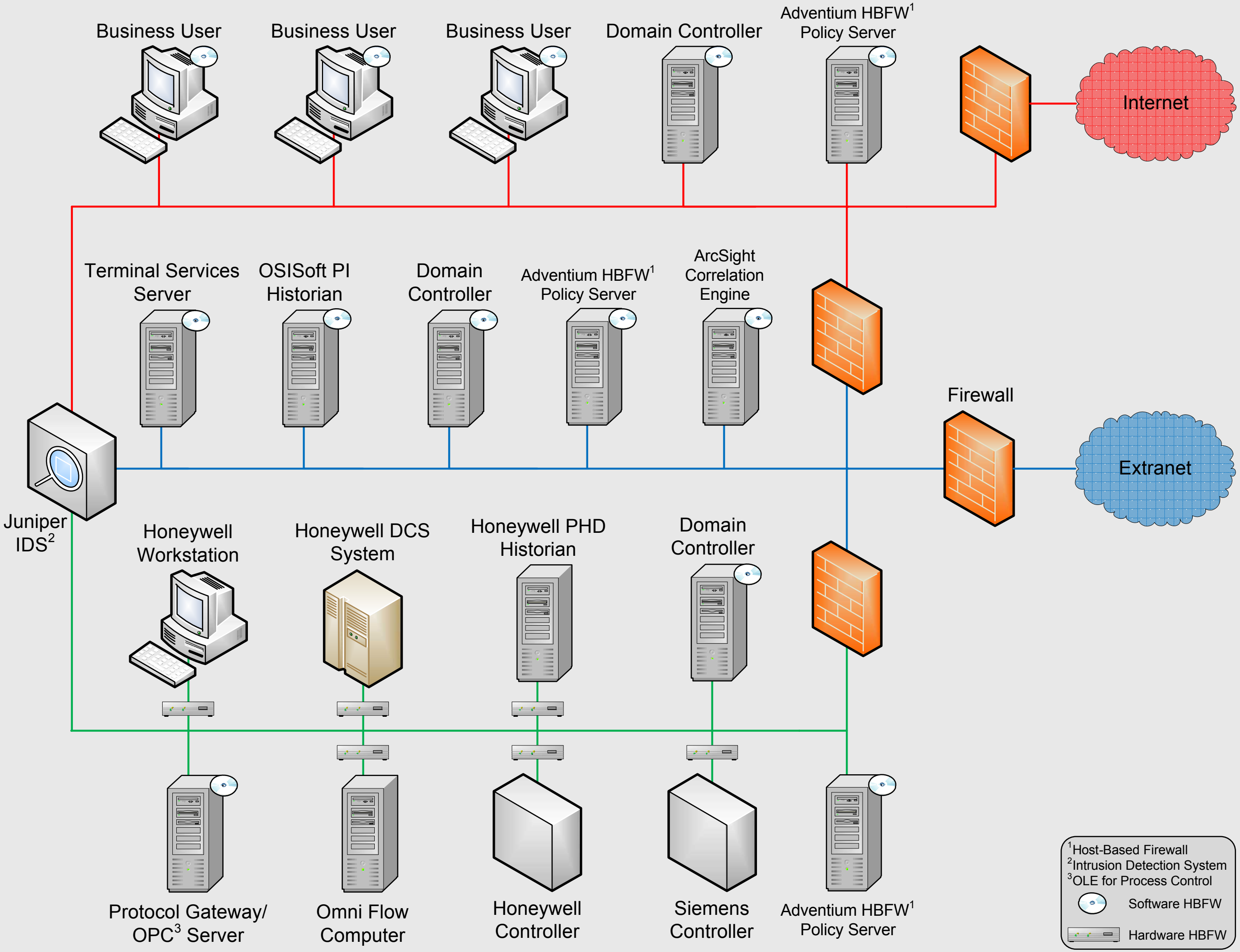
PCS / Process / Threat Data

Start with Defense-In-Depth



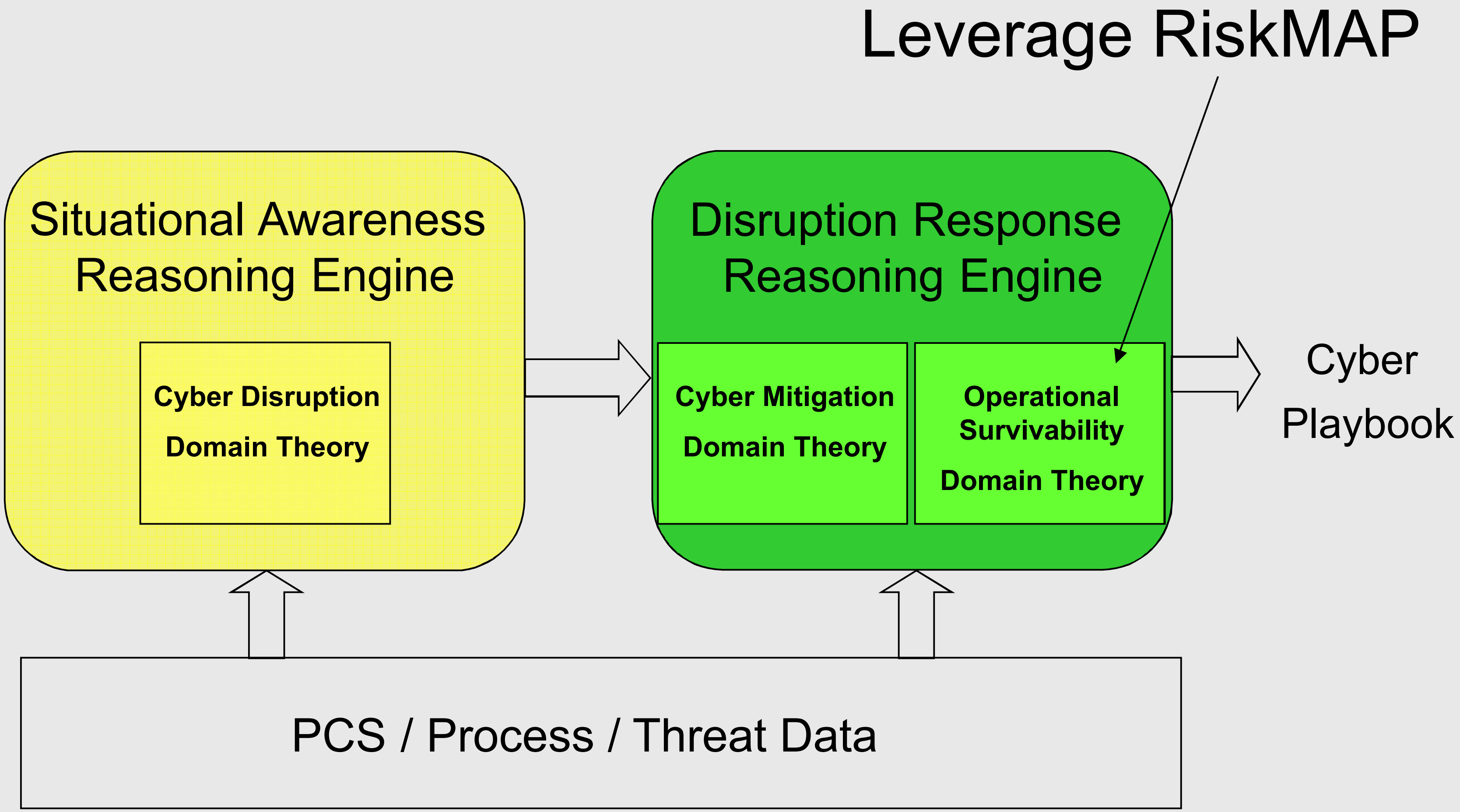
[1] Host-Based Firewall
[2] Intrusion Detection System
[3] OLE for Process Control

Achieve Situational Awareness Through Correlation



[1] Host-Based Firewall
[2] Intrusion Detection System
[3] OLE for Process Control

ROBUST Analysis Framework

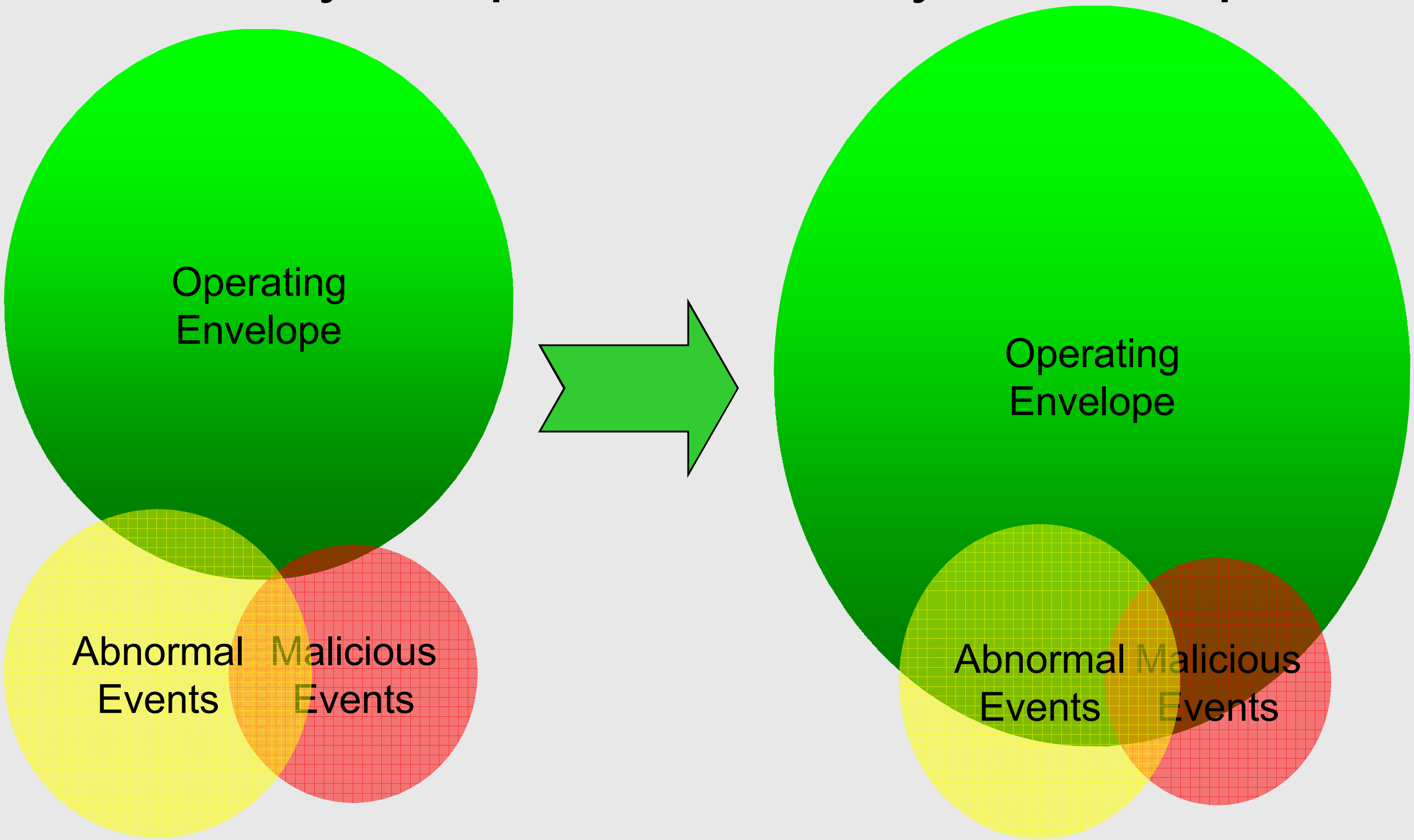

Leverage RiskMAP
Situational Awareness Reasoning Engine
Cyber Disruption Domain Theory
Disruption Response Reasoning Engine
Cyber Mitigation Domain Theory
Operational Survivability Domain Theory
Cyber Playbook
PCS / Process / Threat Data

What’s Unique?

- Research in control system security to date has focused on prevention (best practices, etc.) and detection
- This thrust is currently the only funded systems research in survivability
- Sandia is building on previous work in LOGIIC, which looked solely at situational awareness (no response component)
- Project will leverage other I3P thrusts like MITRE’s RiskMAP, Tulsa’s SecSS, and UIUC’s APT

Benefits of ROBUST

Integrated approach and planning tool to ensure continuity of operations to cyber disruptions



What can I do today?

- Come to Sandia booth this afternoon
  - Find out more about ROBUST
  - Share your ideas
  - Hear about API 1164
- Employ methodologies such as defense-in-depth
- Consider business continuity planning
- Review standards and guidelines available today
- Leverage past research products
- Get involved in ongoing research activities

Resources

More Information

- Contact Ben Cook (bkcook@sandia.gov) or Annie McIntyre (amcinty@sandia.gov) at Sandia National Laboratories
- I3P Risk Characterization Report (https://www.thei3p.org/repository/researchrepo9.pdf)
- Sandia Sustainable Security Report (http://www.sandia.gov/scada/documents/SustainableSecurity.pdf)
- DHS LOGIIC Correlation Project (www.logiic.org)

Available Elsewhere

- NIST special pubs (http://csrc.nist.gov/publications/PubsSPs.html)
  - 800-82 Guide to ICS Security
  - 800-53 Recommended Security Controls for Federal Info Systems
  - 800-61 Incident Handling Guide
  - 800-97 Establishing Wireless Robust Security Networks: IEEE 802.11i
- SCADA Security: Advice for CEOS (http://www.wurldtech.com/library/pdf/SCADA%20Security%20Advice%20for%20CEO's.pdf)
- CPNI British guidelines (www.cpni.gov.uk/ProtectingYourAssets/scada.aspx)
- Business Continuity Planning
  - Business Continuity Institute (www.thebci.org)
  - Disaster Recovery Institute (www.drii.org)