

Autonomic Defense System (ADS)

Salim Hariri

High Performance Distributed Computing (HPDC)
Laboratory

<http://www.ece.arizona.edu/~hpdc>

hariri@ece.arizona.edu

(520) 621-4378



On Going Research Projects:

- Autonomia Environment – Self* Computing Systems and Services
 - *Self-Configuration*
 - *Self-Protection (the focus of the ARL project)*
 - *Self-Healing*
 - *Self-Optimizing*
- Root-Cause Analysis of Network Attacks M&S Environment
- OPNET Modeling and Simulation of Network Attacks and Protection against insider attacks in Wireless Ad-hoc Networks
- Power and Performance Optimization – DEVS M& S Environment

Autonomic Computing: Next Era of Computing System Design

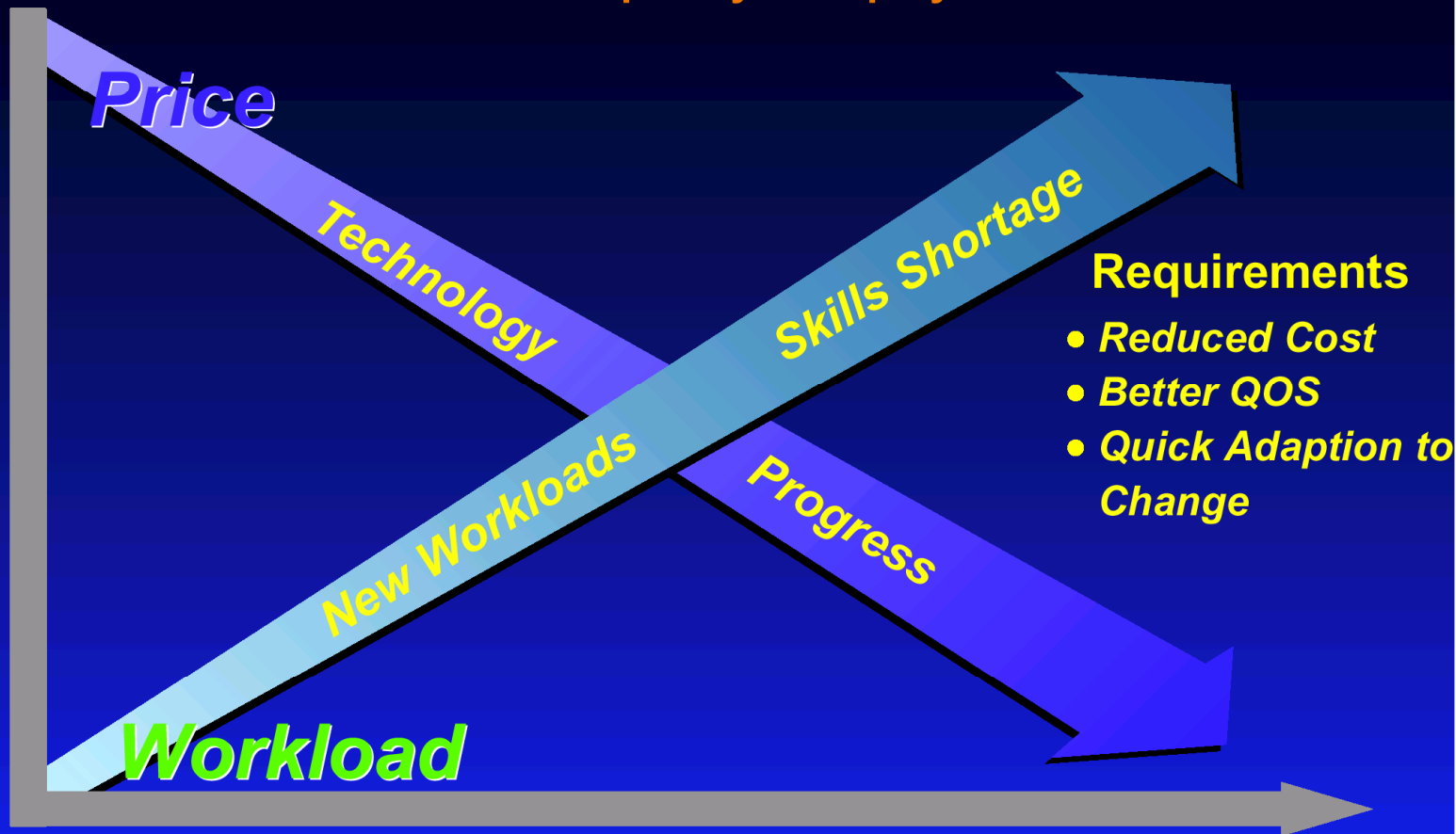
- Motivation
- Approach

Unmanageable and Insecure IT Systems

- Explosion growth in information and integration technology (billions of devices)
- Ubiquitous Access to information through PCs, PDAs, Cells, smart appliances, etc. (millions of users)
- Severe shortage in skilled IT workers (hundreds of thousands in US); will increase 100% in the next six years
- Bottom Line
 - *The increasing system complexity is reaching a level beyond human ability to manage and secure*

The e-business IT Infrastructure Challenge

Price performance gains in technology are more than offset by the scale and complexity of deployments



Self-managing systems are a necessity!

Page 4

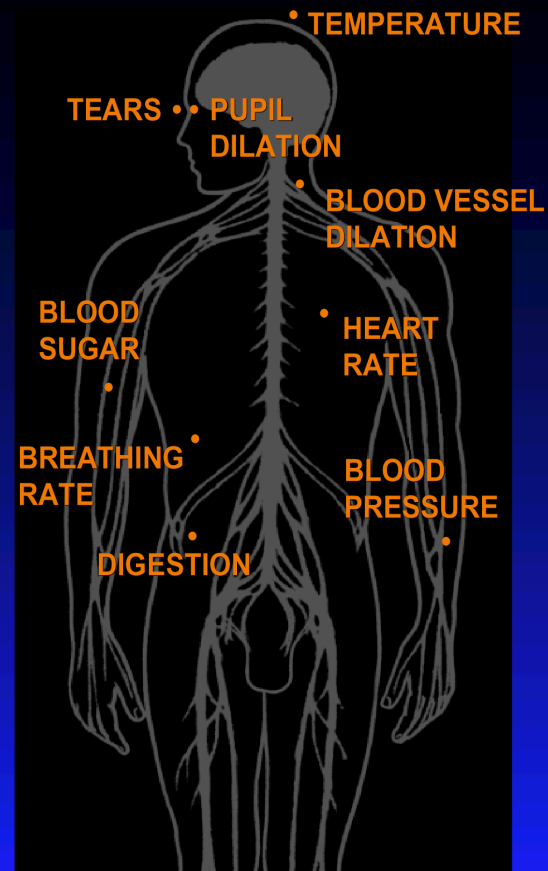


Biological Systems: Lessons Learned

- Focus on Applications, Middleware manages applications
 - Fault
 - Performance
 - Security, etc.
- Need Biological Like Metrics
 - Temperature,
 - Blood pressure

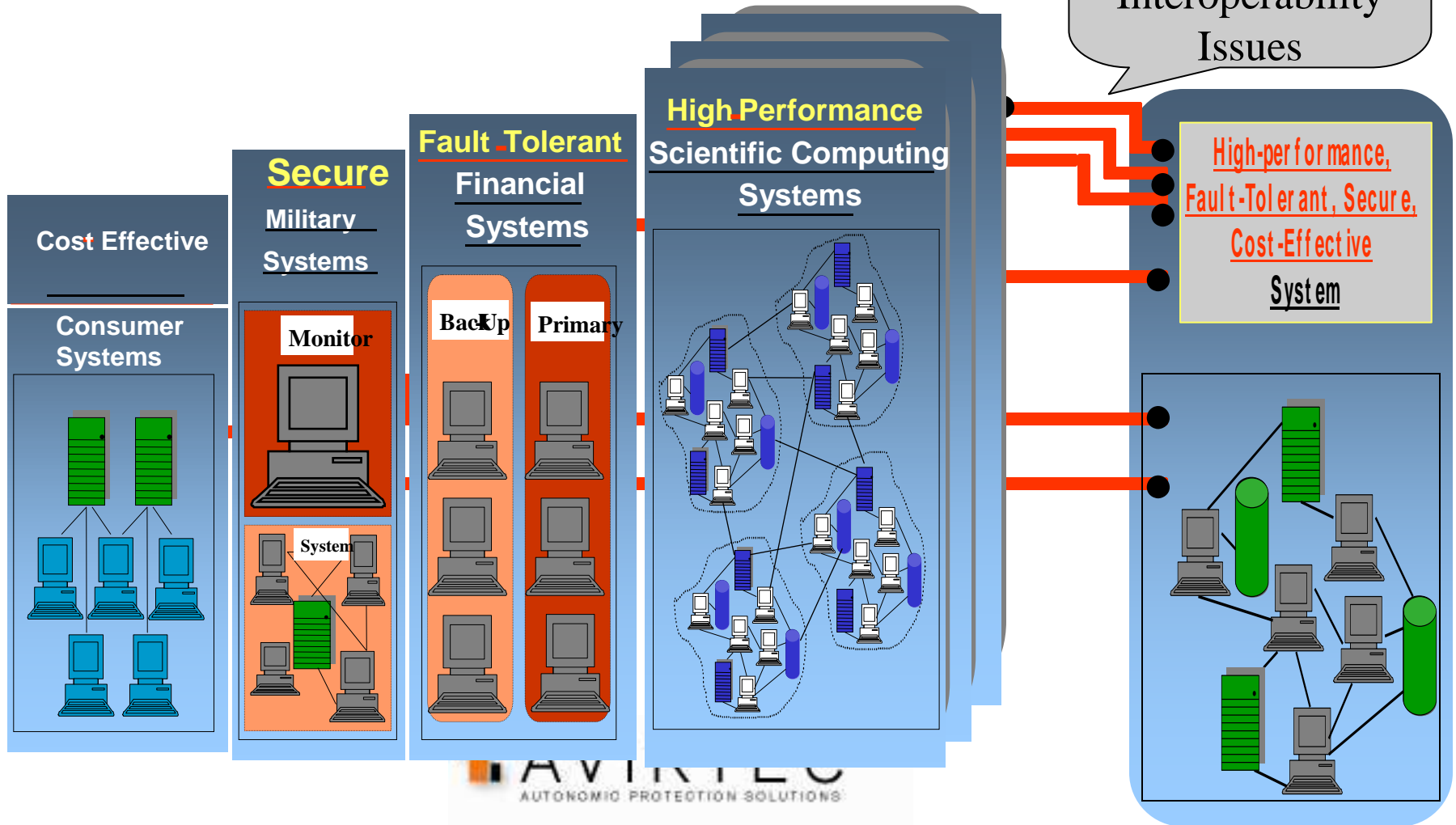
The Autonomic Nervous System Monitors and Regulates:

- without requiring our conscious effort when we run, it increases our heart and breathing rate



holistic System Solutions: Complex and Costly using current technologies

Adds Complexity
High-Cost
Interoperability
Issues



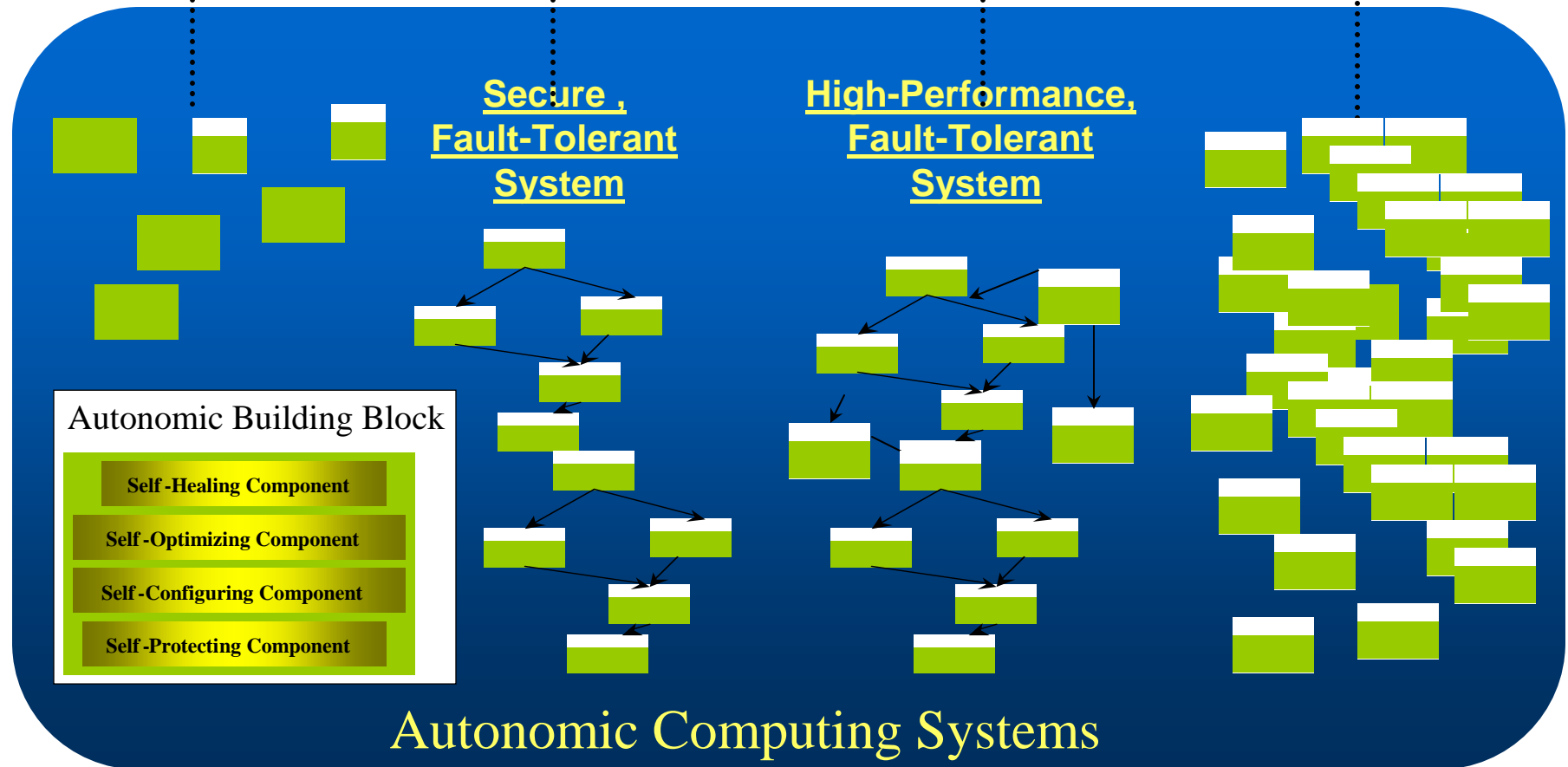
Autonomic Computing Approach: holistic Approach – cost effective, scalable, open, and Self* Manage

Cost-Effective
Consumer
Systems

Secure
Military
Systems

Fault-Tolerant
Financial
Systems

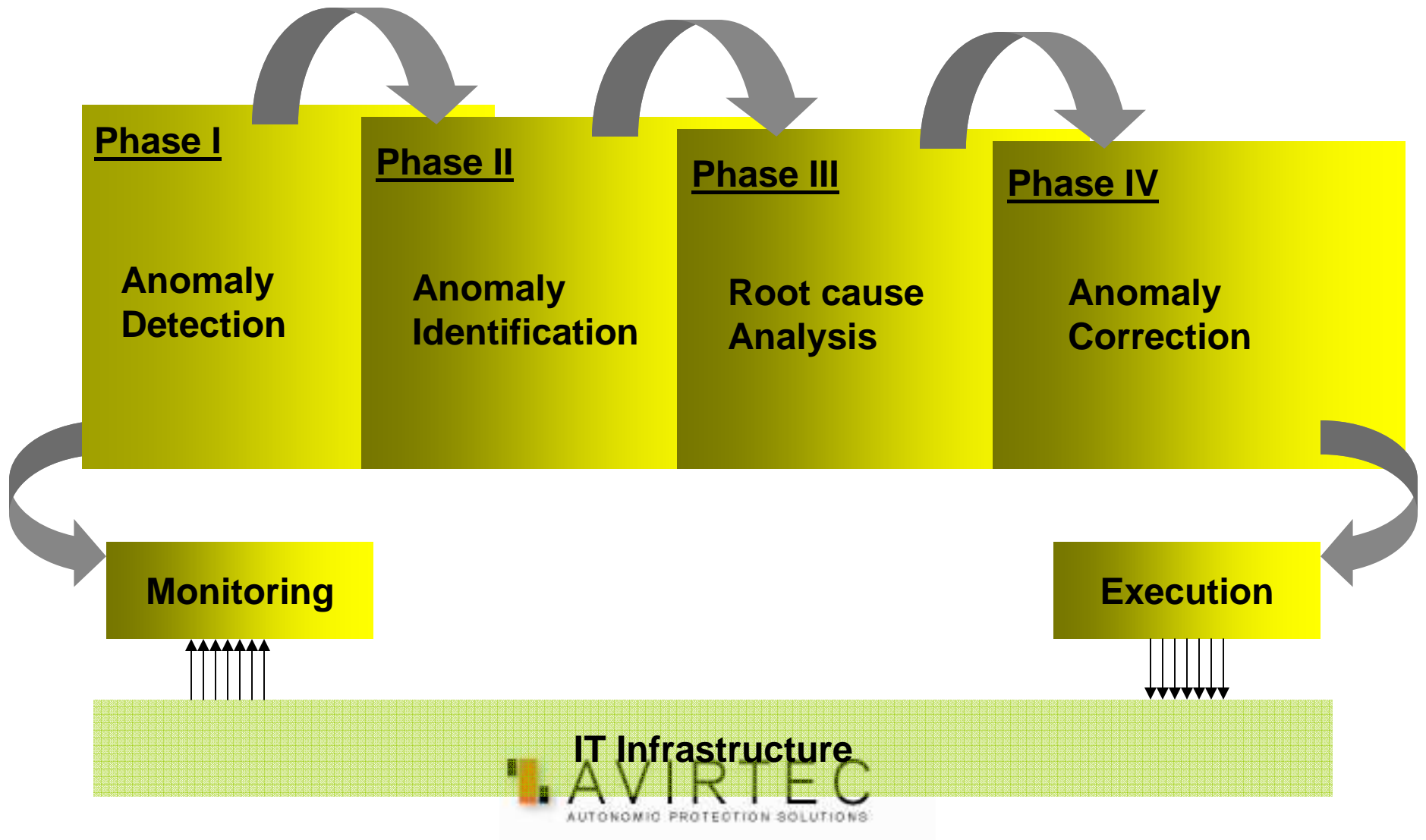
High-Performance
Scientific Computing
Systems



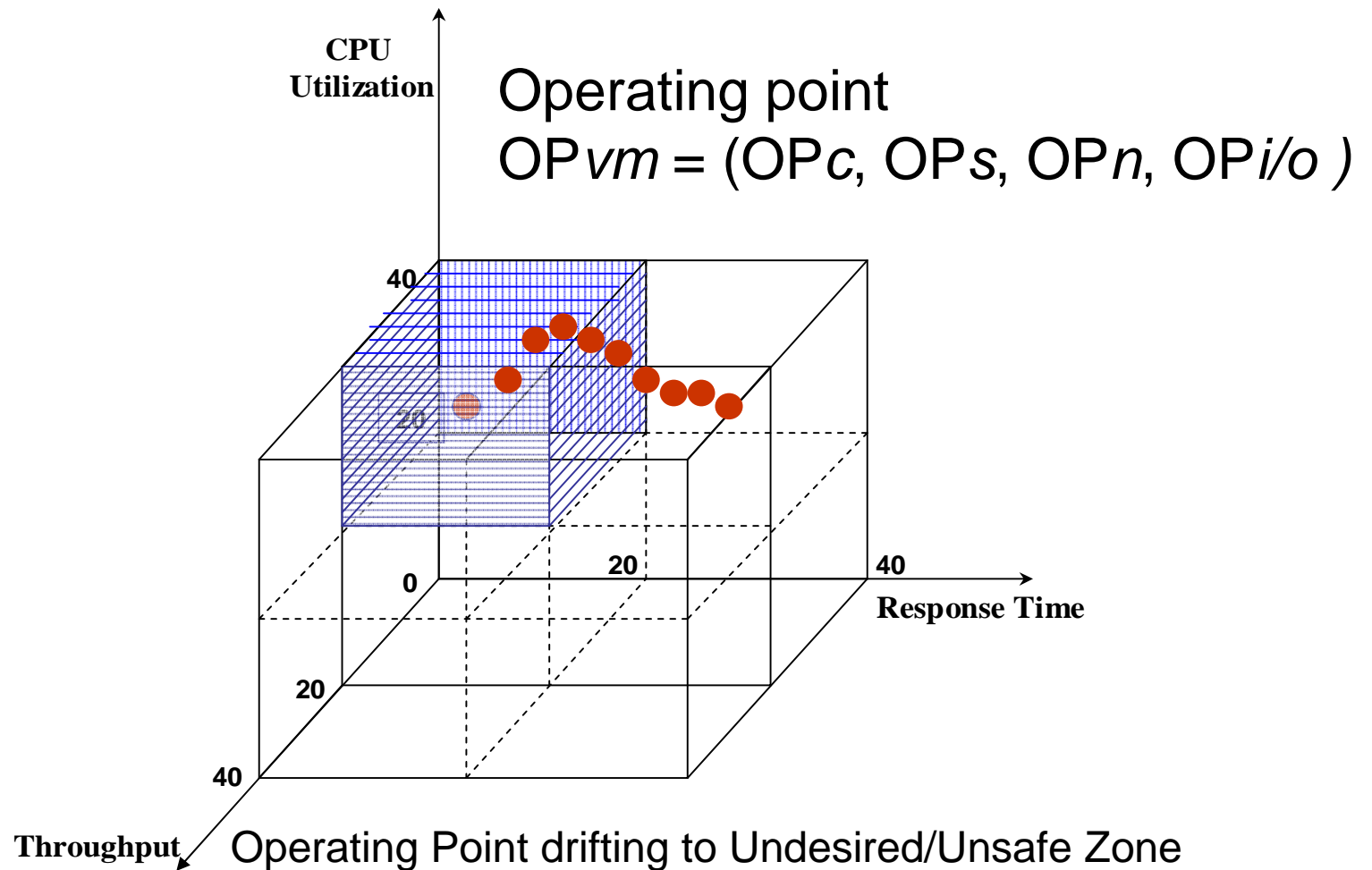
Autonomic Computing: Next Era of Computing System Design

- An integrated design approach that can address all system aspects – security, performance, fault-tolerance, etc.
- Biological-like Metrics – accurately characterize the current state of the system and its behavior

Holistic Design Approach: Anomaly Based Control and Management Framework



Anomaly Identification: Operating Point Drift



AUTONOMIA: An Autonomic Control and Management: for Self* Computing Systems and Services

- Provide **automated composition, registration, discovery** of autonomic components
- Provide **automated configuration/deployment** of autonomic applications and system resources
- Provide **autonomic runtime control and management for both applications and system resources**
 - Self-Configuring
 - Self-Optimizing
 - Self-Protecting
 - Self-Healing

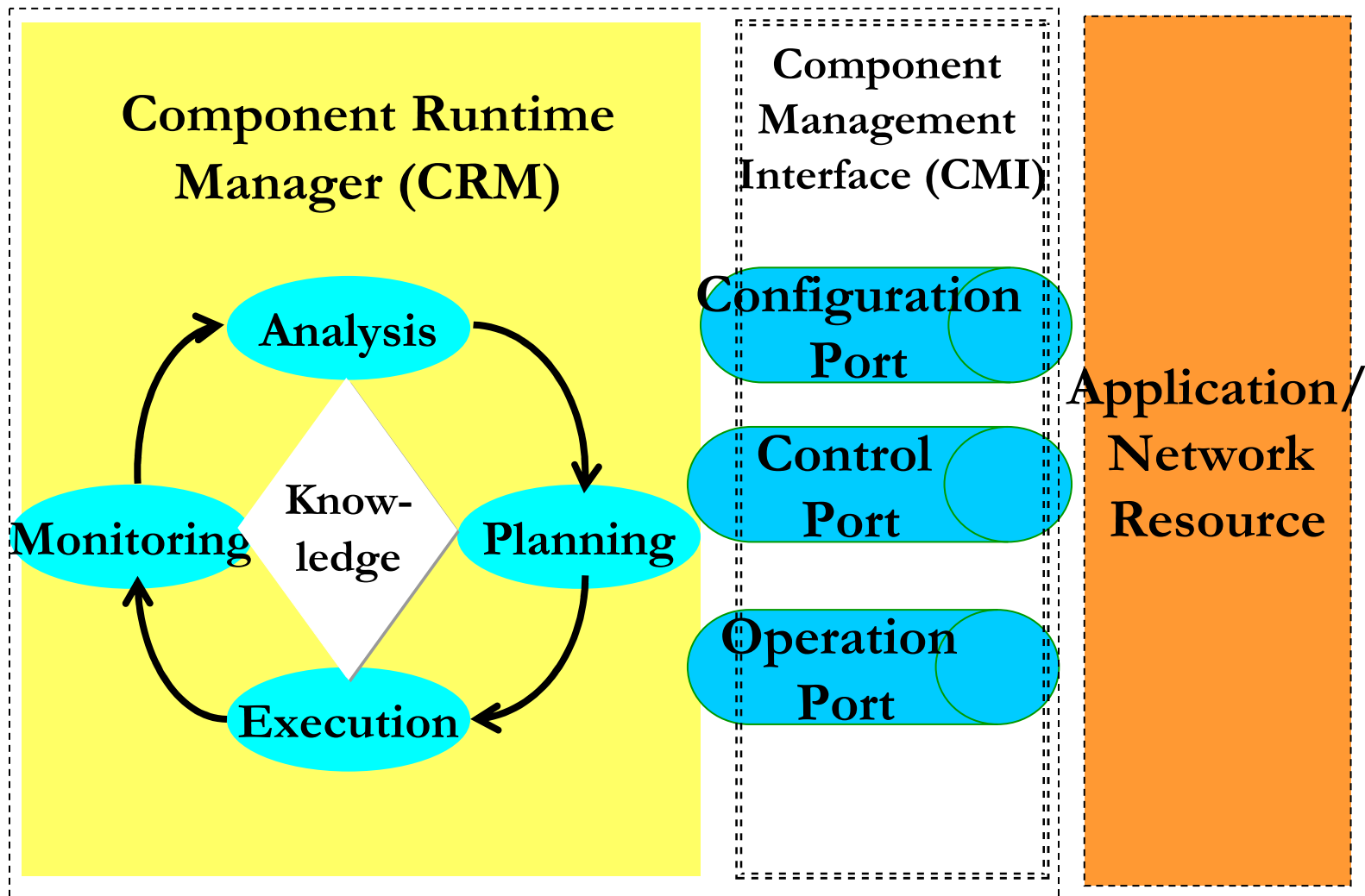
Autonomia Implemented Services

- Self-Configuration and Self-Deployment
- Self-Protection
- Self-Optimization
- Self-Healing

What is Self-Configuration?

- The ability of the system to automatically and dynamically adapt to changing environments using policies provided by the IT professional
- The changes in environment include deployment of
 - *New software components*
 - *Removal of existing ones*
 - *Adding/removing resources*
 - *Drastic changes in network traffic or computational loads*

Autonomic Component



```

<Control_port>
  <function name=" TranslatetoExtDB">
    <inputs>
      <input name=" ext_data_source " type="String" value=""/>
      <input name=" data_string " type="String" value=""/>
      <input name=" ext_data_string " type="String" value=""/>
    </inputs>
    <outputs>
      <output name="Translate_to_status" type="boolean"/>
    </outputs>
  </function>
</Control_port>
<operation_port>
  <interaction_policy>
    <Policy>
      <conditions condition="receive Message ACCESS DB4 with
data_string"/>
      <actions action=" invoke_service"
inputs="Format_Translation,Client_Format,DB4_Format">
        <return name="invoke_status" type="boolean"/>
      </actions>
      <else_actions/>
    </Policy>
    <Policy>
      <conditions condition=" Translate_to_status = true"/>
      <actions action="Query" input="DB4, data_string">
        <return name="query_status" type="boolean"/>
      </actions>
      <else_actions>
    </Policy>
  </interaction_policy>
</operation_port>

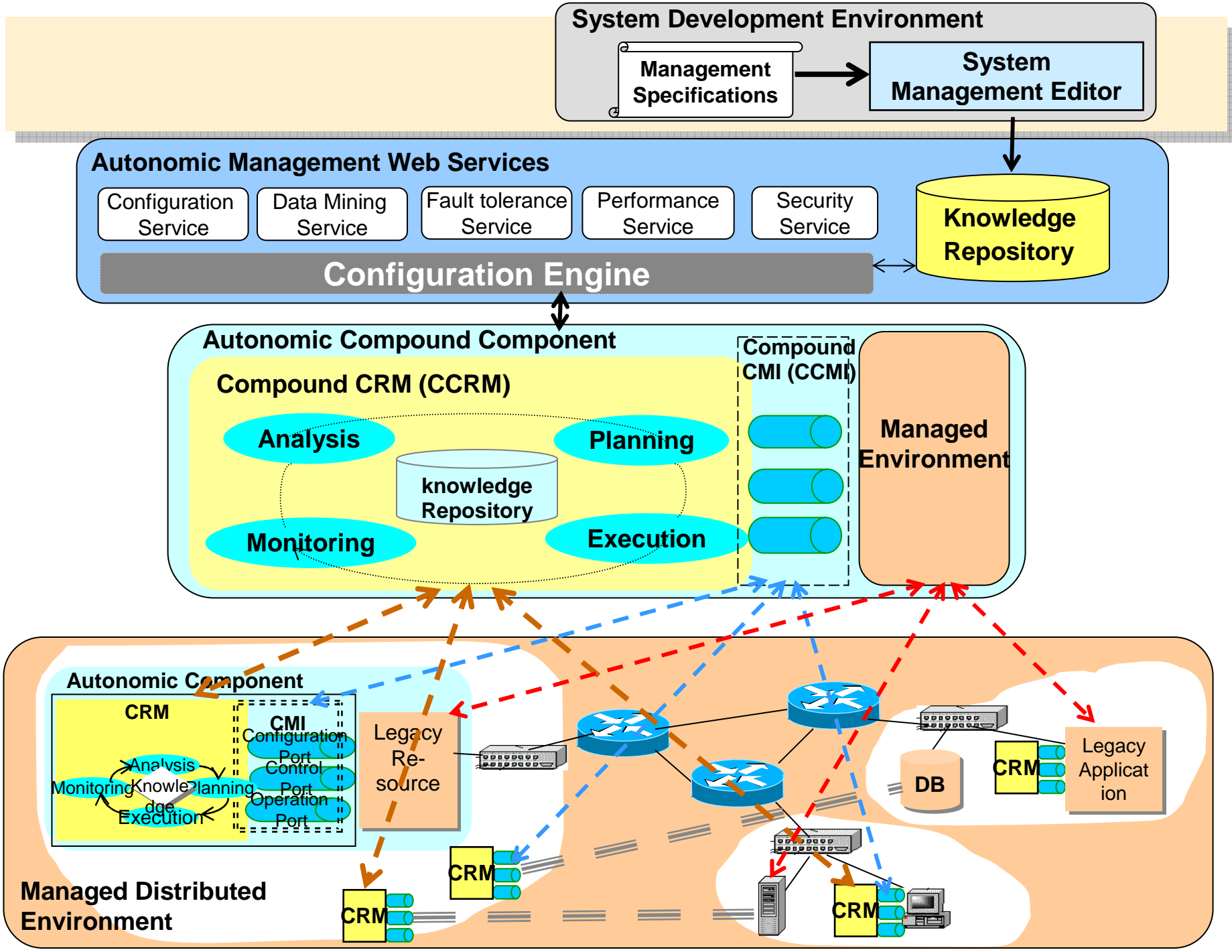
```

Operational
Port

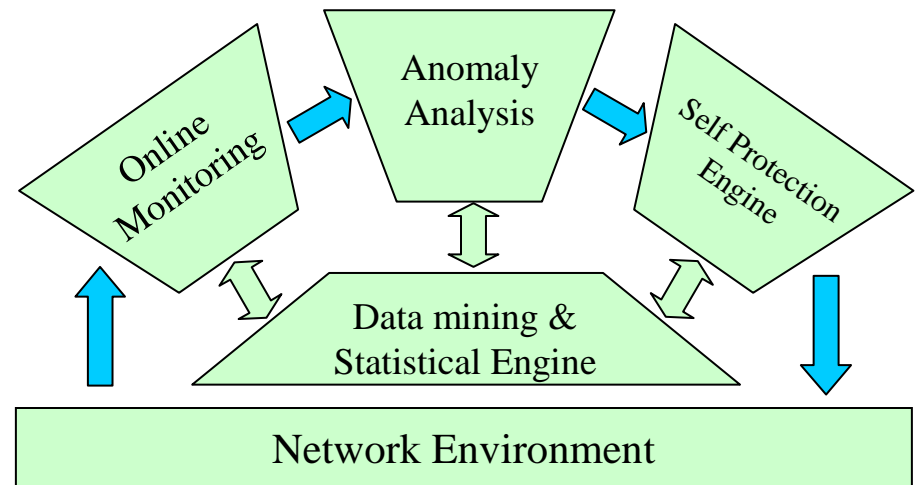
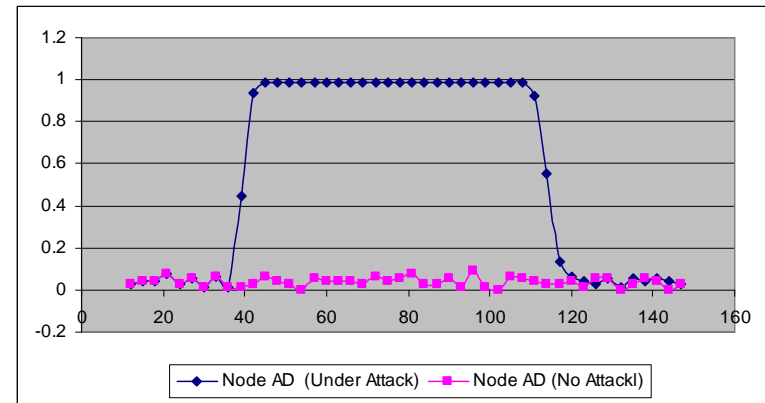
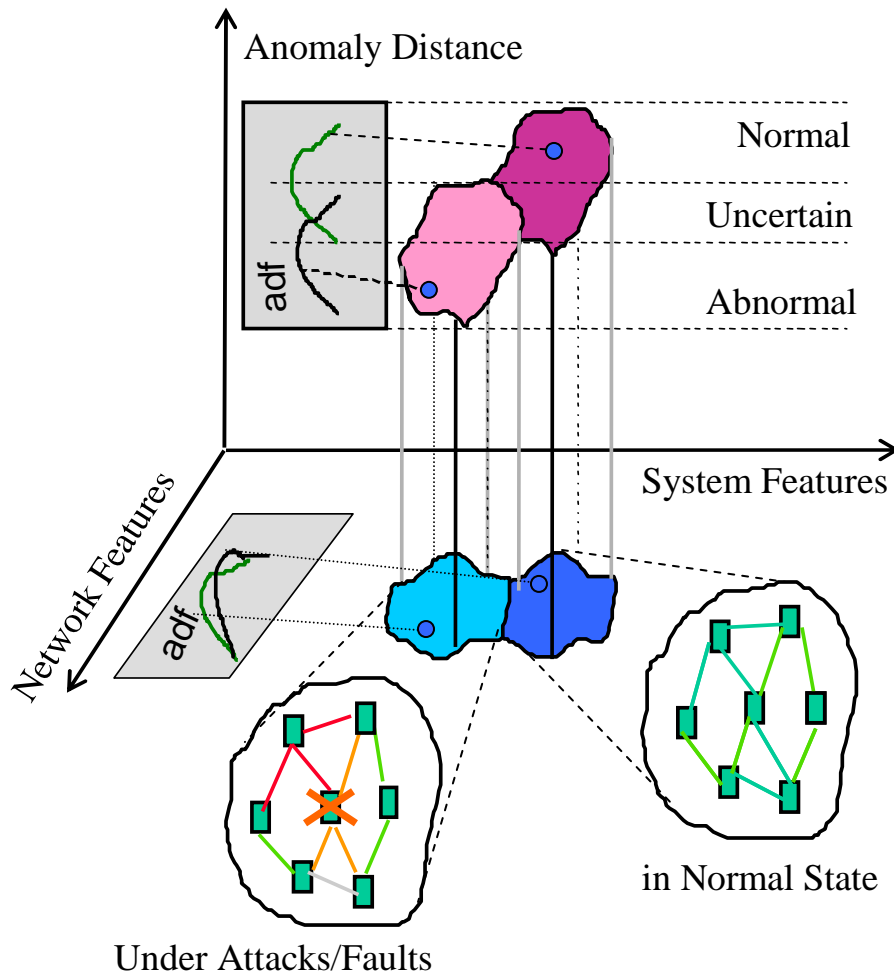
Control
Port

Configuration
Port

Managed
Resource
Or
Component



Self-Protection Methodology



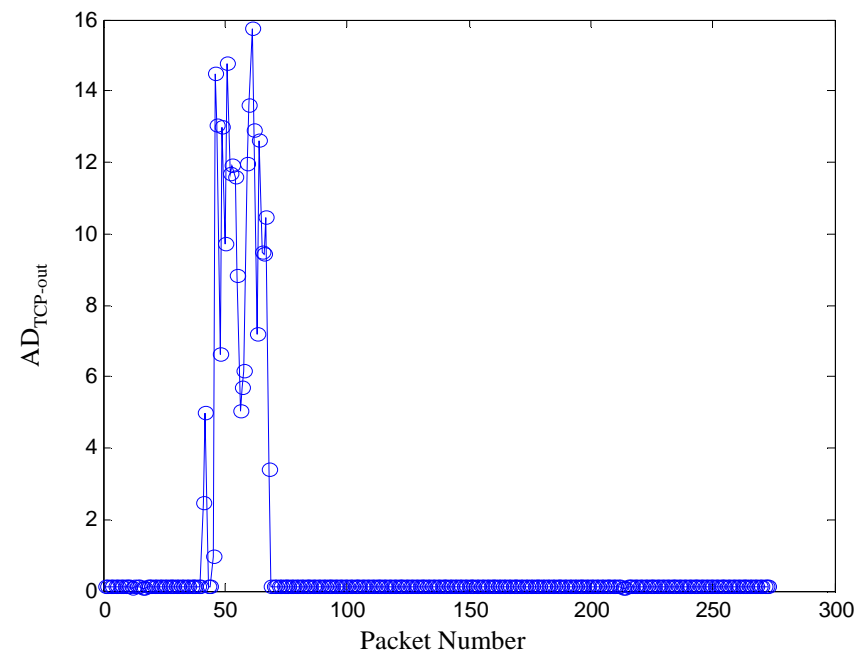
Anomaly Distance (AD)

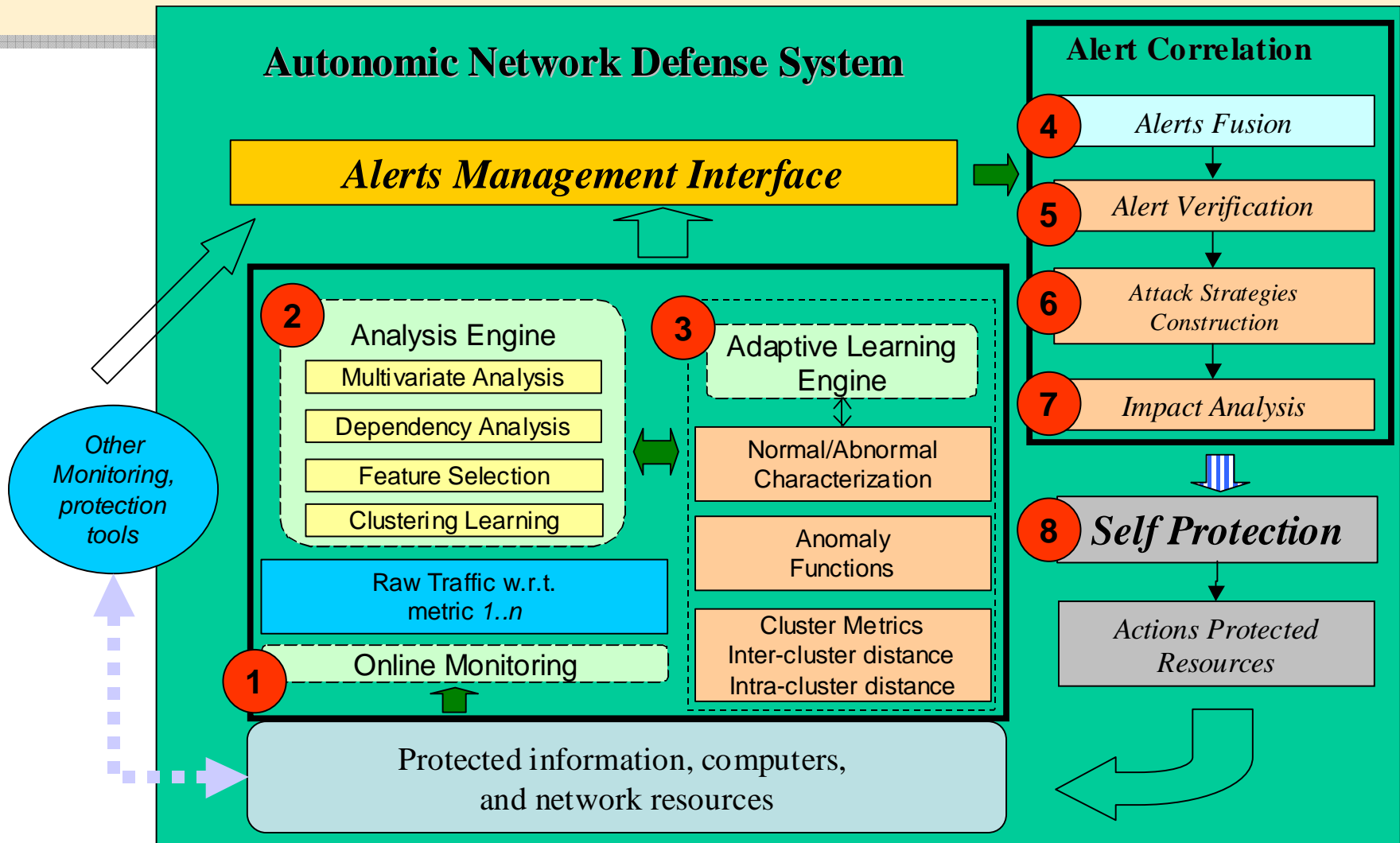
- *Abnormality Distance* of measurement attributes is used as an abnormality metric for profile modeling of the component behavior.

$$AD_k = [(MA_k(t) - \mu_{MA_k}) / \sigma_{MA_k}]^2$$

where μ_{MA_k} and $\sigma_{MA_k}^2$ are the mean and variance under the normal operation condition corresponding to the online measurement of attribute k .

Right figure shows the AD_{tcp_out} based on the single measurement attribute measure where the larger magnitude of the AD_{tcp_out} indicates the abnormal behavior that might be due to an attack.





Analysis Engine

1. Information theory is used to filter network traffic and identify the most important features that must be analyzed in real-time.
2. Genetic algorithm is used obtain the threshold and coefficients used by the linear rule for network intrusion detection.
3. Threshold and coefficients are then used by the self-protection engine to detect a wide range of network attacks

Results

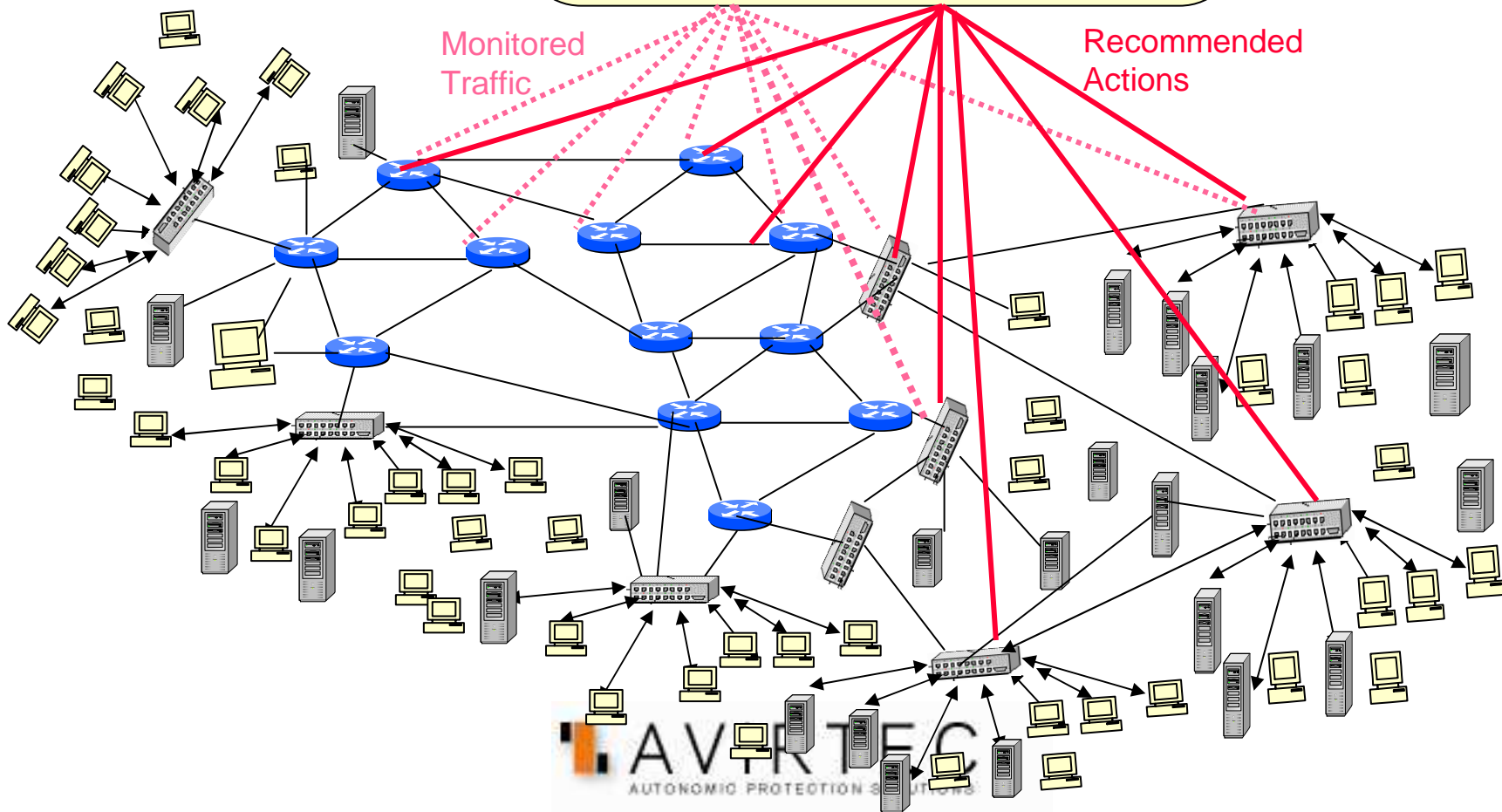
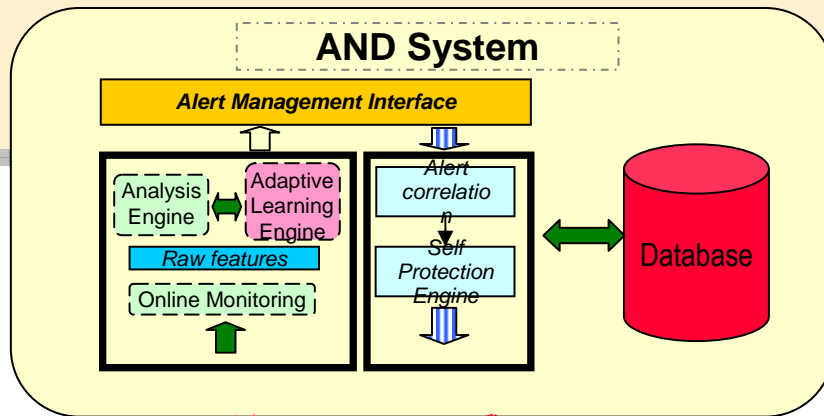
1. We compare the results of our approaches with DARPA/KDD99 winner and CTree methods. The results show that using combined features (continuous and discrete) can yield better results.

Class	Our Approach using Continuous and Discrete Features	Our Approach using Discrete Features only	Winner Entry using C5.0	CTree
Normal	98.45%	98.34%	99.5%	92.78%
Dos	99.93%	99.33%	97.1%	98.91%
U2R	75.34%	63.64%	13.2%	88.13%
R2L	41.34%	5.86%	8.4%	7.41%
PROBE	99.91%	93.95%	83.3%	50.35%

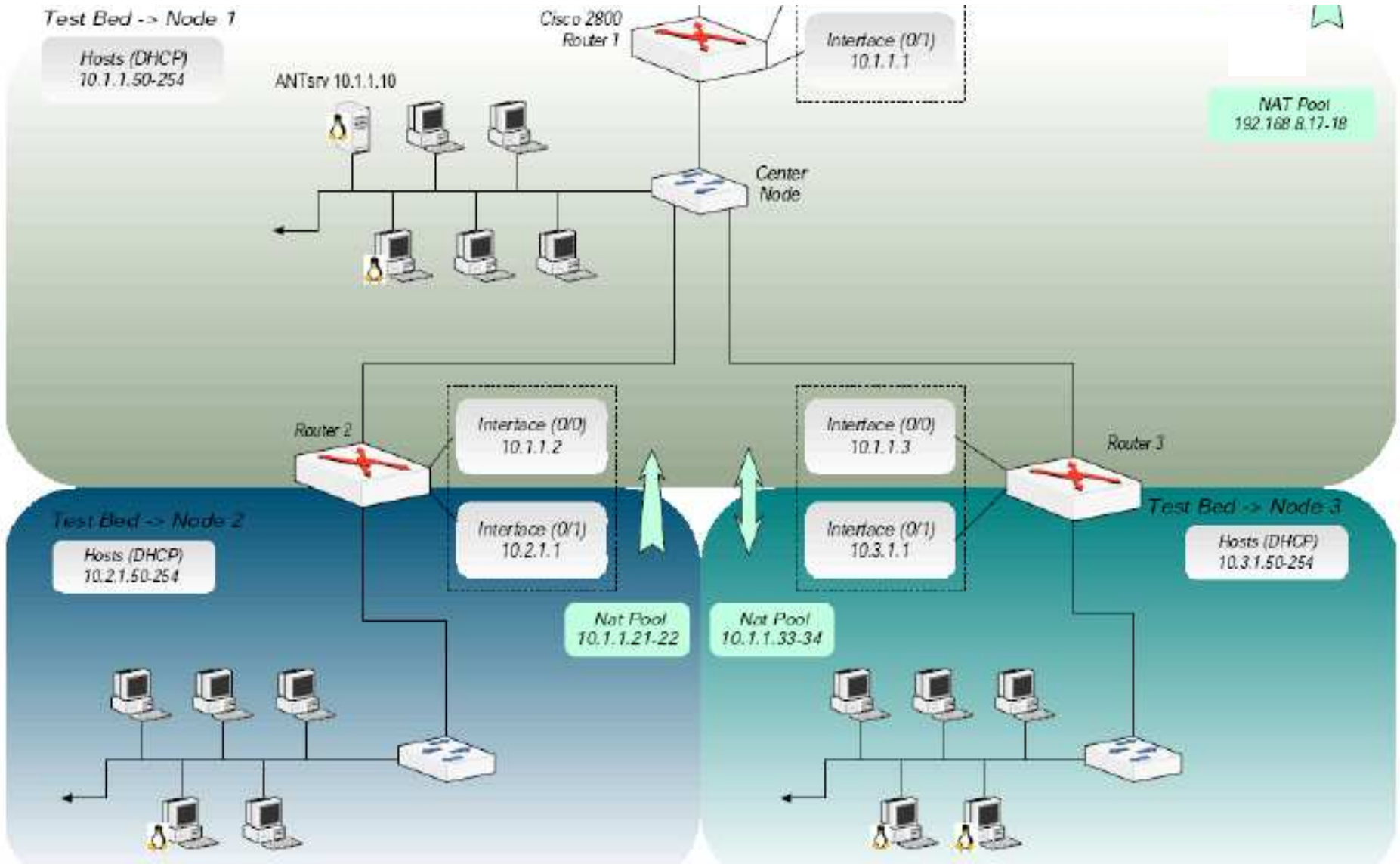
Dependency Analysis Results

U2R and R2L attacks are difficult to detect (can be seen from the results)
After doing dependency analysis, we tried to reduce the redundancy among the features, we can gain good results.

Features Set	Results for U2R Attacks detection with Dependency Analysis		
	False Alarm	Detection Rate	Number of Features
{service, dst_host_count}	6.1%	91.57%	2
{service, dst_host_count, dst_host_same_src_port_rate}	9.8%	96.23%	3
{service, dst_host_count, dst_host_same_src_port_rate, src_bytes}	4.9%	92.56%	4
{service, dst_host_count, dst_host_same_src_port_rate, src_bytes, root_shell}	8.25%	92.56%	5



UA Test Bed Topology



Attack Library

- In order to learn and evaluate ADS we have developed a rich Network Attack Library that can be programmed to launch attacks
 - *Denial of Service Attacks*
 - *TCP SYN attack*
 - *ICMP flood attack*
 - *UDP flood attack*
 - *Distributed DoS*
 - *MS Stream Attack*
 - *Worm*
 - *SQL Slammer Worm*

Training Dataset

- Total Records 290872
- Normal records 70089, abnormal records 220783
- Normal network behaviours include:
 - *Web browsing*
 - *video/audio streaming traffic*
 - *Ftp, telnet, remote desktop, windows file sharing*
 - *IM (google talk, MSN, ICQ, etc.)*
 - *P2P traffic*
- Abnormal network traffic

Xprobe2 Attack

Test Scenario 1 – launch Xprobe2 attack from node **10.1.1.41** to attack node **10.3.1.15**

The image displays two screenshots of the RouterControl UI. The top screenshot shows the configuration for 'router1' with the 'INSIDE' ACL type selected. The bottom screenshot shows the configuration for 'R0uter.2' with the 'OUTSIDE' ACL type selected. Both screenshots show a table of ACL rules with 'deny tcp 10.1.1.41 0.0.0.0 10.3.1.15 0.0.0.0 eq 35', 'deny tcp 10.1.1.41 0.0.0.0 10.3.1.15 0.0.0.0 eq 24', and 'deny tcp 10.1.1.41 0.0.0.0 10.3.1.15 0.0.0.0 eq 28' rules, and a 'permit ip any any' rule at the bottom. The bottom screenshot also includes 'click to remove' buttons for each deny rule.

RouterControl UI - router1

rule
deny tcp 10.1.1.41 0.0.0.0 10.3.1.15 0.0.0.0 eq 35
deny tcp 10.1.1.41 0.0.0.0 10.3.1.15 0.0.0.0 eq 24
deny tcp 10.1.1.41 0.0.0.0 10.3.1.15 0.0.0.0 eq 28
permit ip any any

RouterControl UI - R0uter.2

rule	
deny tcp 10.1.1.41 0.0.0.0 10.3.1.15 0.0.0.0 eq 35	click to remove
deny tcp 10.1.1.41 0.0.0.0 10.3.1.15 0.0.0.0 eq 24	click to remove
deny tcp 10.1.1.41 0.0.0.0 10.3.1.15 0.0.0.0 eq 28	click to remove
permit ip any any	click to remove

***Results: successful
Deny of the attack***

Performance of Current Prototype on External Attacks Detection

- The system can successfully detect and protect against these attacks with more than 99% detection rate and less than 5% false alarms
- Only 3 alarms generated after applying more than 3 million traffic records generated during 3 day demonstration/evaluations

1. SYN Stealthy Scan

2. Connection Scan

3. ACK Stealthy Scan

4. FIN/ACK Stealthy Scan

5. NULL Stealthy Scan

6. Xmas Tree Stealthy Scan

7. TCP Window Scan

8. IP Protocol Scan

9. Nikto

10. Nessus

11. Land Attack

12. Xprobe2

13. Apanet

14. SYN Flood (with spoofing)

15. sara

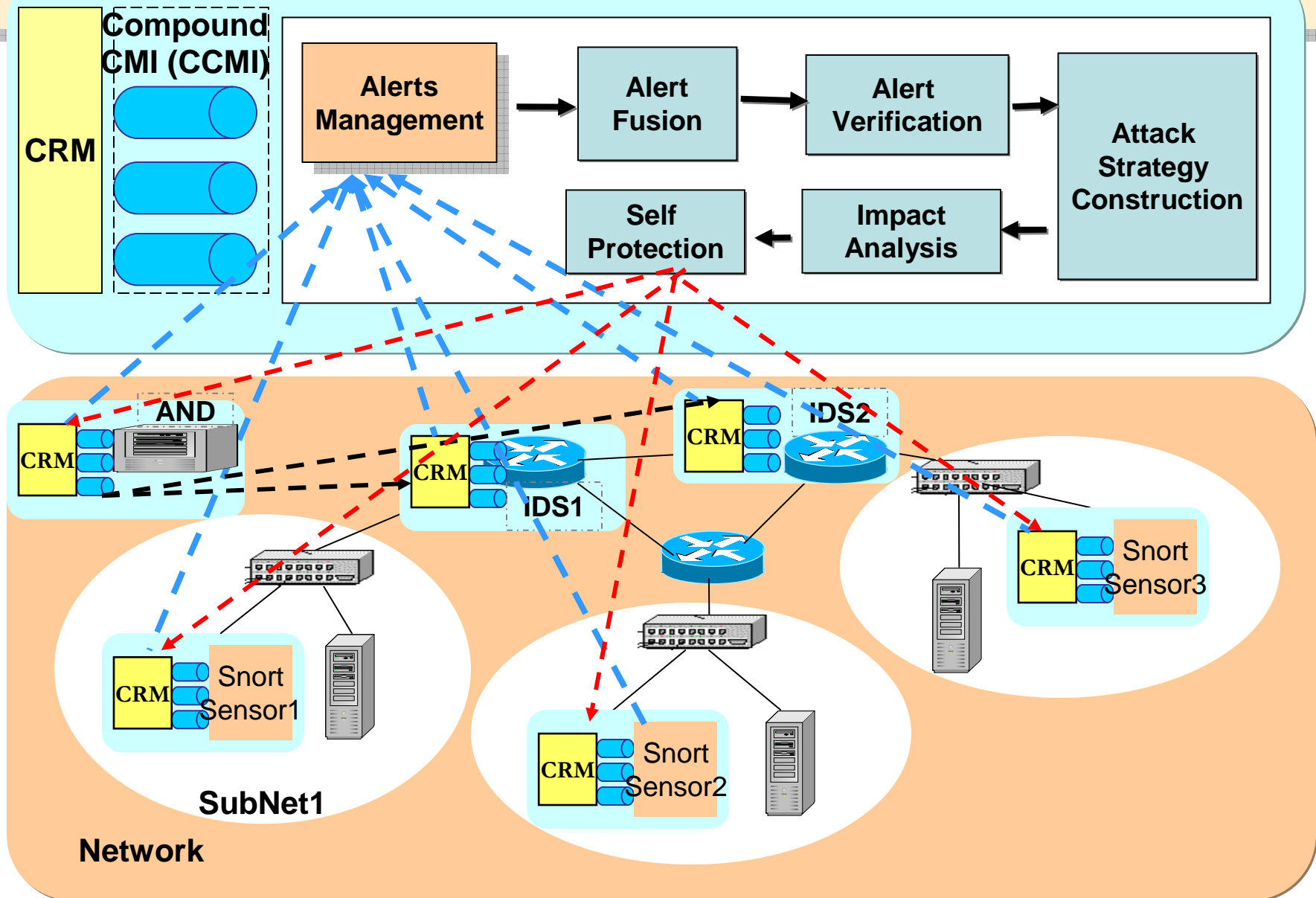
16. netcat

17. NMap port scan w/out ping

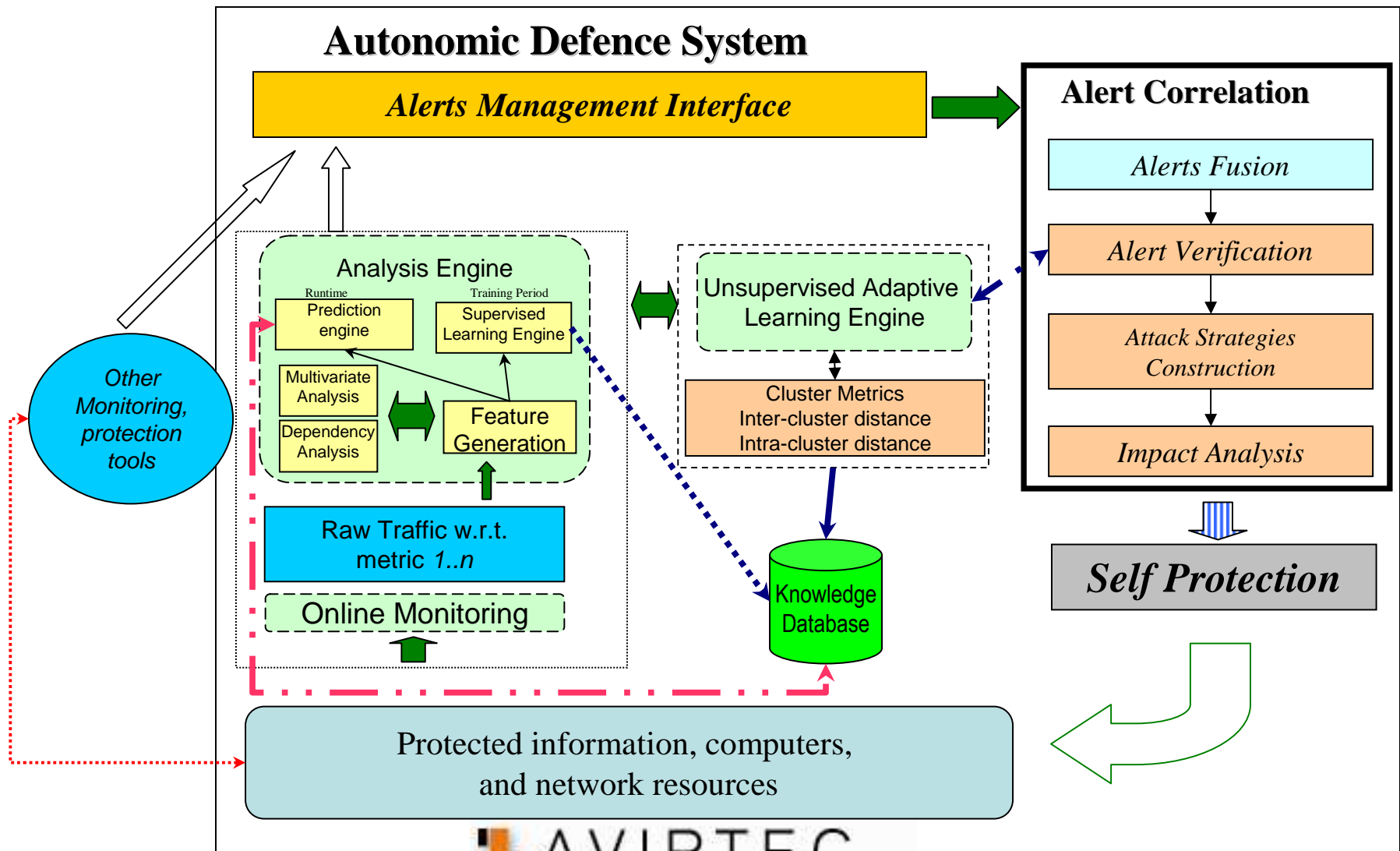
18. Standard Nmap

19. worms attack

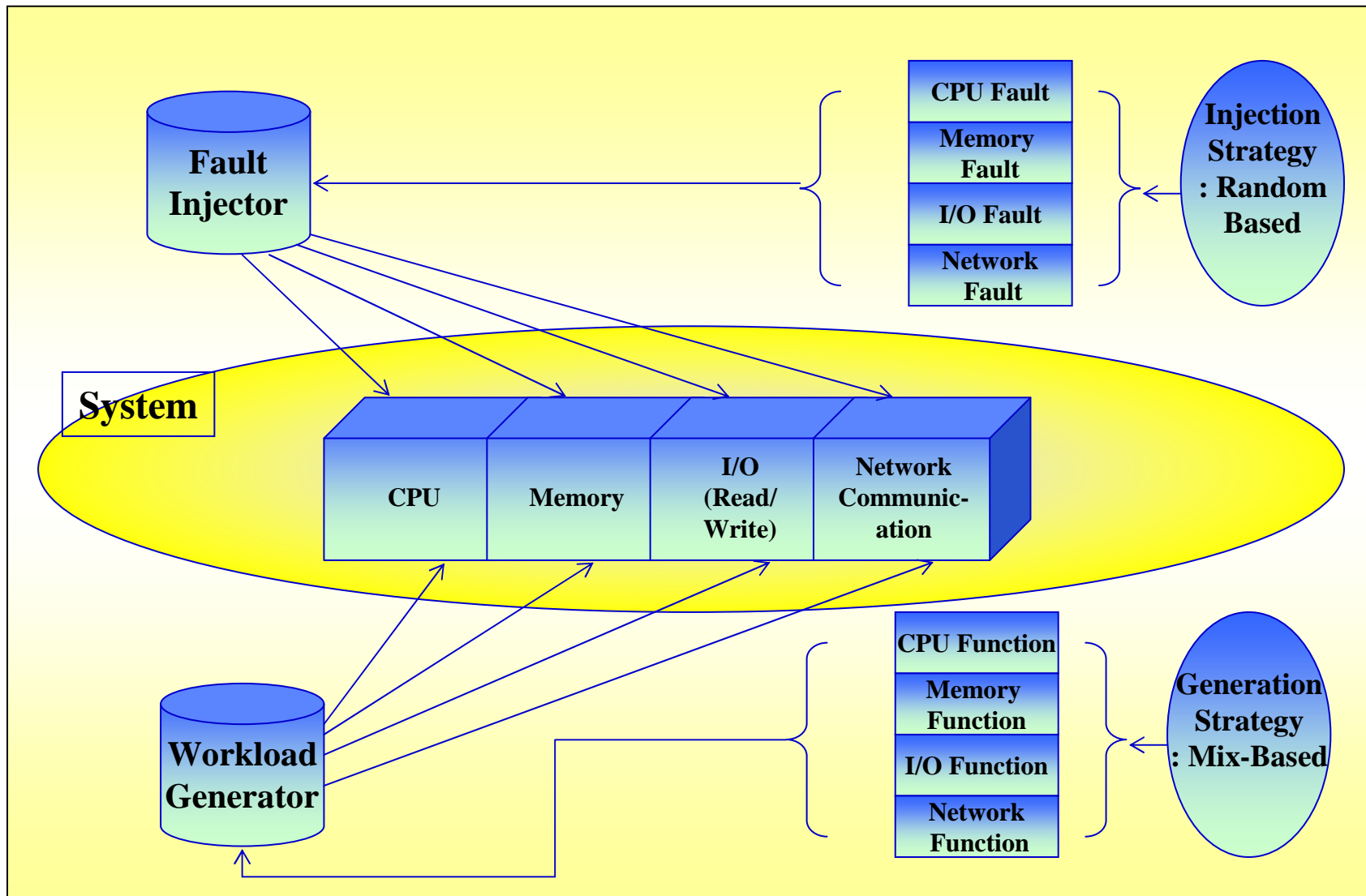
Autonomic Defence System (ADS)



ADS Implementation



Self Healing Test Bed



Summary and Concluding Remarks

- Increased complexity, heterogeneity, uncertainty, and scale require new paradigms to design, control and manage systems and applications
- Systems and Applications need to operate reliably, securely, efficiently and cost-effectively
 - *Need holistic Approach that can dynamically integrate and address all these issues simultaneously at the layers of the system and application hierarchy*
- Autonomic Computing Provides an interesting, pragmatic approach to address these issues
- Many challenges are ahead including composing and analyzing in real-time the operations and states of systems and applications
 - need new bio-inspired metrics that accurately characterize and quantify the system and application normal and abnormal states