High Confidence Software & Systems

Report to PITAC

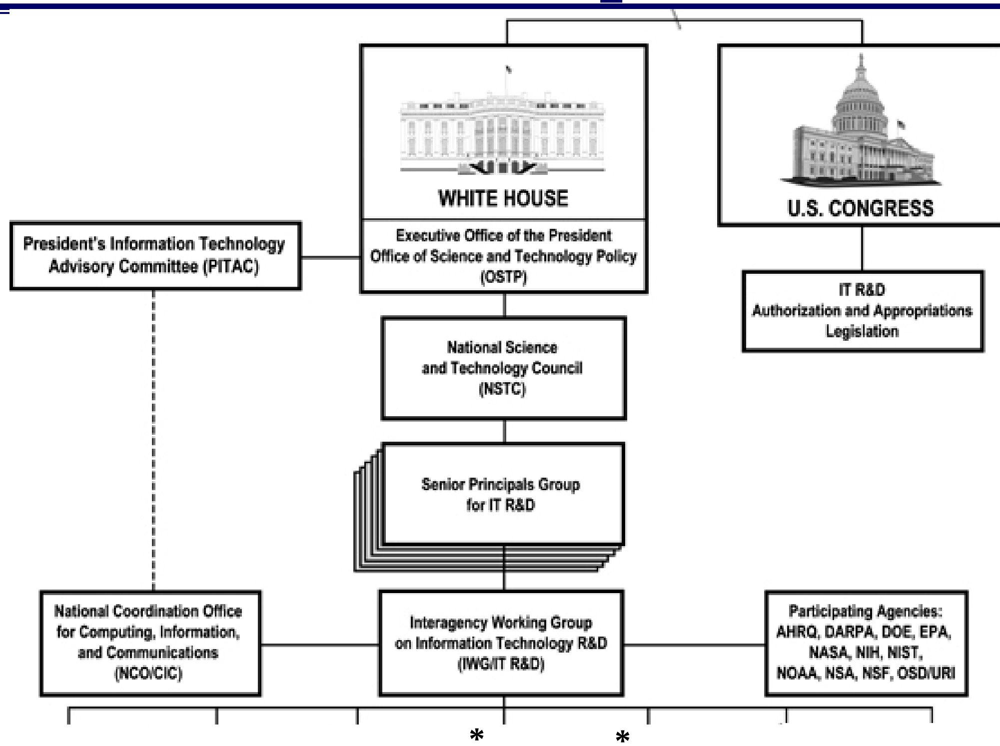
May 10, 2001

Dr. Shankar Sastry, UC-Berkeley
(Former Director, DARPA/ITO)

Dr. Helen Gill, NSF/DARPA
(HCSS CG Co-Chair)

Dr. Gary Koob, DARPA
(HCSS CG Co-Chair)

Information Technology Research and Development



***new PCA**

HCSS Coordinating Group

- Group Structure and Activities
  - Agencies currently actively participating: DARPA, NSF, NASA, NSA, NIST, FAA, FDA, other DoD organizations
  - HCSS Research Needs developed with input from research community
  - HCSS Interagency Workshops
    - Critical Aviation Systems, February 1, 2000
    - PKI for Advanced Network Technologies, April 27-28, 2000
    - High Confidence Aviation Systems, June 21, 2000
    - Future Directions in Hybrid and Embedded Systems, October 25, 2000
    - Medical Devices Software Safety Workshop, November 20, 2000
  - Separate HCSS PCA established

HCSS Technology Goals

- *Provide a sound theoretical, scientific, and technological basis for assured construction of safe, secure systems.*
- *Develop hardware, software, and system engineering tools that incorporate ubiquitous, application-based, domain-based, and risk-based assurance.*
- *Reduce the effort, time, and cost of assurance and quality certification processes.*
- *Provide a technology base of public domain, advanced-prototype implementations of high-confidence technologies to enable rapid adoption.*
- *Provide measures of results.*

HCSS Research Agenda

- Foundations
  - Safety
  - Security
  - Assurance
- Engineering & Experimentation
  - Assured PKI
  - Control Systems
  - Hardware Verification
- Technology & Tools
  - Programming Languages, tools, environments
  - Systems Software
  - Metrics & Evidence
  - Robust System Design
- Pilot Applications
  - Aviation Safety
  - Medical Device Safety
  - Digital Government
  - PKI for Advanced Networks

HCSS Basic and Technology Research

HCSS Foundations:

Supporting theory and scientific base for engineering and certifying High Confidence Software & Systems

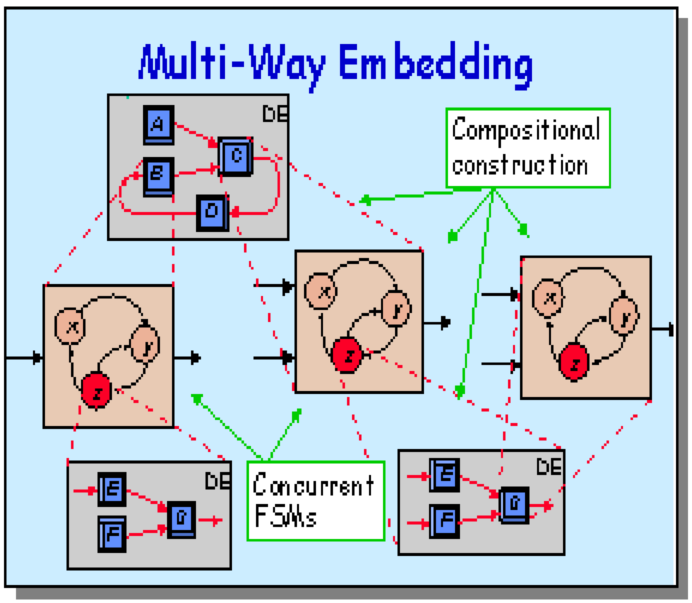
- Research areas:
  - Theory
    - Safety
    - Security
    - Assurance
  - Specification
  - Interoperability
  - Composition

HCSS Tools and Techniques:

Developing the engineering tools, libraries, and techniques required to build and certify large-scale, high confidence systems.

- Research Areas:
  - Assurance-bearing programming languages & tools, and correct-by-construction code synthesis environments
  - Modeling and simulation
  - Robust system design
  - Monitoring and detection
  - Validation
  - Evidence and metrics
  - Process

Foundations - Issues

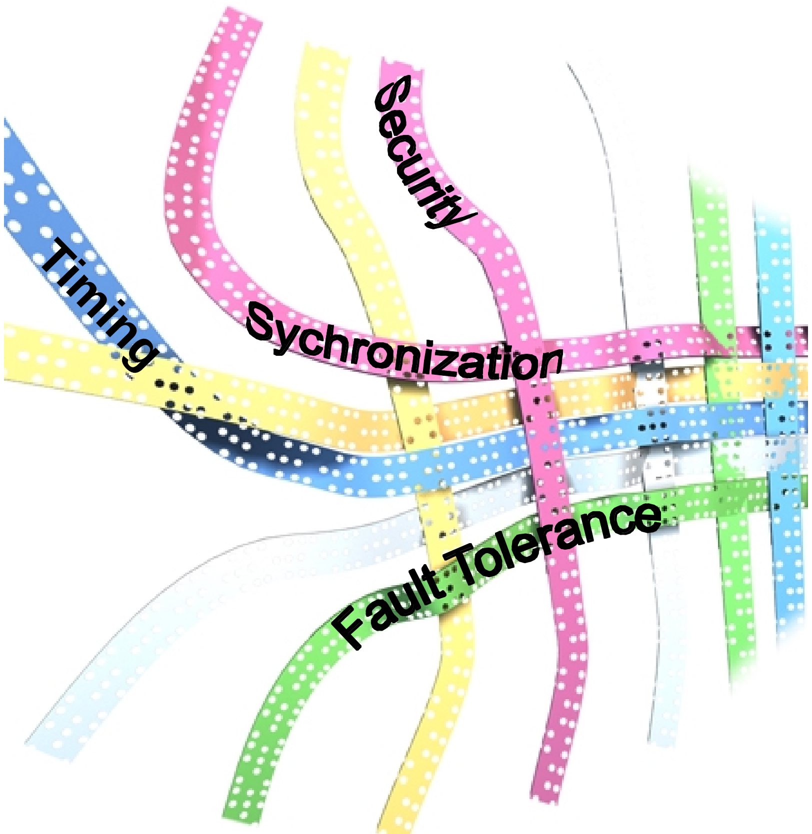


- Theory
  - Modeling and reasoning
    - Physical effects of system actions controlled by software, hybrid discrete/continuous models
    - Assurance and trustworthiness, criticality, uncertainty
    - Event detection and propagation analyses, scalable approaches to evidence and forensics
    - Model validation
  - Domain theories: safety, security, adaptive software and systems; critical properties
- Composition
  - Scalability
    - Hierarchical model composition: refinement/abstraction, peer hierarchies
  - Interference
    - Property composition and interaction

Foundations - Issues

- Specification
  - Notations
    - General purpose vs. domain-specific, problem-based
    - Usability, soundness, support for analysis
    - Language and logic automation/interaction
- Interoperability
  - Mixed strategies and theories
    - Formal/informal; complete/incomplete; deterministic/non-deterministic/stochastic; general/domain-specific; discrete/continuous; abstract/concrete/multilevel; compositional/interfering
    - Software, operating systems, and middleware
    - Layered vs. peer components, sound theoretical frameworks for specialization, staging, adaptation

Tools & Technologies - Issues



- Interoperable robust system design technology
  - Domain and requirements analysis tools
  - End-to-end (system, environment, uncertainty/disturbance) modeling and simulation tools, model-based runtime frameworks
  - Verified design patterns and instantiation support
  - Monitoring, detection, fault identification, tolerance, and adaptation mechanisms
- Assured software technology
  - Language as a carrier for logic
  - Correct-by-construction software
    - Integrated mathematical design and software generation technology
    - High-confidence middleware and OS components
    - Formal aspect-oriented programming
  - Domain-specific language and tool technology

Tools & Technologies - Issues

- Evidence and assurance technology
  - – Tools for practical, sound evidence extraction and management
    - ➢ Coordinated formal, analytic and test-generating tools
    - ➢ Lightweight verification and extended type systems
    - ➢ Proof-carrying code
    - ➢ Assume-guarantee reasoning
    - ➢ Testing for validation
- Next generation hardware/software co-design
- HCSS Building Blocks
  - – Technology base of components for implementing and checking high-confidence properties

HCSS Technology Evaluation and Transition

HCSS Engineering and Experimentation:

- Evaluate tools and techniques at realistic scales
- Derive empirical data about increased confidence and cost effectiveness
- Provide reference implementations & evidence
- Experiment in challenging system engineering areas
- Provide useful building blocks
  - Software control of physical systems
  - Hardware /software platforms
  - High mobility systems
  - Assured public key infrastructure
  - Assured middleware

HCSS Pilot Applications:

- Critical Domain Applications, e.g.,
  - Aviation, Transportation Safety
  - Medical/Biological Device Safety
  - Digital Government
  - Public Key Infrastructure for Advanced Networks
  - Others to be Defined

Critical Aviation Systems Workshop

- Held February 1, 2000, and hosted by FAA
- Organized by NASA, FAA, DARPA and AFRL
  - Sponsored by HCSS Coordinating Group
- Current Research Concerns
  - NASA: Small Aircraft Transport System (SATS) Program development, aviation safety mission
  - FAA: certification – RTCA Task Force IV, future national airspace planning, free flight
  - DARPA: Software Embedded Control, autonomous systems
  - AFRL: collision avoidance, special air space, CONUS flight
- Conclusion – major research needs:
  - Airspace management
  - Cost of certification, re-certification
  - Strong potential exists for useful collaboration among NASA, FAA, DARPA, and AFRL

PKI for Advanced Network Technologies Workshop

- Held April 27-28, 2000 at NIST
- Organized by NIST (host), CIAO, with help from DARPA
- Coordinated activity of
  - High Confidence Software and Systems Coordinating Group
  - Coordinating Group for Large Scale Networking/SII
  - Critical Infrastructure Protection
- Focus
  - Discuss technical context for High Confidence Public Key Infrastructure
  - Explore roadmap for High Confidence PKI
    - Optimized PKI for next generation networks
    - Tools for high confidence – test and assurance
    - Legal and policy frameworks for HC PKI
    - PKI applications: High confidence authentication and authorization
    - Managing technology transfer

High Confidence Aviation Systems Workshop

- Held June 21, 2000, and hosted by DARPA
- Objectives
  - Convene leading embedded software and assurance researchers with aviation specialists to develop new technical vision for high confidence aviation systems
  - Identify research directions that promise significant safety, time and cost improvements in certification process for future, highly complex airborne systems
  - Identify scientific directions needed to enable dramatic increases in aviation safety and capability through assured information technology
- Conclusions
  - Testing-based verification costs are too high, and inhibit adoption of new and modified technologies
  - Research is needed in the development of mixed initiative systems
  - A program in high confidence software and systems with a significant aviation challenge problem should be proposed to DARPA management

Workshop: Future Directions in Hybrid and Embedded Systems

- Held October 25, 2000 -- hosted jointly by NSF and DARPA
- Video teleconference with panel of key EU researchers
- Objectives
  - Develop strategy to broaden research investment base for full-fledged research discipline of hybrid and embedded software and systems
  - Inform potential new research emphases at NSF and DARPA
  - Identify promising directions for achieving better integration of observed and controlled physical systems with real-time software, networks, distributed systems, and information technology to revolutionize embedded systems
- Conclusions
  - Current scientific foundations in distributed real-time embedded systems are inadequate to build the complex, adaptive, and deeply embedded systems needed now and increasing for future
  - The “embedded system” problem has changed – many causes
  - Problems are interdisciplinary -- critical issues include: discrete & continuous reasoning and computation, timing & concurrency; middleware strategies
  - Impossible to achieve our vision for future embedded systems without a high-confidence basis for construction -- currently lacking
  - Inter-agency collaboration is needed to expand research in this critical area

Medical Device Software Safety Workshop

- Held November 20, 200 and hosted by Walter Reed Army Institute of Research
- Organized by DARPA, FDA, ARO, and WRAIR
  - Sponsored by HCSS Coordinating Group
- Objectives
  - Identify issues related to the development of high confidence software for medical devices
- Conclusions
  - Currently no organization is coordinating the research and development of high confidence software for medical devices
  - FDA software certification personnel number ~ 5, activities limited to "best practice" advisory role
  - Explosion of bio-research will lead to upsurge in demands on FDA device certification role

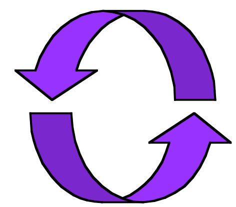
DARPA, DDR&E/CIP MURI Topics

- **Assurance MURI Research Solicitation**
  - Interoperable programming languages and design, analysis, synthesis, and reasoning tools that can assure domain-specific requirements;
  - Run-time and operating system mechanisms that assure critical properties such as timing, security, and fault isolation and tolerance;
  - Mathematically rigorous (both probabilistic and deterministic) approaches for modeling software, supporting abstraction, and modular, composable, and scalable reasoning;
  - Model-based paradigms for embedded systems;
  - Correct-by-construction methods for embedded software generation; and
  - Frameworks that accommodate complementary methods for reasoning about interacting properties of systems and about justified confidence in those properties.

Walter Reed

Army Institute for Research

- Respirator
- Infusion pump



FDA

- Clean Room
- Technology?

ARO Assurance MURI

- University of Pennsylvania
- Carnegie Mellon University
- Kansas State University

New Plans for HCSS: Information Assurance and Survivability Programs

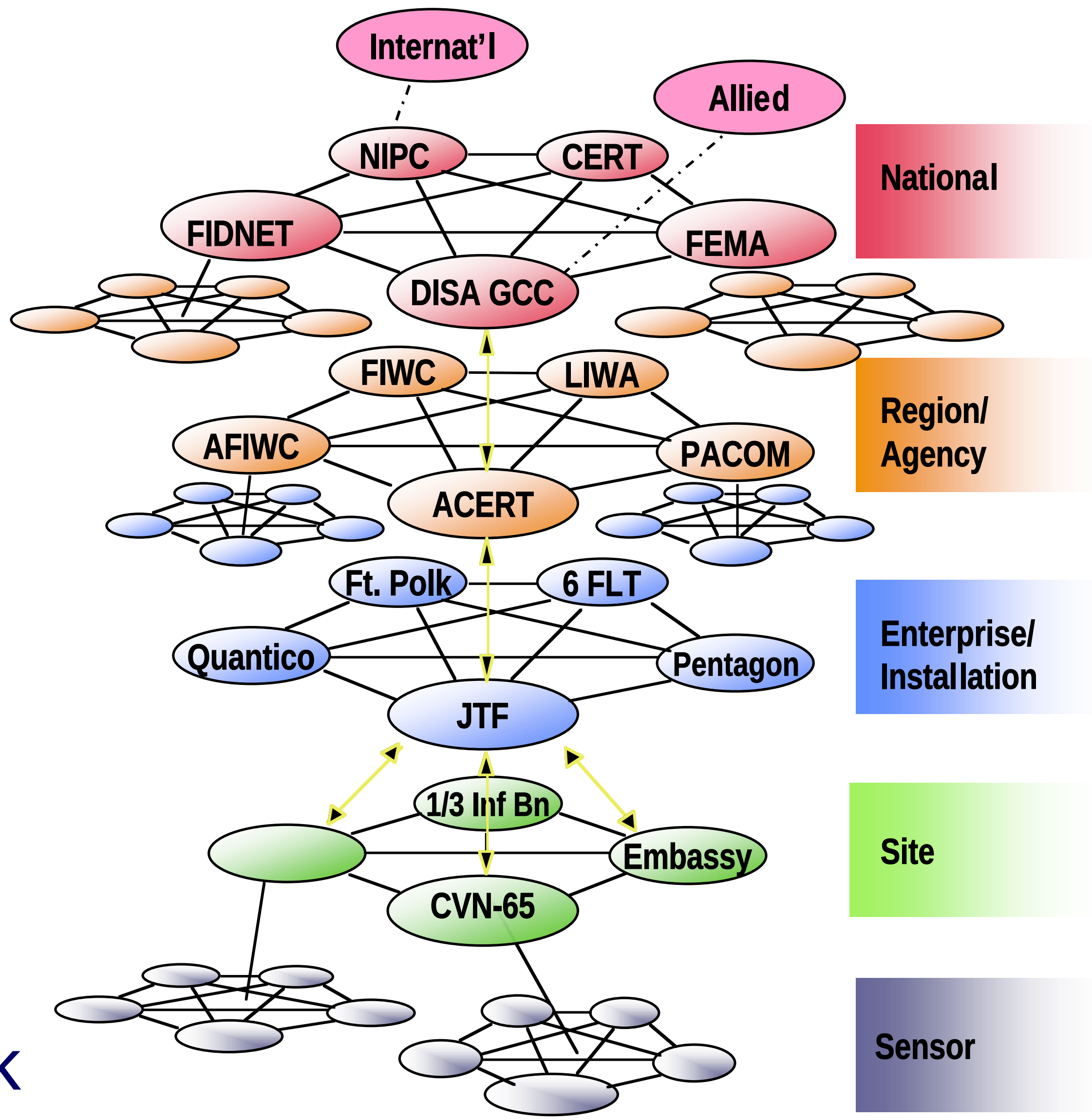
Where we are?

Where we need to go?

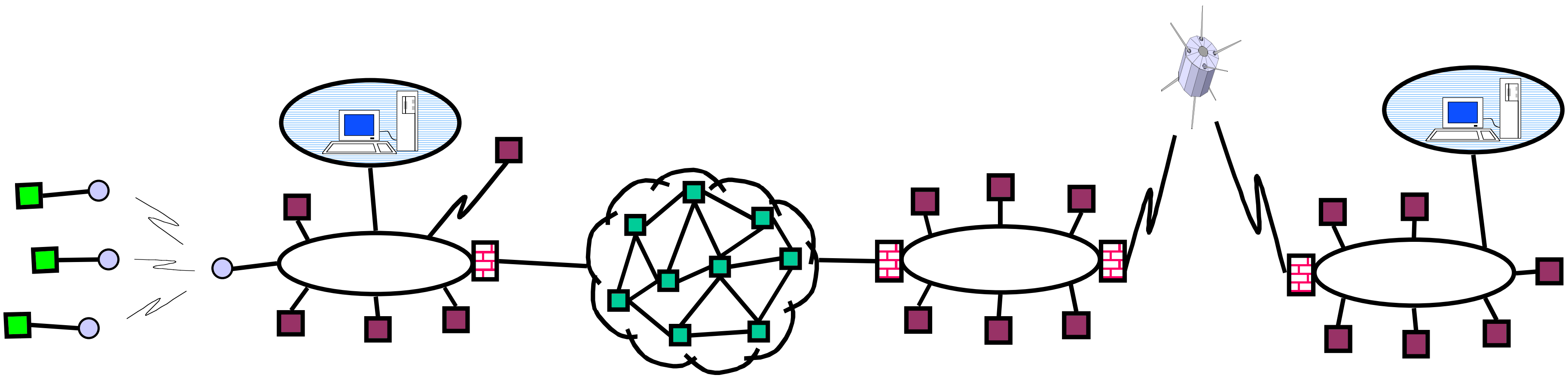
Reliance on Networks is Pervasive

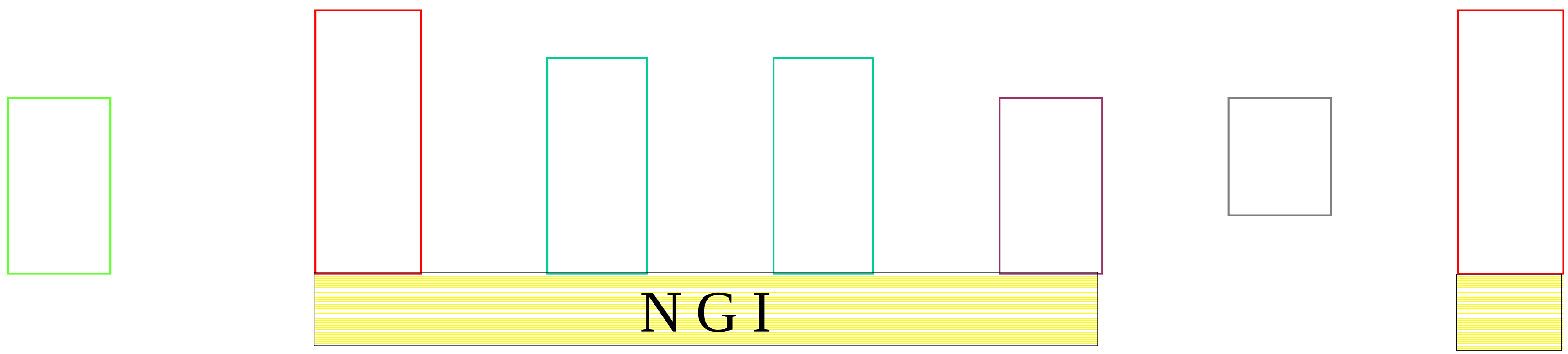
- DoD/Commercial world depends on networking technology for information dominance at all levels of command hierarchy, BUT …

- DoD/Enterprise networks are increasingly vulnerable to attack

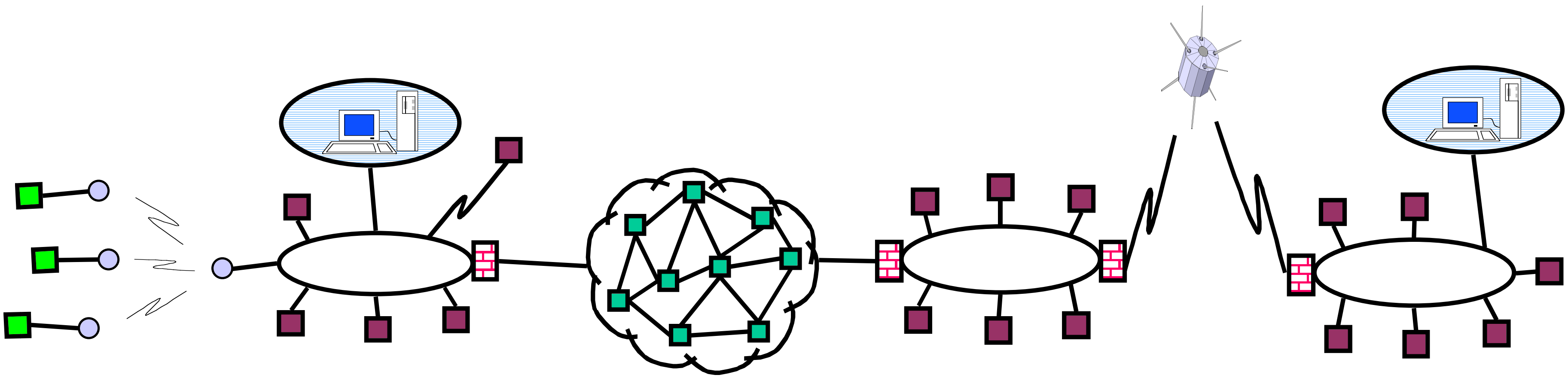


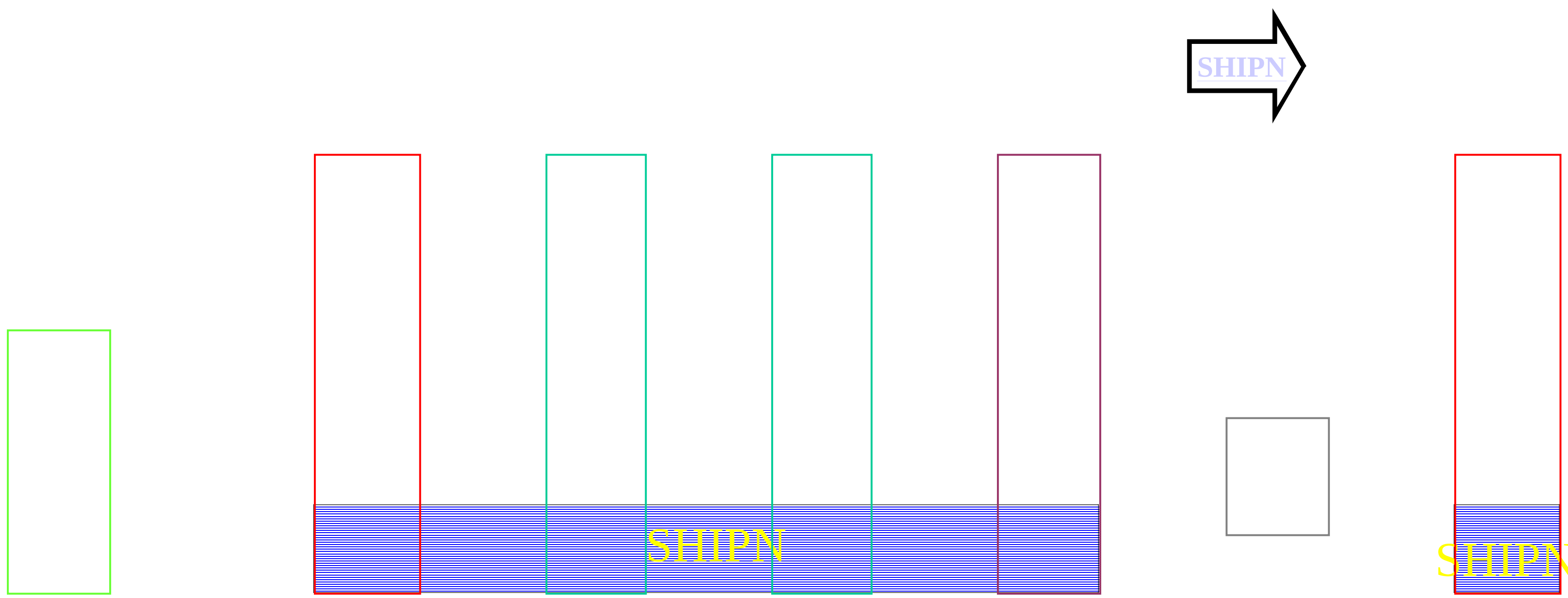
Networks and Systems
IA&S Vision



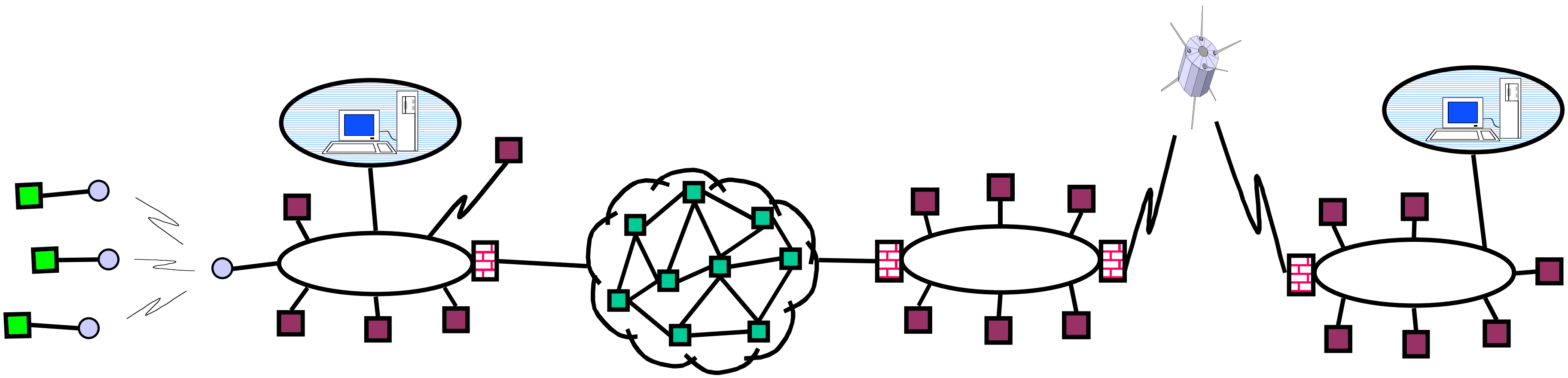


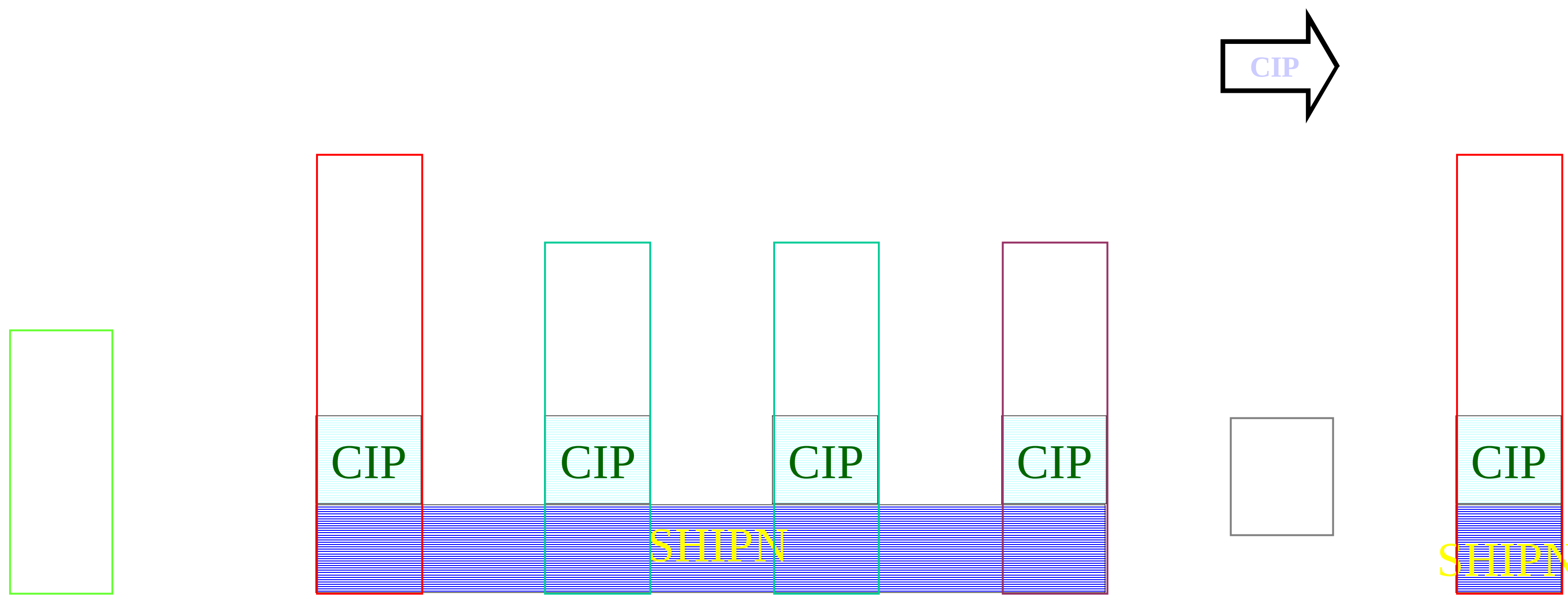
Secure High Speed IP Networking (SHIPN)



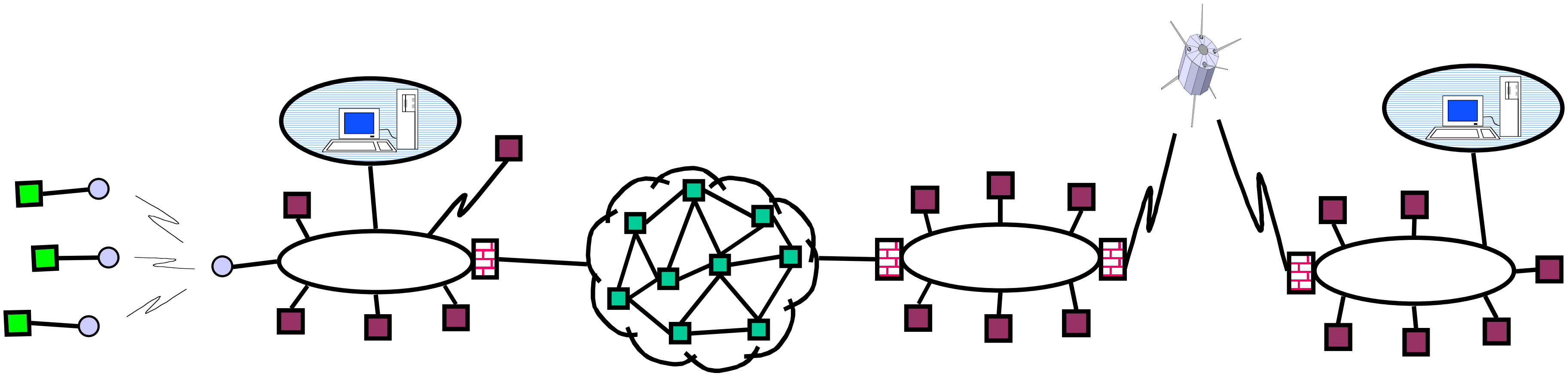


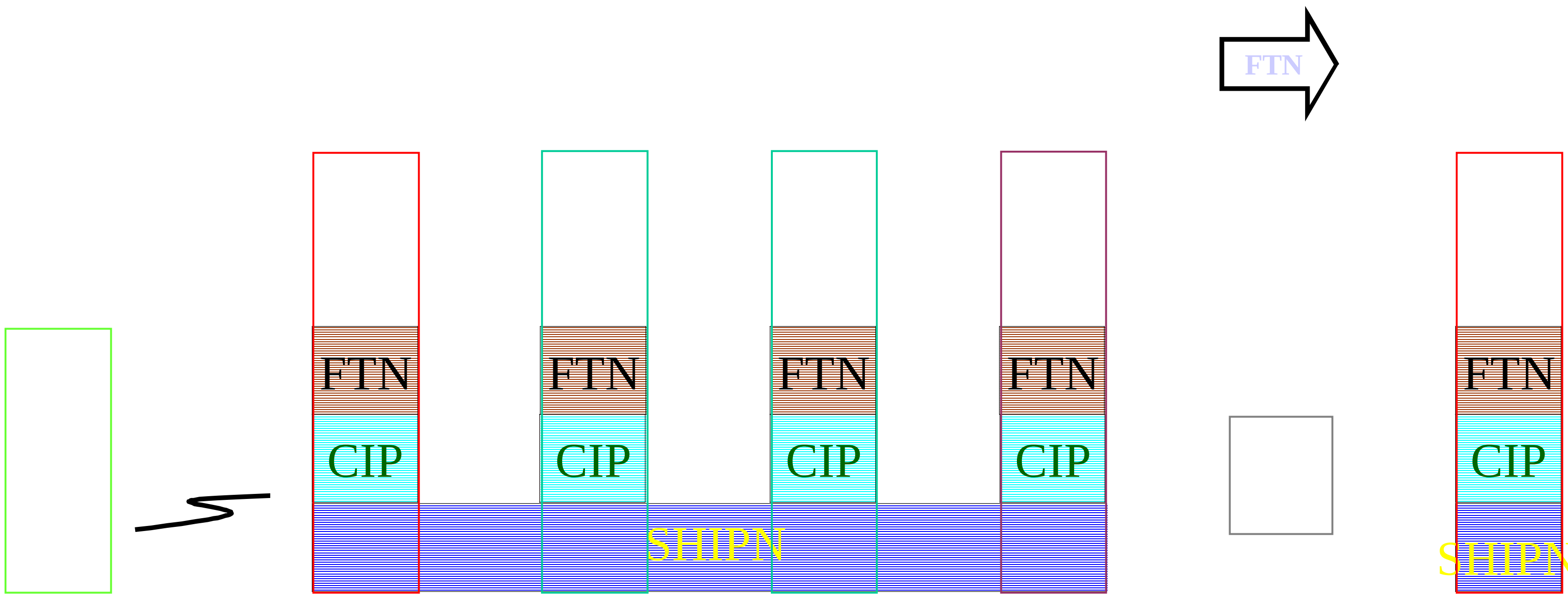
Critical Infrastructure Protection (CIP)



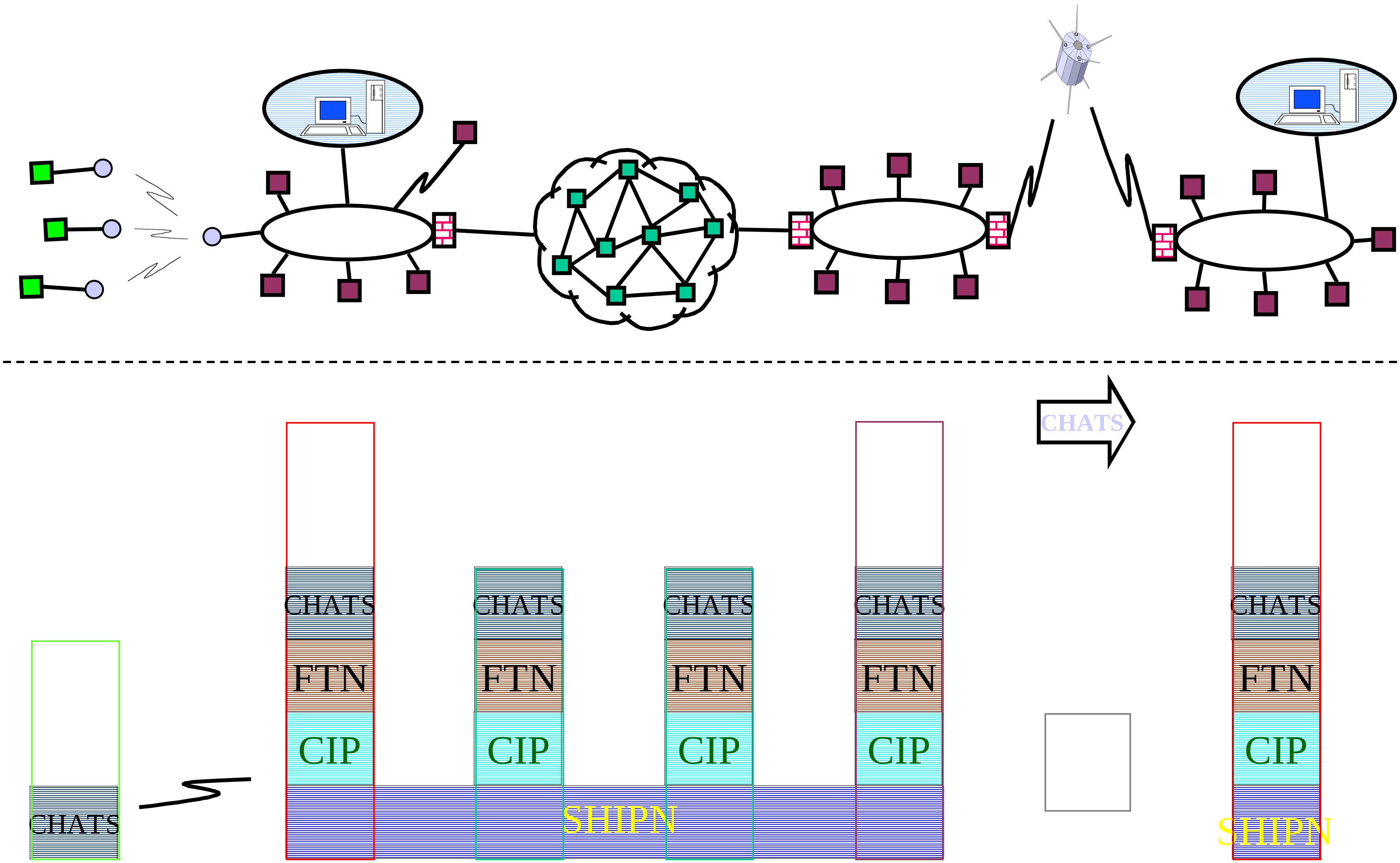


Fault Tolerant Networking (FTN)

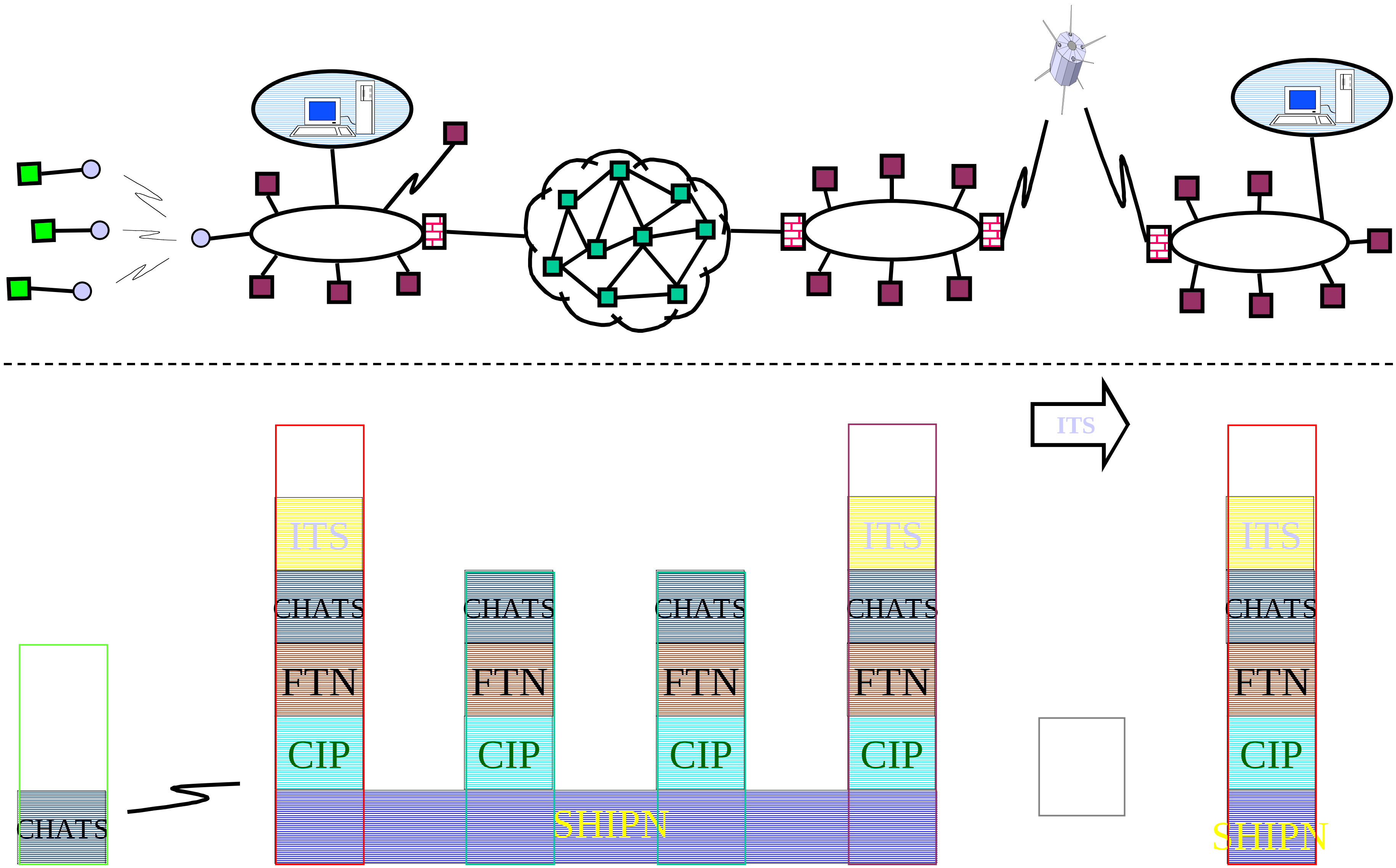




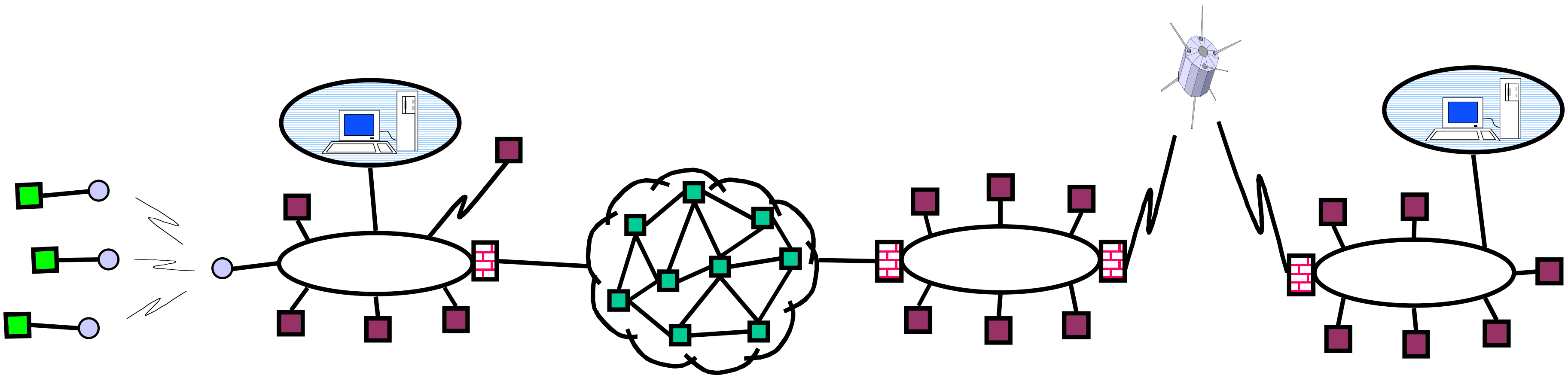
Composable High Assurance Trusted Systems (CHATS)

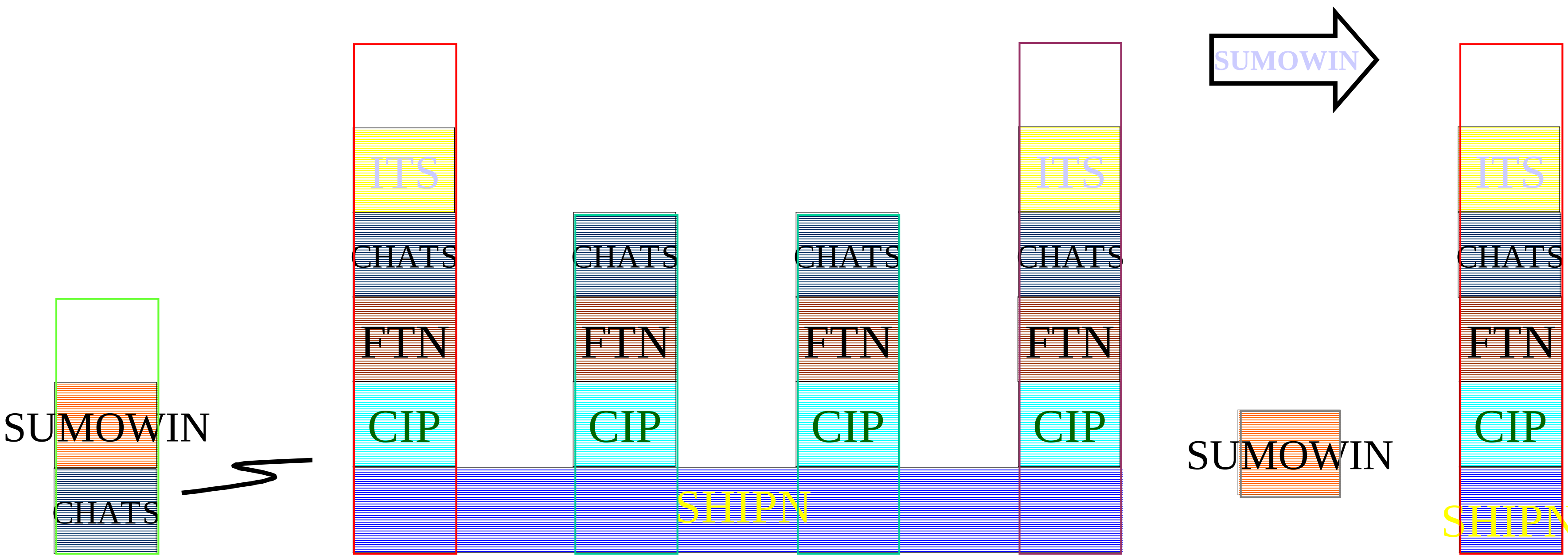


Intrusion Tolerant Systems (ITS)

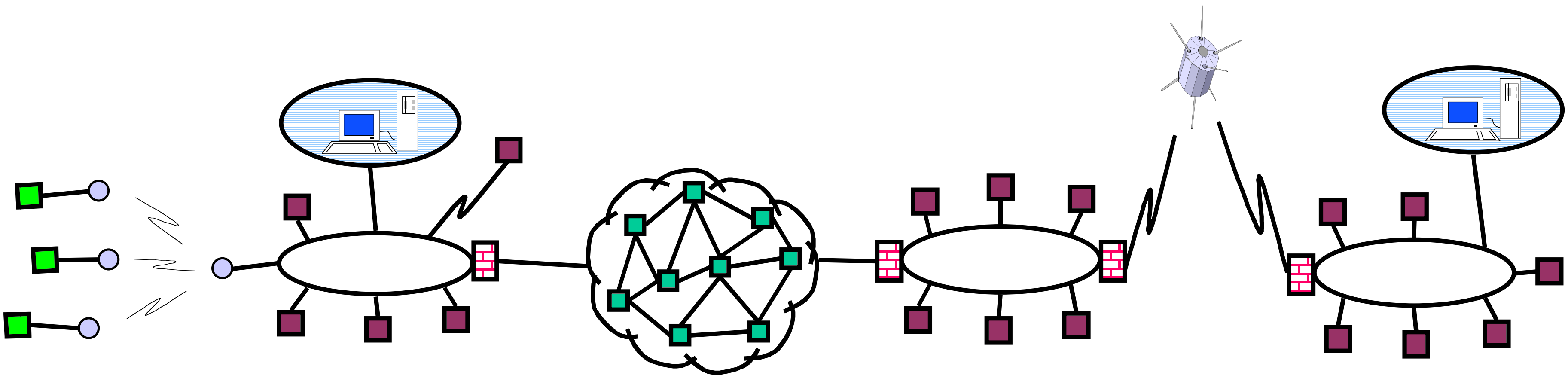


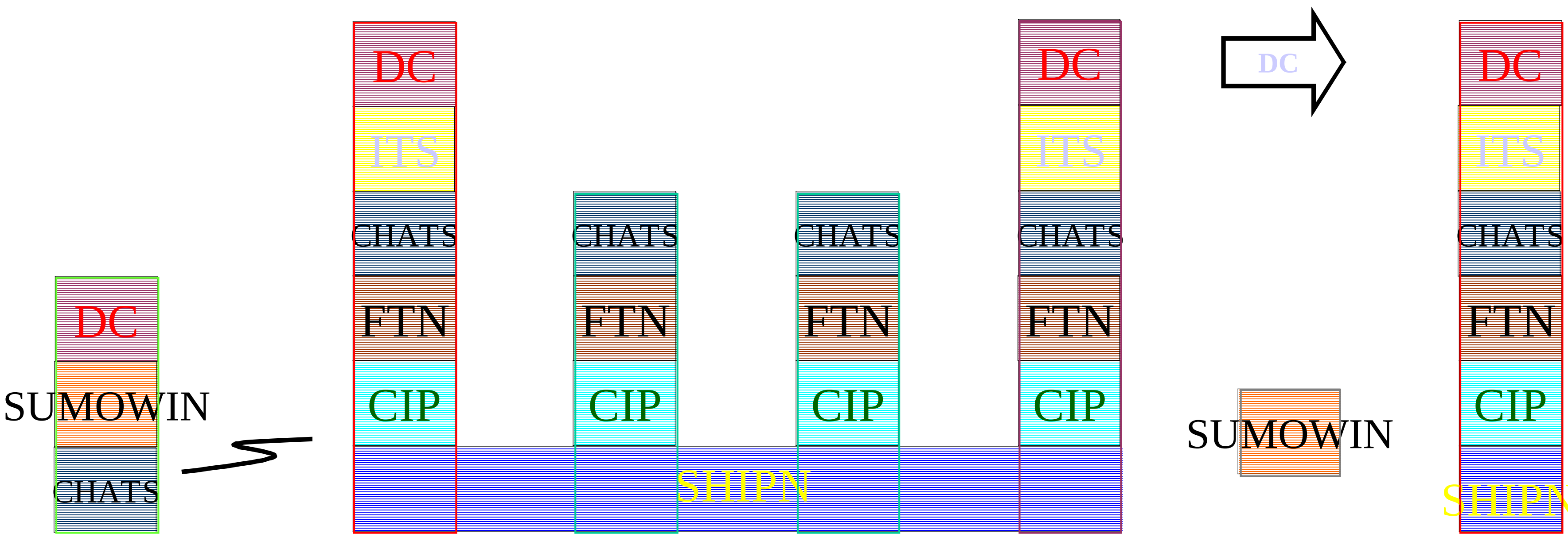
Survivable Mobile Wireless Networking (SUMOWIN)



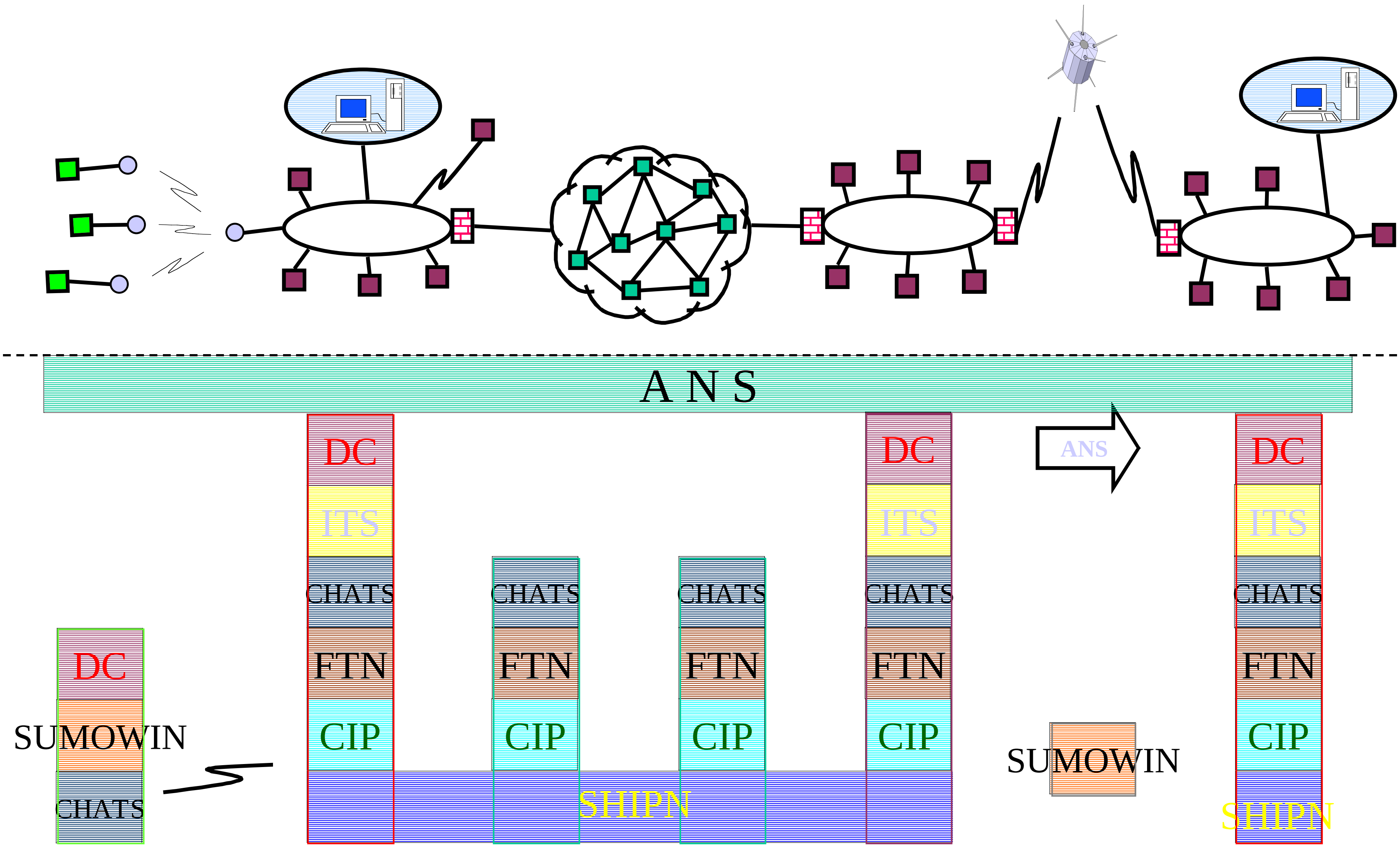


Dynamic Coalitions (DC)

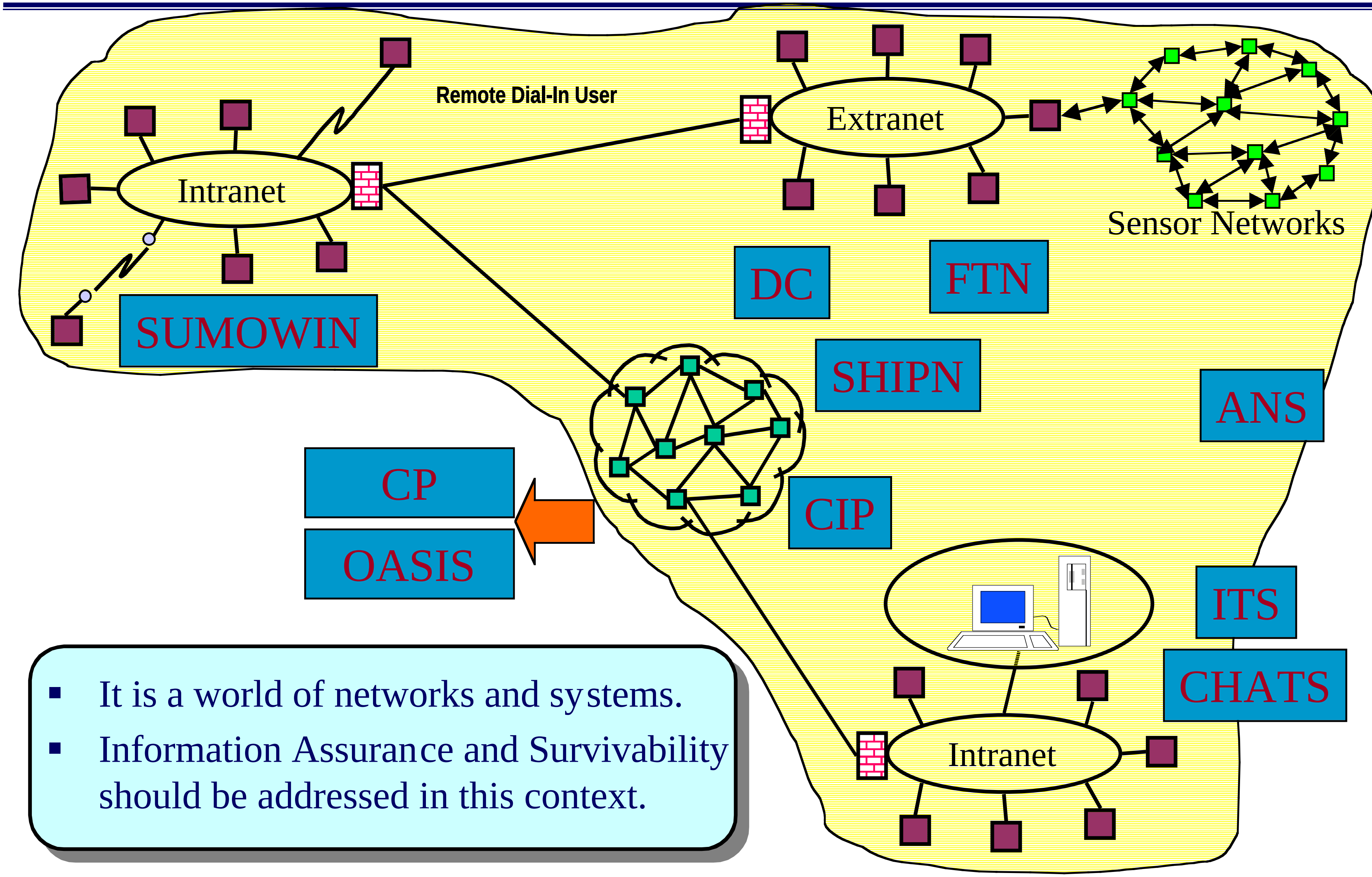




Advanced Network Surveillance (ANS)



IA&S Vision



- It is a world of networks and systems.
- Information Assurance and Survivability should be addressed in this context.