

The Willow Project: Survivability Through Reconfiguration

Alexander Wolf and Dennis Heimbigner

University of Colorado at Boulder

John Knight

University of Virginia

Prem Devanbu, Michael Gertz and Karl Levitt

University of California at Davis

<http://www.cs.colorado.edu/serl/willow/>

Threats To Service

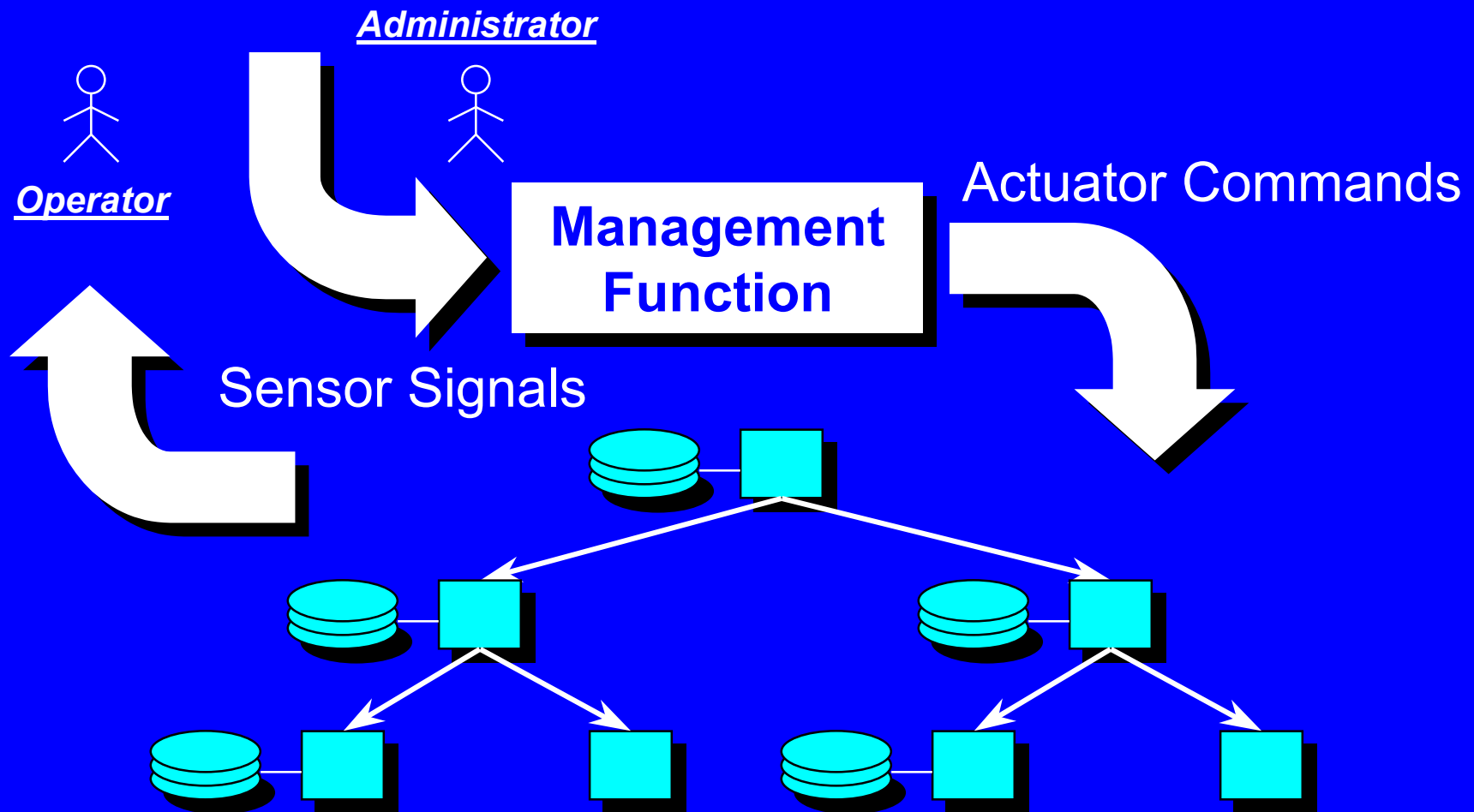
- ◆ Errors by Operators
- ◆ Errors in Operational Procedures
- ◆ Software Faults
- ◆ Software Design Degradation
- ◆ Changes in Environmental Conditions
- ◆ Hardware Degradation Faults
- ◆ Hardware Design Faults
- not to mention...
- ◆ Malicious Attacks

Secure Configuration/Reconfiguration

- ◆ Plan and Evaluate Survivability Strategies
- ◆ Configure and Monitor Deployed Systems
 - Sensors and actuators
- ◆ Reconfigure to Meet Level of “Threat”
 - Proactive
 - Implies appropriate configuration available
- ◆ Reconfigure in Response to “Damage”
 - Reactive
 - Implies operable configuration available

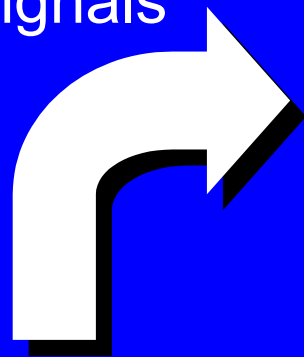
Survivability as Active Management

Intelligence, Planning, and Development

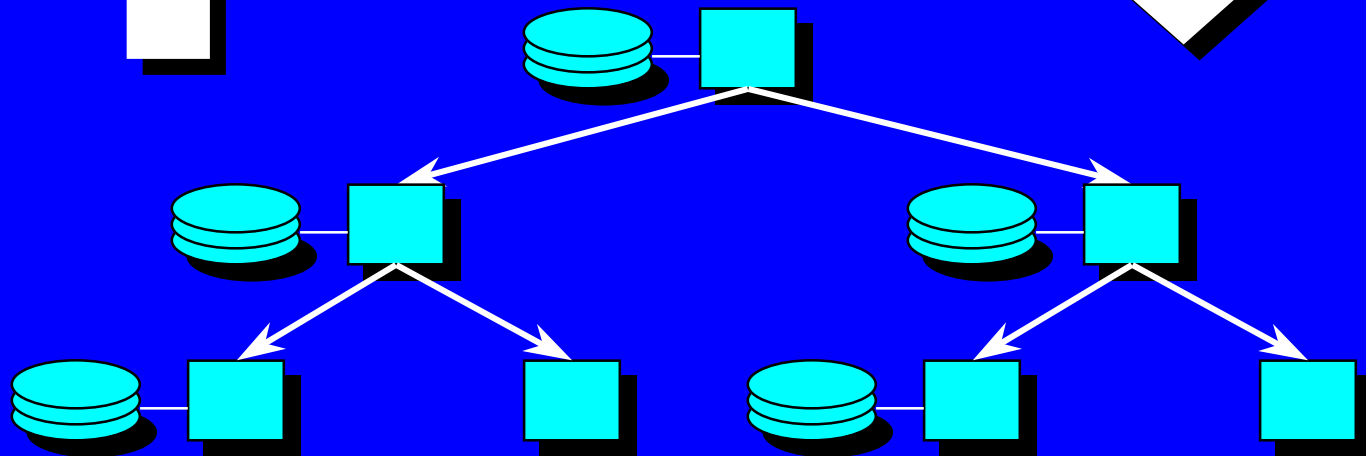
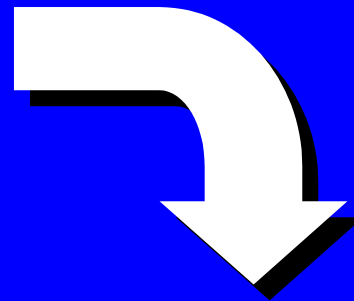


Survivability as Active Control

Sensor Signals



Actuator Commands



Recent Activities and Accomplishments

- ◆ Reoriented the Administrator Workbench
 - From “user centric” to “network centric”
- ◆ Adopted a “Workflow” Reconfiguration Model
 - Describes goals and tasks in unified framework
 - Mediates requests from multiple task “experts” administrators, network repair agents, ...
 - Enables reflection on network state
- ◆ Developed JBI Survivability Demonstration
 - With cooperation from AFRL JBI Team

Joint Battlespace Infosphere

- ◆ Information exchange through Publish/Subscribe
- ◆ Transformation of data into knowledge through Fuselets
- ◆ Tailorability and flexibility through Force Templates
- ◆ Distributed collaboration through Knowledge Objects



The JBI is a system of systems that integrates, aggregates, and distributes information to users at all echelons, from the command center to the battlefield

JBI Application Mockup

- ◆ *Command Theater Viewer*

- ◆ Three data sources

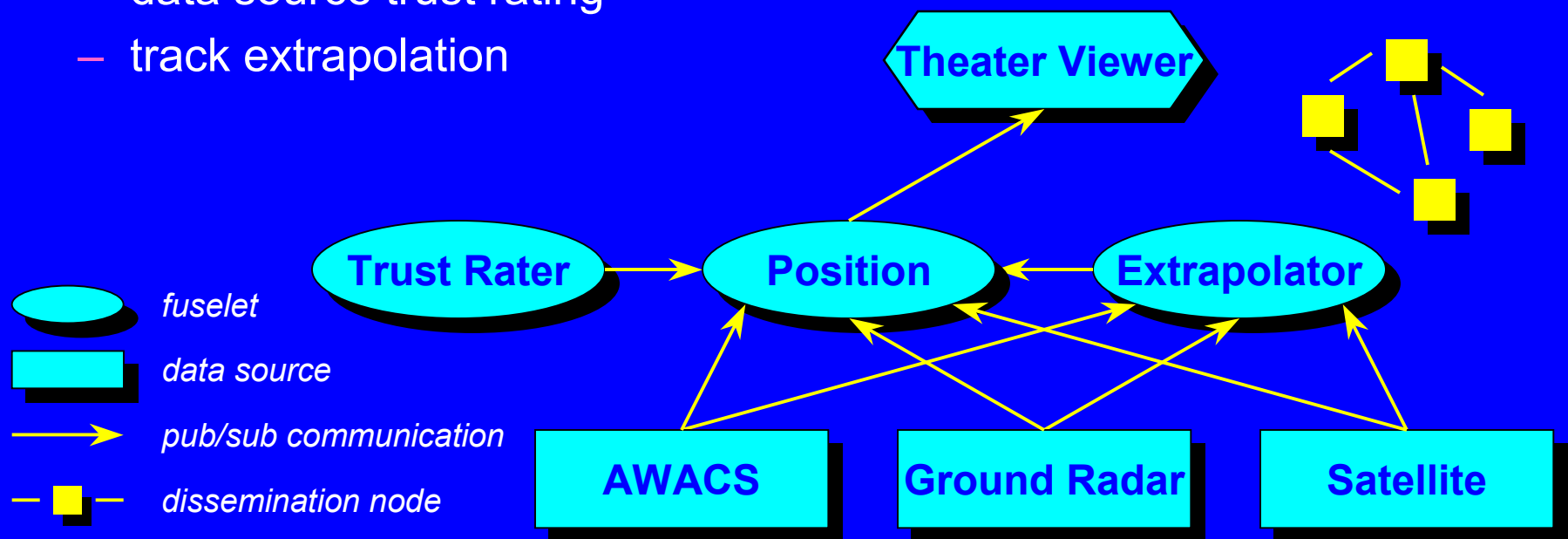
- force tracking

- ◆ Three fuselets

- position resolution
- data source trust rating
- track extrapolation

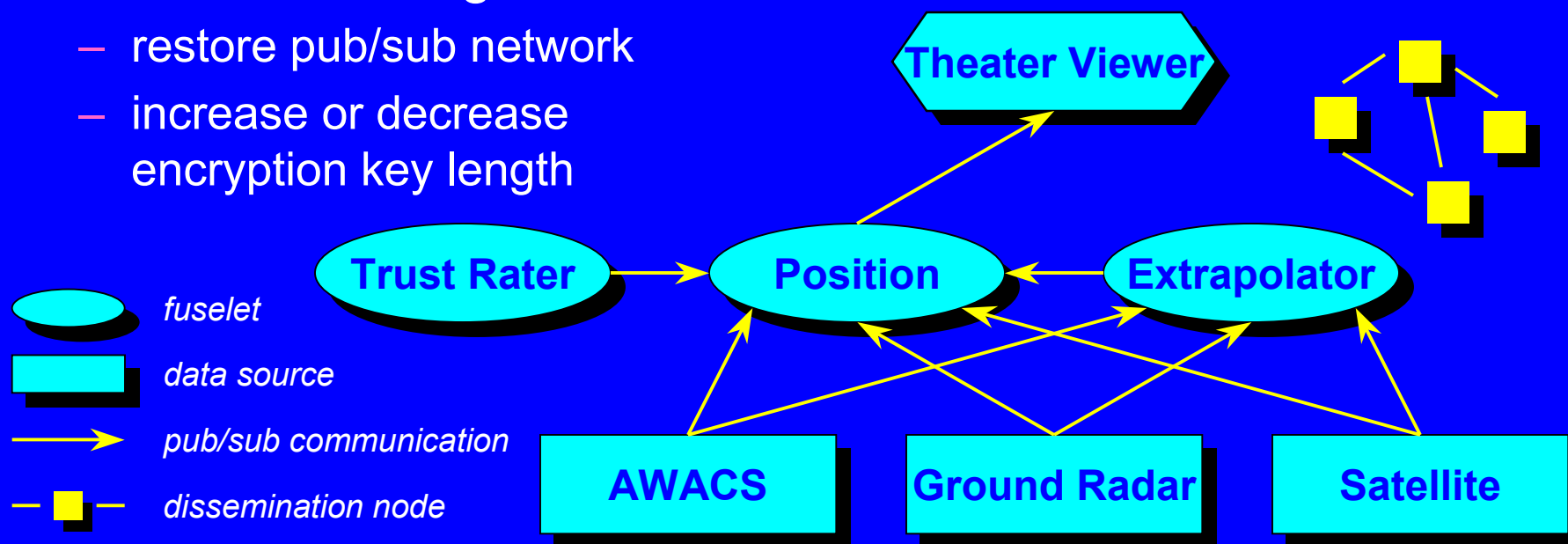
- ◆ Dissemination network

- distributed publish/subscribe message routing
- implemented using Siena wide-area publish/subscribe event notification service

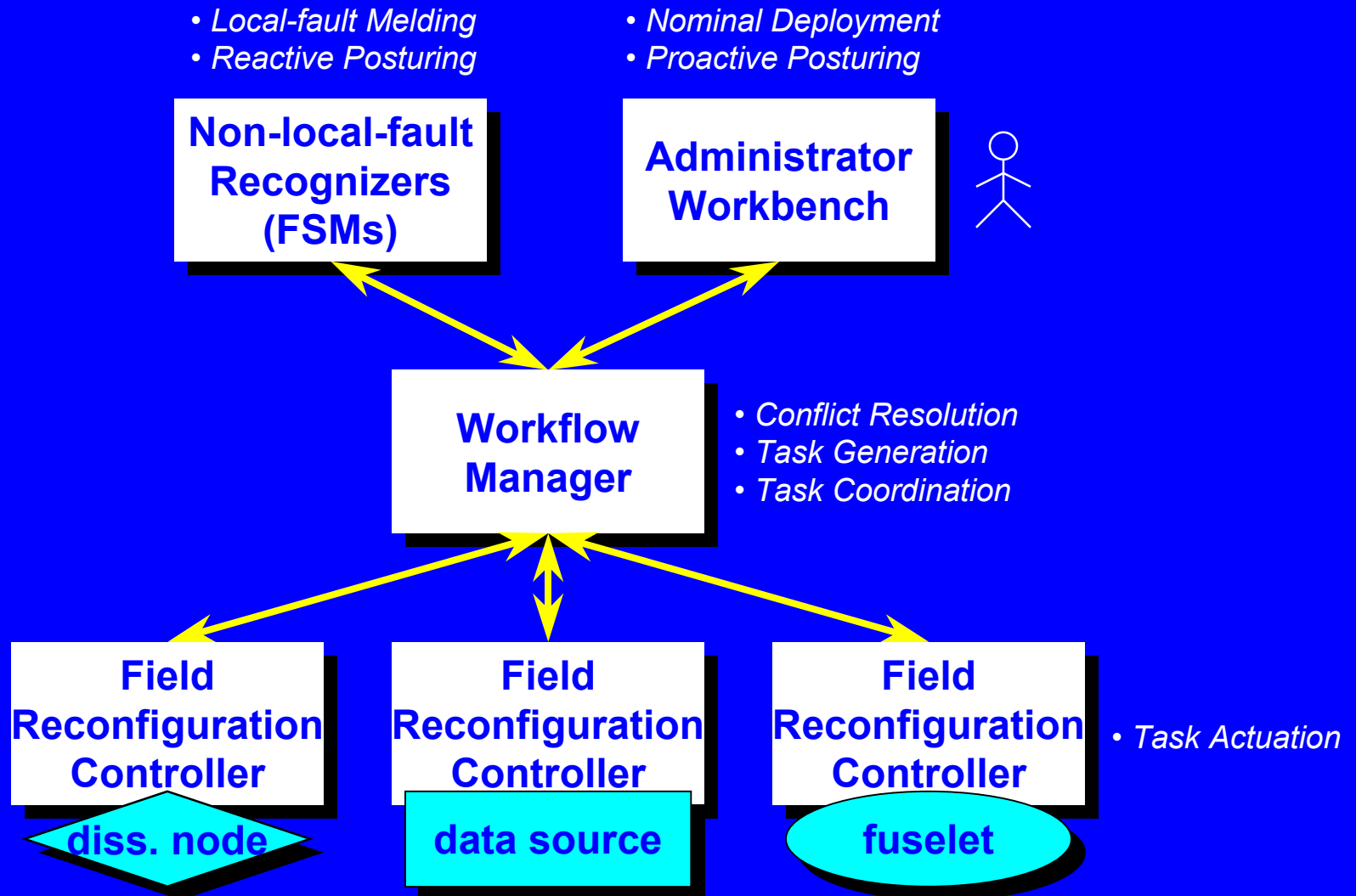


Scenarios

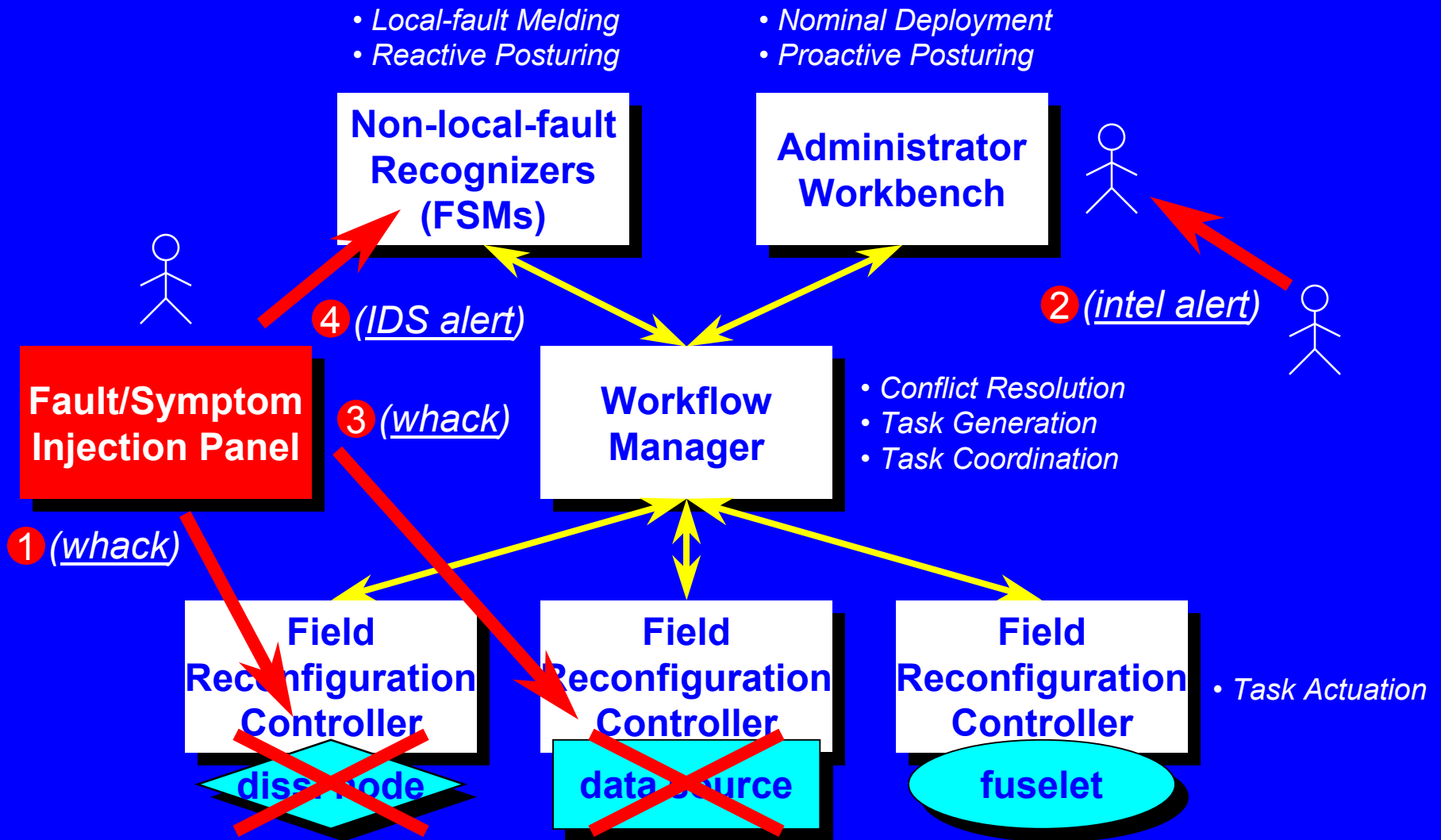
- ◆ Initial deployment
 - dissemination nodes, data sources, and fuselets
- ◆ Proactive reconfiguration
 - deploy extrapolator fuselet
- ◆ Reactive reconfiguration
 - restore pub/sub network
 - increase or decrease encryption key length
- ◆ Symptoms, faults, and intelligence
 - dissemination-node failure
 - data-source under attack
 - data-source failure
 - IDS snooping notification



Willow Infrastructure



Fault/Symptom Harness



Conclusion

- ◆ JBI provides many interesting challenges
- ◆ Integration process helps reveal architectural mismatches, opportunities for connection points, new ways to solve hard problems
- ◆ Some of the many next steps
 - Expand JBI demonstration
 - Fully address fault detection and network state
 - Gain finer control over running applications
 - » move from “whole programs” to program components
 - Secure the infrastructure (e.g., pub/sub network)