



# Virtual Vulnerability Modeling for Spacecraft Ground Systems

**GSAW 2002**

**Peter In\*, Steve Liu\*, Scott Pool\*\*, Sung-Oh Jung\***

**\* Dept. of Computer Science**

**\*\* Dept. of Speech Communication**

**Texas A&M University**

**College Station, TX 77843-3112**



# V<sup>2</sup>\* Modeling Overview

- ◆ **Motivation and Challenges**
- ◆ **Virtual Vulnerability Modeling**
- ◆ **Preliminary Results: Security Risk Assessment**
- ◆ **Expected Contributions**

\* V<sup>2</sup>: *Virtual Vulnerability*



# Motivation: Virtual Vulnerability ( $V^2$ )

## – Definition and characteristics

- Security breaching caused by malicious remote software attacks
  - Technologies plus user misbehavior
- Continuous process, not one time event
- Not standalone defense, but coordinated group defense

## – Needs

- Quantified, scientific methodologies for understanding the nature and costs of  $V^2$



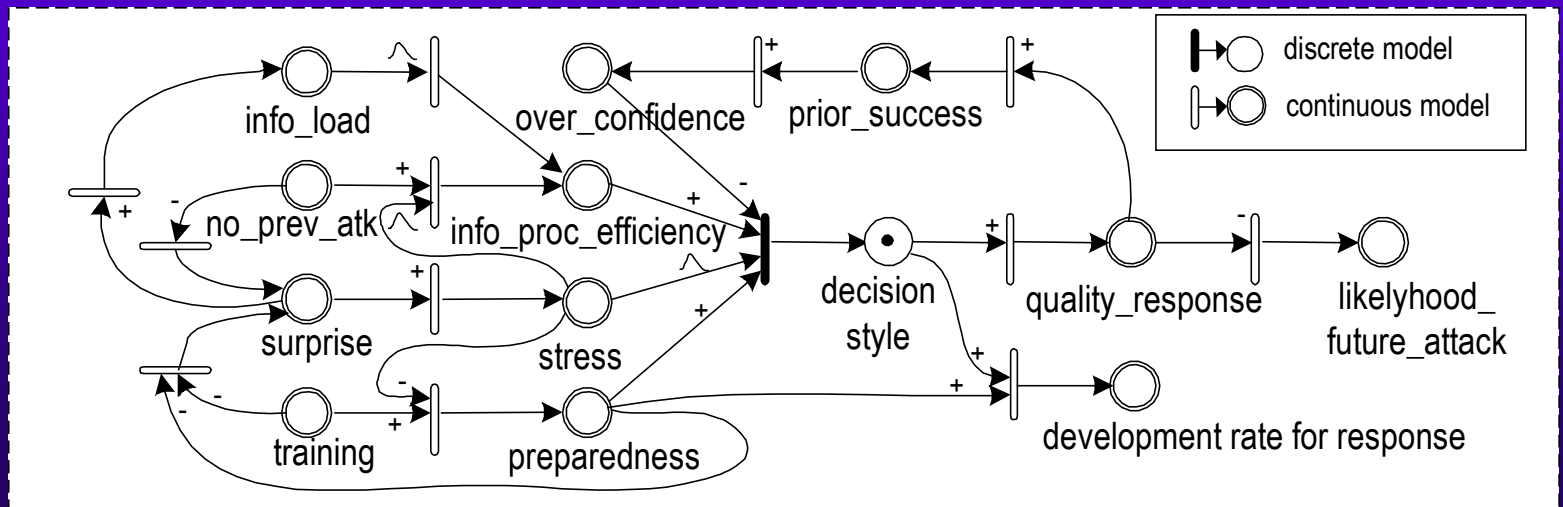
# Challenges

- ◆ Integrated Man-Machine Modeling
  - Group Behavior
  - Systems
- ◆  $V^2$  Economics
  - for Effective Response to  $V^2$  Attacks
- ◆ Group-Aware Secure Software Design



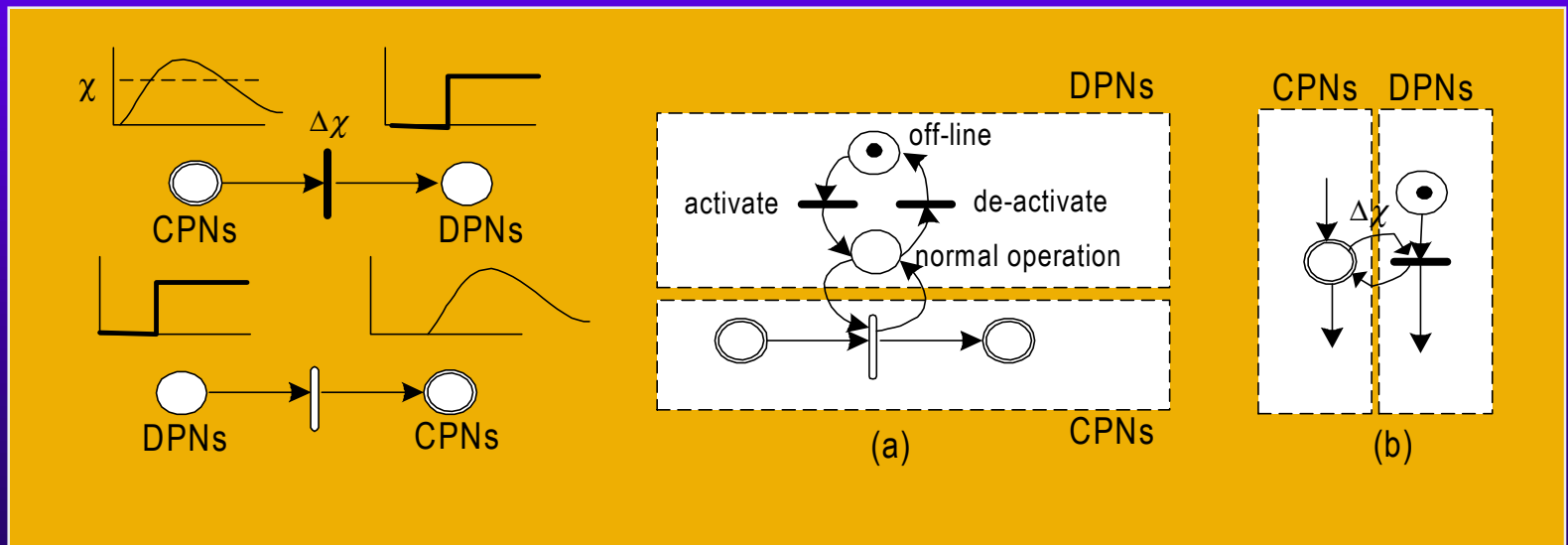
# Group Behavior Modeling

- ◆ Outcomes: quality\_response, response rates
- ◆ Decision Style: A key variable
  - Vigilant
  - Nonresponsiveness
  - Hypervigilance



# Hybrid Petri-Nets Simulation Modeling

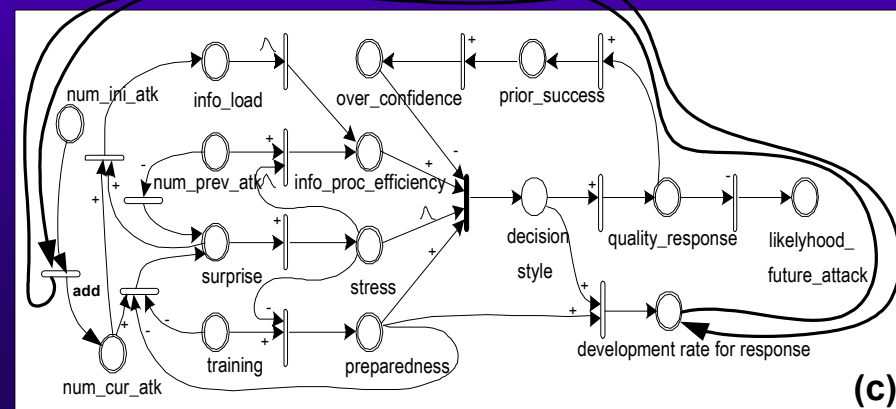
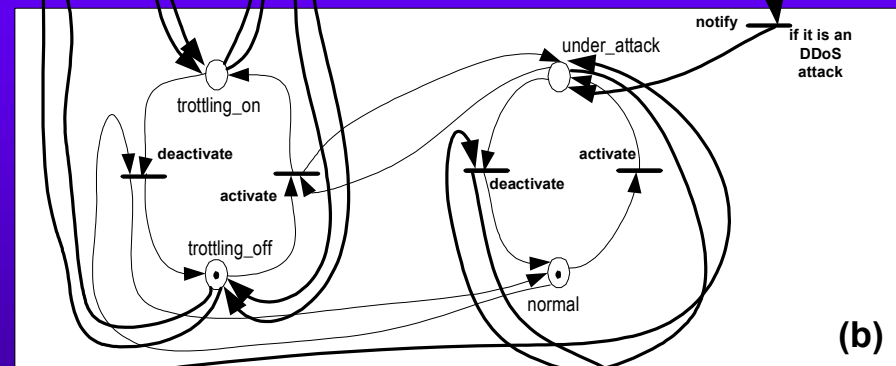
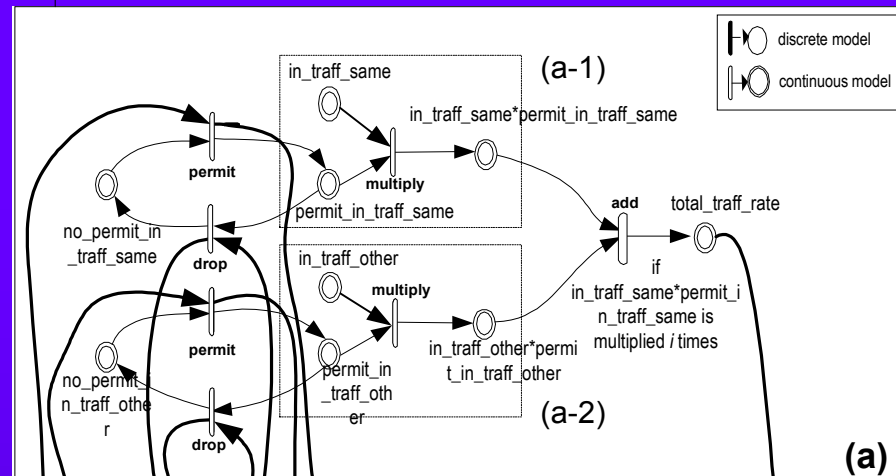
- ◆ Simulation of virtual warfare strategy
  - A human-machine simulation tool using a stochastic, continuous-discrete model approach





# DDoS: An Example

- ◆ Modeling monitoring, control, responses
- ◆ Interaction: a key for the modeling





# An Example on more detailed modeling

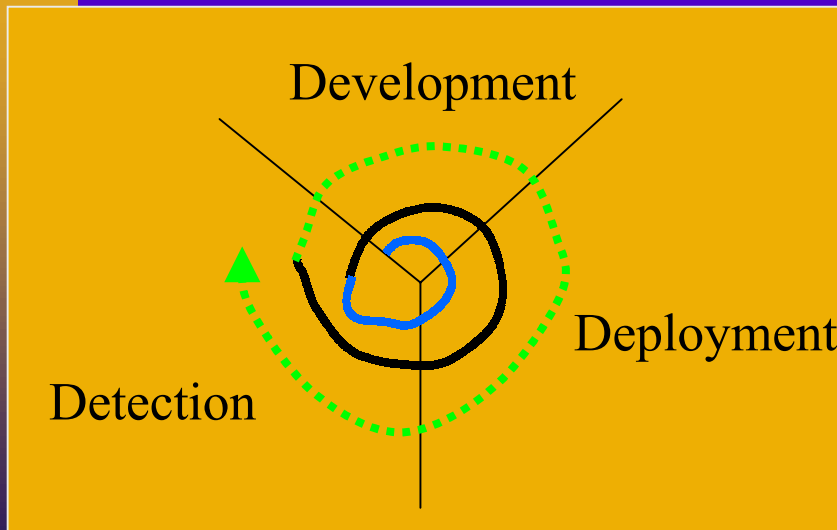
- ◆ Information security is difficult to measure
  - A risk “probability” means little to corporate management
  - How to allocate CSHR?
- ◆ Performance Measures
  - peak attack periods, expected system down time, etc
- ◆ Excellent for model development
  - Numerous technology factors
  - Massive stakeholders
    - developers, users, standards bodies, etc
  - Critical battlefield for every major IT company

# Life Cycle Model

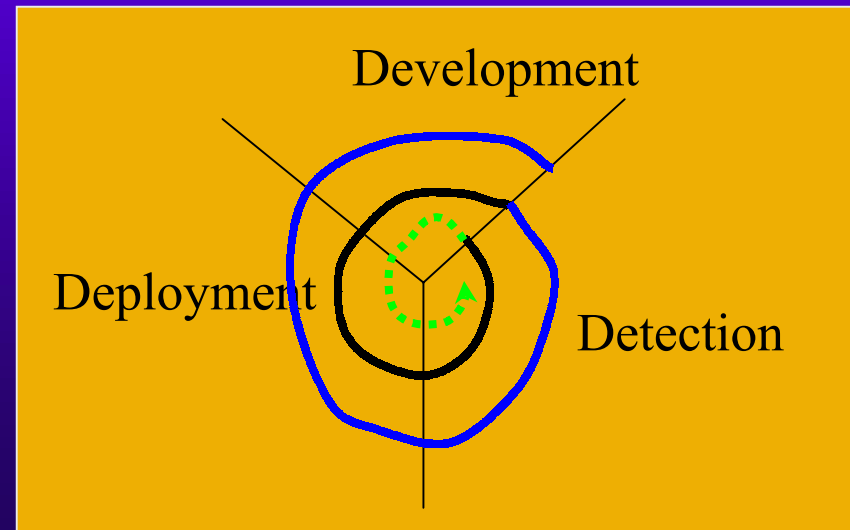
## ◆ life cycles

- $C_{\text{Defender}} = \{development, deployment, detection\}$
- $C_{\text{Attacker}} = \{development, deployment, attack\}$

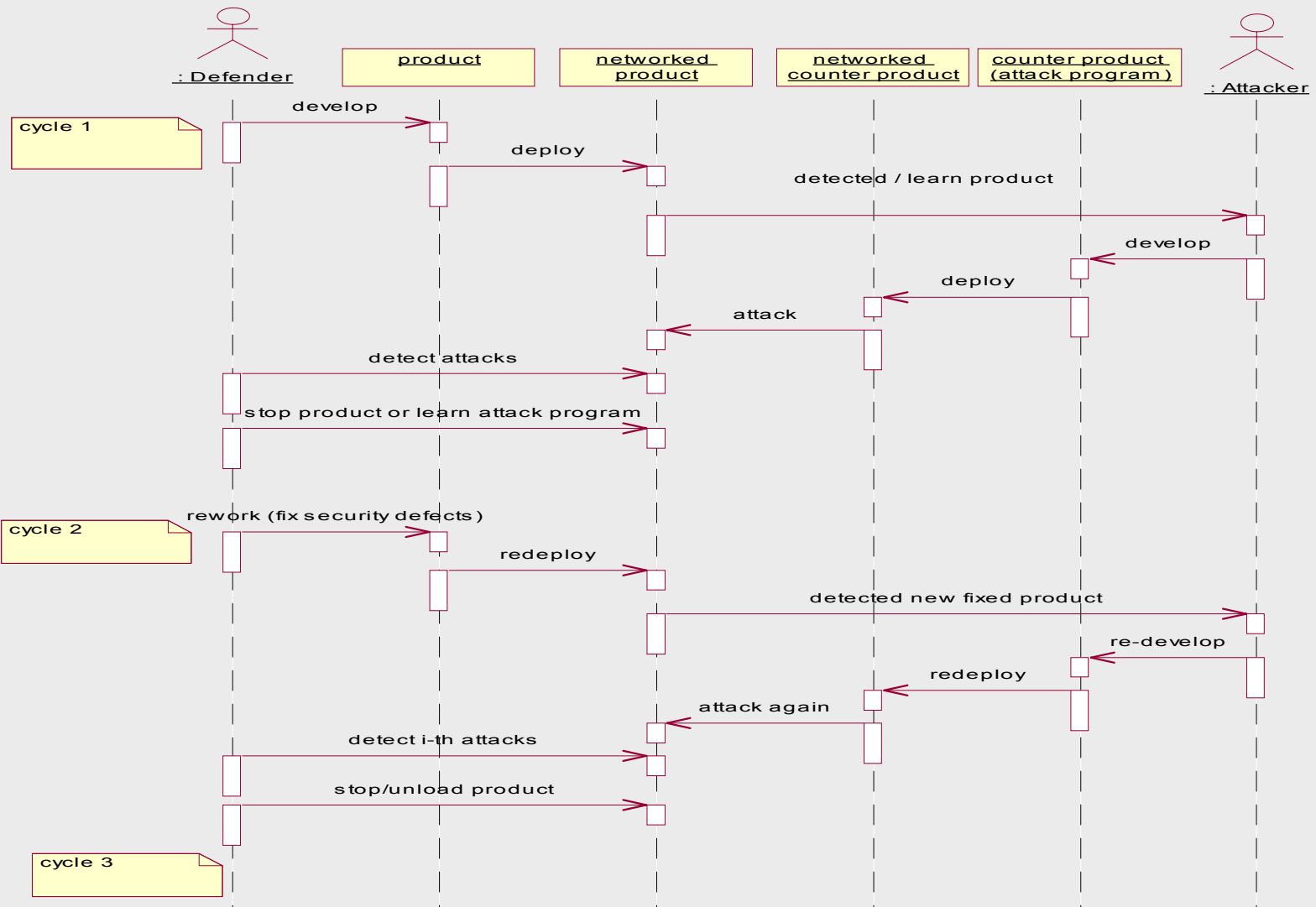
## Spiral



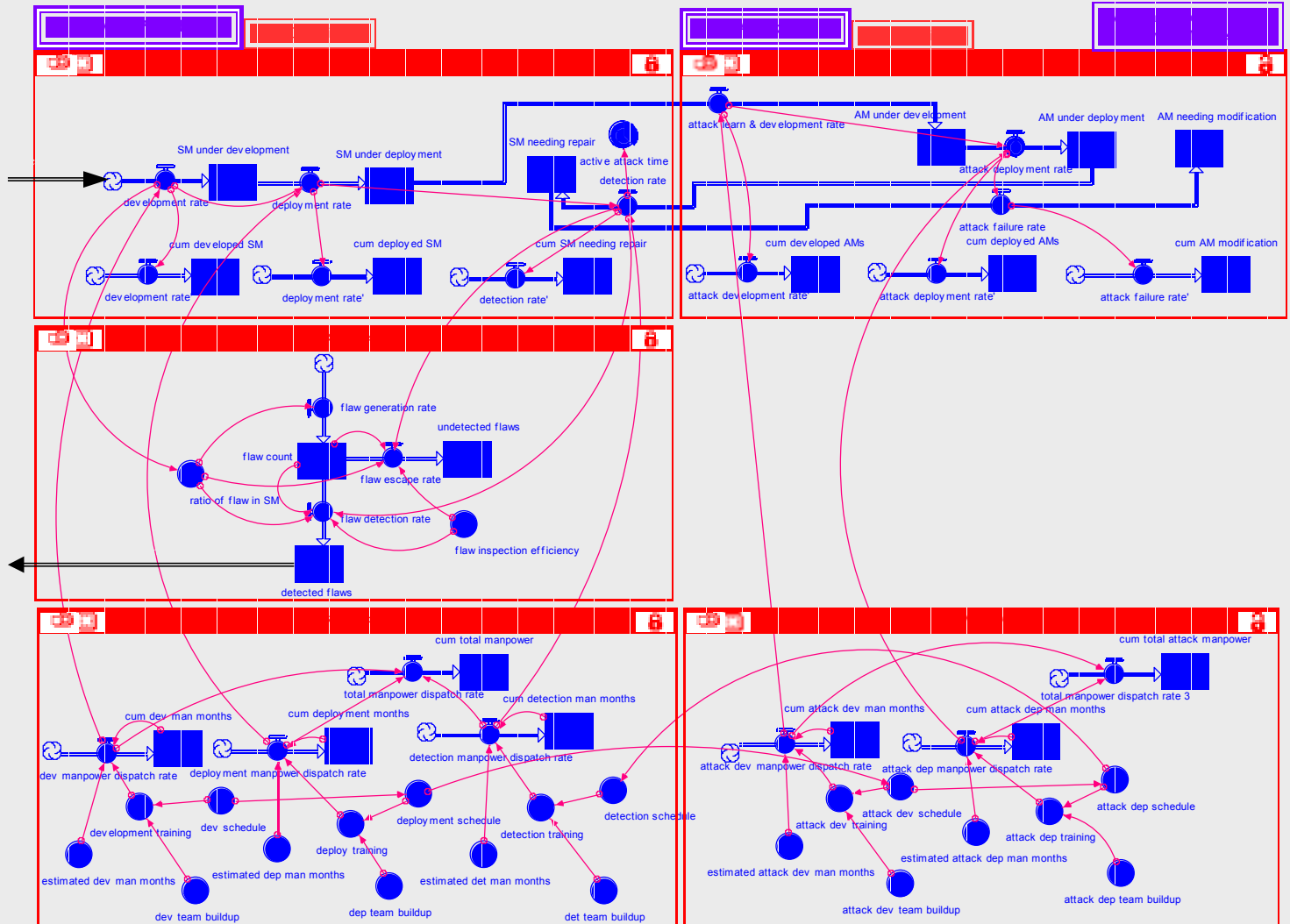
## Reverse-Spiral



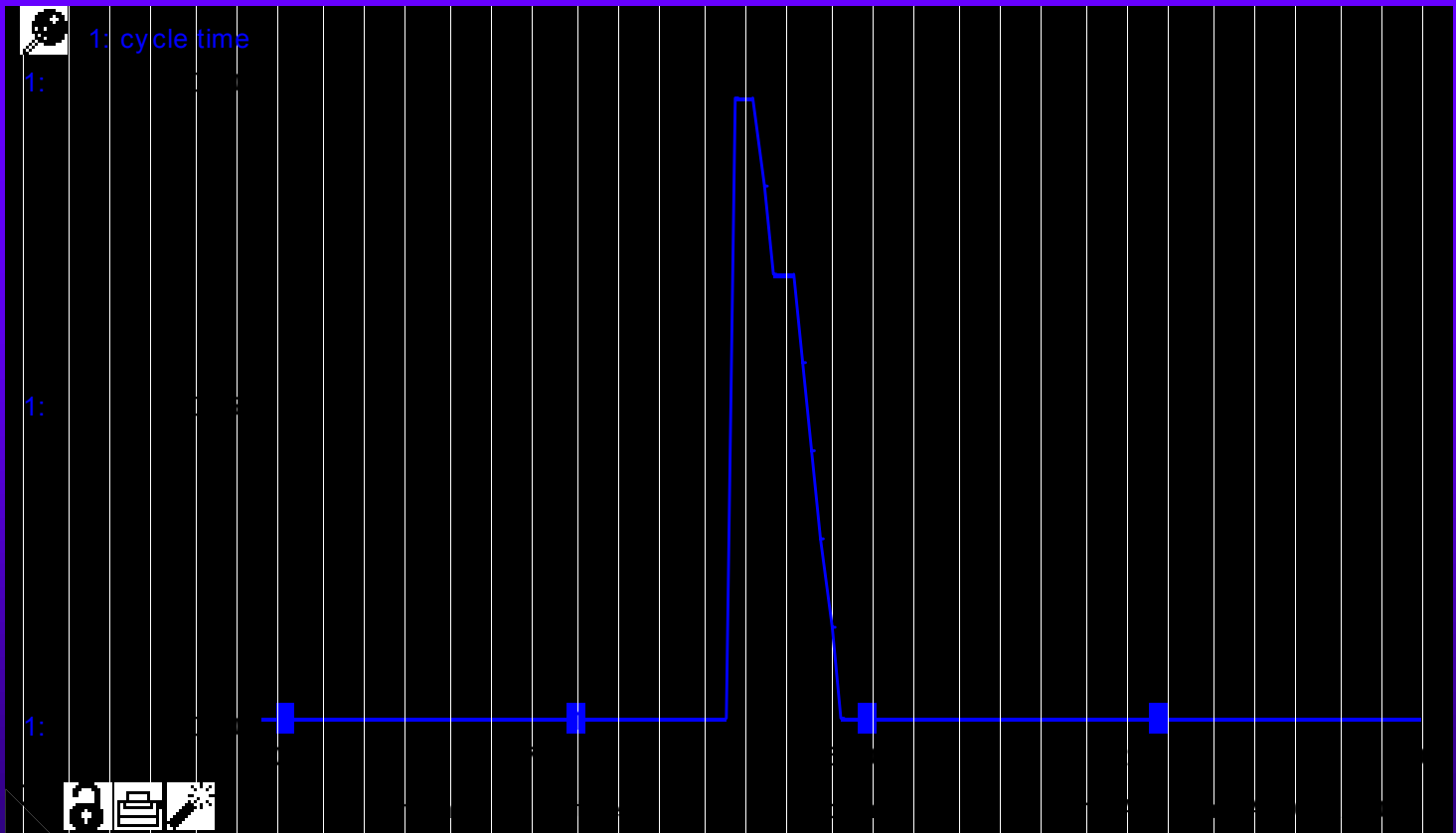
# Defense and Attack Interaction Model



# Simulation Modeling

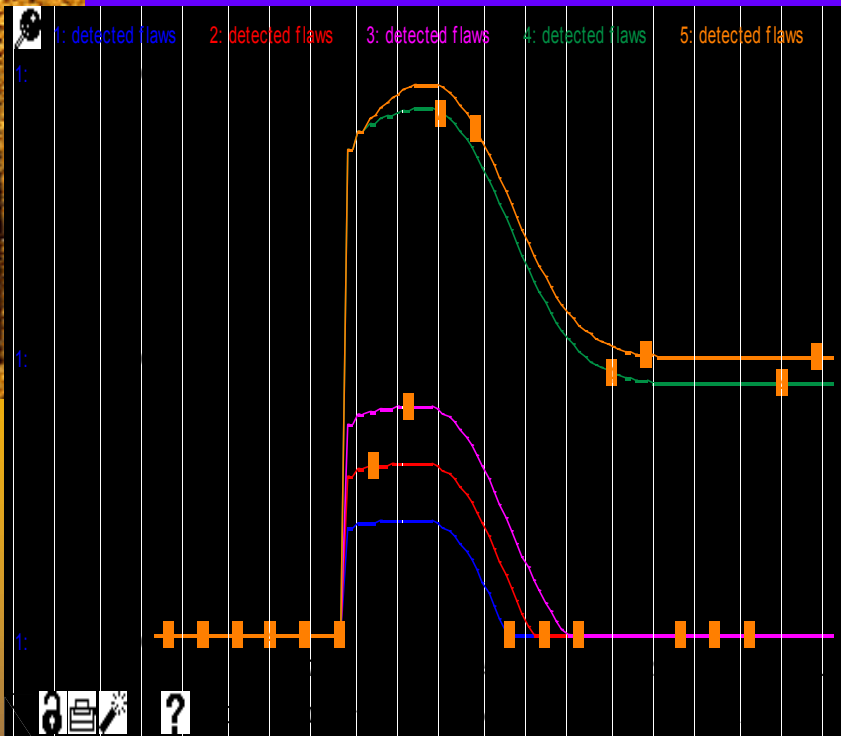


# Result 1: Active Attack Time



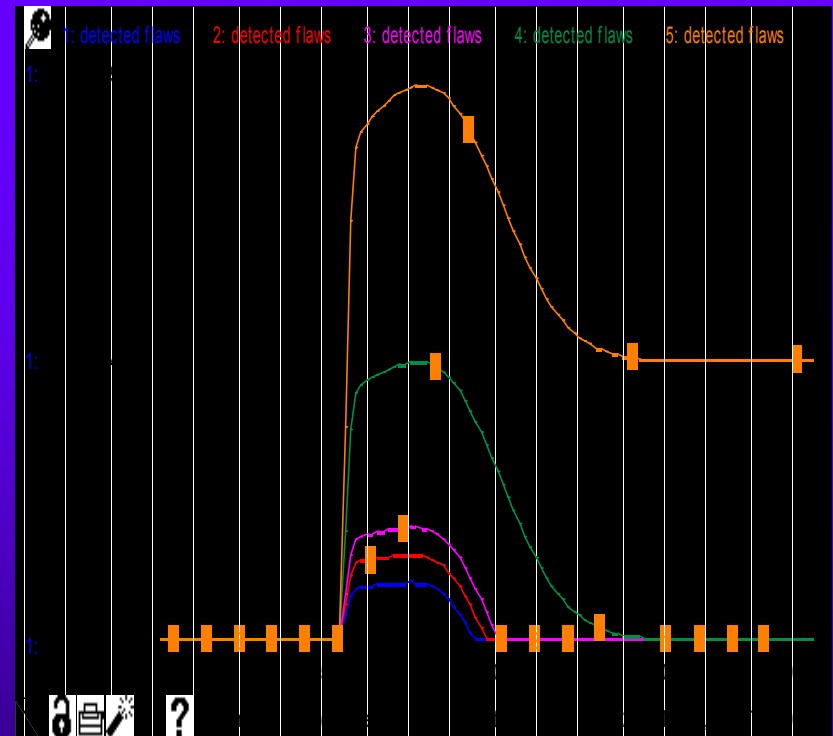
Active Attack Time (relevant to business loss) is defined  
From the time when the system begins to be attacked  
To the time when the attack is detected

# Result 2: Detection Rates vs. Flaw Inspection Efficiency



(a) Manpower of attack detection = 50

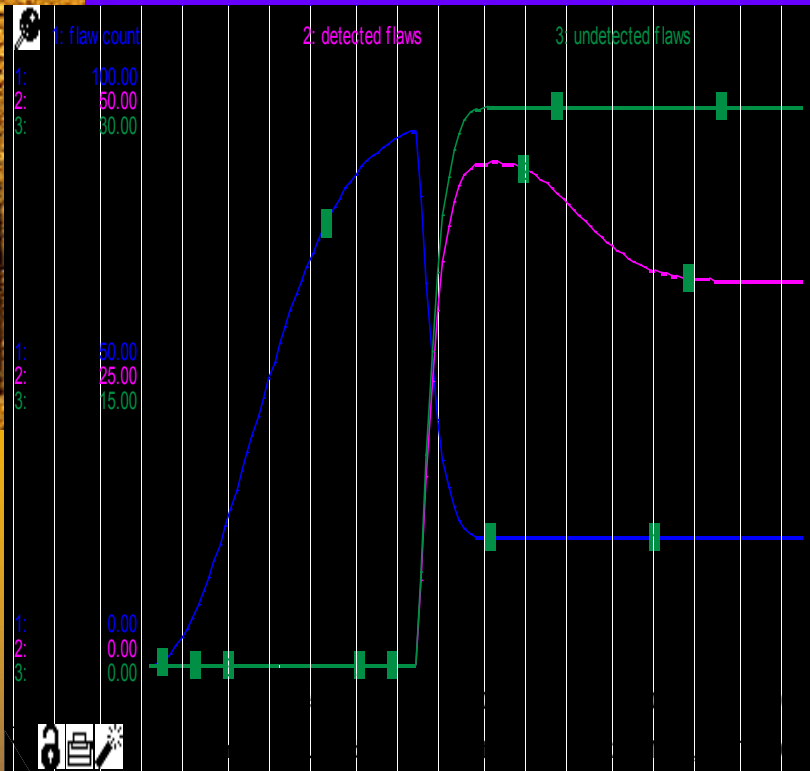
No further visible improvement can be observed if flaw inspection efficiency  $> 0.5$



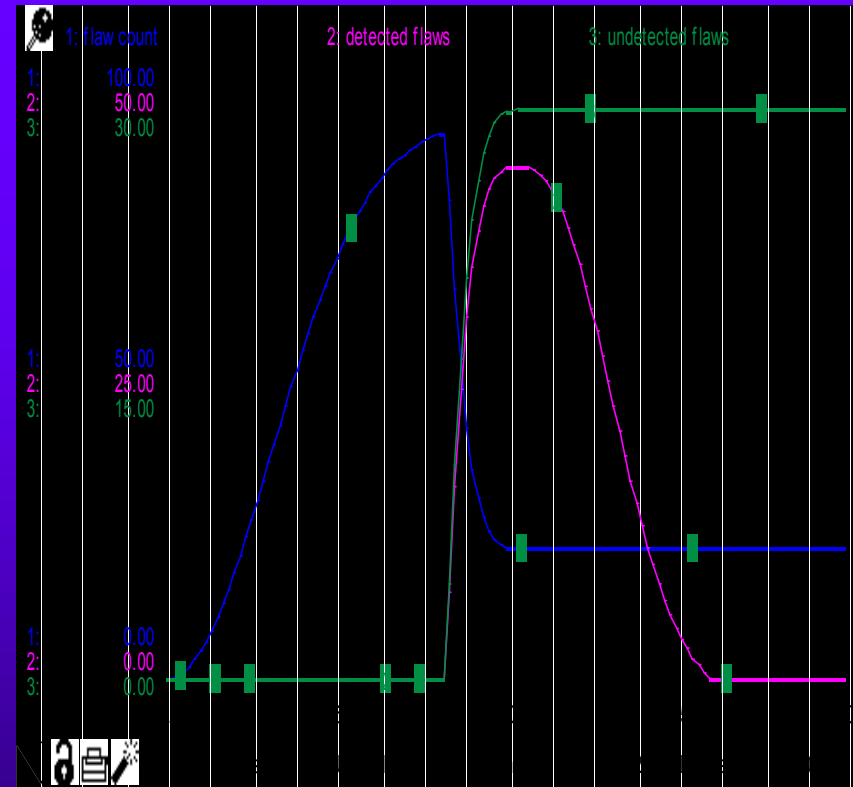
(b) Manpower of attack detection = 10

Zero flaw policy is effective if the manpower of attack detection is low.

# Result 3: Investment Level for Flaw Patching



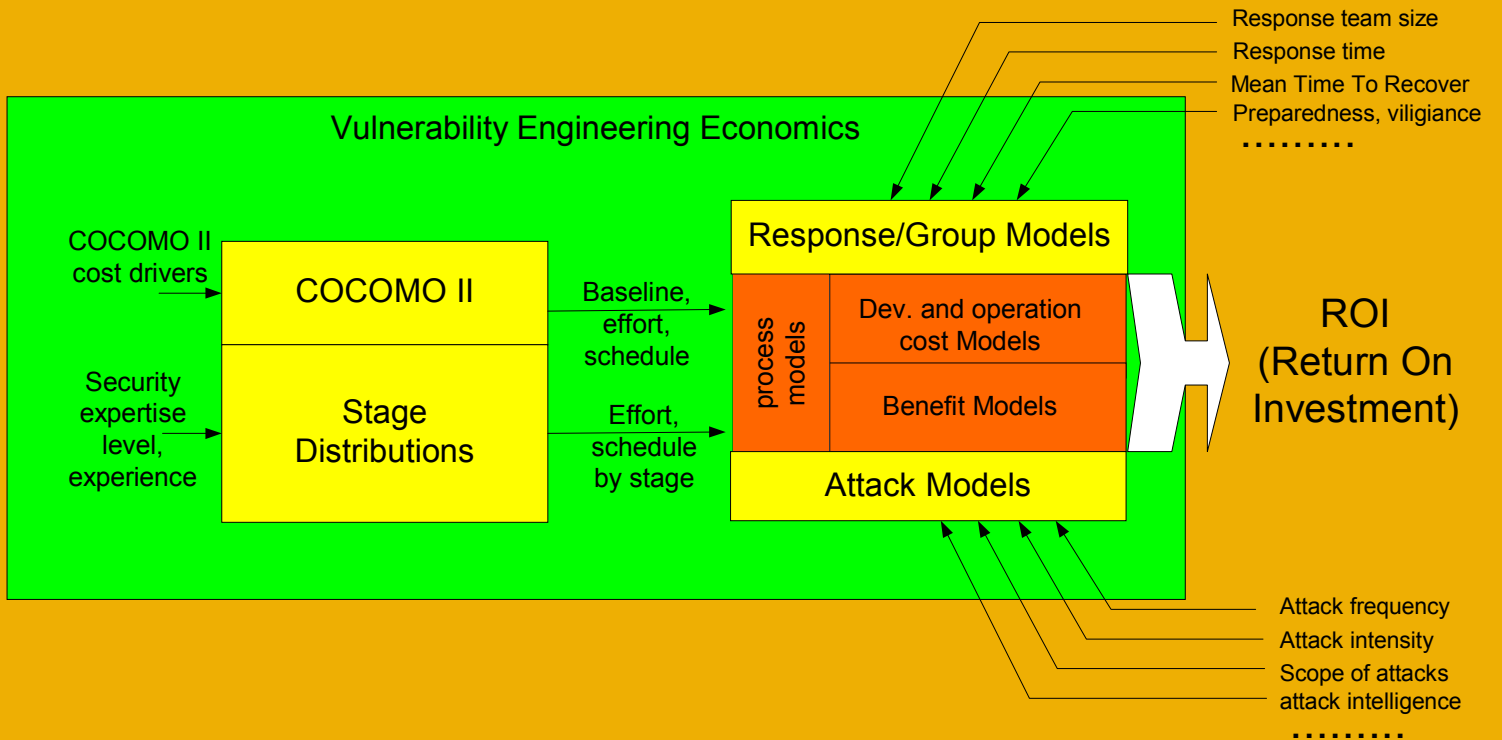
(a) In-coming Flaw, Detected, and Undetected flaws if development manpower of the second cycle is equal to 10% of that of the first cycle



(b) In-coming Flaw, Detected, and Undetected flaws if development manpower of the second cycle = 21%

If the ratio is lower than 21% (like a threshold), then the number of detected flaws never becomes zero.

# 3. V<sup>2</sup> Economics

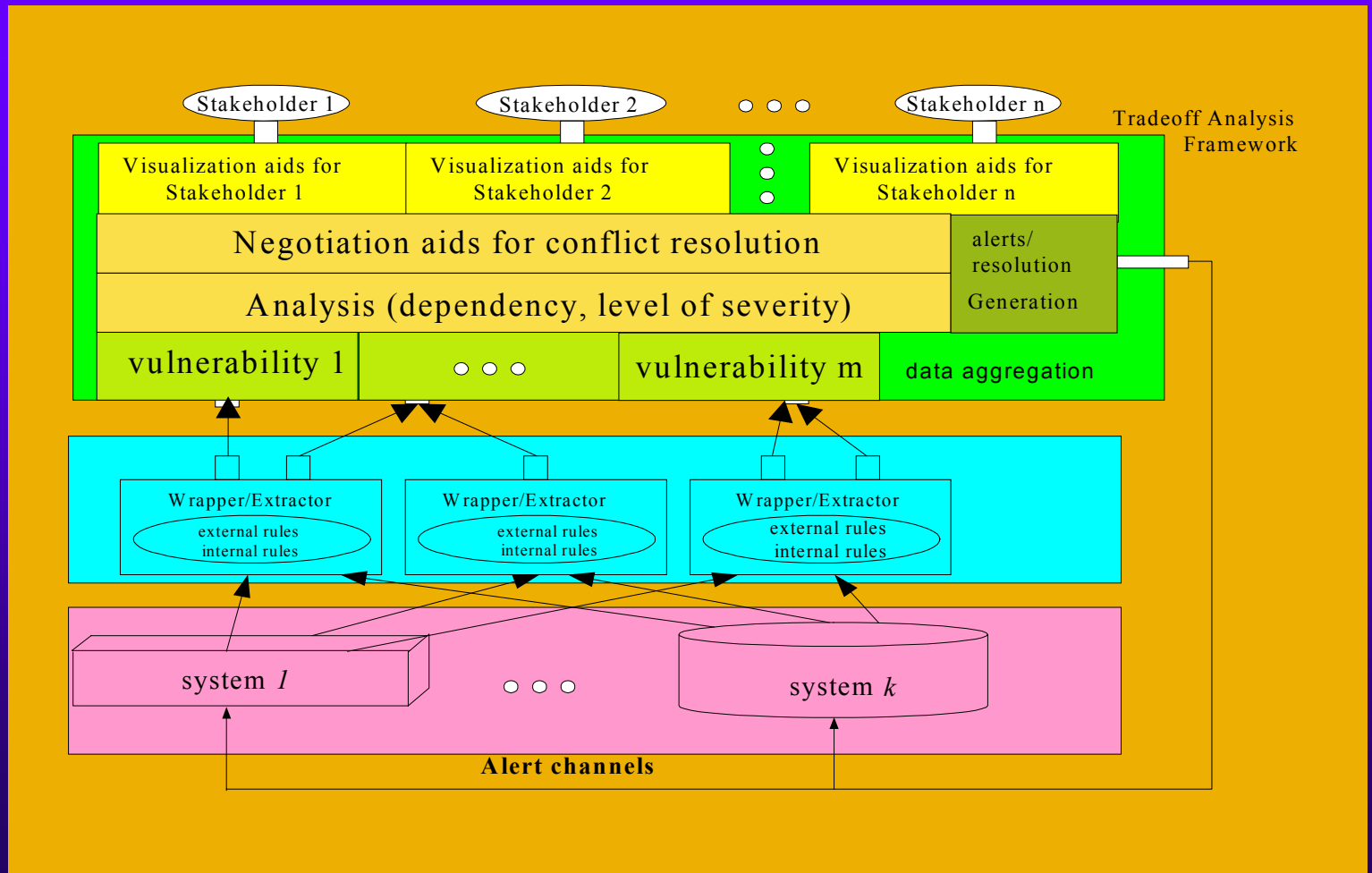




# Expected Contributions

- ◆ On-going life-cycle process modeling to explore the dynamics of V2
- ◆ Incorporating group dynamics into the system
  - More realistic attack-defense model
- ◆ Optimization of resource allocation
  - To information assurance investment
- ◆ Precise description of crisis response teams
  - Group behavior science research advance

# 4. Secure Software Design Methodology





Questions?