SYSTEMS ENGINEERING
Research Center
A US DoD University Affiliated Research Center

System-Aware Cyber Security Architecture

Rick A. Jones

October, 2011

SYSTEMS ENGINEERING Research Center

Research Topic Description

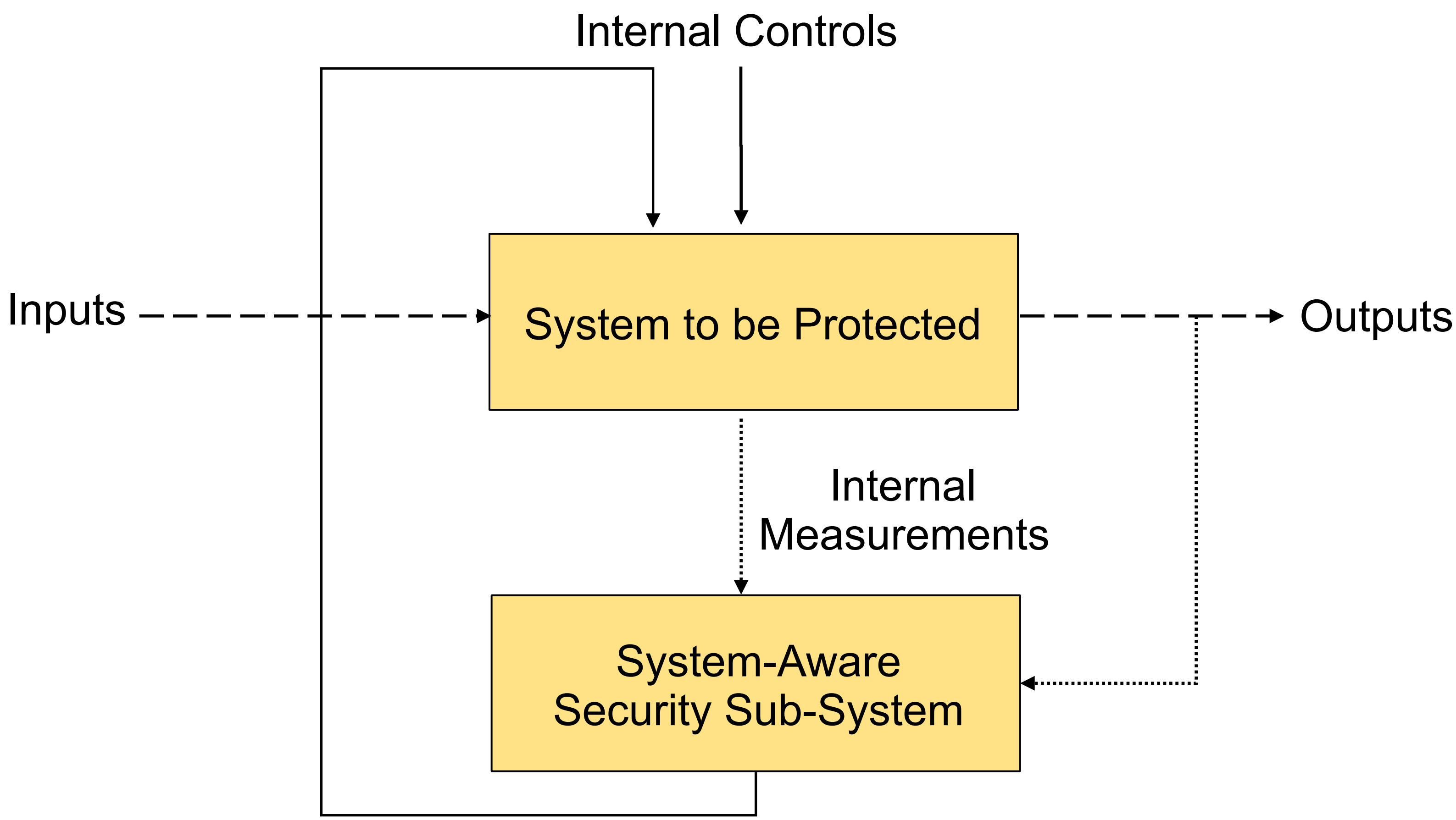
- System-Aware Cyber Security Architecture
  - Addresses supply chain and insider threats
  - Embedded into the system to be protected
  - Includes physical systems as well as information systems
- Requires system engineering support tools for evaluating architectures factors
- To facilitate reusability requires establishment of candidate Design Pattern Templates and initiation of a design library
  - Security Design
  - System Impact Analyses

SYSTEMS ENGINEERING Research Center

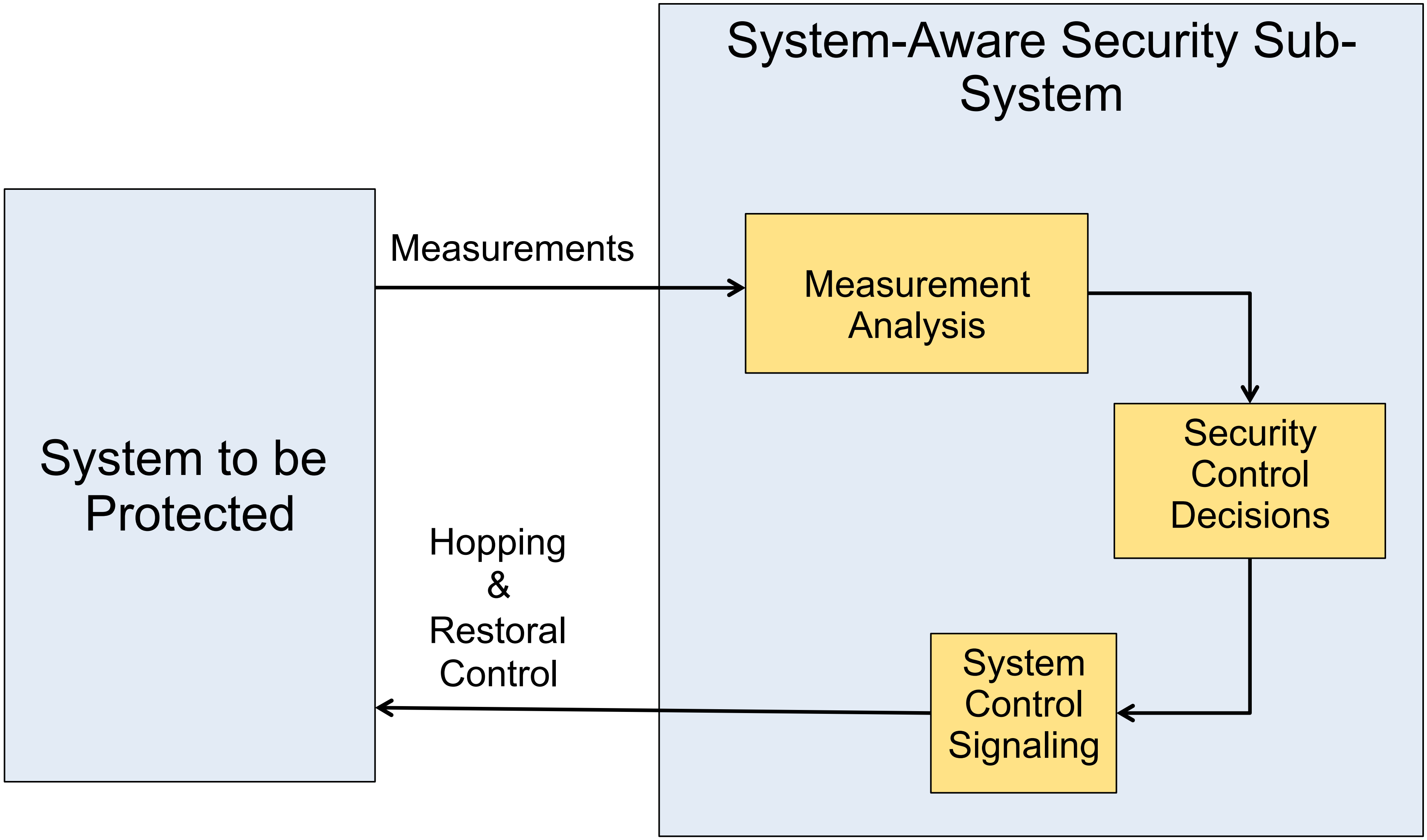
Incorporating Recognized Security Functions into an Integrated System-Aware Security Solution

- Fault-Tolerance
  - Diverse Implementations of Common Functions
  - Data Continuity Checking via Voting
- Cyber Security
  - Moving Target with Diversity
    - Physical Configuration Hopping
    - Virtual Configuration Hopping
  - Adversary-Sensitive System Reconstruction
- Automatic Control Systems
  - Data Continuity Checking via State Estimation
  - System Identification
    - Tactical Forensics

System-Aware Security Architecture



System-Aware Cyber Security Subsystem

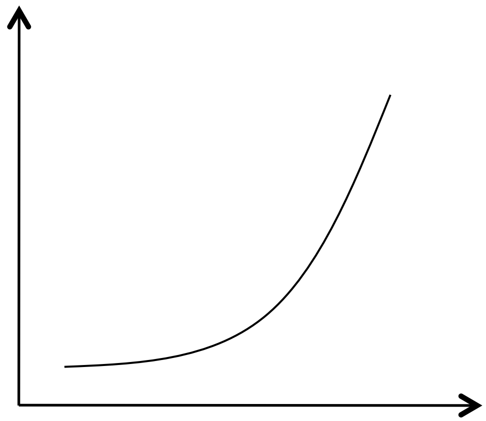


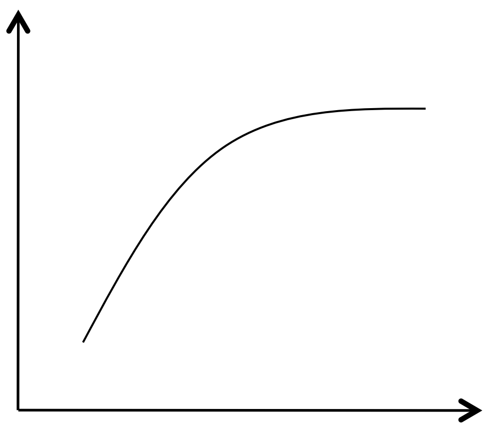
System-Aware Security Analysis

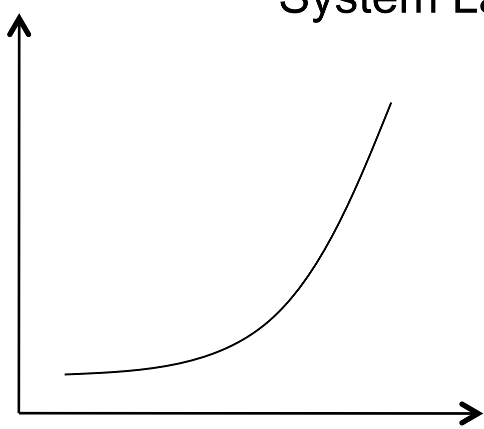
Mission-Risk
Ranked
System Functions

Selected set for hopping:

(1)
(2)
(3)
(4)
⋮
(N)







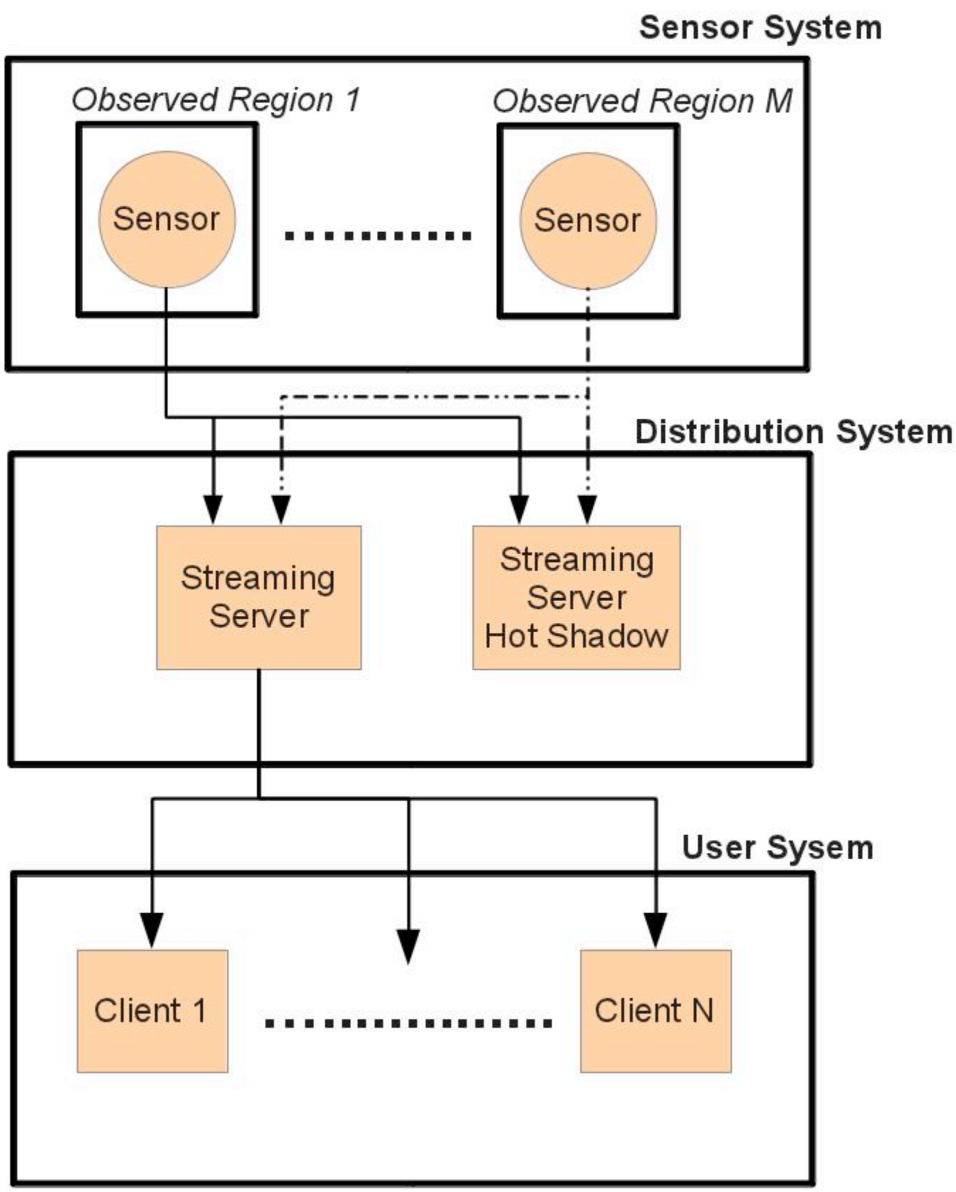
System-Aware Security for Facility Defense

SYSTEMS ENGINEERING Research Center

Facility Defense System to be Secured

- We consider a facility defense system consisting of:
  - Streaming sensors continuously monitoring discrete areas
  - Streaming Servers distributing sensor data, received over a wired network, to mobile users over a wireless broadcast network
  - Mobile users receiving alerts and streaming data regarding potential problems

Illustrative Architectural Diagram for Candidate Facility Defense System for System-Aware Security



SYSTEMS ENGINEERING
Research Center

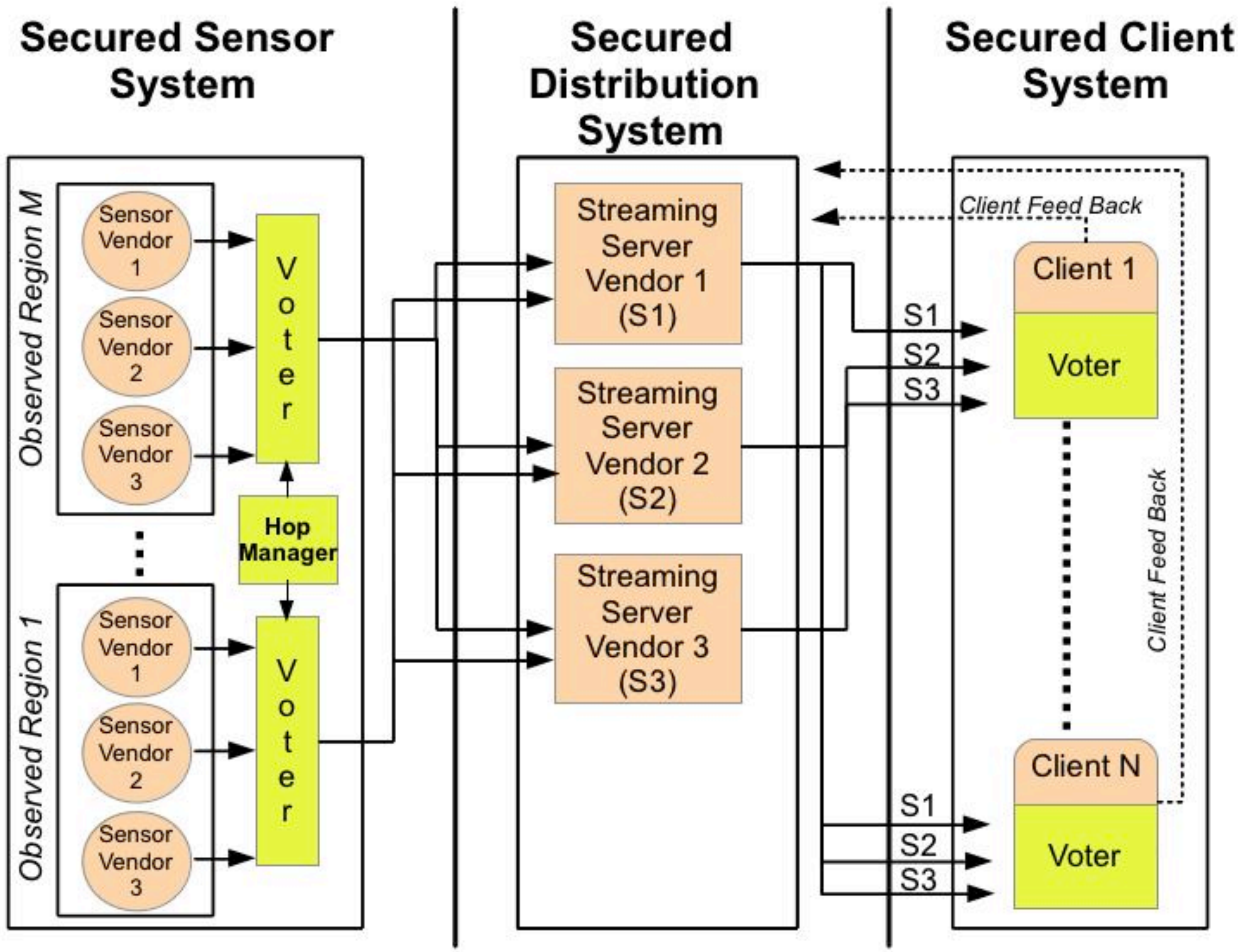
Potential Cyber Attacks

- Replay attacks masking malicious activity initiated through
  - Sensor system
  - Streaming servers
  - User devices
- DoS attacks addressed through redundancy
  - Sensor system
  - Streaming servers
  - Operational procedures and redundancy regarding user devices

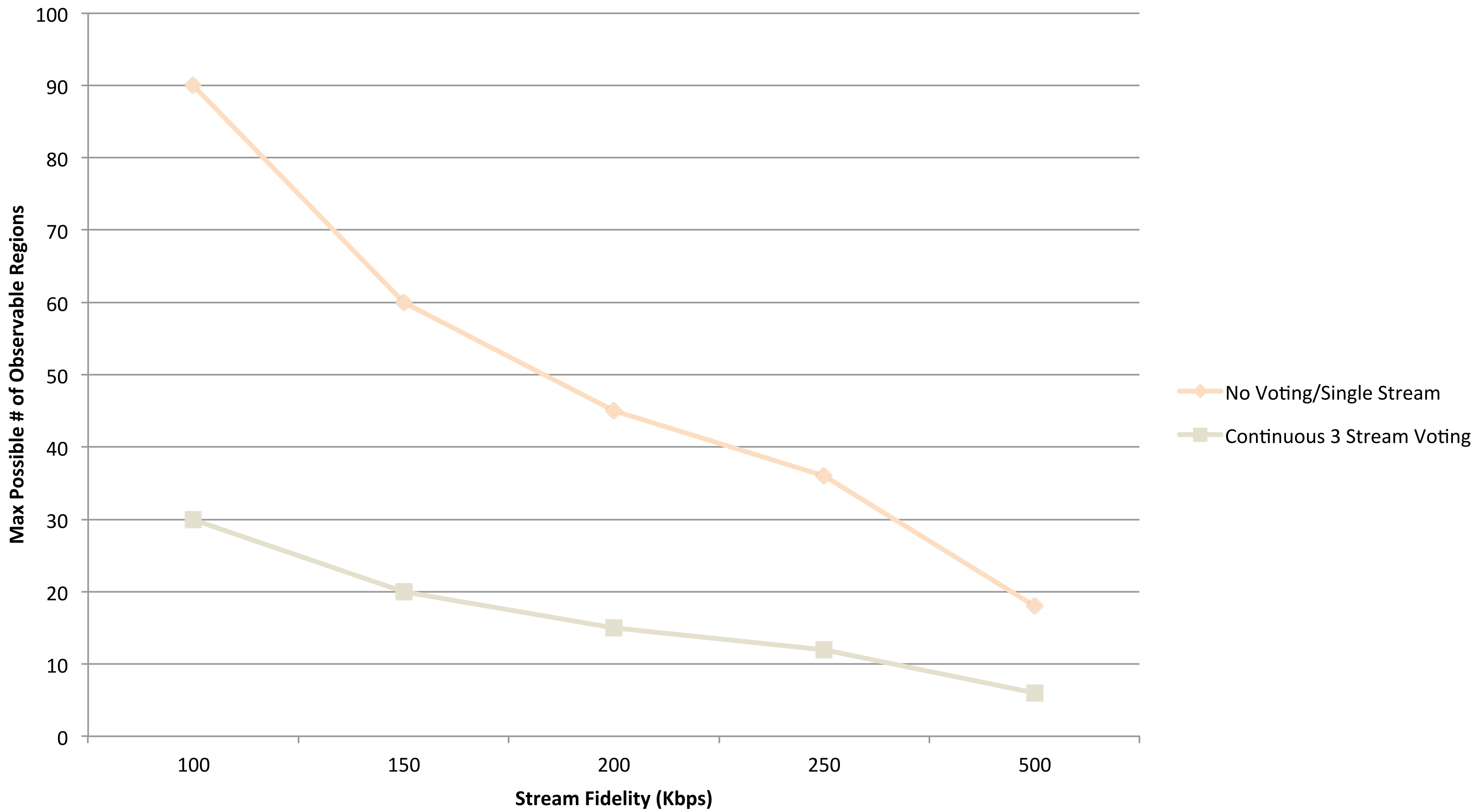
System-Aware Solution for Securing the Facility Defense System

- Replay attack defense
  - Diversely Redundant Streaming Sensors, with Voting (Data Continuity Checking)
  - Diversely Redundant, Virtually Hopped Streaming Servers
  - Diverse User Devices, with Rotating User Surveillance Assignments and Device Use
  - Mobile User based Data Continuity Checking
- DoS defense
  - Redundancy at the Sensor and Streaming server levels
  - Streaming servers / User feed back loops to enable redistribution of data and job responsibilities

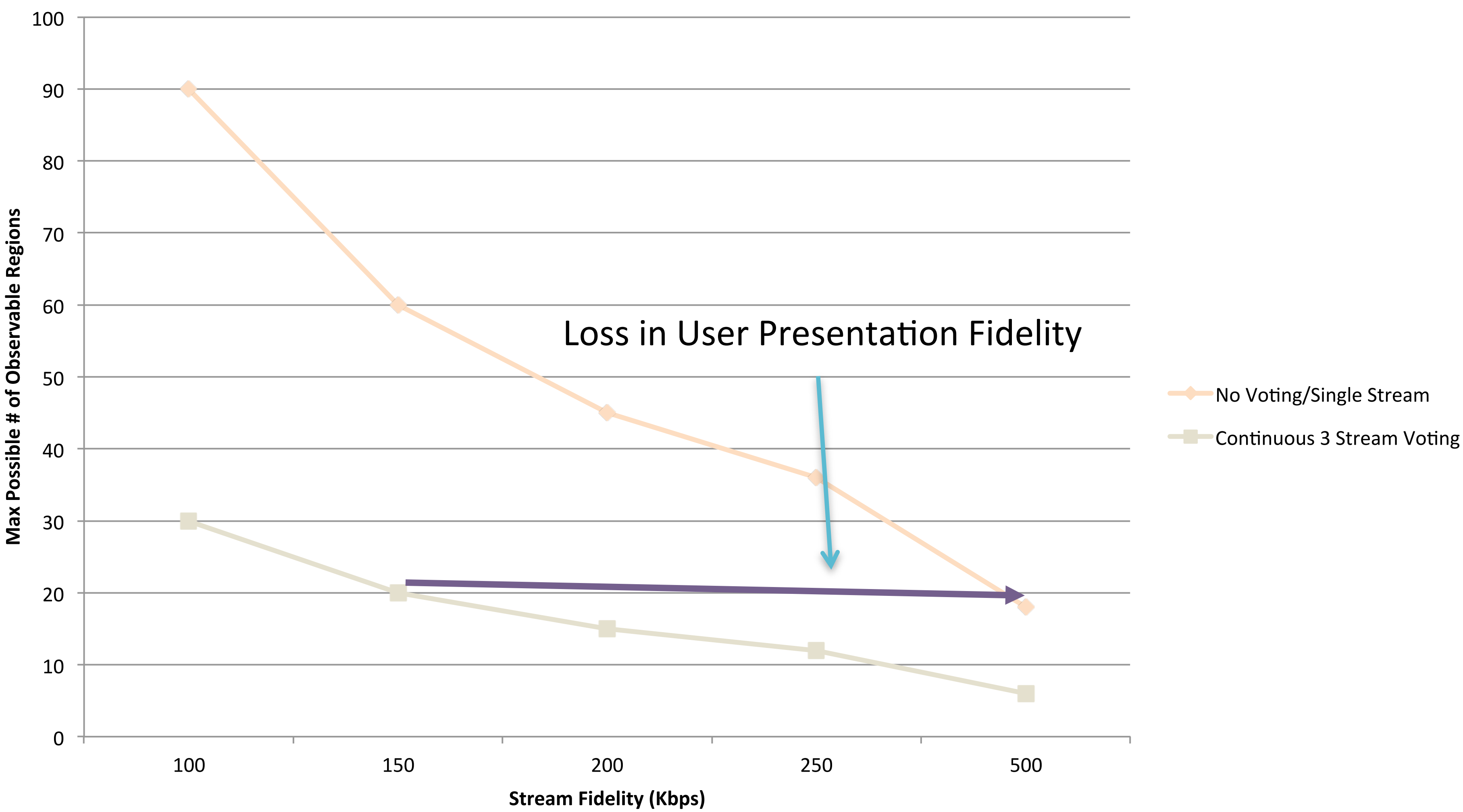
Illustrative System-Aware Solution Architecture



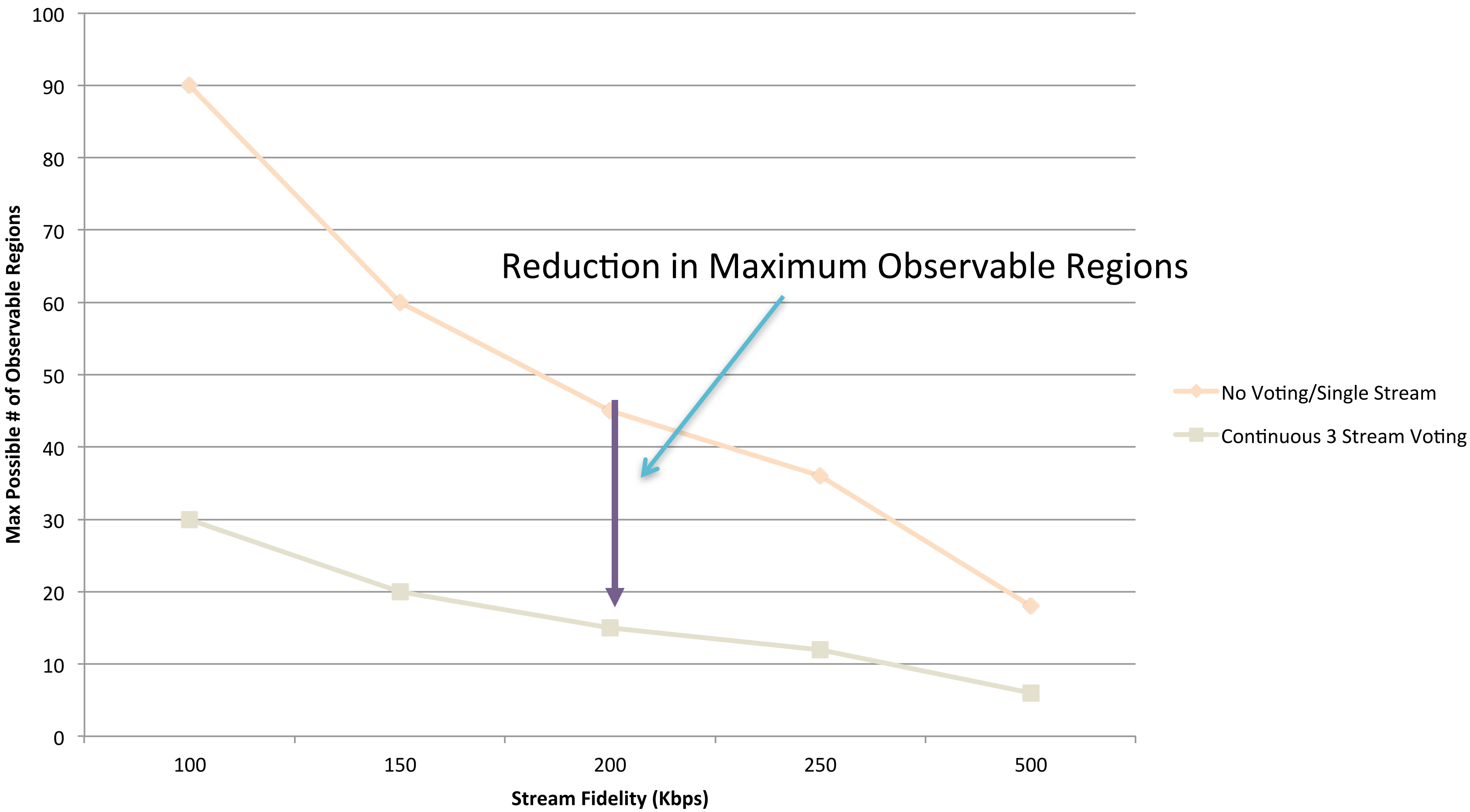
Observable Regions / User Fidelity Impacts of 3 Stream Continuous Voting



Observable Regions / User Fidelity Impacts of 3 Stream Continuous Voting



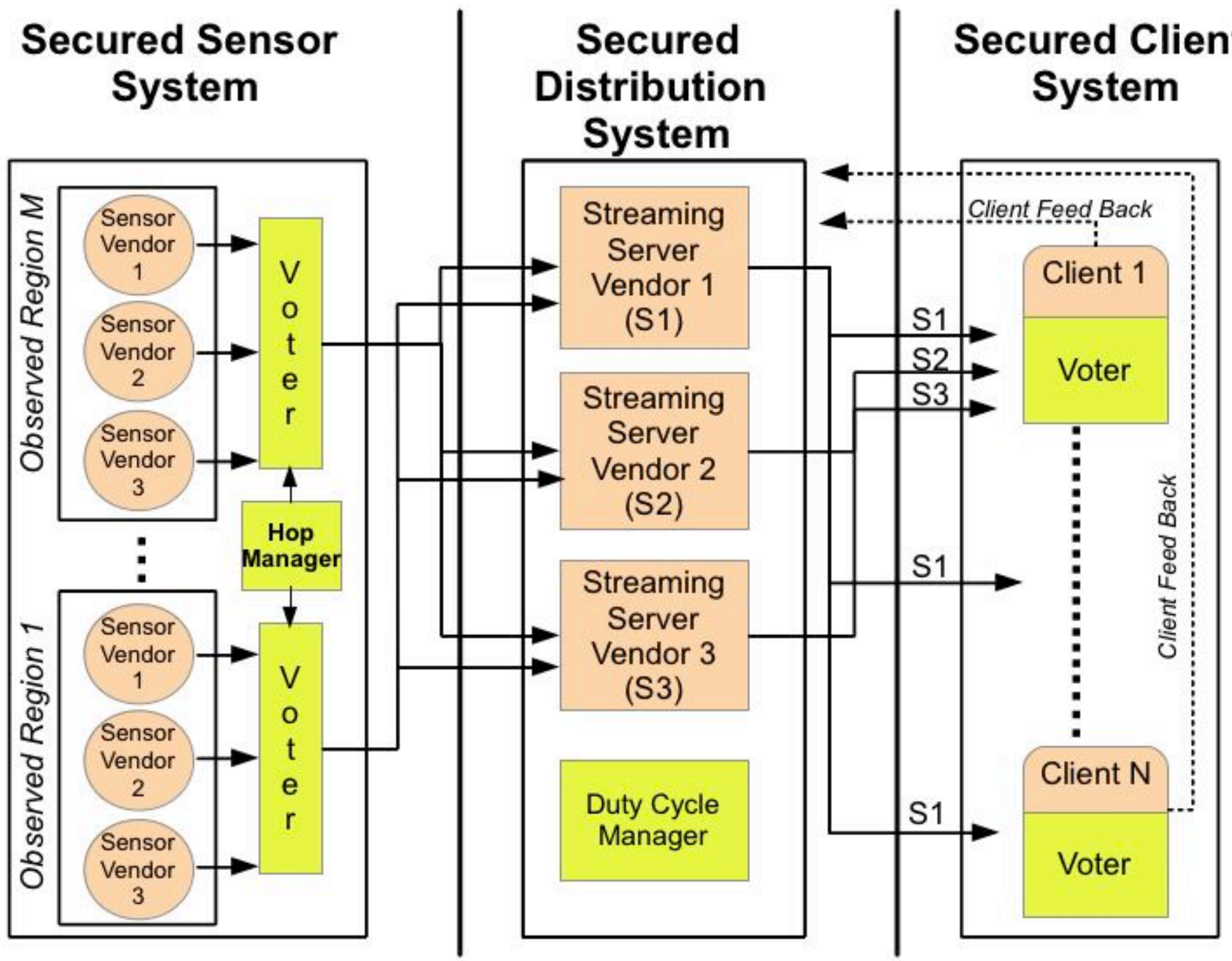
Observable Regions / User Fidelity Impacts of 3 Stream Continuous Voting



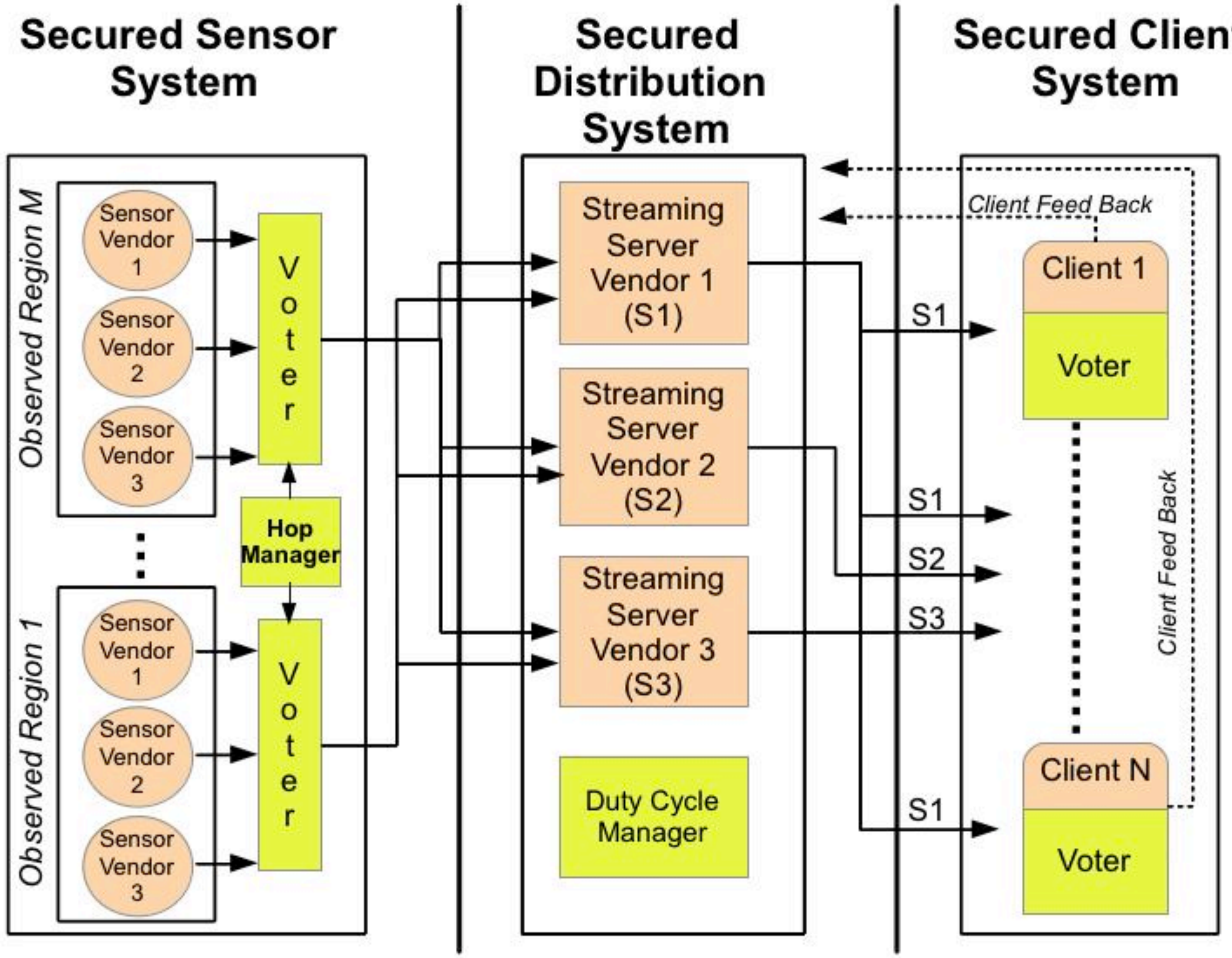
Duty Cycle Voting for Increasing the Possible Number of Observable Regions

- Concept – Use of time division for voting permits an increase in the number of possible surveillance points
  - User compares streams concurrently received from multiple diversely redundant servers to discover discontinuities
  - 3 parameters can be utilized to govern voting
    - Number of Observed Regions
    - Deemed acceptable Voting Interval for data continuity checking across all regions
    - Streaming period time allotted for continuity checking (Voting Time), which can be less than the Voting Interval
  - Given the Voting Time can be a subset of the Voting Interval, the use of time division can be utilized to manage information distribution over the broadcast network, interleaving multiple streams for voting users with single streams for other users who are not voting

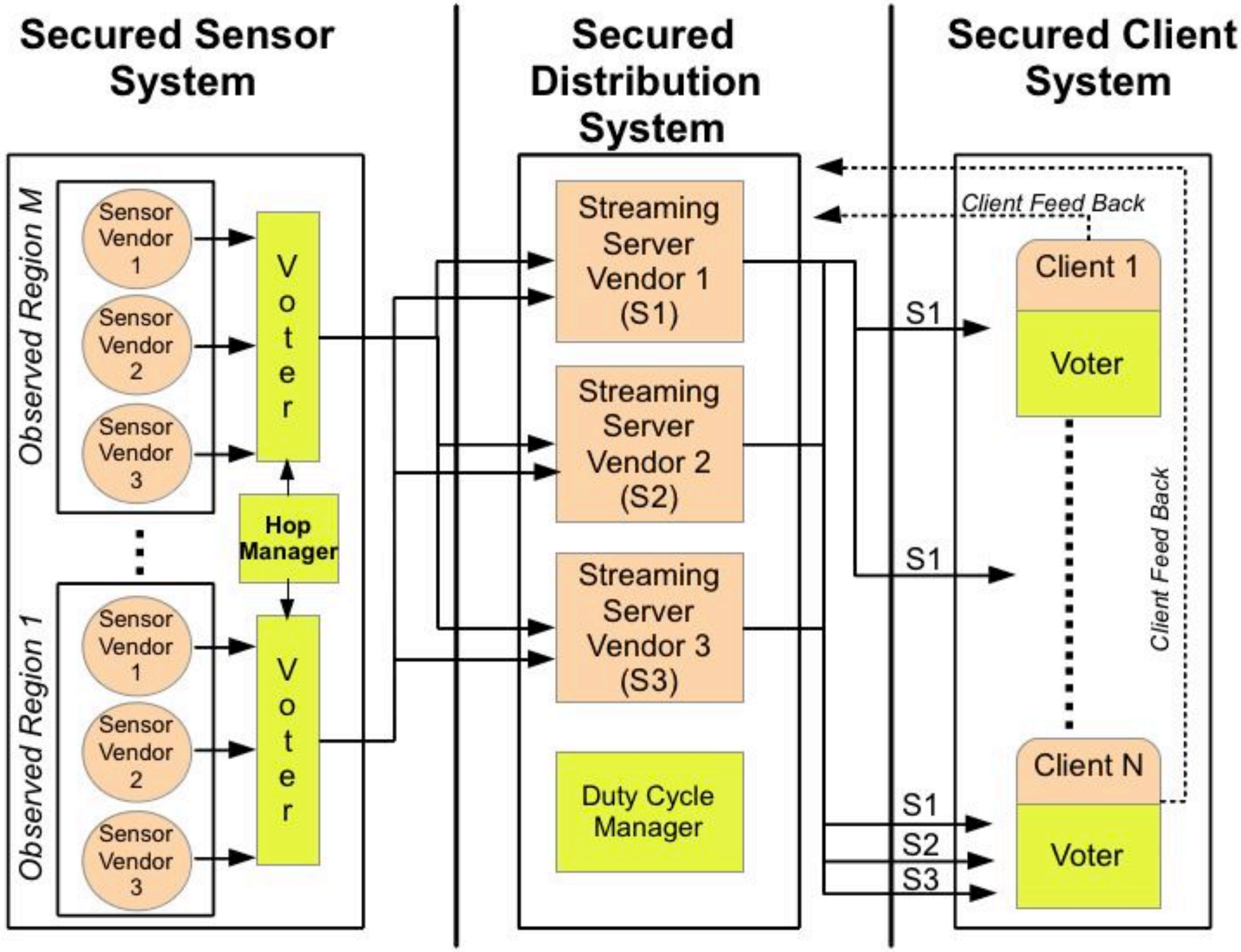
Illustrative System-Aware Solution Architecture with Duty Cycle Voting



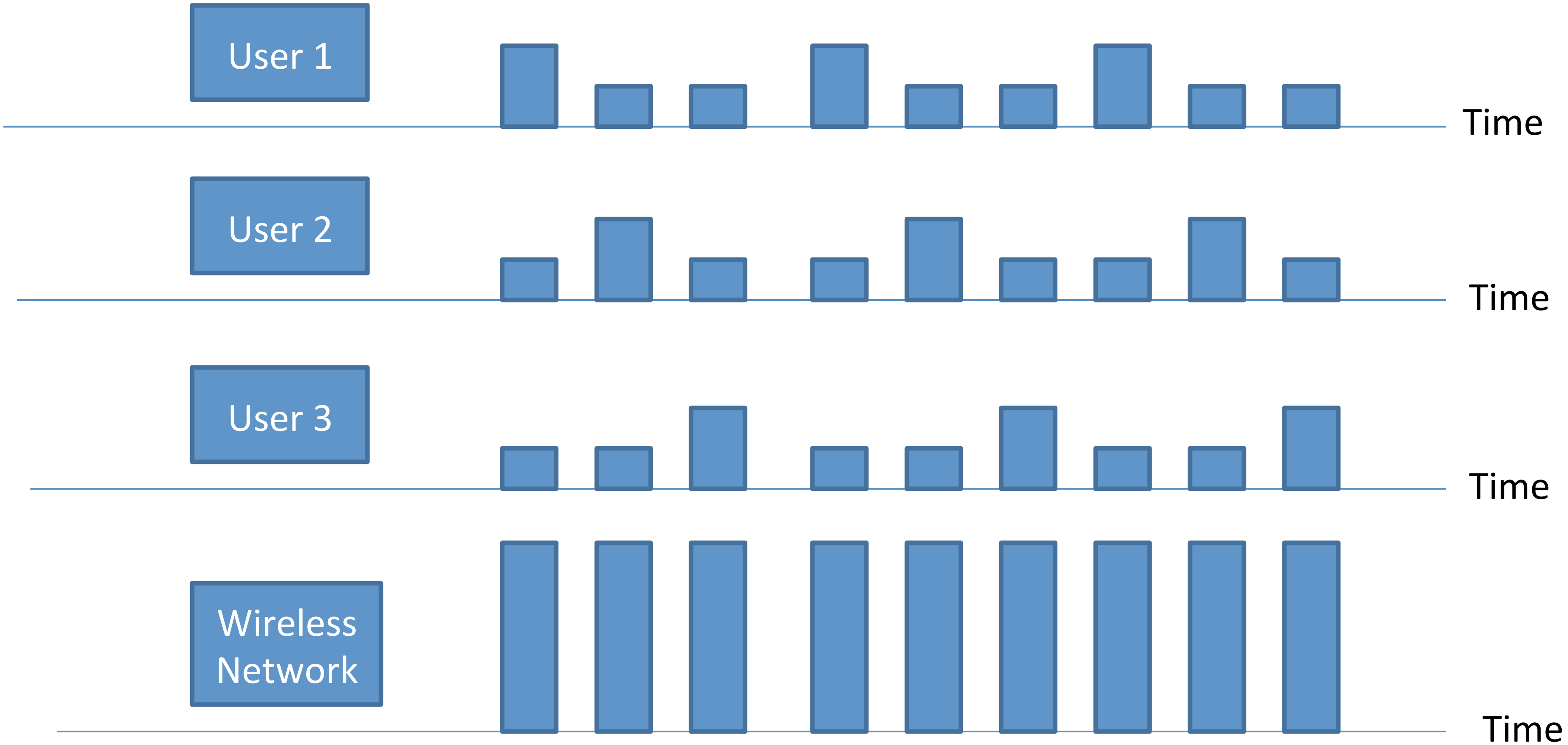
Illustrative System-Aware Solution Architecture with Duty Cycle Voting



Illustrative System-Aware Solution Architecture with Duty Cycle Voting

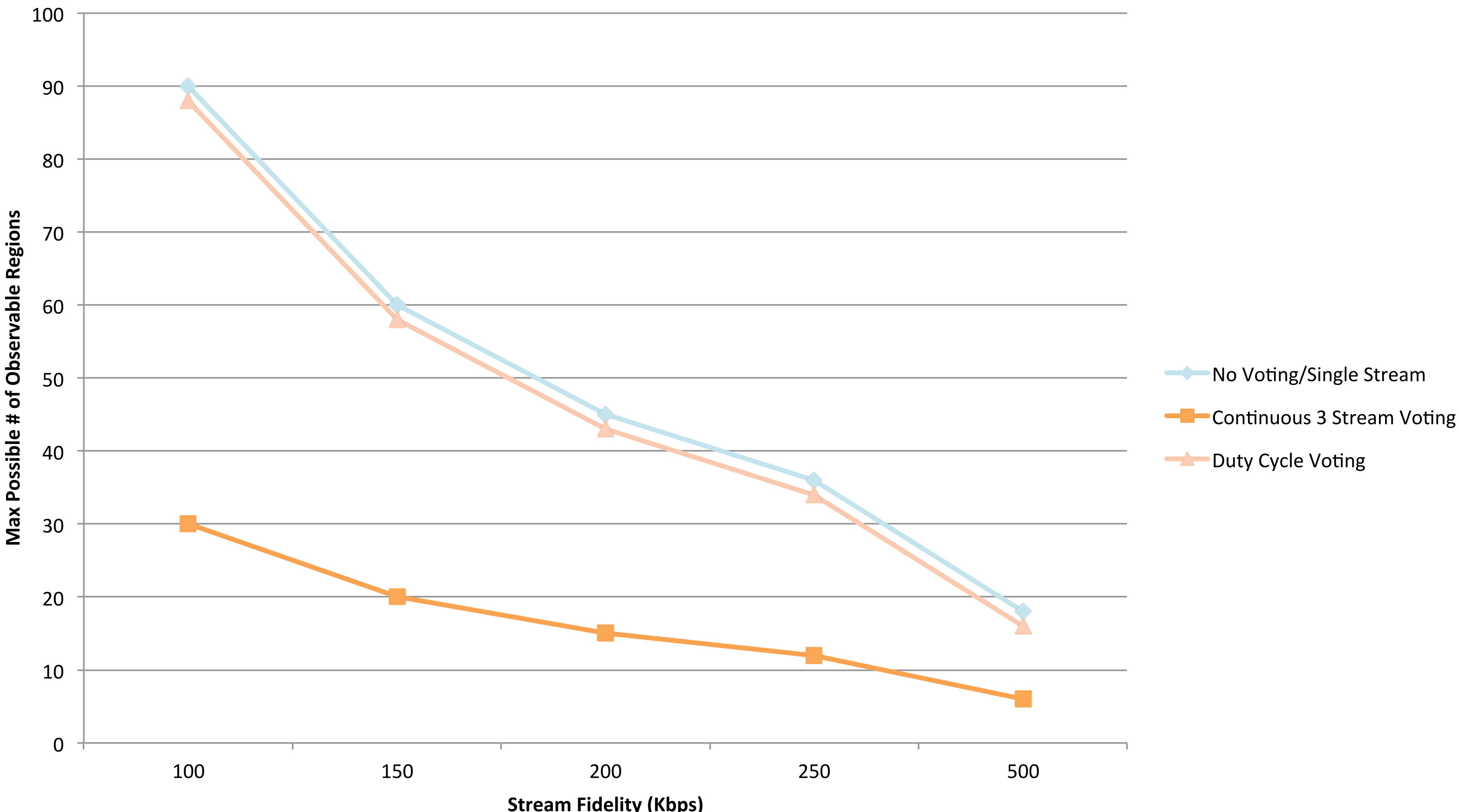


Duty Cycle Voting for Increasing the Possible Number of Observable Regions



Column Heights = Data / Time Interval

Observable Regions / User Fidelity Impacts of 3 Stream Continuous Voting



SYSTEMS ENGINEERING
Research Center

Additional Collateral System Impacts

- Common Cause Failures are reduced
- MTBF increases in relationship to the individual diverse component reliabilities
- Development cost increases based on the cost to develop voting and duty cycle management components, as well as to resolve lower level technical issues that may arise
  - Synchronization needs
  - Software integration
  - Performance impact measurements and enhancement needs (e.g. CPU utilization, memory, and energy usage)
- One time and life cycle cost increase in relationship to the increased complexity

Scoring Framework

SYSTEMS ENGINEERING
Research Center

Need: Methodology for Evaluating Alternative Security Solutions for a Particular System

- A methodology is required in order to clarify reasoning and prioritizations regarding unavoidable cyber security vagaries:
  - Relationships between solutions and adversarial responses
  - Multidimensional contributions of individual security services to complex attributes, such as deterrence

- Scores can be derived in many different forms
  - Single scalar value where bigger is better
  - 2 scalar values: (1) security value added, (2) system-level disvalues
  - Multi-objective component scores providing more transparency

Metrics

- Attack phase-based security value factors:
  - Pre-Attack (Deterrence)
  - Trans-Attack (Defense)
  - Post-Attack (Restoration)
- Would include collateral system impact metrics for the security architecture:
    - Performance
    - Reliability, Safety
    - Complexity, Costs

System-Aware Security System Scoring Matrix

Relative Value Weights	k_1	k_2	k_3	k_4	k_5	k_6	k_j
Value Factors → / Security Services ↓	Deterrence	Real Time Defense	Restor-ation	Collateral System Impacts	Implemen-tation Cost	Life Cycle Cost	Other
Diversity (s_1)	s_{11}	s_{12}					s_{1j}
Hopping (s_2)	s_{21}	s_{22}					s_{2j}
Data Continuity Checking (s_3)	s_{31}	s_{32}					s_{3j}
Tactical Forensics (s_4)	s_{41}	s_{42}					s_{4j}
Other (s_i)	s_{i1}	s_{i2}					s_{ij}

System-Aware Security System Scoring Matrix

Relative Value Weights	k_1	k_2	k_3	k_4	k_5	k_6	k_j
Value Factors → / **Security Services ↓**	**Deterrence**	**Real Time Defense**	**Restor-ation**	**Collateral System Impacts**	**Implemen-tation Cost**	**Life Cycle Cost**	**Other**
Diversity (s_1)	s_{11}	s_{12}					s_{1j}
Hopping (s_2)	s_{21}	s_{22}					s_{2j}
Data Continuity Checking (s_3)	s_{31}	s_{32}					s_{3j}
Tactical Forensics (s_4)	s_{41}	s_{42}					s_{4j}
Other (s_i)	s_{i1}	s_{i2}					s_{ij}

$$\sum_{j=1}^{p} k_j = 1$$

s_{ij} = Assurance Level of the ith service as related to the jth value factor

s_{ij} = Quantized Assurance Level = 0…M

$$\text{Security Score} = \sum_{j=1}^{p} \sum_{i=1}^{n} k_j s_{ij}$$

Max Possible Score = n x M

Example Facility Defense Scoring Matrix

Relative Value Weights	K_1 =0.30	K_2 = 0.20	k_3 =0.10	K_4 = 0.20	K_5 = 0.05	K_6 = 0.15
Value Factors → / **Security Services ↓**	**Deterrence**	**Real Time Defense**	**Restor-ation**	**Collateral System Impacts**	**Implemen-tation Cost**	**Life Cycle Cost**
Diversity (s_1)	4	3	4	4	2	2
Hopping (s_2)	3	4	3	1	2	3
Data Continuity Checking (s_3)	2	4	3	1	4	3
Tactical Forensics (s_4)	3	0	4	5	4	2

Max Possible Score = 20 Facility Defense Score = 11.5

Strongest Area is Restoration
Weakest Area is Life Cycle Cost

SYSTEMS ENGINEERING
Research Center

On Going Exploration

- A practical methodology for determining Assurance Level Values
  - Methodology for addressing uncertainty in assigning Assurance Level Values
- Methodology for utilizing Relative Value Weights
- Tradeoffs between scoring simplicity and transparency of results

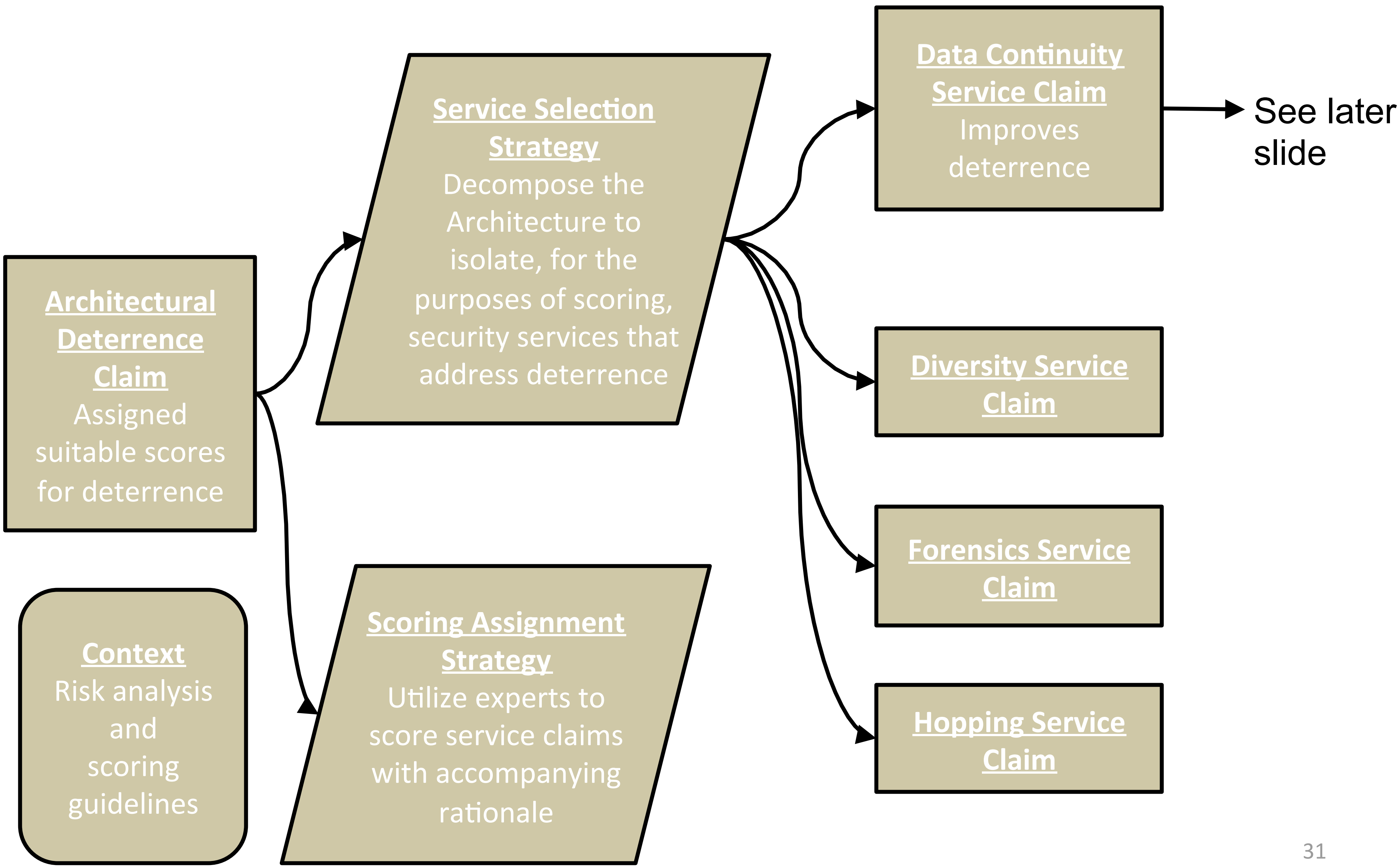
SYSTEMS ENGINEERING Research Center

Structured Arguments for System Scoring

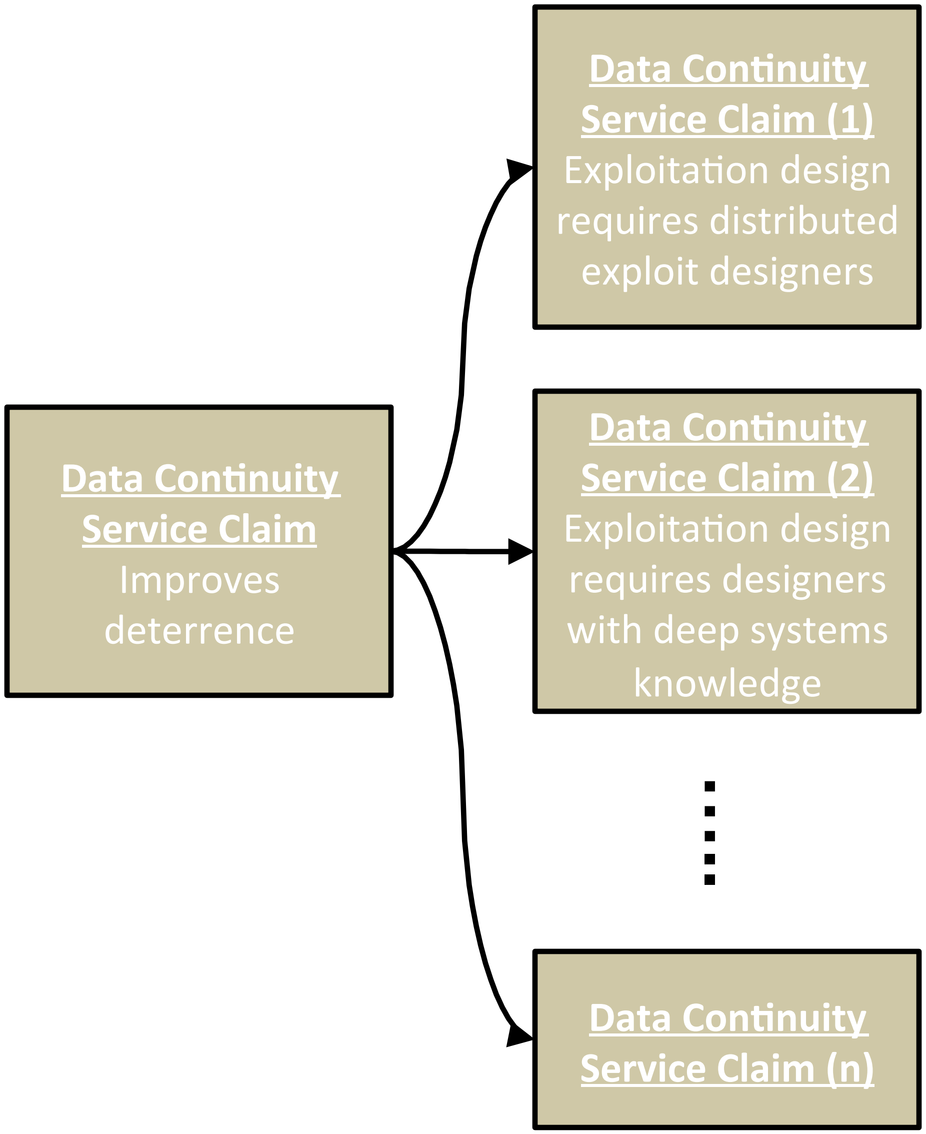
- Builds upon the legacy of work developed for safety and information assurance case evaluations
- Utilizes Goal Structuring Notation (GSN) for communicating arguments to support assigned scores in a repeatable and clear manner
- System-Aware security scoring arguments for a particular system architecture include:
  - Context supplied by the system owner and includes an available risk analysis for the system being protected and scoring guidelines
  - System supplier provides the list of security services to be applied and characterizes the purposes expected of security services that are deemed as most pertinent to reducing risk
    - Specific claims about value factors and the anticipated effects of security services on these factors
    - Explanations of how each security service is anticipated to impact specific value factor claims, including explicitly dividing each service into policy, process, and technology components with corresponding explanations of value

SYSTEMS ENGINEERING Research Center

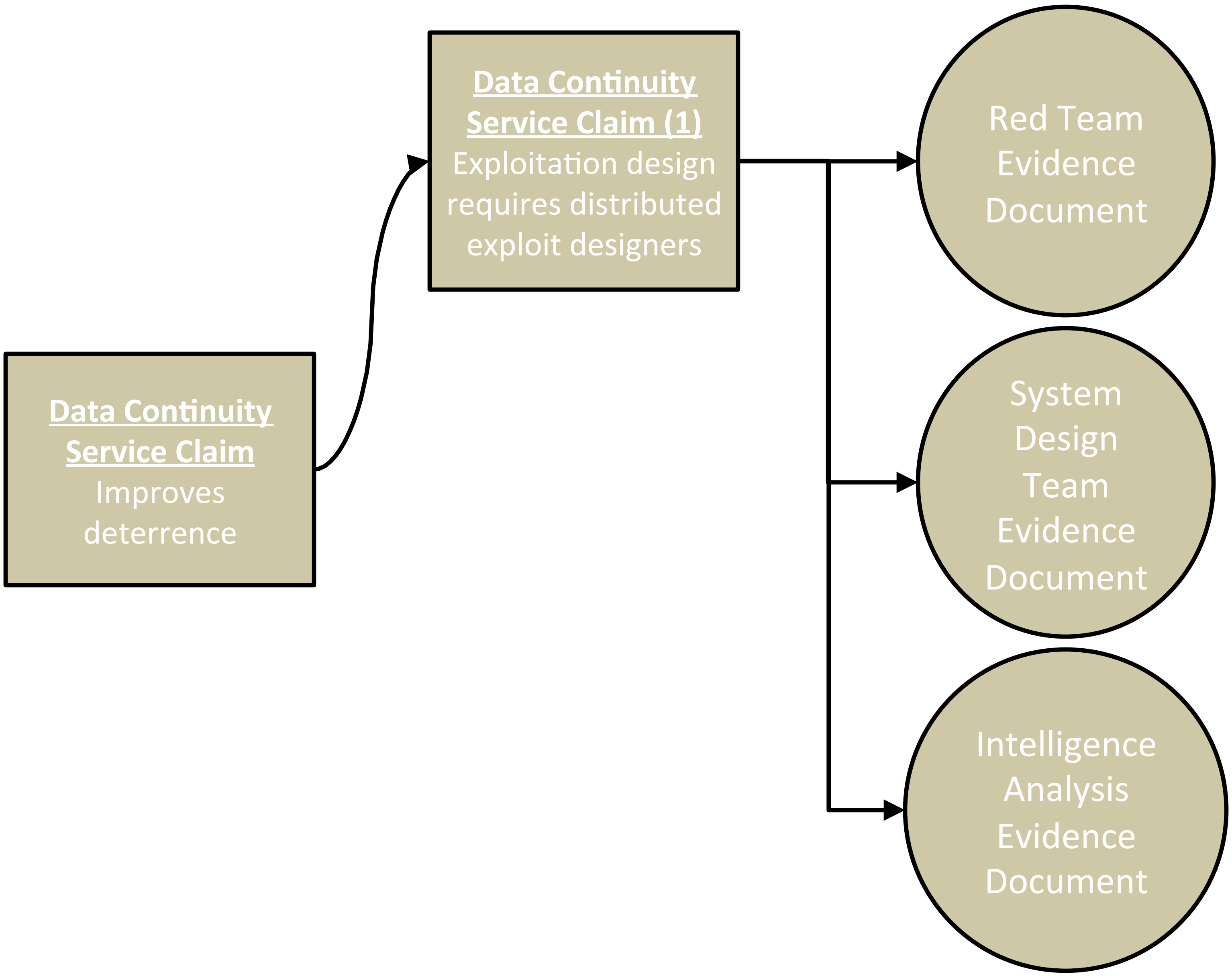
Simplified Diagrammatic Representation of a Structured Argument for Deterrence Scoring (1)



Simplified Diagrammatic Representation of a Structured Argument for Deterrence Scoring (2)



Simplified Diagrammatic Representation of a Structured Argument for Deterrence Scoring (3)



Simplified Diagrammatic Representation of a Structured Argument for Deterrence Scoring (4)