

The Willow Survivability Architecture

International Survivability Workshop

20 March 2002

Dennis Heimbigner and Alexander Wolf

University of Colorado at Boulder

John Knight

University of Virginia

Premkumar Devanbu, Michael Gertz, and Karl Levitt

University of California at Davis

Survivability

- ◆ Goal: Address response and recovery
 - Continue “sufficient” level of service in the face of unintended and ill-intended disruptions
- ◆ System context
 - Large-scale, heterogeneous, and distributed
 - Component-based and evolving

Large-Scale Distributed Systems

- ◆ Vast numbers of hosts and users
- ◆ Multiple administrative domains
- ◆ Multiple sources/producers of components
- ◆ Long life times with high costs
- ◆ Systems of systems
- ◆ Increased impact of...
 - Heterogeneity
 - Network latency
 - Autonomy
 - Security
 - Mobility
 - Continuous operation

What Are We Trying To Survive?

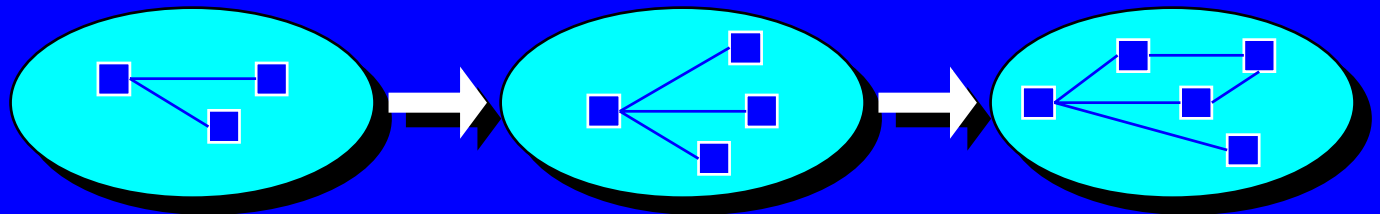
- ◆ Malicious and criminal attacks
 - => Intrusion tolerance
- ◆ More generally: non-maskable faults
 - Errors by operators
 - Errors in operational procedures
 - Hardware degradation faults
 - Hardware and Software design faults
 - Software degradation faults
 - Environmental stress
 - ...

High Level Research Hypotheses

- ◆ Dynamically change posture of software systems to protect against faults and threats
 - Using assured, secure, automated, reconfiguration
- ◆ Why reconfiguration?
 - Powerful approach to surviving non-maskable service disruptions
 - Faster, more accurate, and more scalable Vs. manual
- ◆ Two modes: reactive recovery and proactive protection

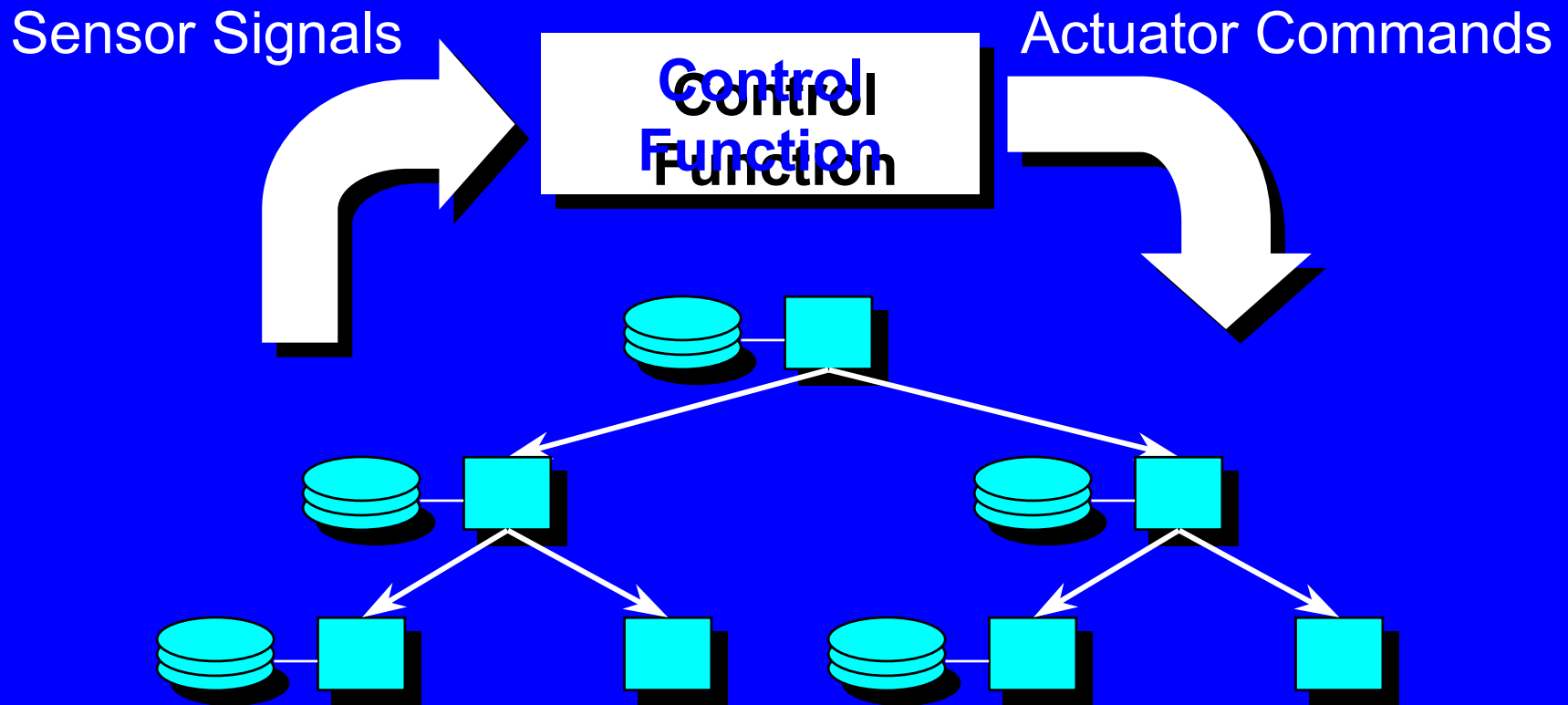
Primary Tool: Reconfiguration

- ◆ Any and all planned changes applied to the communication, interconnection, componentization, and functionality of a system
 - Initial deployment of application systems
 - Periodic updates: application and operating system
 - » Including patches / service-packs / etc.
 - Planned changes in response to anticipated threats.
 - Planned fault tolerance in response to anticipated component failures.
 - Systematic best efforts to deal with unanticipated failures.



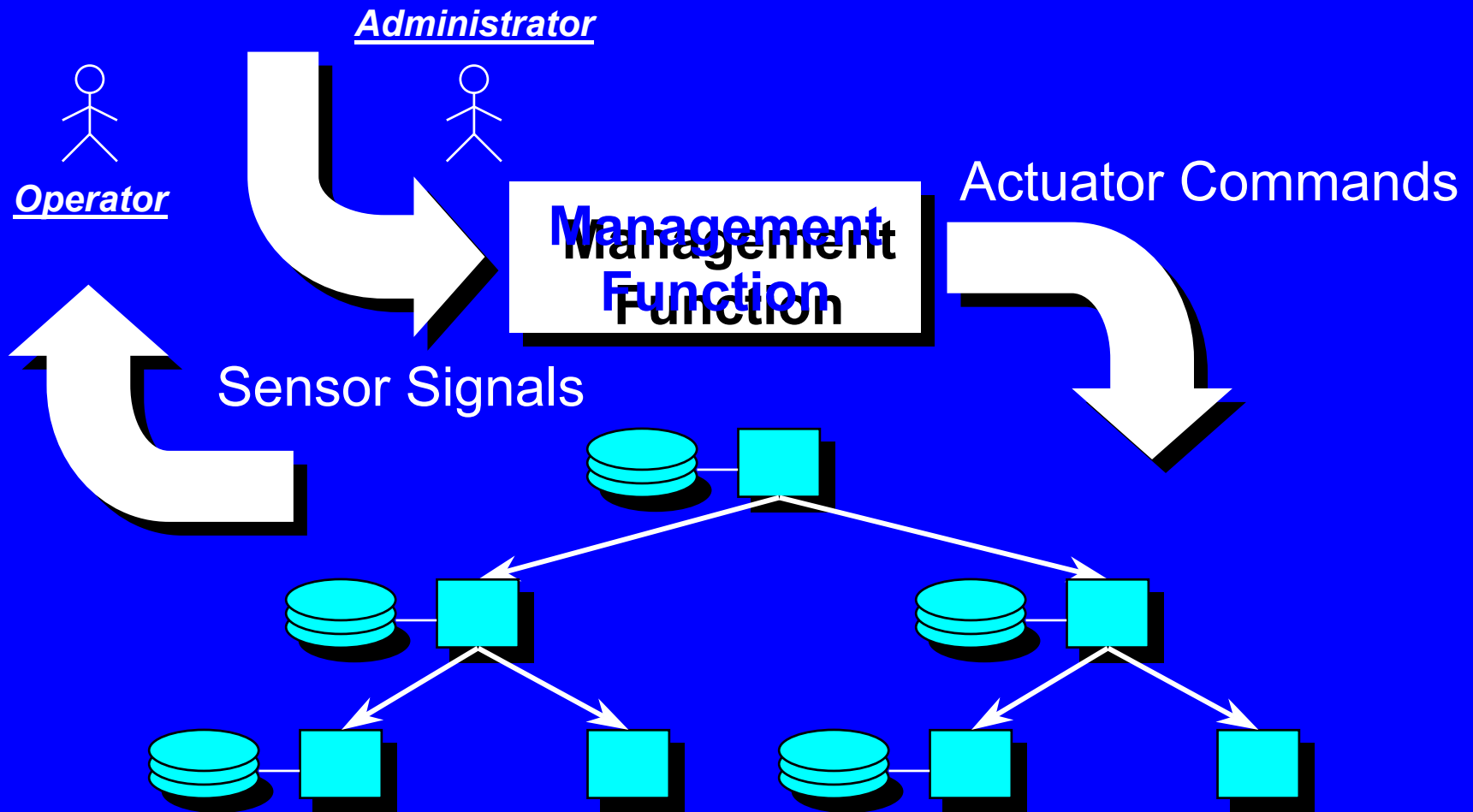
Survivability as (Re-)Active Control

- Control-loop model
- Automatic



Survivability as (Pro-)Active Management

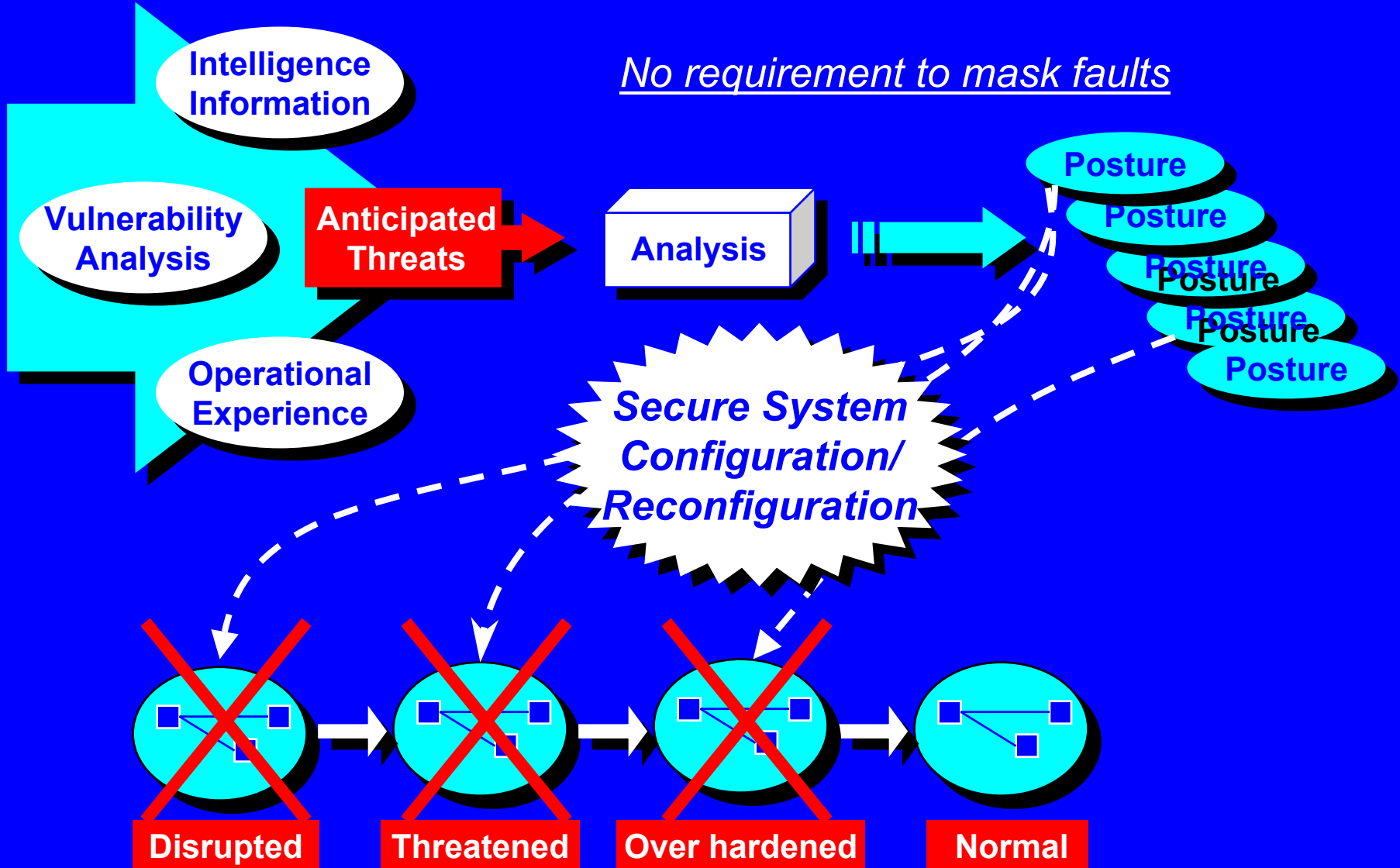
Intelligence, Planning, and Development



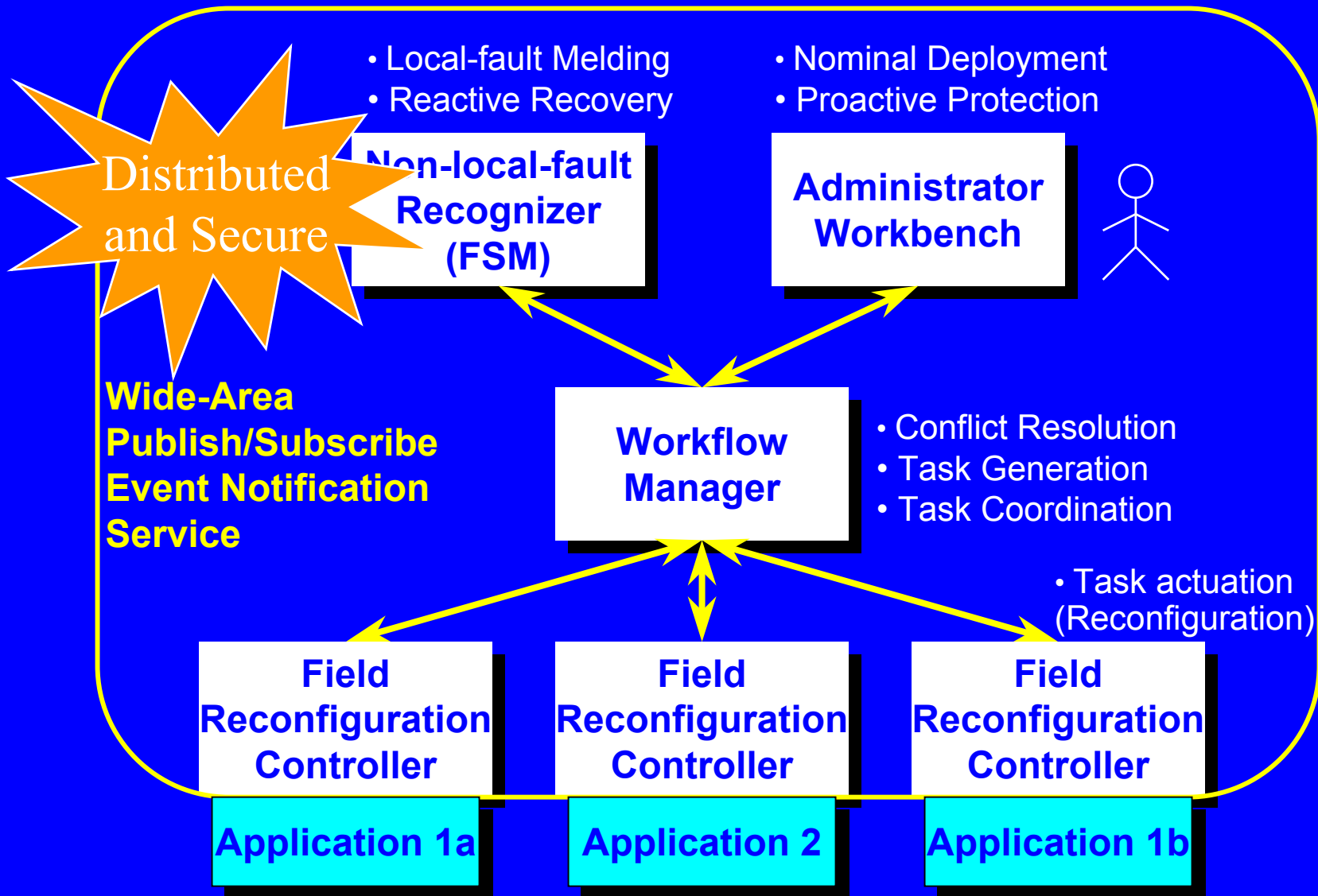
Postures

- ◆ Set of policies and procedures ensuring survivability
 - Against a particular set of threats to service
 - Tradeoff performance against protection
- ◆ Embodied as a particular configuration of components
 - providing a particular level of functionality
 - within a particular range of performance and security parameters

Posturing Process



Willow High Level Architecture



Case Study: Joint Battlespace Infosphere

- ◆ Goal: break open stovepipe information systems
- ◆ A JBI is:
 - a system of systems
 - that integrates, aggregates, and distributes information
 - to users at all echelons, from the command center to the battlefield



- ◆ Information exchange through Publish/Subscribe
- ◆ Transformation of data into knowledge through Fuselets

JBI Application Mockup

- ◆ *Command Theater Viewer*

- ◆ Three data sources

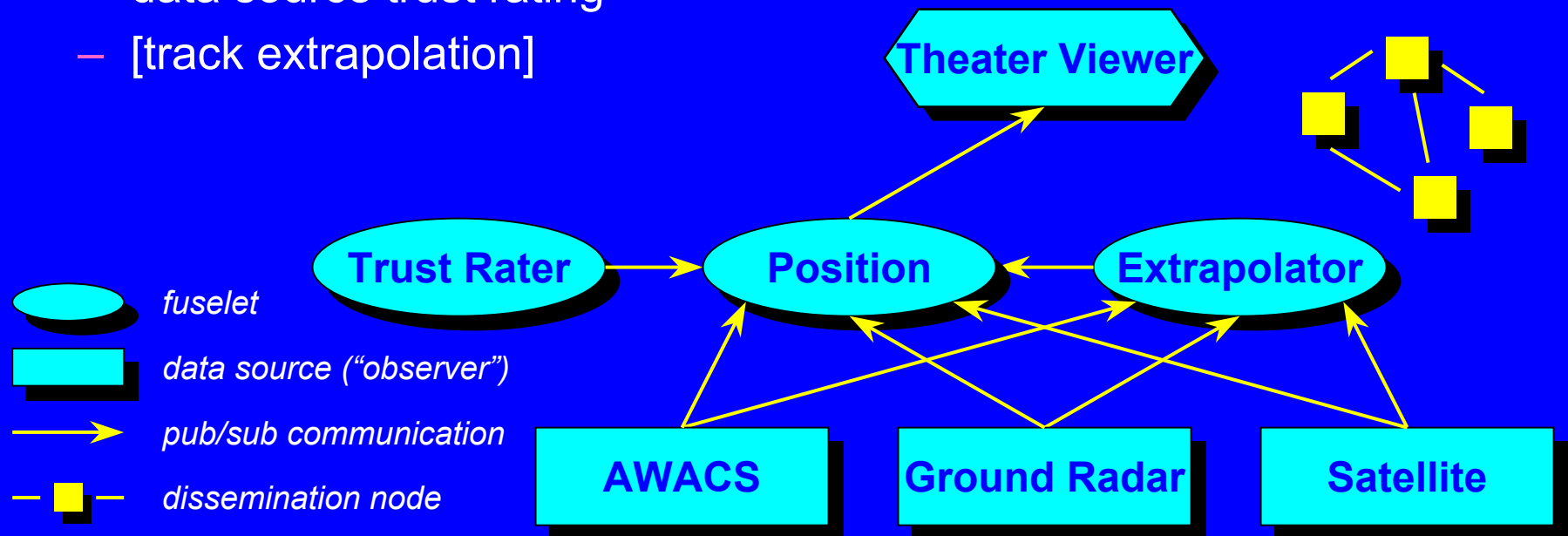
- force tracking

- ◆ Three fuselets

- position resolution
- data source trust rating
- [track extrapolation]

- ◆ Dissemination network

- distributed publish/subscribe message routing



JOINT BATTLESPACE INFOSPHERE

Visible Coordinates

29° 10' 0" N to 36° 20' 0" N Lat. 89° 43' 20" W to 103° 36' 40" W Long.

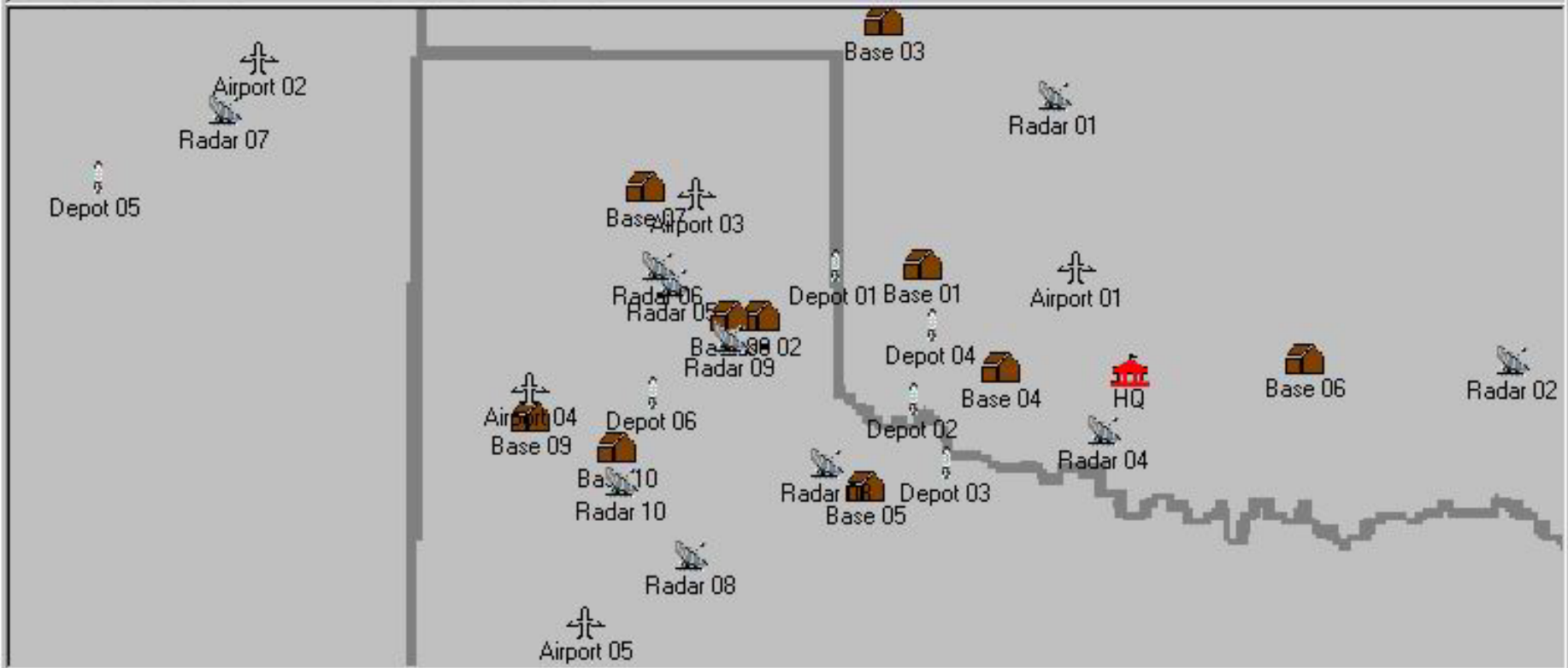
Airport Artillery Depot Base Headquarters Radar

Observable Attributes

ID: ° ' " N Lat. ° ' " W Long.

Mouse At

36° 6' 34" N Lat. 98° 52' 17" W Long.



JOINT BATTLESPACE INFOSPHERE

Visible Coordinates

29° 10' 0" N to 36° 20' 0" N Lat. 89° 43' 20" W to 103° 36' 40" W Long.

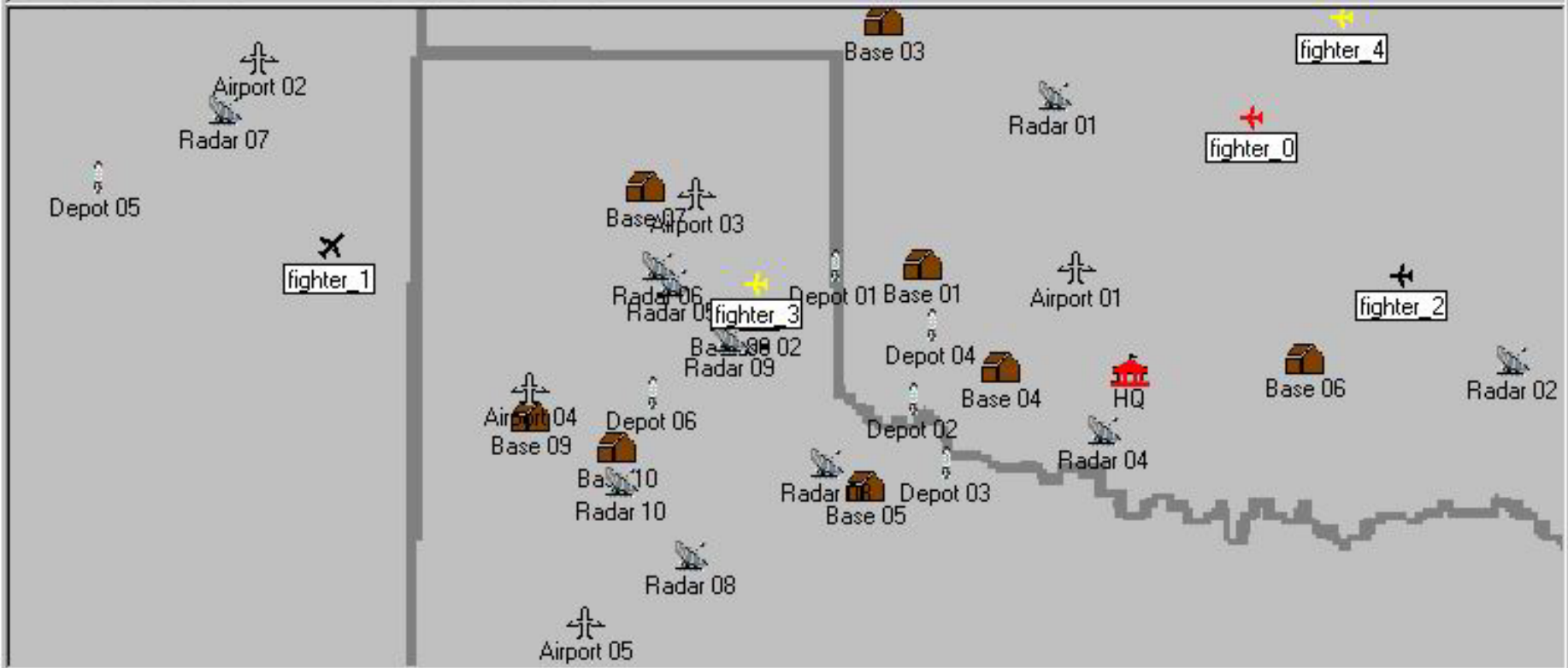
Airport Artillery Depot Base Headquarters Radar

Observable Attributes

ID: 35° 9' 12" N Lat. 92° 30' 24" W Long.

Mouse At

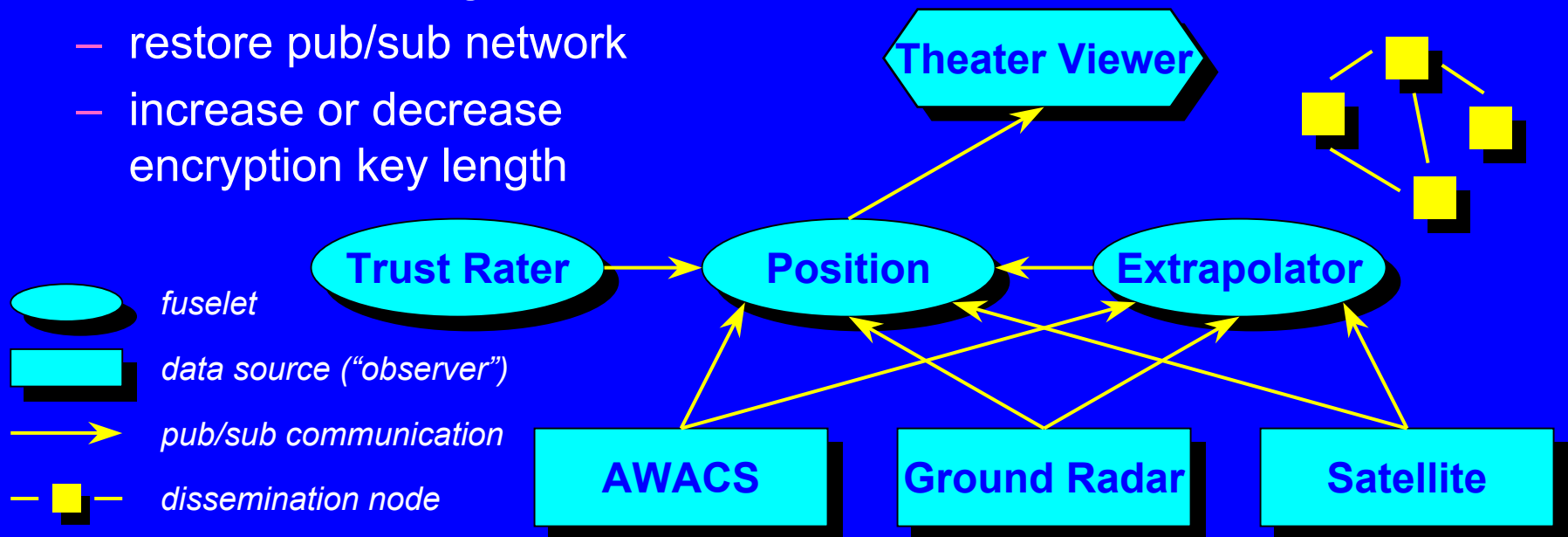
30° 50' 47" N Lat. 93° 9' 28" W Long.



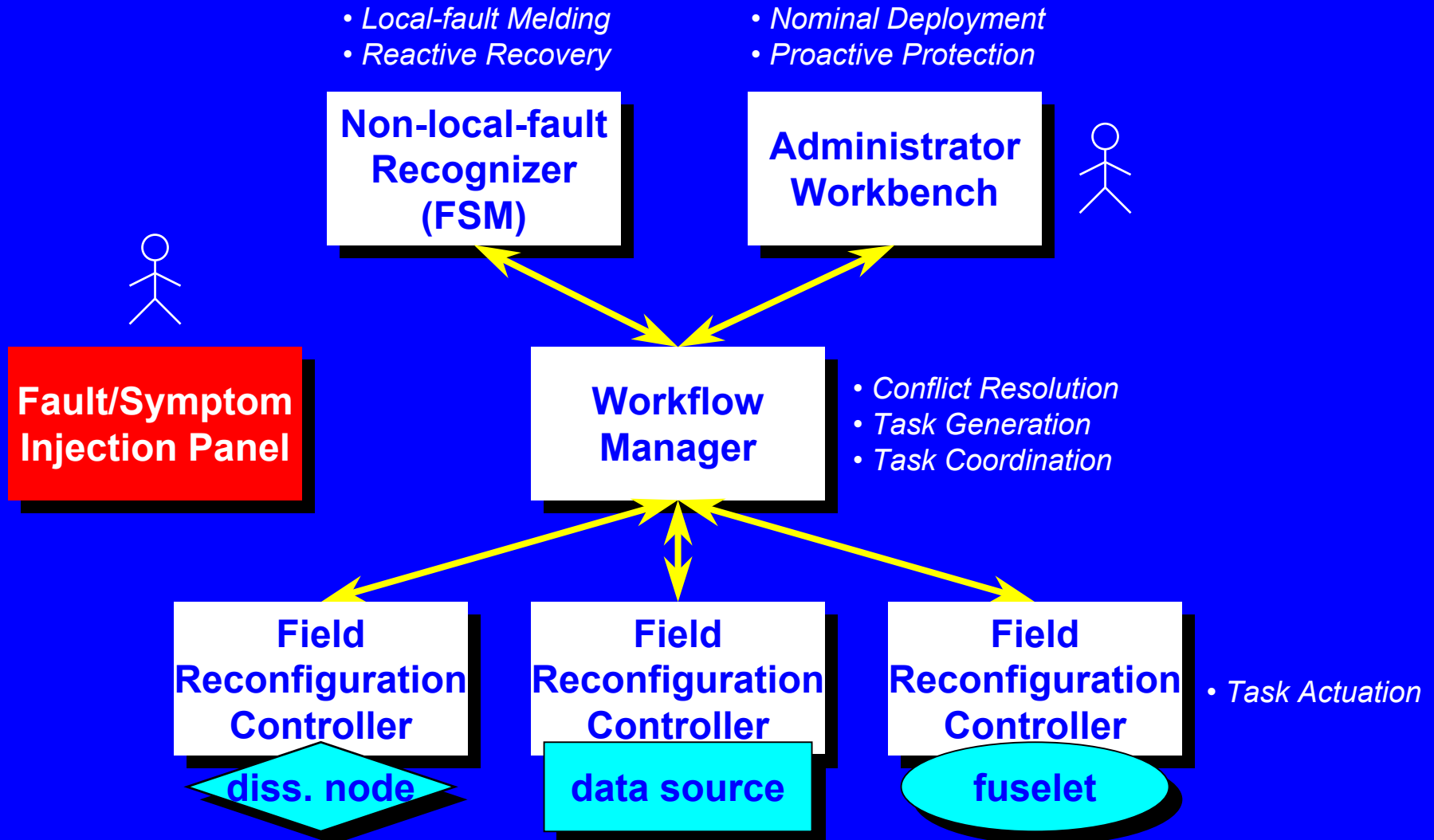
Scenarios

- ◆ Initial deployment
 - dissemination nodes, data sources, and fuselets
- ◆ Proactive reconfiguration
 - deploy extrapolator fuselet
- ◆ Reactive reconfiguration
 - restore pub/sub network
 - increase or decrease encryption key length

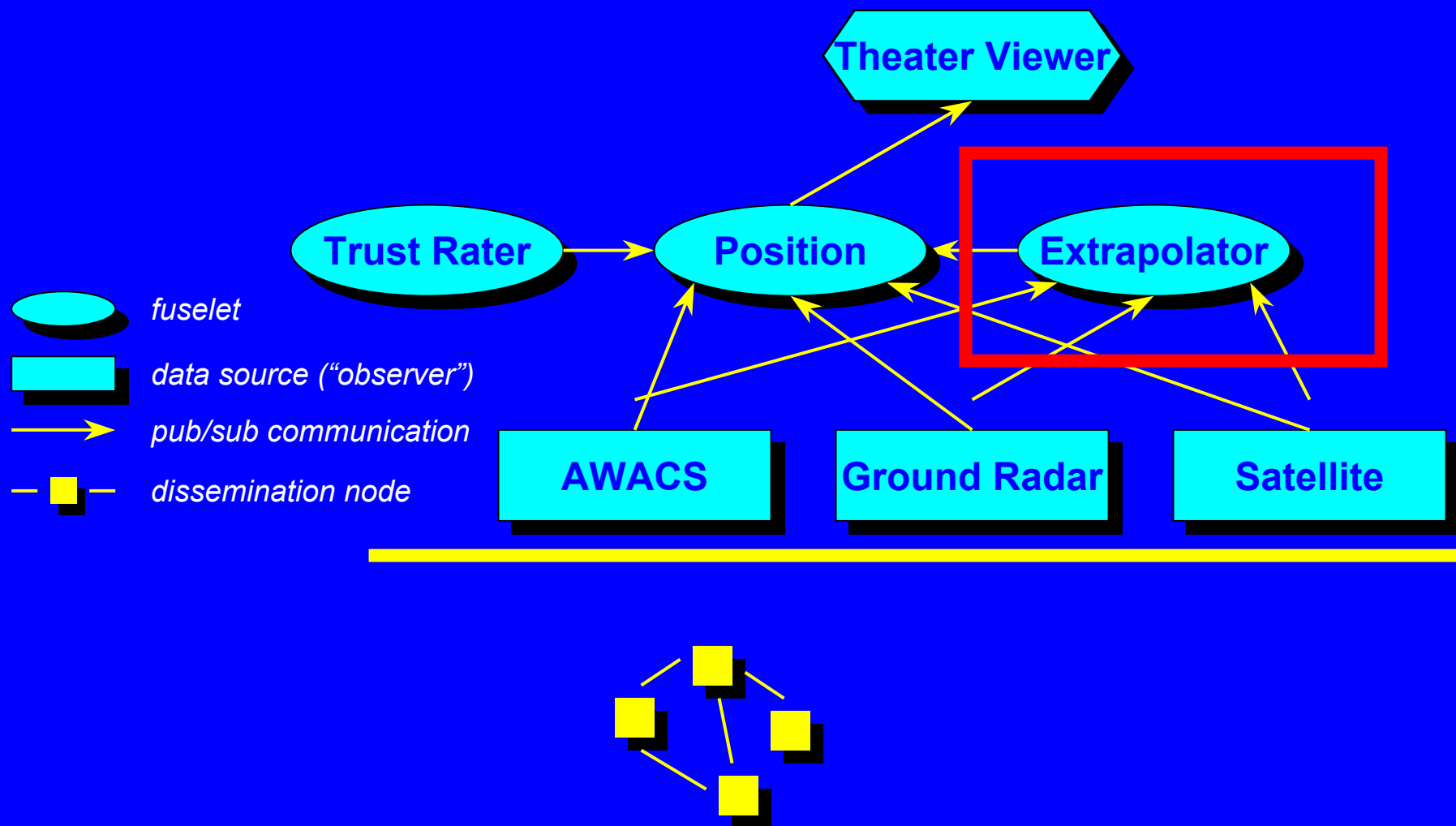
- ◆ Symptoms, faults, and intelligence
 - dissemination node failure
 - data source under attack
 - data source failure
 - IDS snooping notification



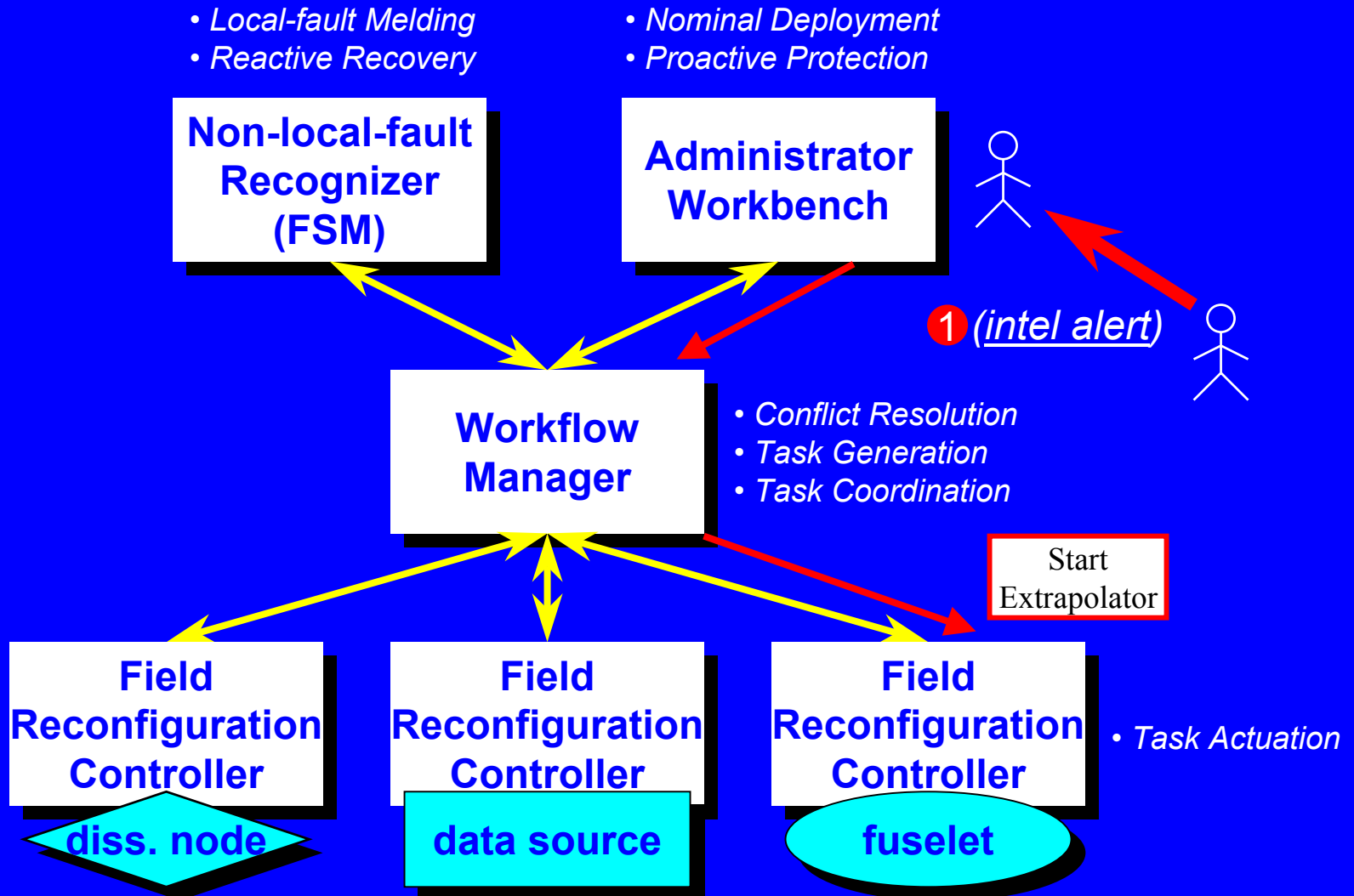
Willow Infrastructure for JBI



Step 1: Starting the Extrapolator



Proactive Instantiation of the Extrapolator



Administrator's Workbench Interface

Administrator's Workbench

Willow Controls

Install Uninstall

Network Operations

Query Release Sites Query Field Sites Reset

Release Sites

URL: Inventory: Update

Field Sites

Hosts: Inventory: Reset Update

Property Assignments

Property	Type	Value	
			Update

Controls

Monitor

Install
 Update
 Reconfigure
 Adapt
 Remove

Activities

Install Adapt/Repair Update
Remove Reconfigure Constrain

Notices

Host	Process	System	Success
tempest.adhoc	Install	jbi-0.0	<input checked="" type="checkbox"/>
elektra.adhoc	Install	jbi-0.0	<input checked="" type="checkbox"/>

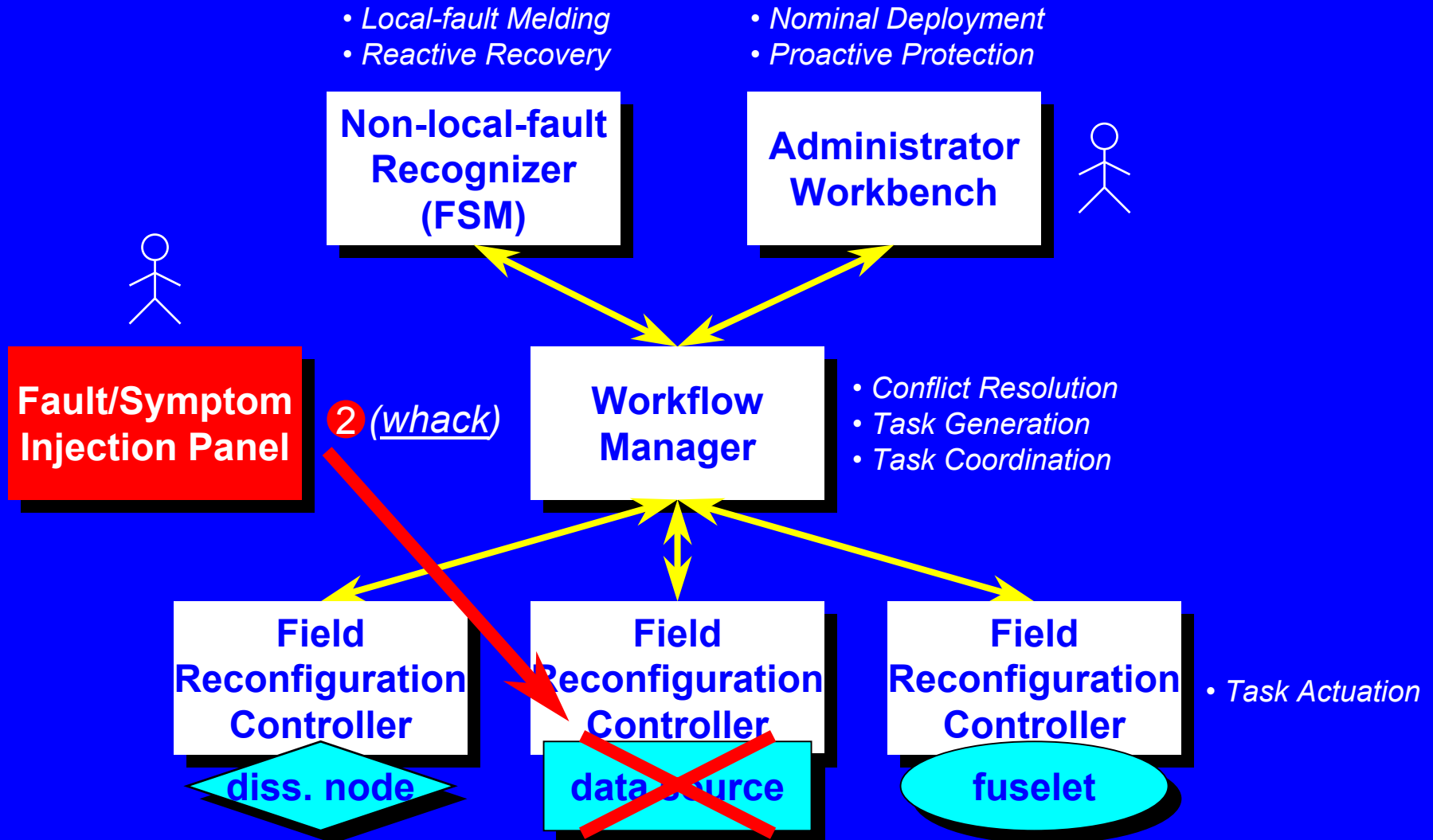
Software

Progress...

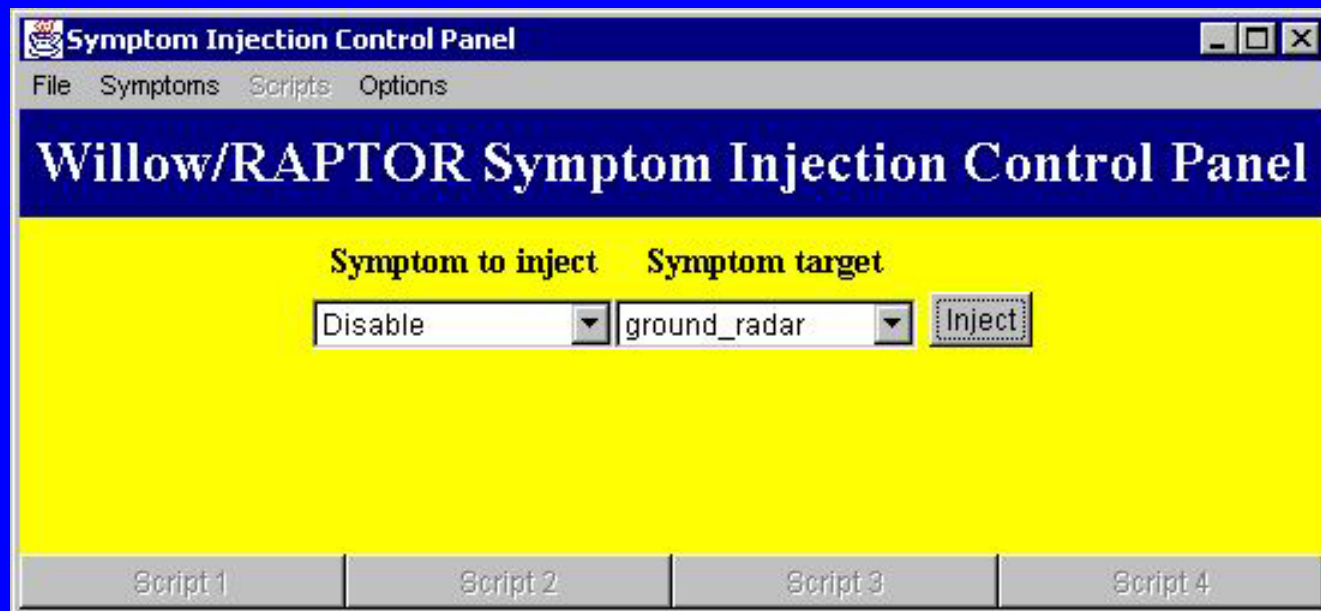
Installing extrapolater

- Retrieving new configuration
- Validating configuration
- Configuring system
- Checking assertions
- Resolving dependencies
- Retrieving artifacts
- Unpacking artifacts
- Post-install activities
- Updating registry

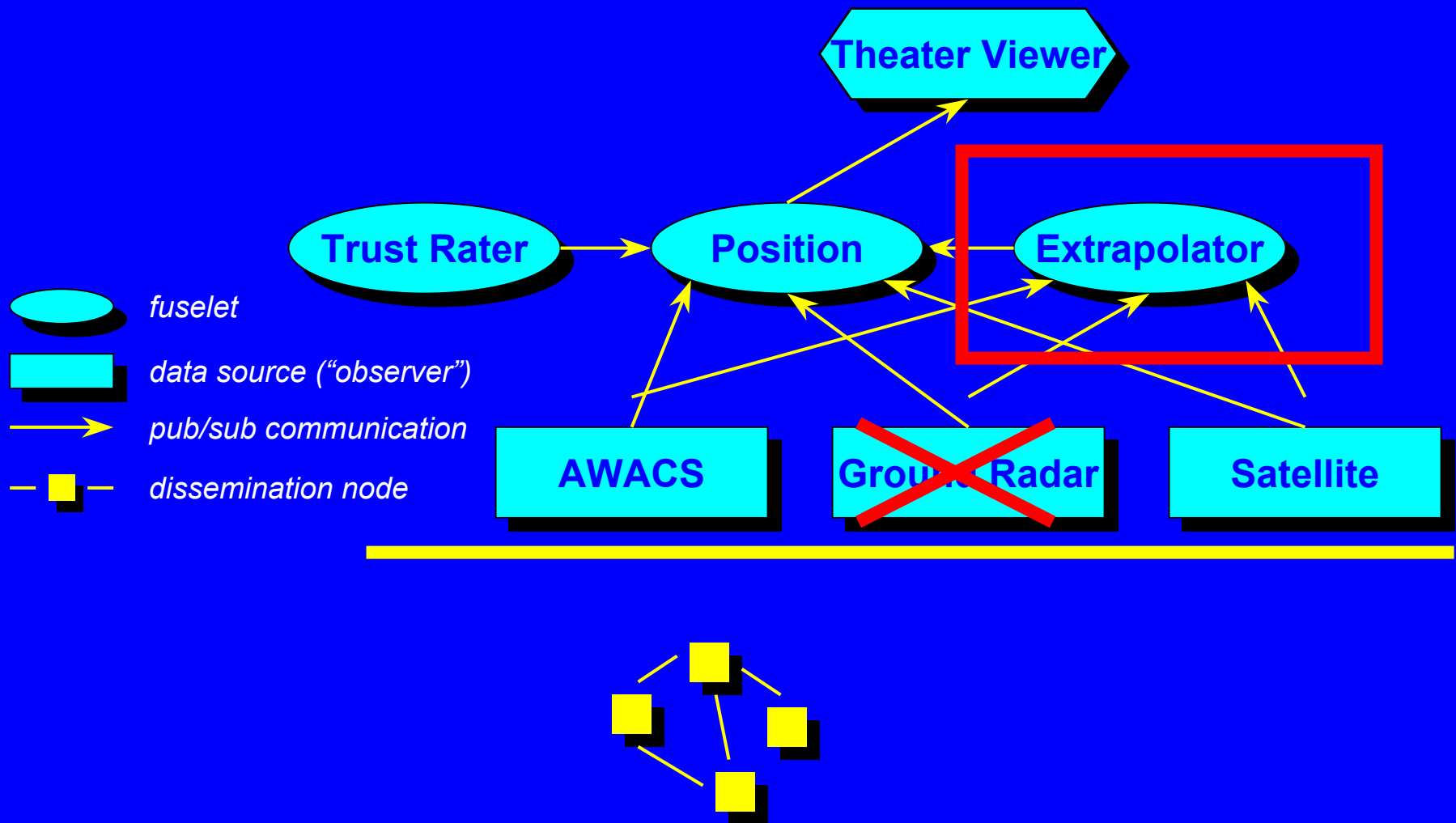
Step 2: "Whack" Ground_Radar Source



Fault Injection Panel Interface



New Configuration



JOINT BATTLESPACE INFOSPHERE

Visible Coordinates

29° 10' 0" N to 36° 20' 0" N Lat. 89° 43' 20" W to 103° 36' 40" W Long.

Airport
 Artillery Depot
 Base
 Headquarters
 Radar

Observable Attributes

ID: 32° 18' 2" N Lat. 98° 20' 32" W Long.

Mouse At

36° 13' 17" N Lat. 97° 57' 10" W Long.



Research Thrusts

- ◆ Vulnerability Analysis / Survivability Planning
 - Modeling large-scale networked applications
 - Synthesizing monitor and control code
- ◆ Configuration/Reconfiguration Services
 - Configurability models and architectures
 - Resident- versus depot-based reconfiguration
- ◆ Securing Management/Control Infrastructure
 - Mediated trust authority management
 - Trusted code on untrustworthy platforms
- ◆ Model development to drive postures
- ◆ Workflow to coordinate reconfigurations

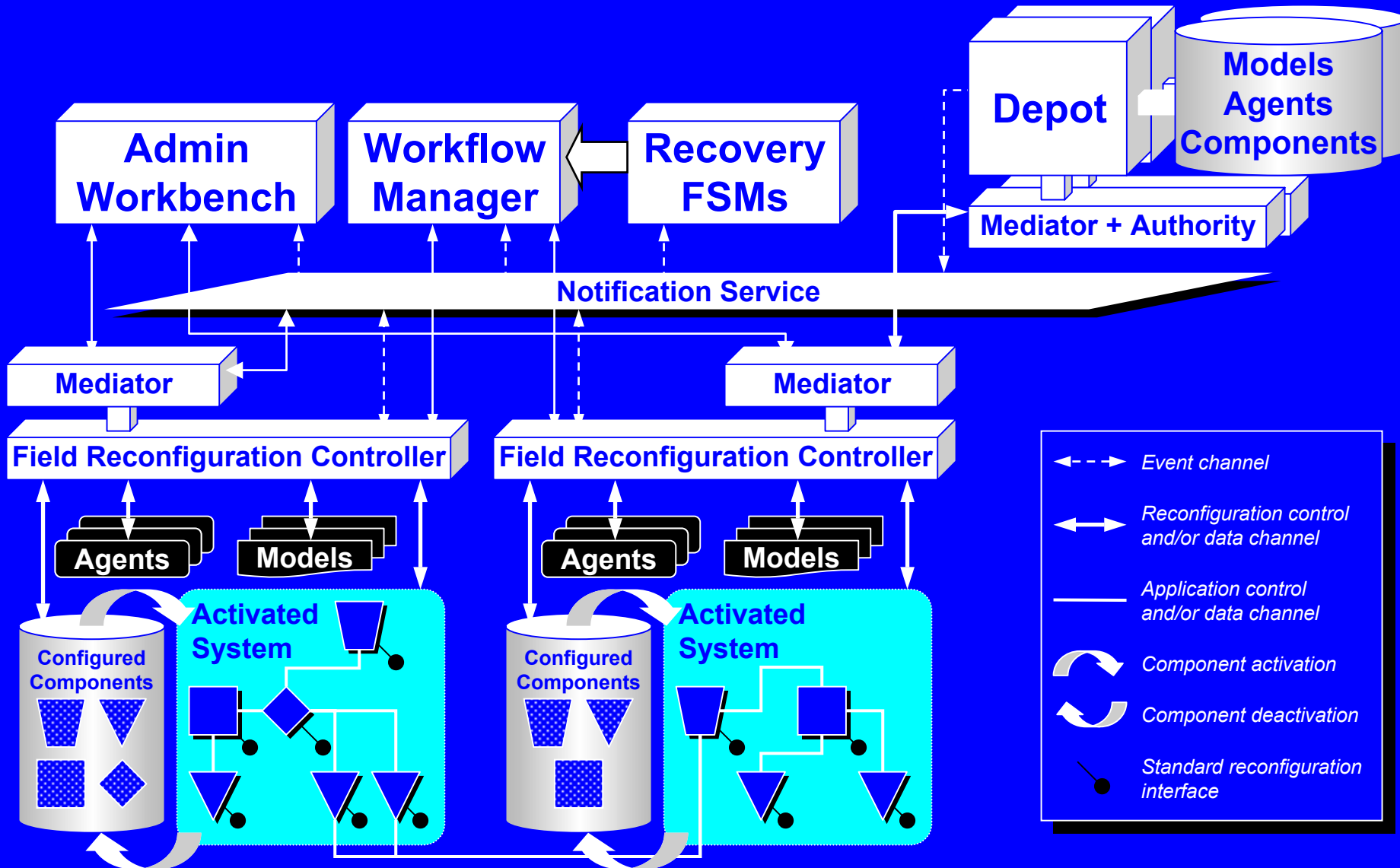
Emerging Principles

- ◆ Control Loop as High-Level Architecture
 - Sensors, actuators, control function
 - (Re-) active control and (pro-) active management
- ◆ Workflow as Model of Conflict Resolution
 - Multiple, independent inputs to control function
- ◆ Pervasive use of architectural models
 - Declarative and Specification-Driven Actions
 - System families, fault detection, reconfiguration
- ◆ Publish/Subscribe to Achieve Scale
 - Loose coupling

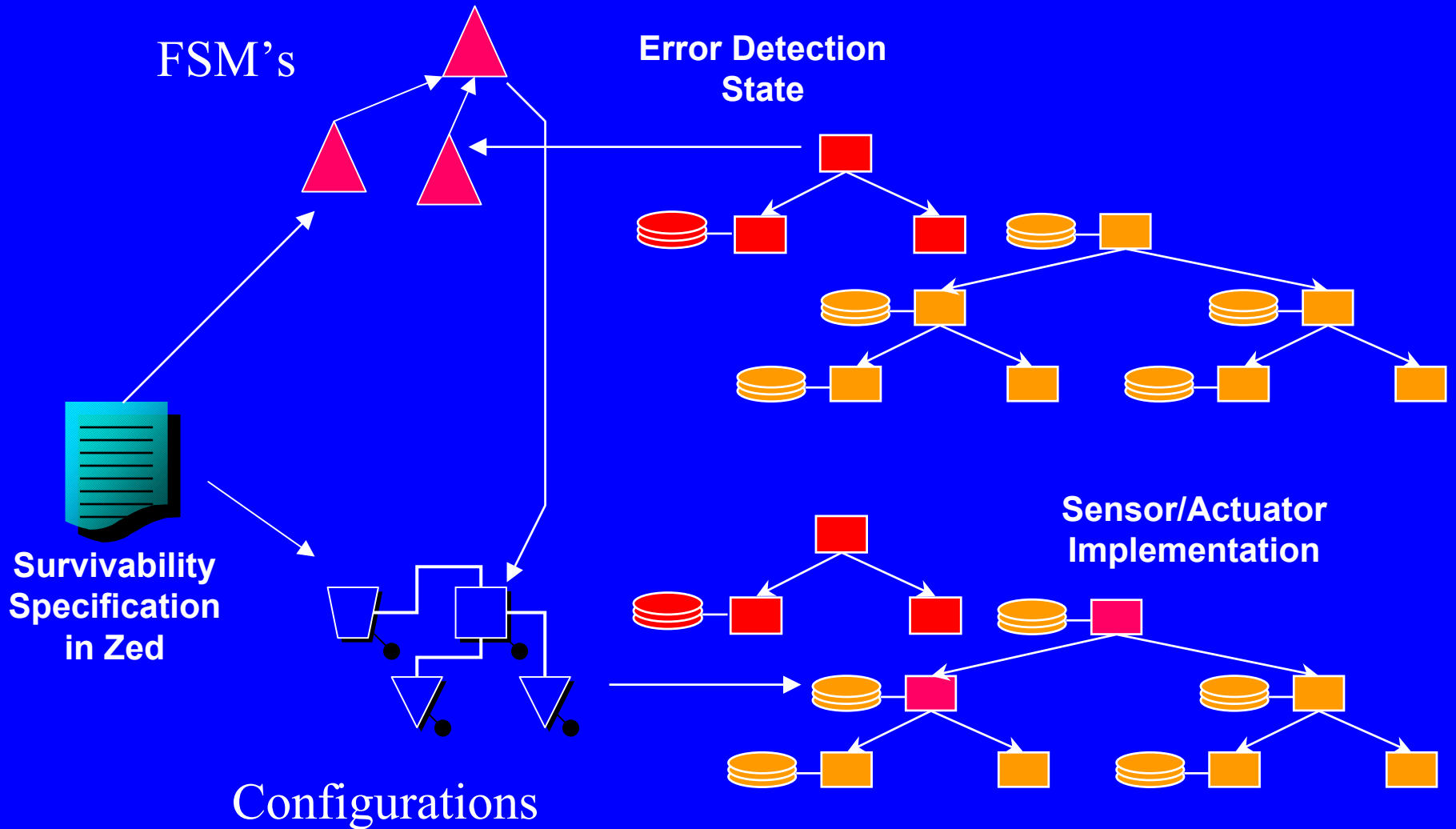
Looking to the Future

- ◆ Devise a sound theoretical basis for reasoning about and controlling the dynamics of survivability strategies and tactics
- ◆ Develop middleware to communicate with large numbers of FRCs by property (versus address)
- ◆ Model the variability and dynamics of large-scale, component-based systems and their run-time environments
- ◆ Develop an improved infrastructure that lowers the entry barrier to adopting our approach

Willow Detailed Architecture



Survivability Analysis



Configuration/Reconfiguration Support

- ◆ Configure and monitor a deployed system
- ◆ Reconfigure in the face of perceived threat
 - Implies appropriate configuration available
- ◆ Reconfigure in the face of actual disruption
 - Implies operable configuration available
- ◆ Architecture for reconfigurable systems
- ◆ Infrastructure for configuring, monitoring, and reconfiguring systems
 - Implies sensors, actuators, and control function