Analysis of Security Automation and Continuous Monitoring (SACM) Use Cases

Adam Montville, amontville@tripwire.com
David Waltermire, david.waltermire@nist.gov

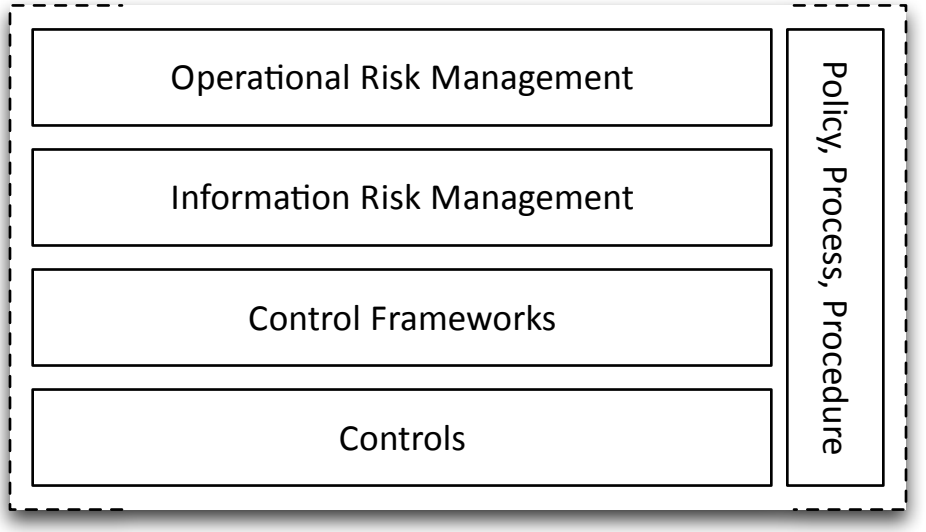
URL: http://tools.ietf.org/html/draft-montville-sacm-asset-identification-00

Abstract:

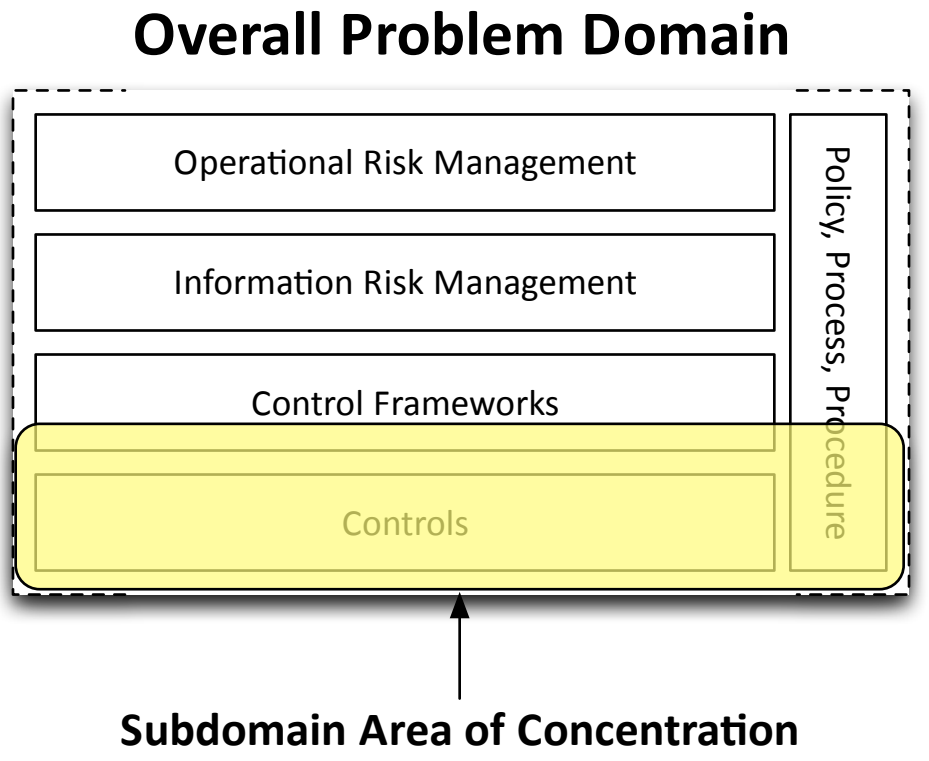
This document identifies foundational use cases, derived functional capabilities and requirements, architectural components, and the supporting standards needed to define an interoperable, automation \infrastructure required to support timely, accurate and actionable situational awareness over an organization's IT systems. Automation tools implementing a continuous monitoring approach will utilize this infrastructure together with existing and emerging event, incident and network management standards to provide visibility into the state of assets, user activities and network \behavior. Stakeholders will be able to use these tools to aggregate and analyze relevant security and operational data to understand the organizations security posture, quantify business risk, and make informed decisions that support organizational objectives while protecting critical information. Organizations will be able to use these tools to augment and automate information sharing activities to collaborate with partners to identify and mitigate threats. Other automation tools will be able to integrate with these capabilities to enforce policies based on human decisions to harden systems, prevent misuse and reduce the overall attack surface.

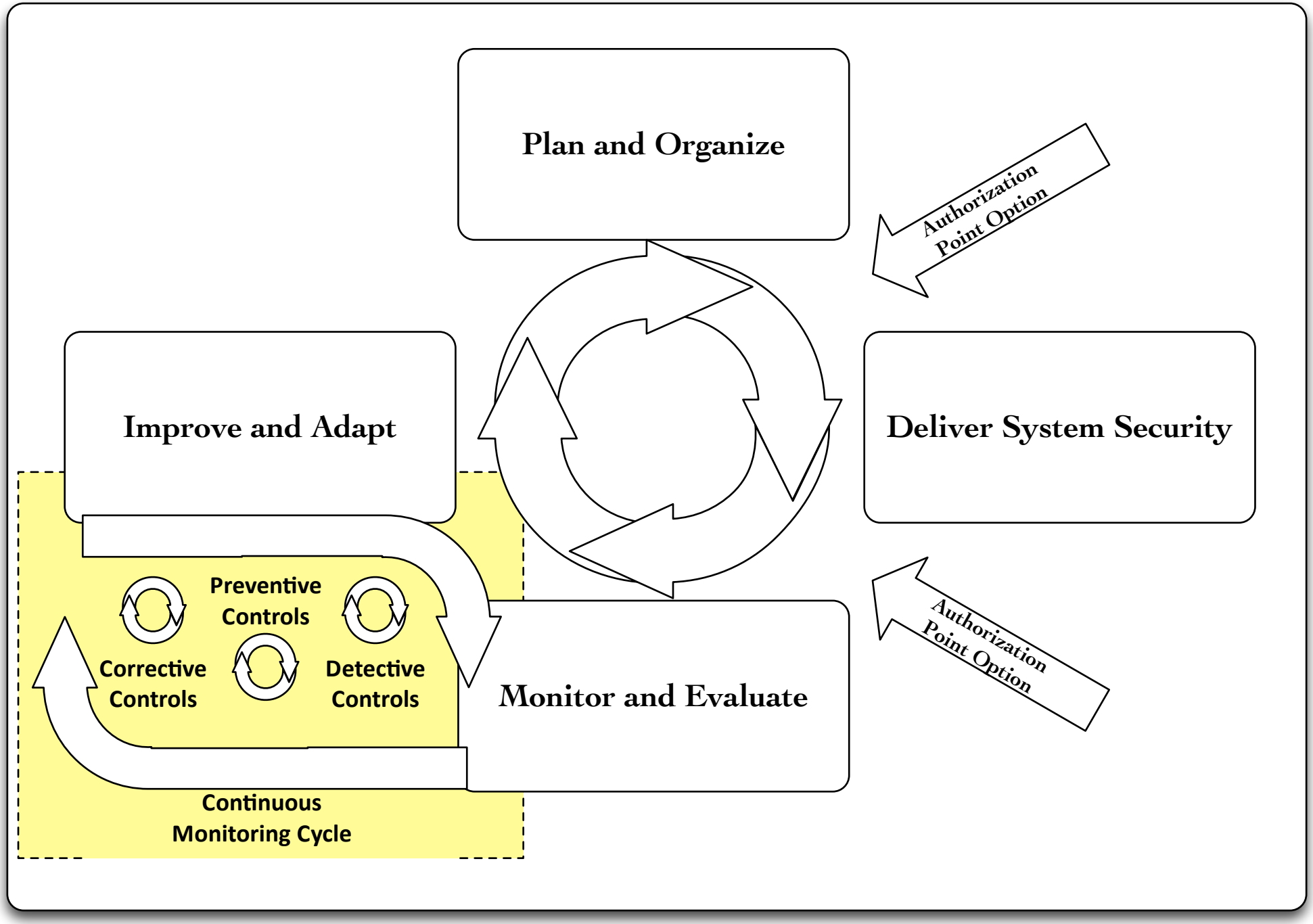
Frame Of Reference

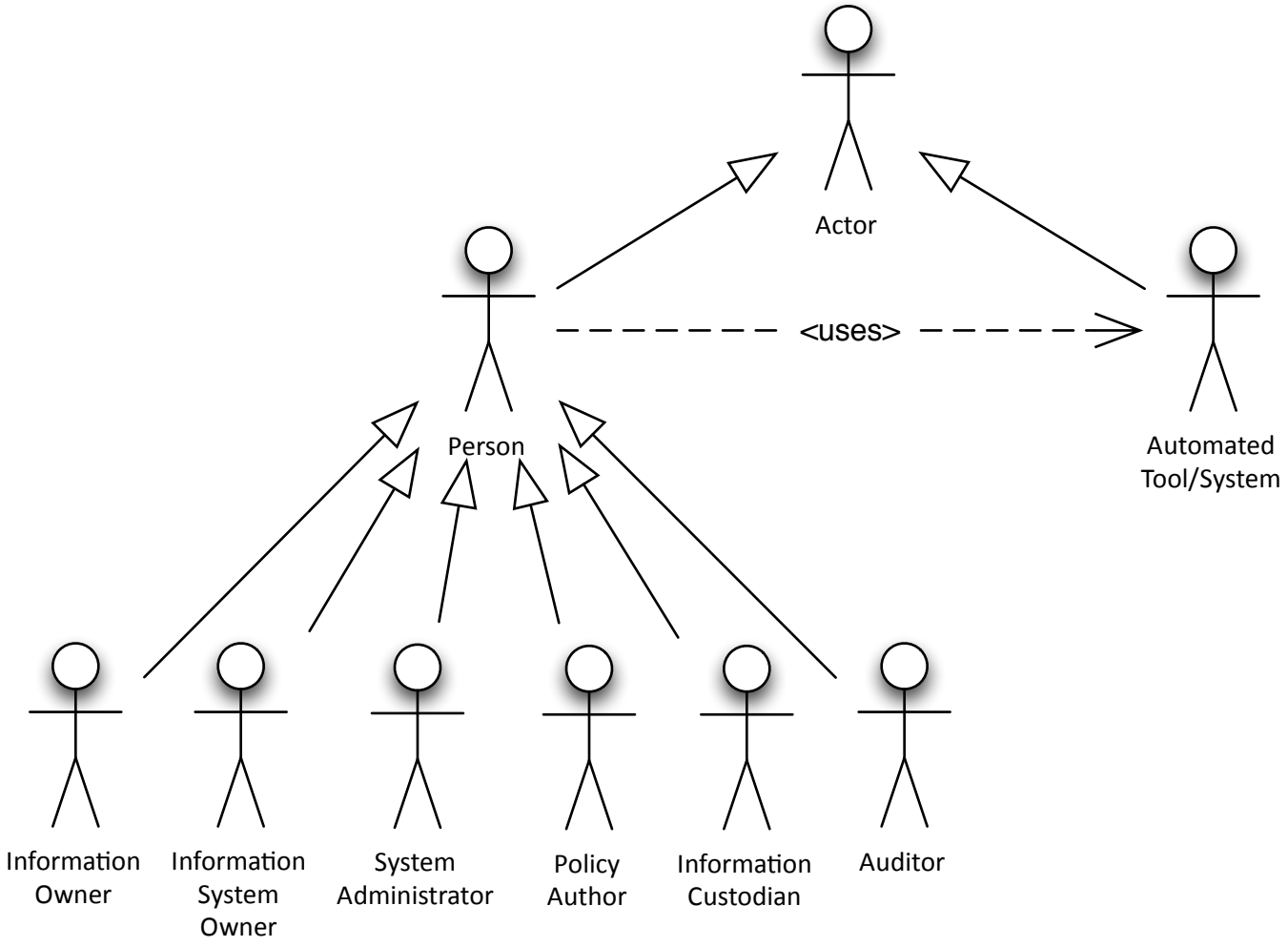
Overall Problem Domain

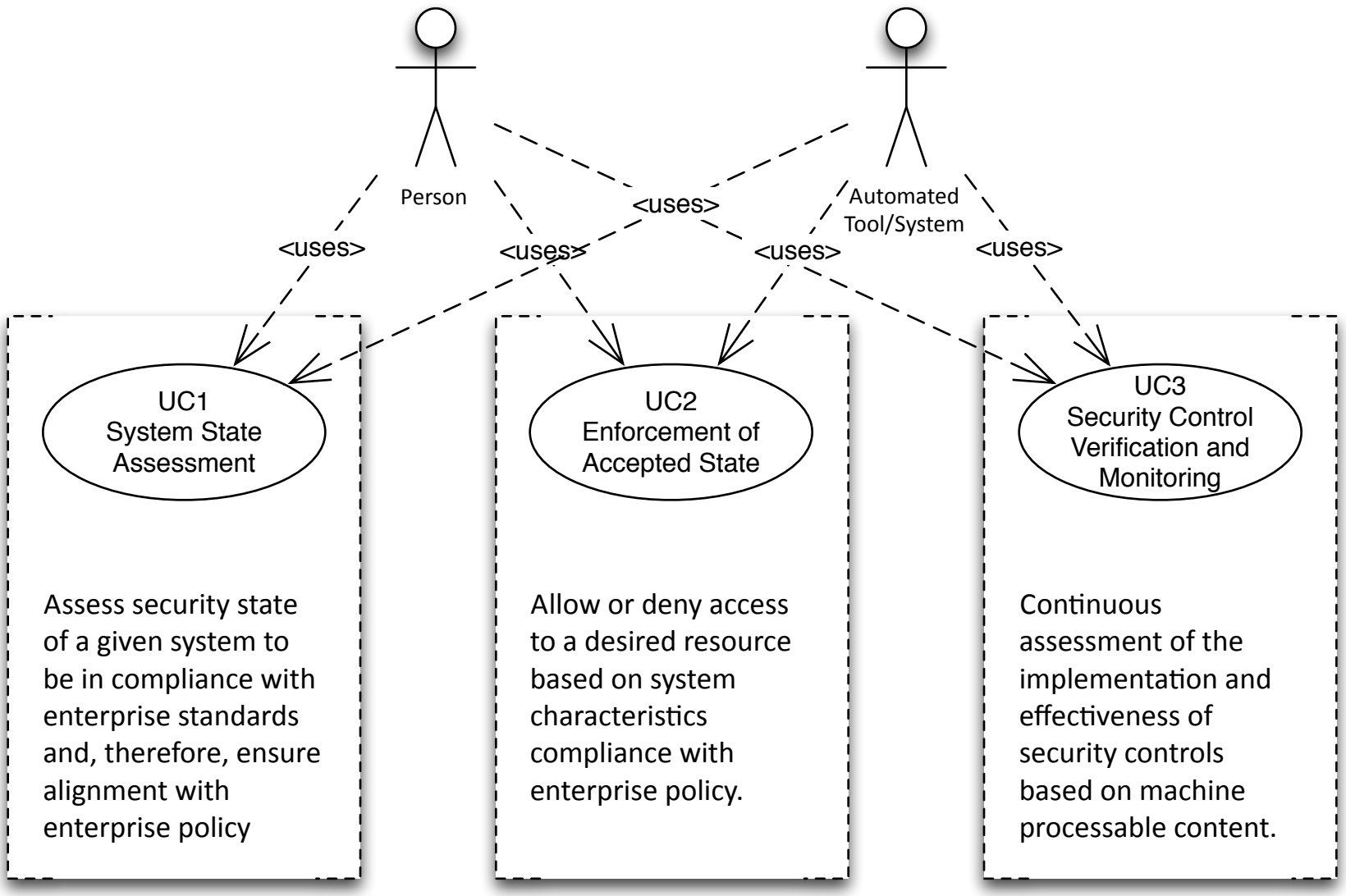


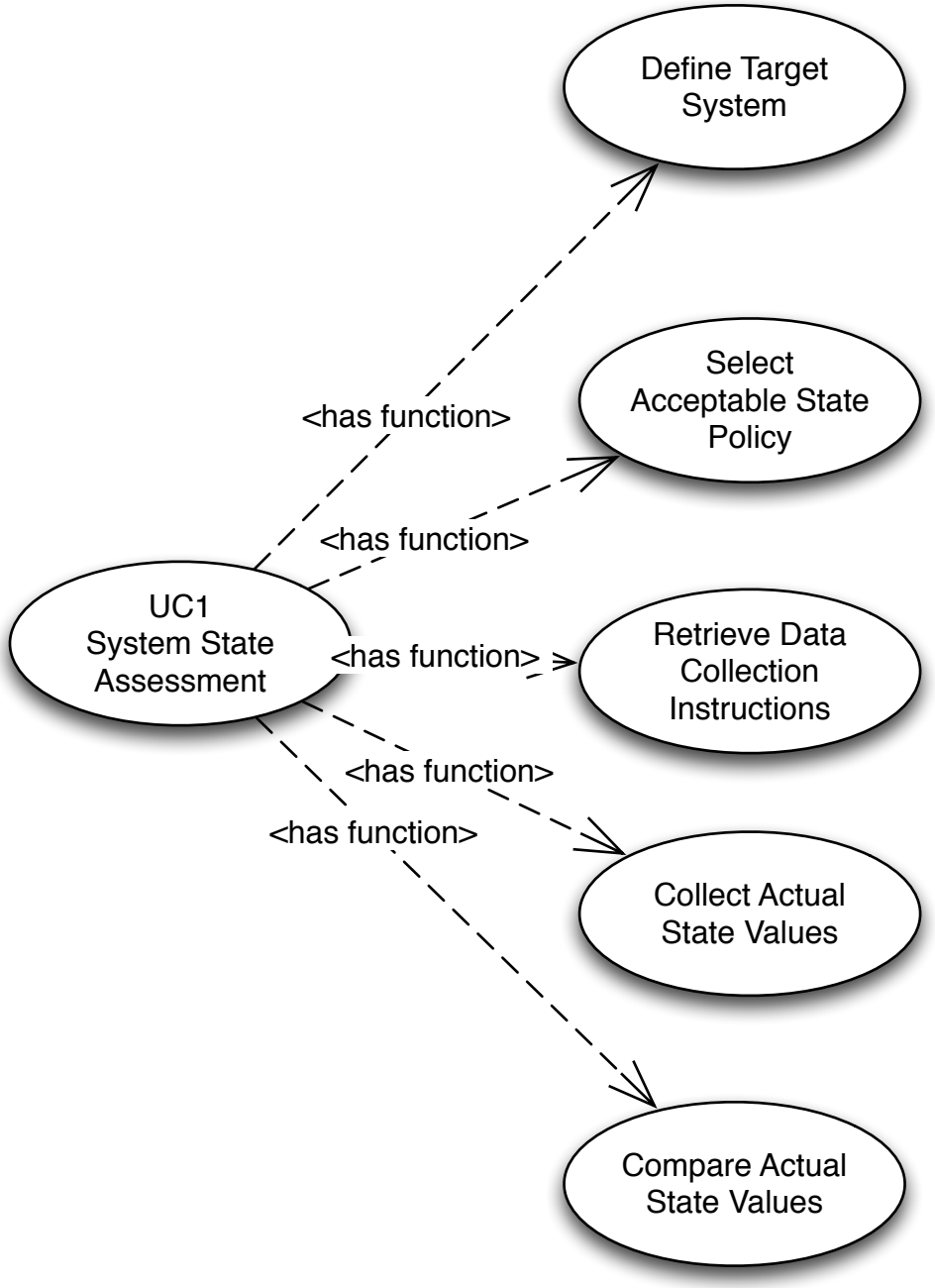
Frame Of Reference

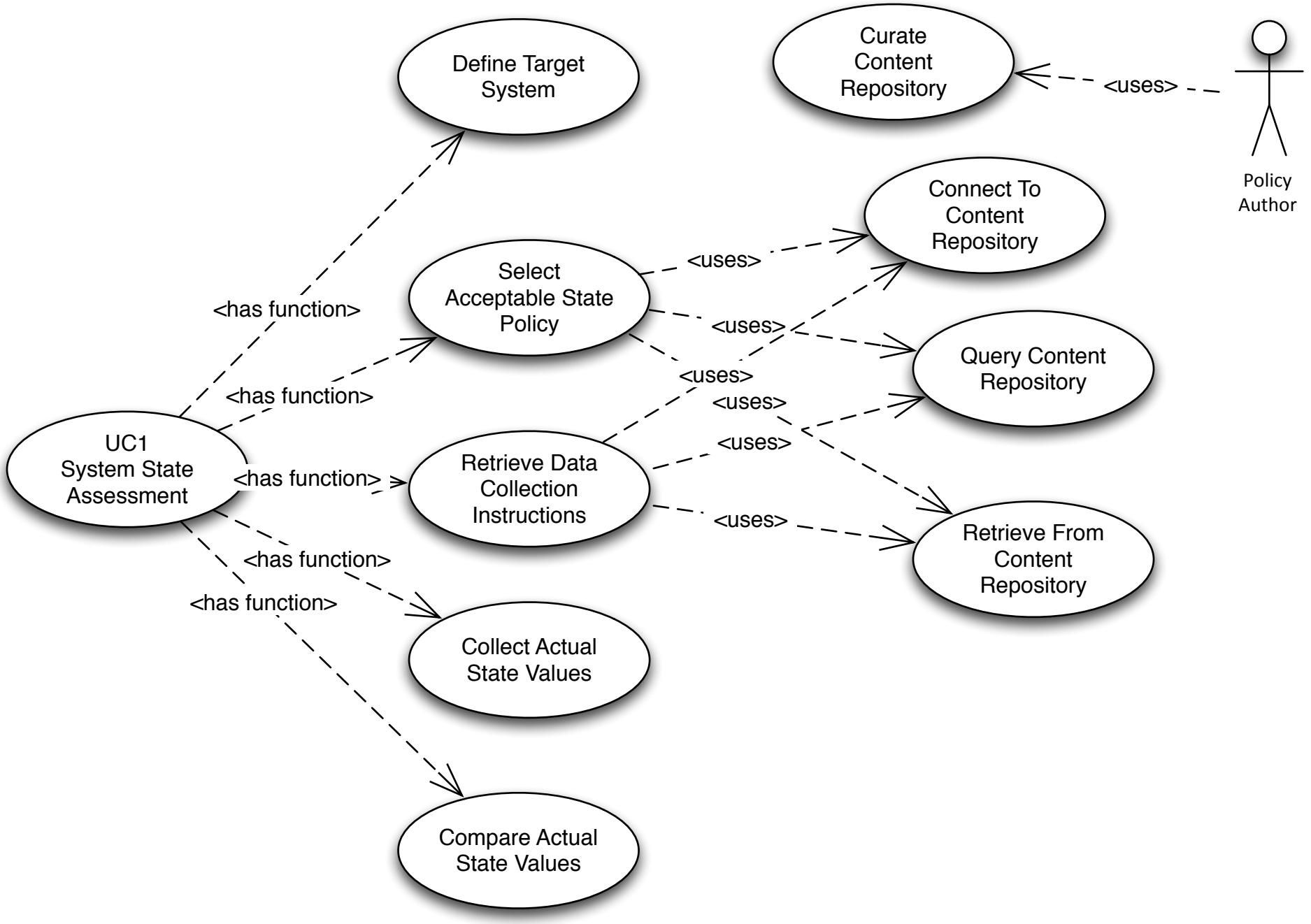


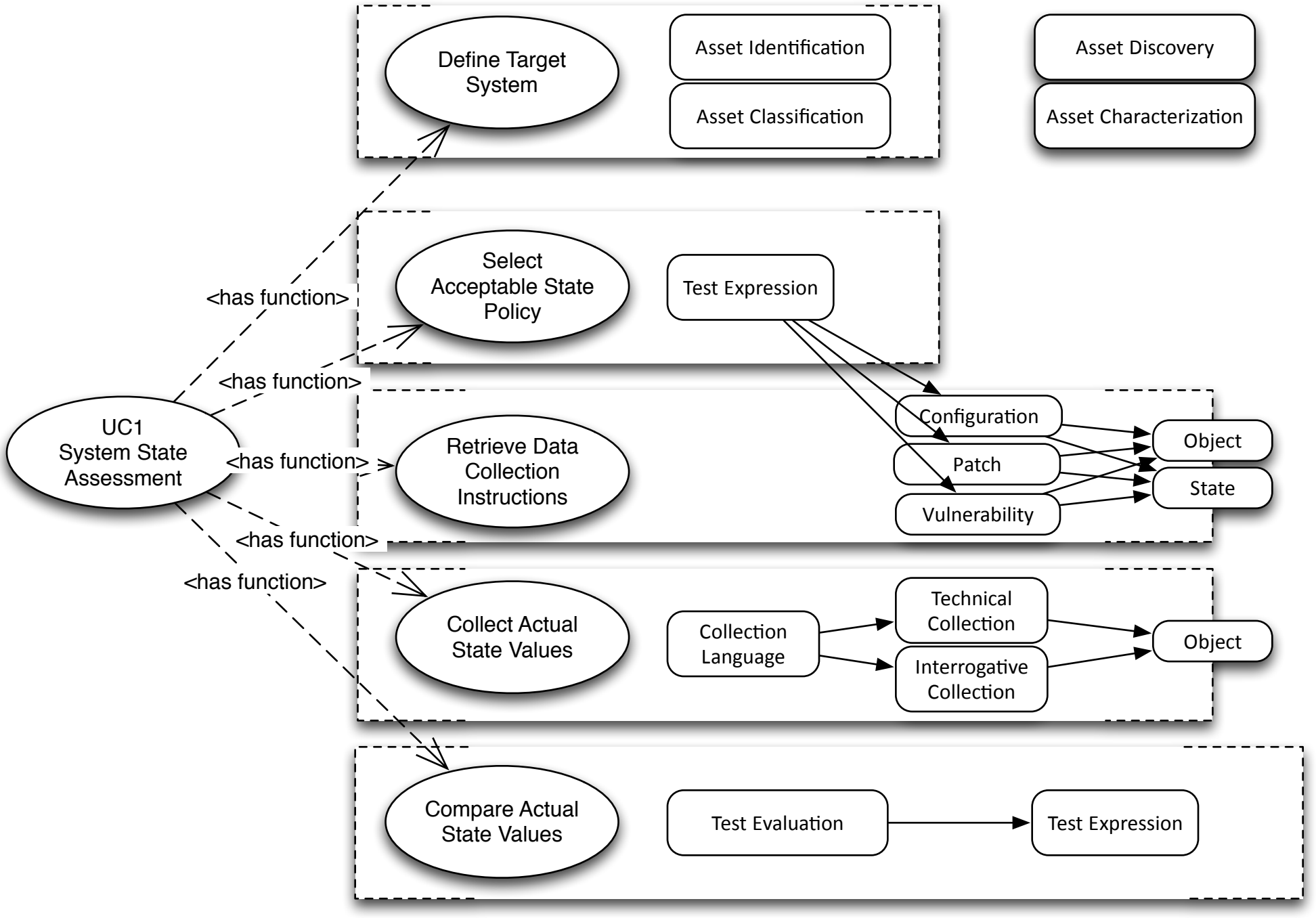

Plan and Organize
Authorization Point Option
Improve and Adapt
Deliver System Security
Preventive Controls
Corrective Controls
Detective Controls
Monitor and Evaluate
Authorization Point Option
Continuous Monitoring Cycle

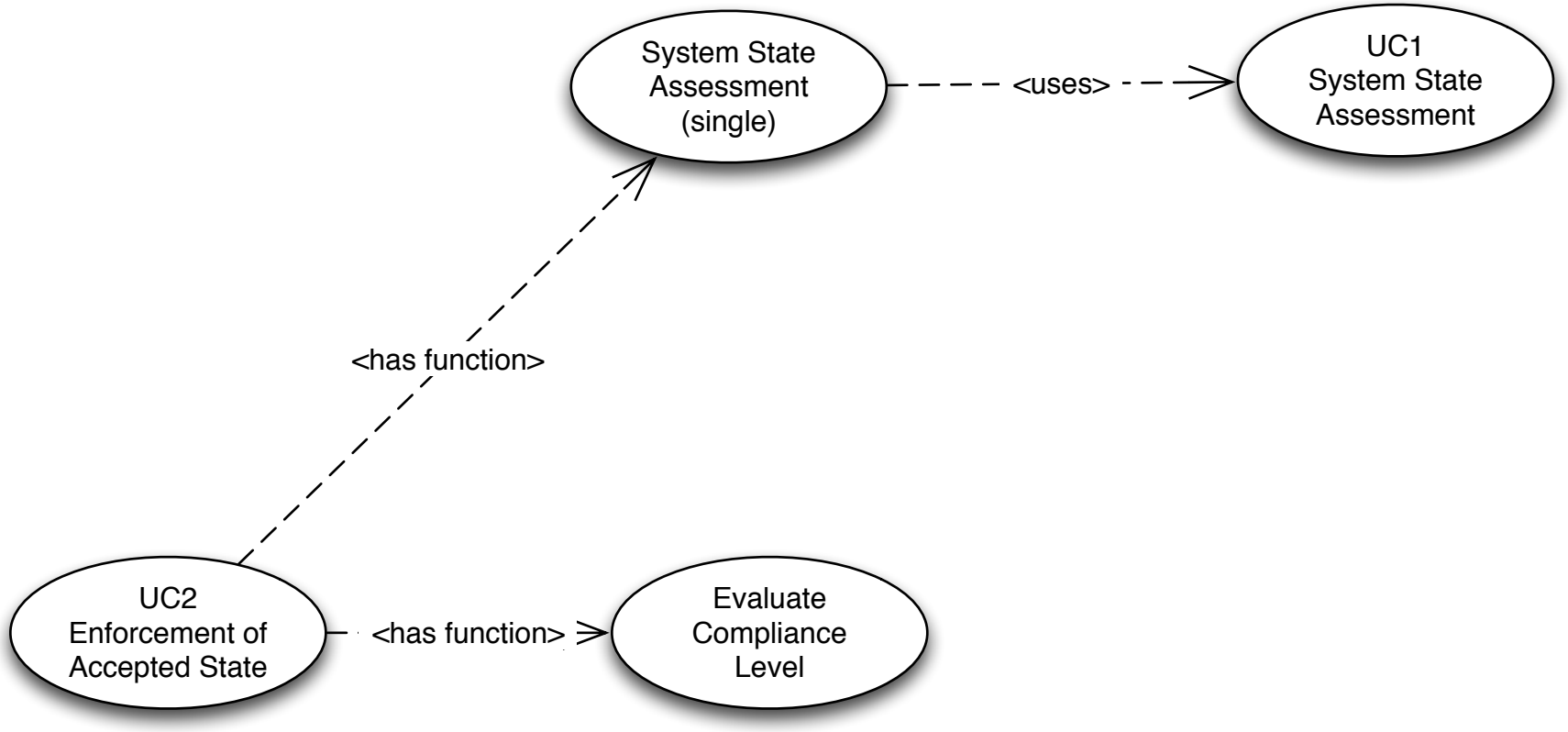

Actor
<uses>
Person
Automated
Tool/System
Information
Owner
Information
System
Owner
System
Administrator
Policy
Author
Information
Custodian
Auditor

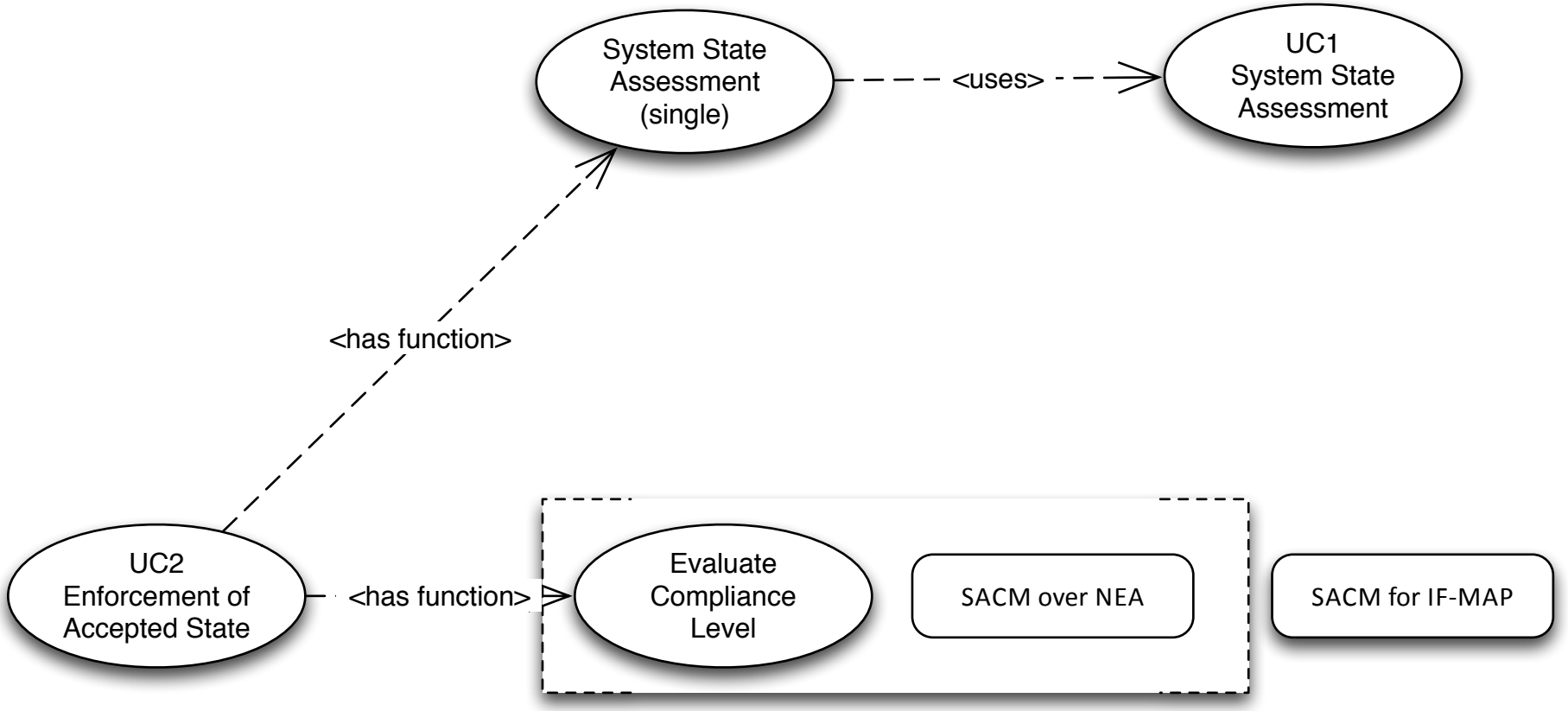

Person
Automated Tool/System
<uses>
<uses>
<uses>
<uses>
<uses>
UC1
System State Assessment
UC2
Enforcement of Accepted State
UC3
Security Control Verification and Monitoring
Assess security state of a given system to be in compliance with enterprise standards and, therefore, ensure alignment with enterprise policy
Allow or deny access to a desired resource based on system characteristics compliance with enterprise policy.
Continuous assessment of the implementation and effectiveness of security controls based on machine processable content.


Define Target System
Select Acceptable State Policy
<has function>
<has function>
UC1 System State Assessment
<has function>
Retrieve Data Collection Instructions
<has function>
<has function>
Collect Actual State Values
Compare Actual State Values

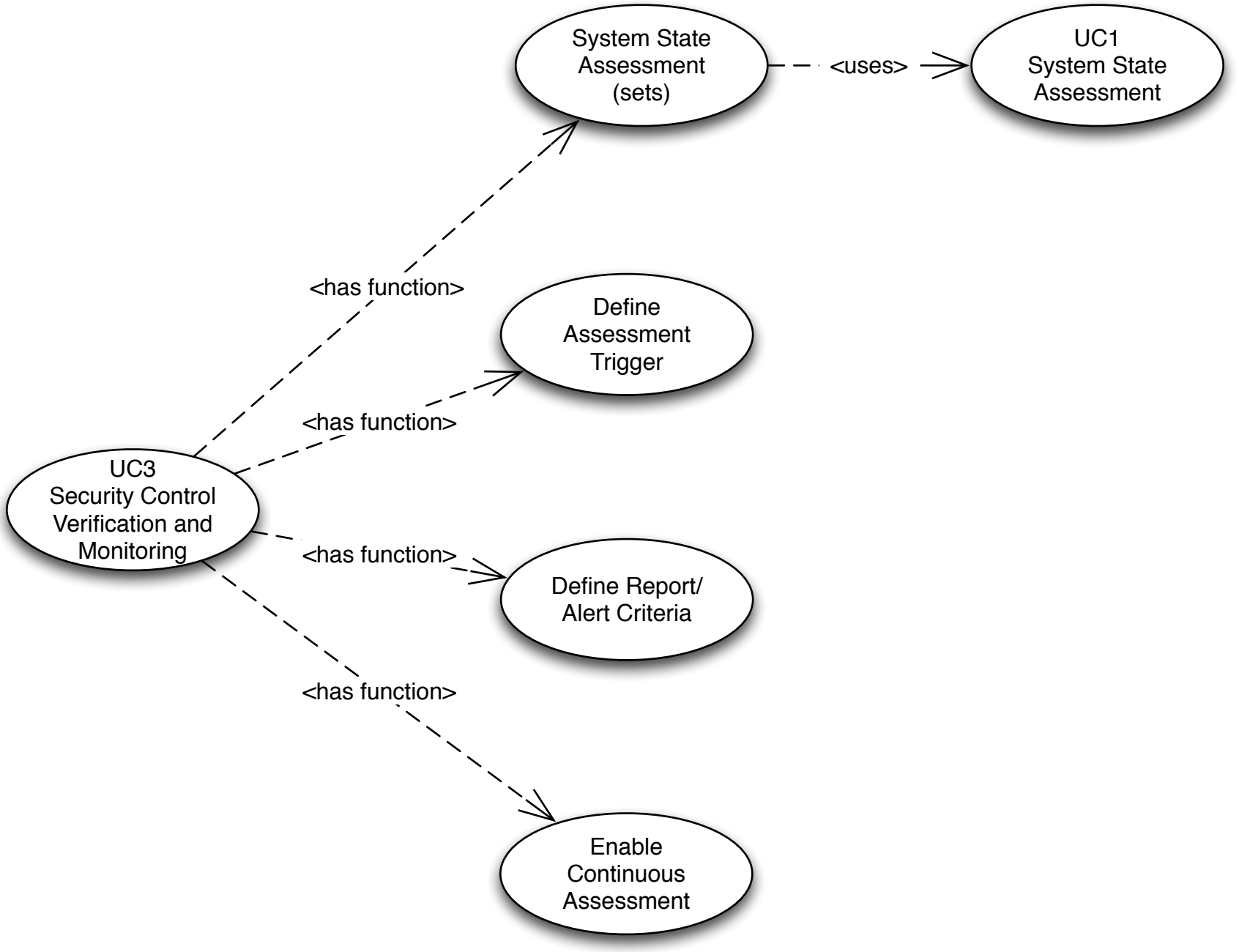

Define Target System
Curate Content Repository
<uses>
Policy Author
Connect To Content Repository
Select Acceptable State Policy
<uses>
<uses>
Query Content Repository
<uses>
<uses>
<has function>
<has function>
UC1 System State Assessment
<has function>
Retrieve Data Collection Instructions
<uses>
<uses>
Retrieve From Content Repository
<has function>
<has function>
Collect Actual State Values
Compare Actual State Values

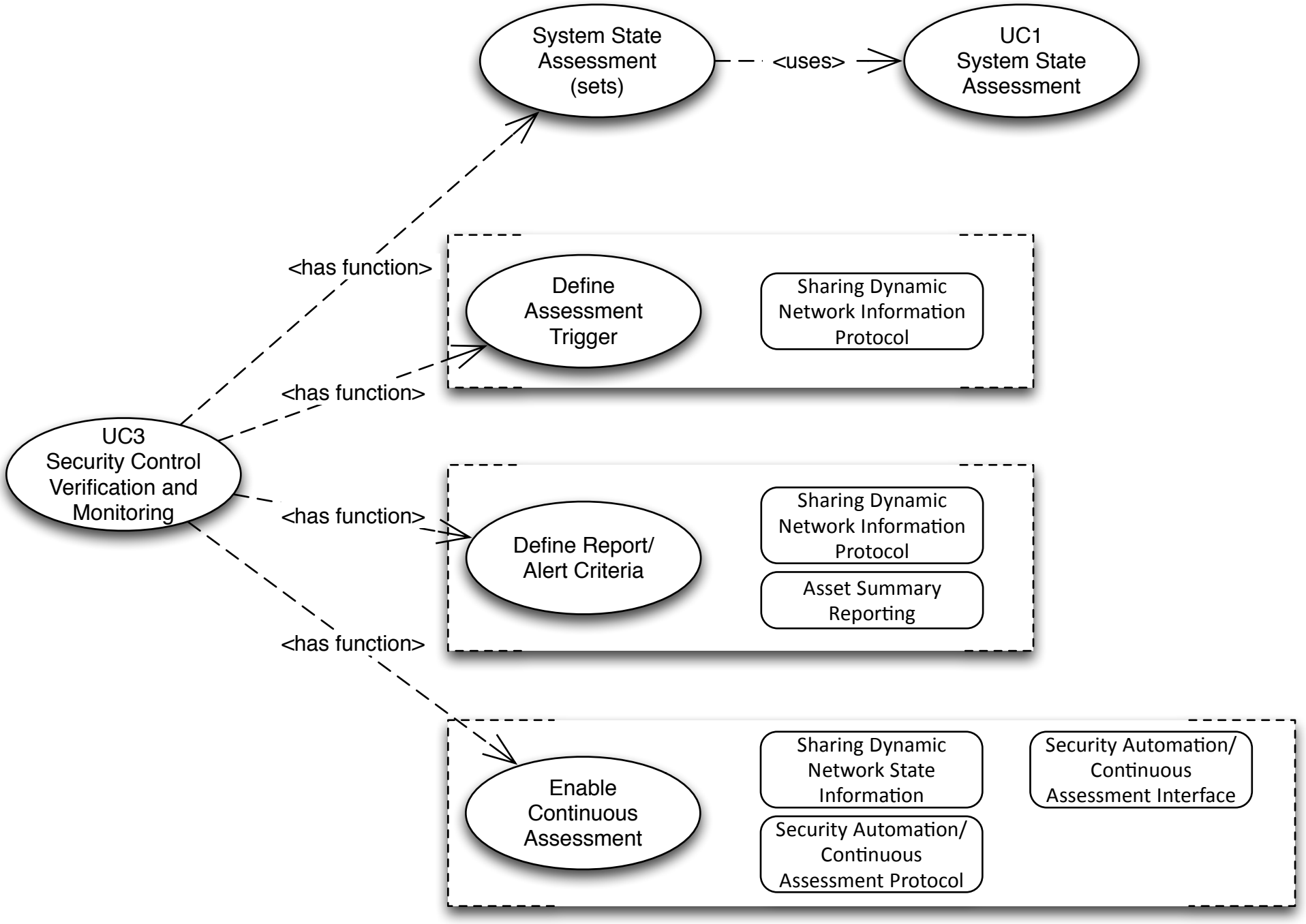

Define Target System
Asset Identification
Asset Classification
Asset Discovery
Asset Characterization
Select Acceptable State Policy
Test Expression
<has function>
<has function>
UC1 System State Assessment
<has function>
Retrieve Data Collection Instructions
Configuration
Patch
Vulnerability
Object
State
<has function>
<has function>
Collect Actual State Values
Collection Language
Technical Collection
Interrogative Collection
Object
Compare Actual State Values
Test Evaluation
Test Expression

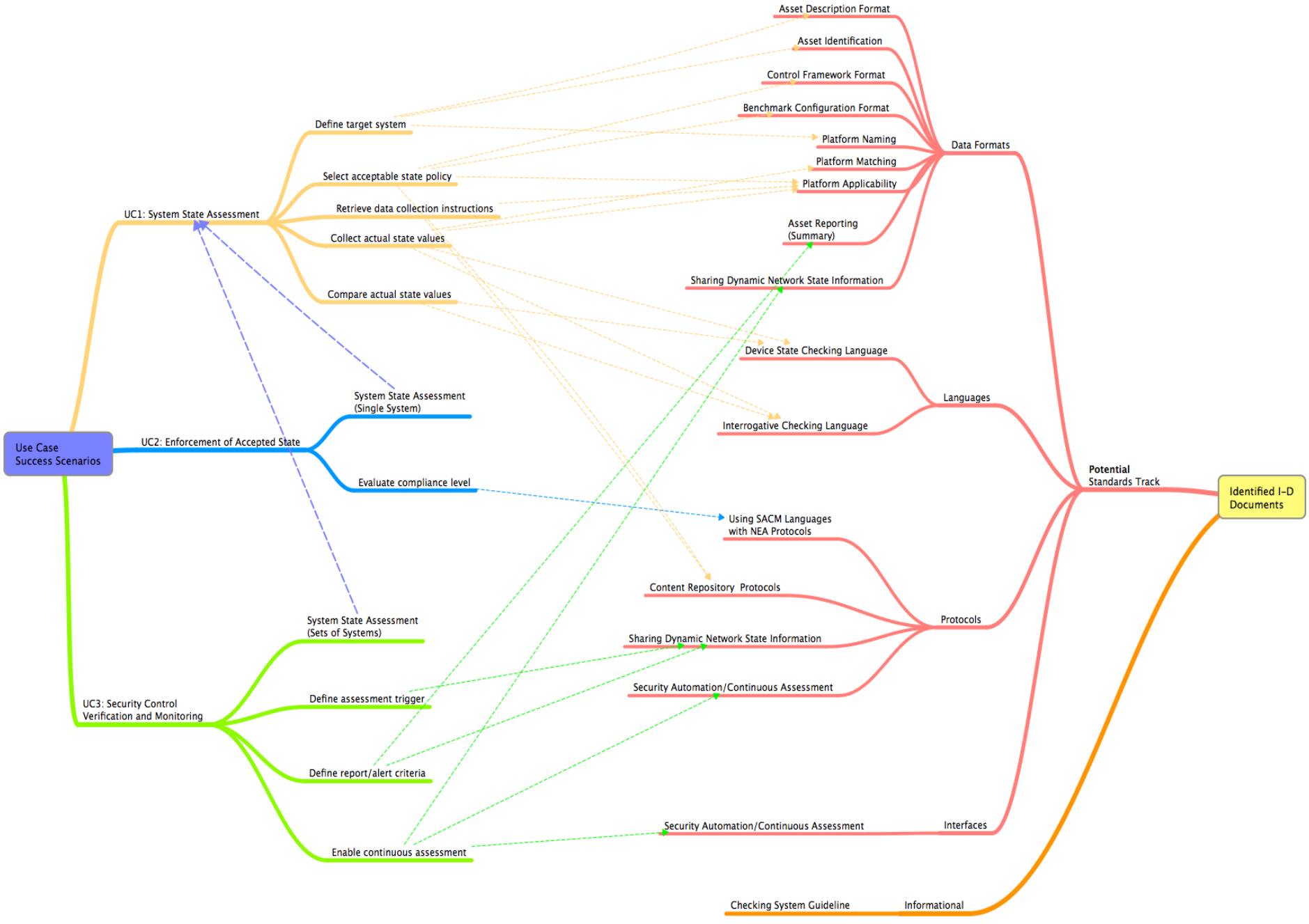

System State Assessment (single)
<uses>
UC1 System State Assessment
<has function>
UC2 Enforcement of Accepted State
<has function>
Evaluate Compliance Level

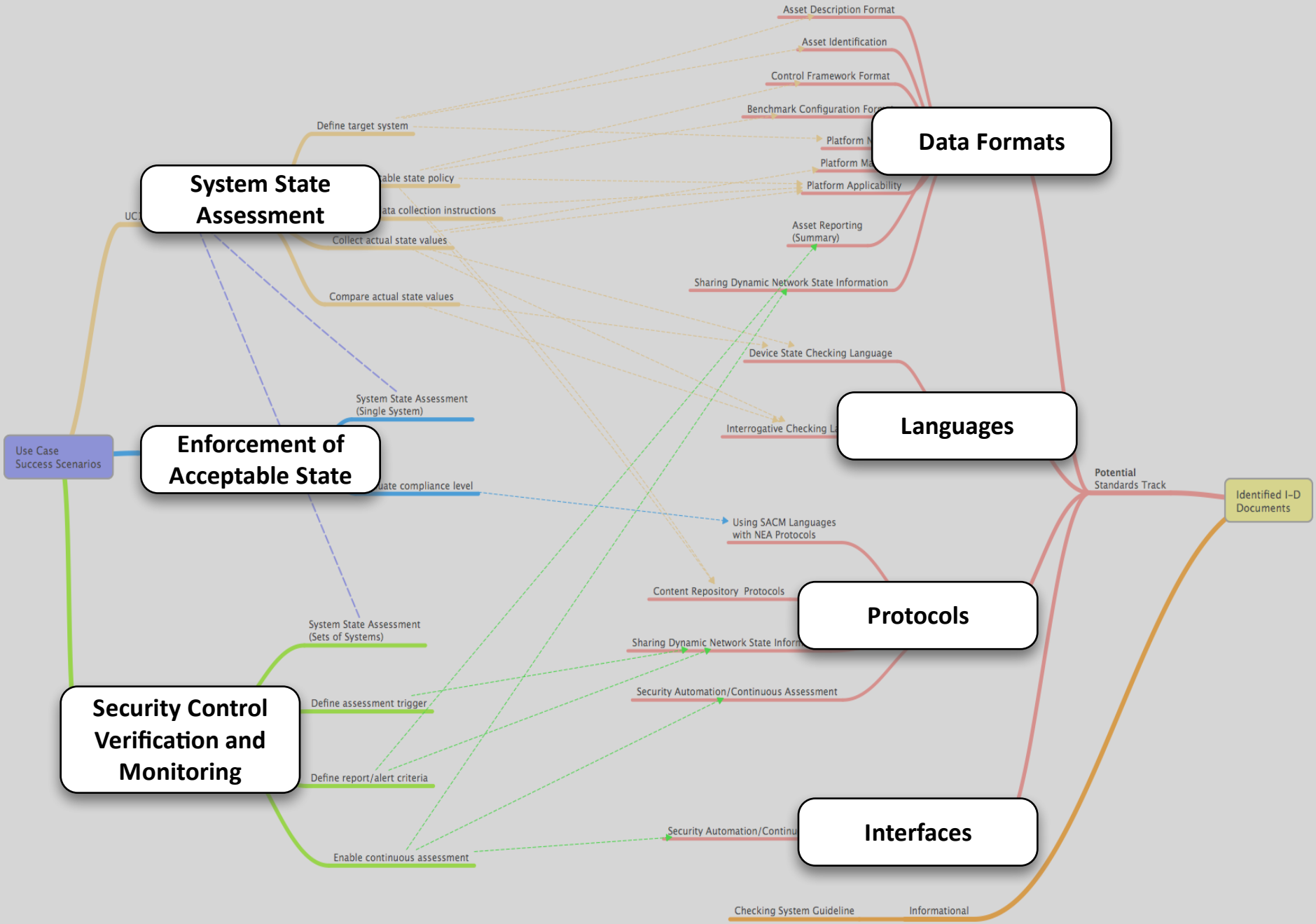

System State Assessment (single)
<uses>
UC1 System State Assessment
<has function>
UC2 Enforcement of Accepted State
<has function>
Evaluate Compliance Level
SACM over NEA
SACM for IF-MAP

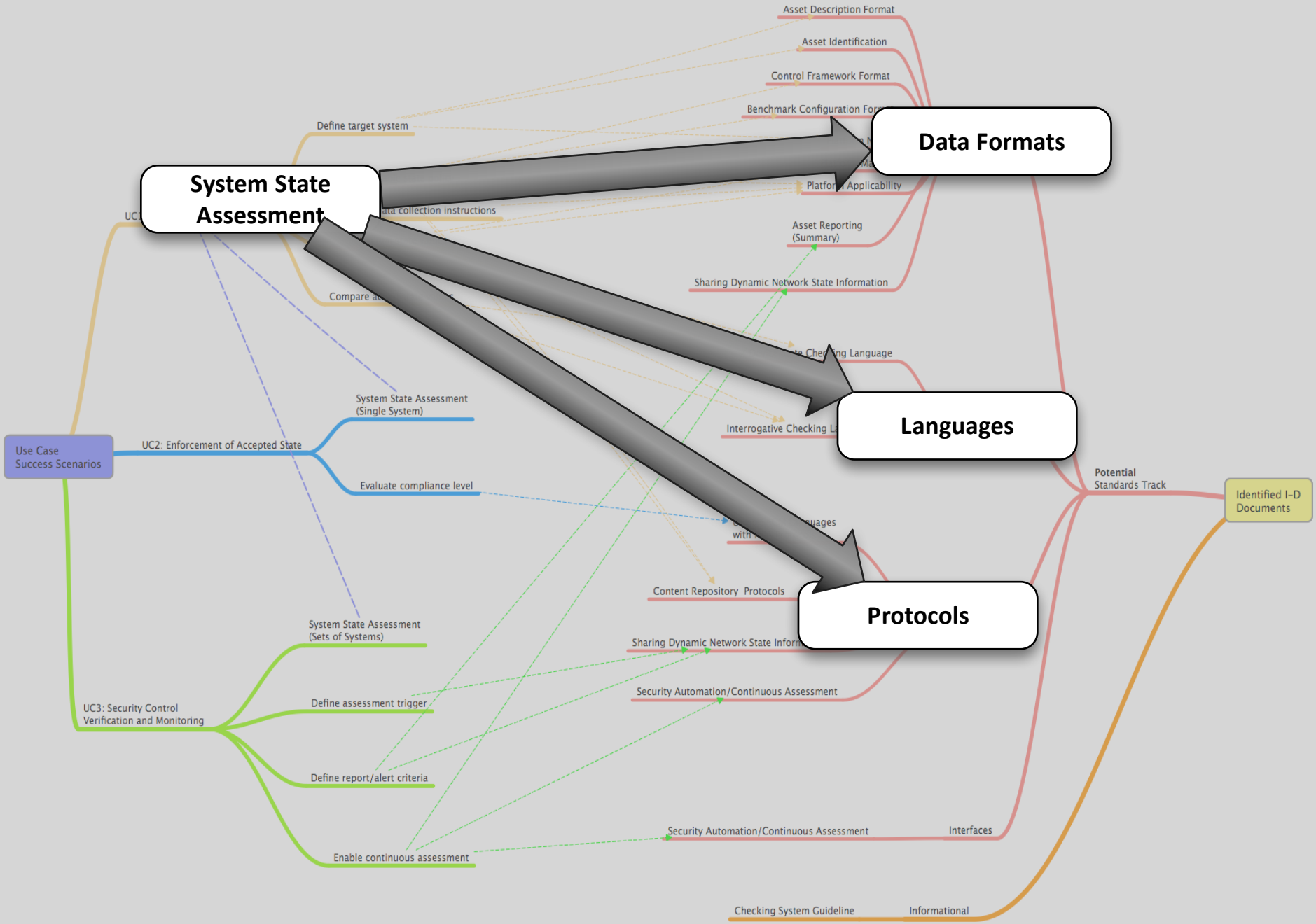
has function

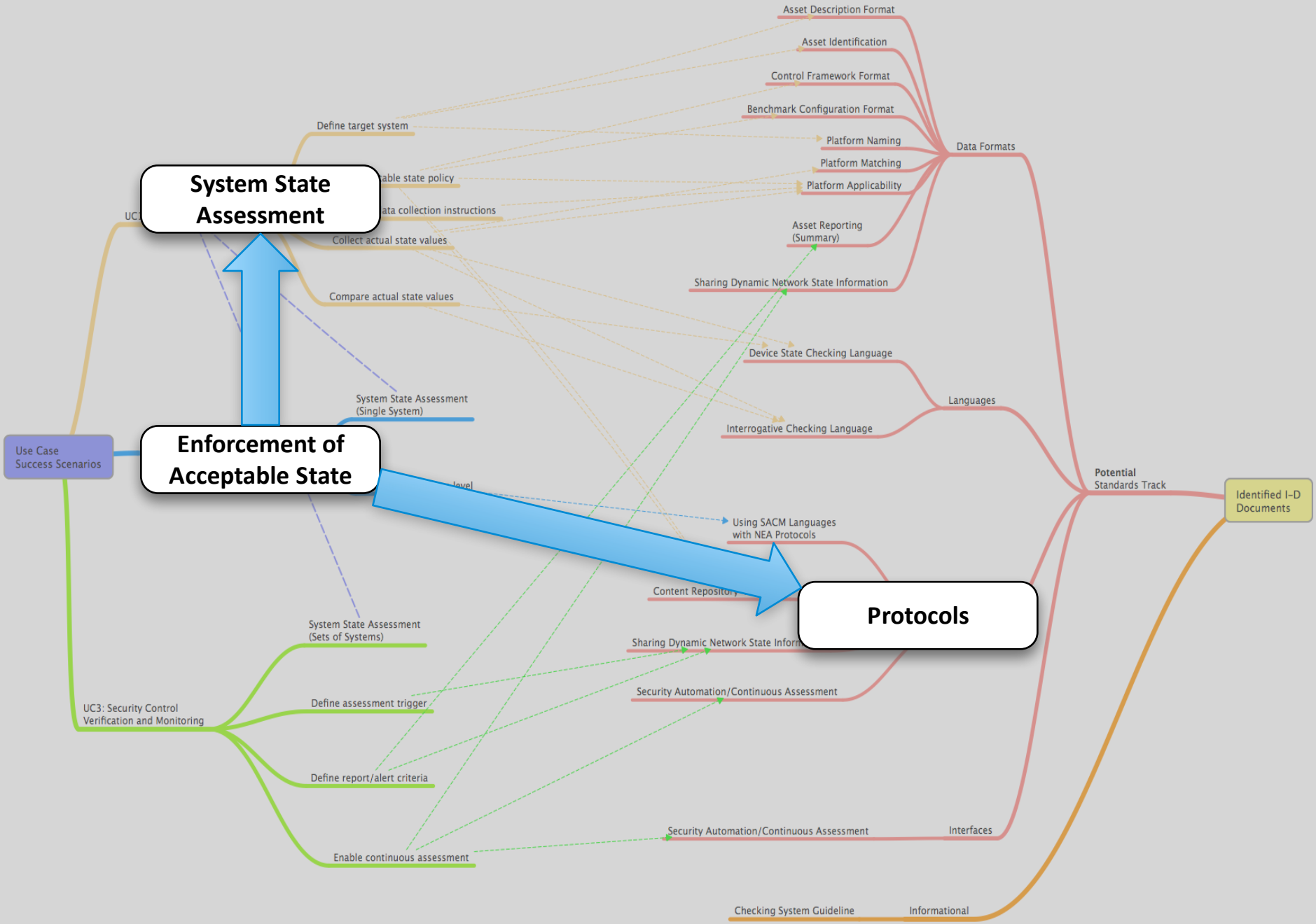


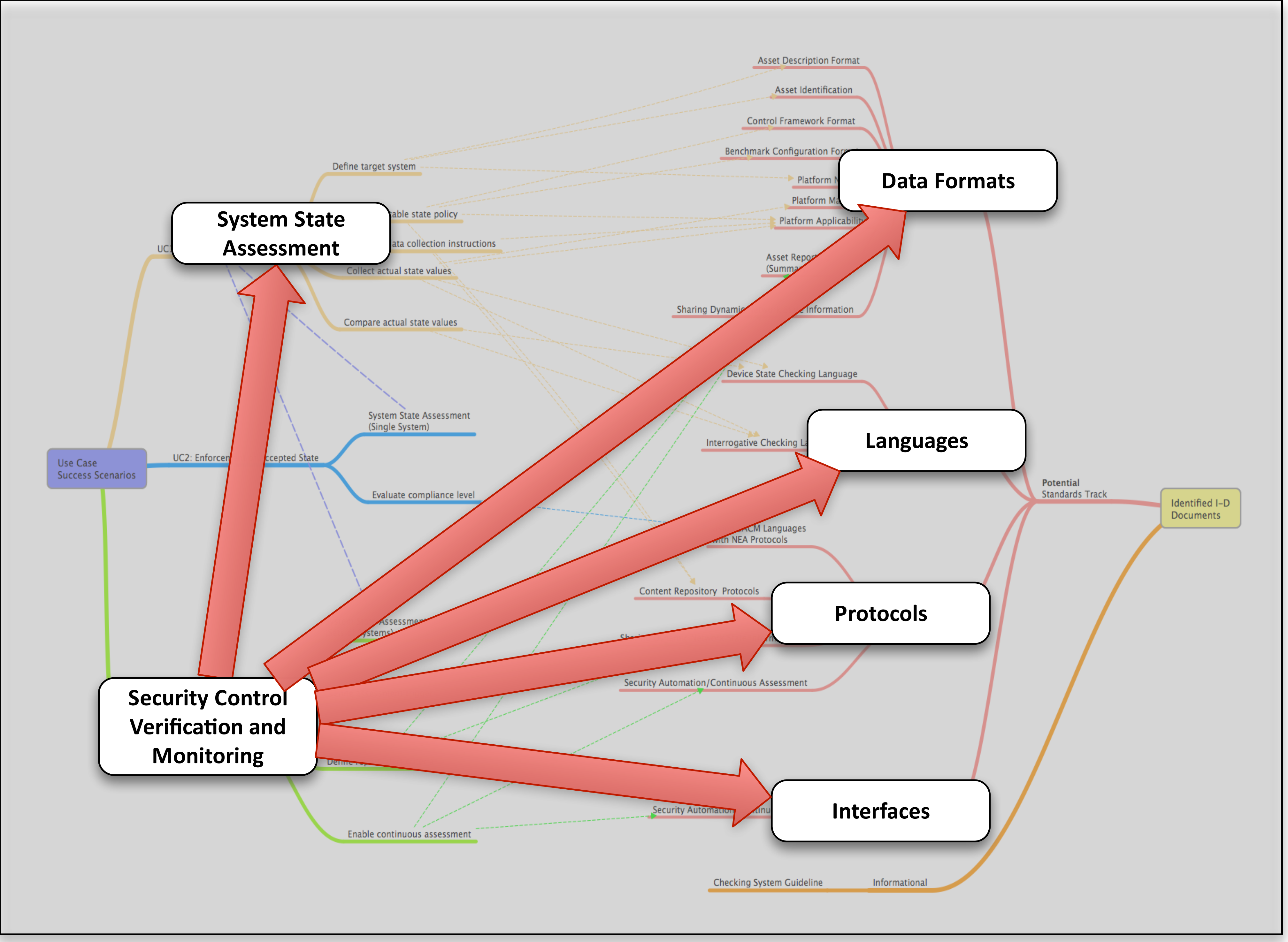

System State Assessment (sets)
<uses>
UC1 System State Assessment
<has function>
Define Assessment Trigger
Sharing Dynamic Network Information Protocol
<has function>
UC3 Security Control Verification and Monitoring
<has function>
Define Report/ Alert Criteria
Sharing Dynamic Network Information Protocol
Asset Summary Reporting
<has function>
Enable Continuous Assessment
Sharing Dynamic Network State Information
Security Automation/ Continuous Assessment Protocol
Security Automation/ Continuous Assessment Interface

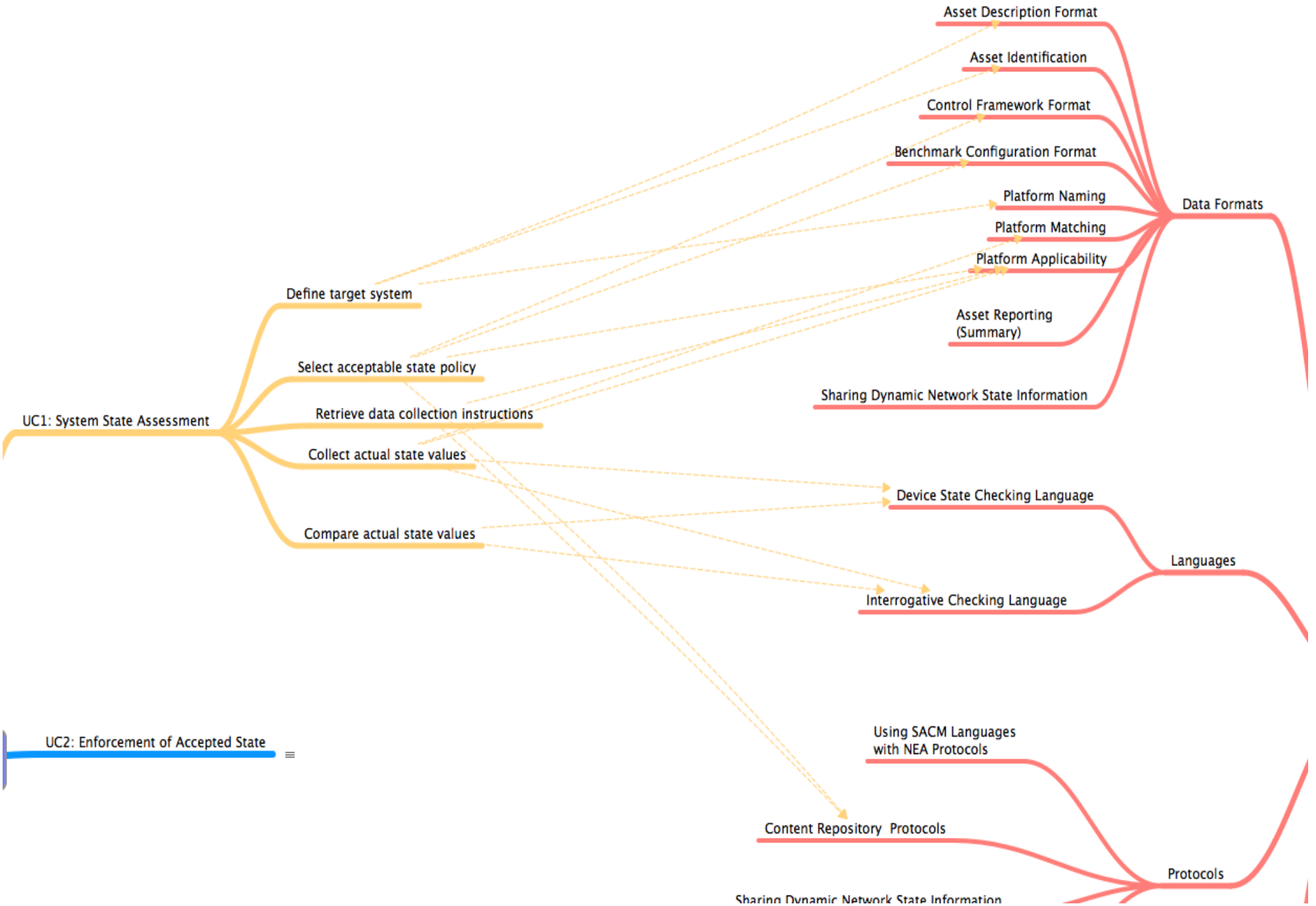

Use Case
Success Scenarios
UC1: System State Assessment
Define target system
Select acceptable state policy
Retrieve data collection instructions
Collect actual state values
Compare actual state values
UC2: Enforcement of Accepted State
System State Assessment
(Single System)
Evaluate compliance level
UC3: Security Control
Verification and Monitoring
System State Assessment
(Sets of Systems)
Define assessment trigger
Define report/alert criteria
Enable continuous assessment
Asset Description Format
Asset Identification
Control Framework Format
Benchmark Configuration Format
Platform Naming
Platform Matching
Platform Applicability
Asset Reporting
(Summary)
Sharing Dynamic Network State Information
Device State Checking Language
Interrogative Checking Language
Languages
Data Formats
Using SACM Languages
with NEA Protocols
Content Repository Protocols
Sharing Dynamic Network State Information
Security Automation/Continuous Assessment
Protocols
Security Automation/Continuous Assessment
Interfaces
Checking System Guideline
Informational
Potential
Standards Track
Identified I-D
Documents

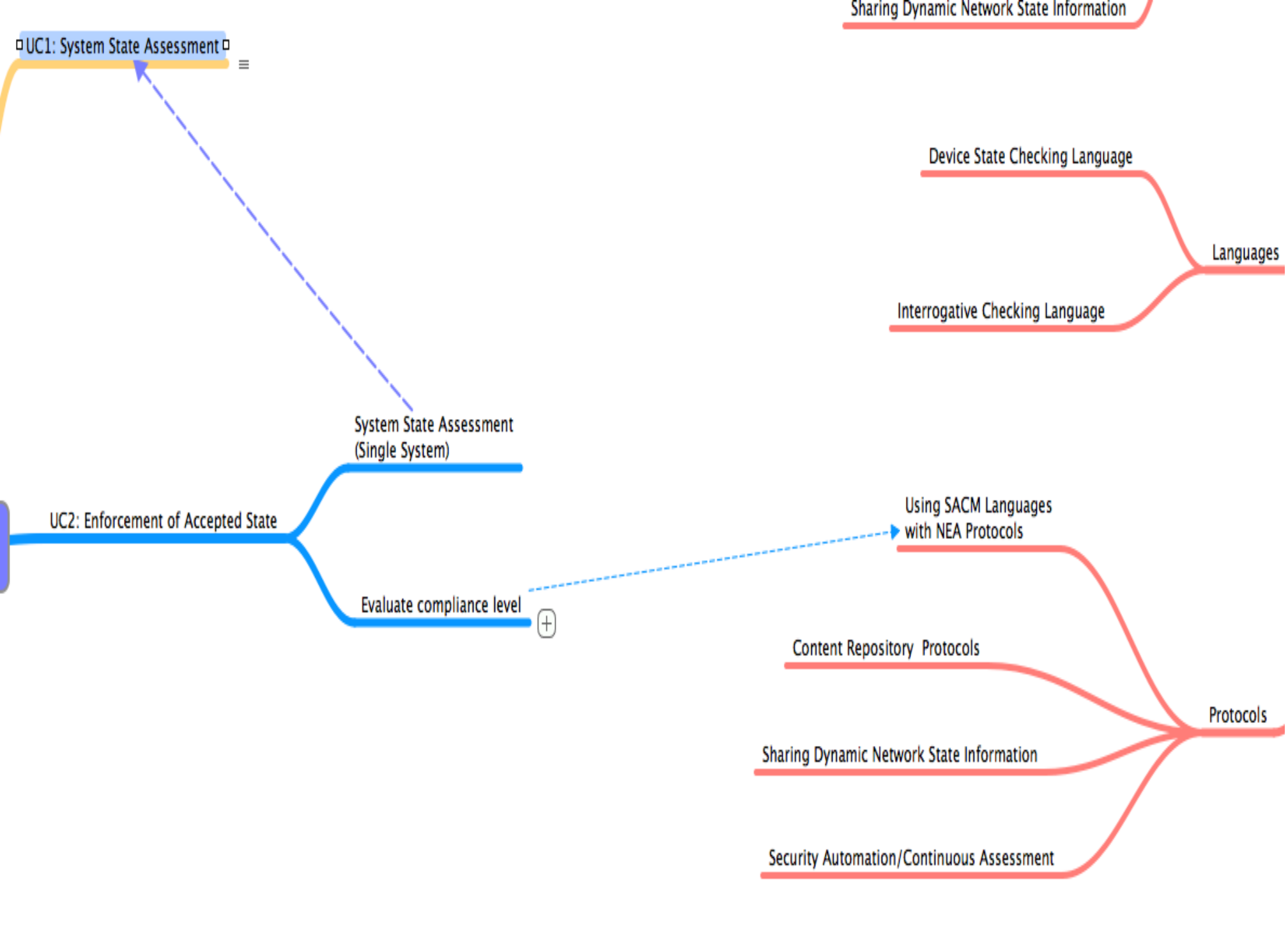

Asset Description Format
Asset Identification
Control Framework Format
Benchmark Configuration For
Platform
Platform
Platform Applicability
Asset Reporting (Summary)
Sharing Dynamic Network State Information
Device State Checking Language
Interrogative Checking
Data Formats
Languages
Define target system
able state policy
ata collection instructions
Collect actual state values
Compare actual state values
System State Assessment
UC
System State Assessment (Single System)
Use Case Success Scenarios
Enforcement of Acceptable State
uate compliance level
Using SACM Languages with NEA Protocols
Content Repository Protocols
Sharing Dynamic Network State Inform
Security Automation/Continuous Assessment
Protocols
Potential Standards Track
Identified I-D Documents
System State Assessment (Sets of Systems)
Define assessment trigger
Define report/alert criteria
Security Control Verification and Monitoring
Enable continuous assessment
Security Automation/Continu
Interfaces
Checking System Guideline
Informational

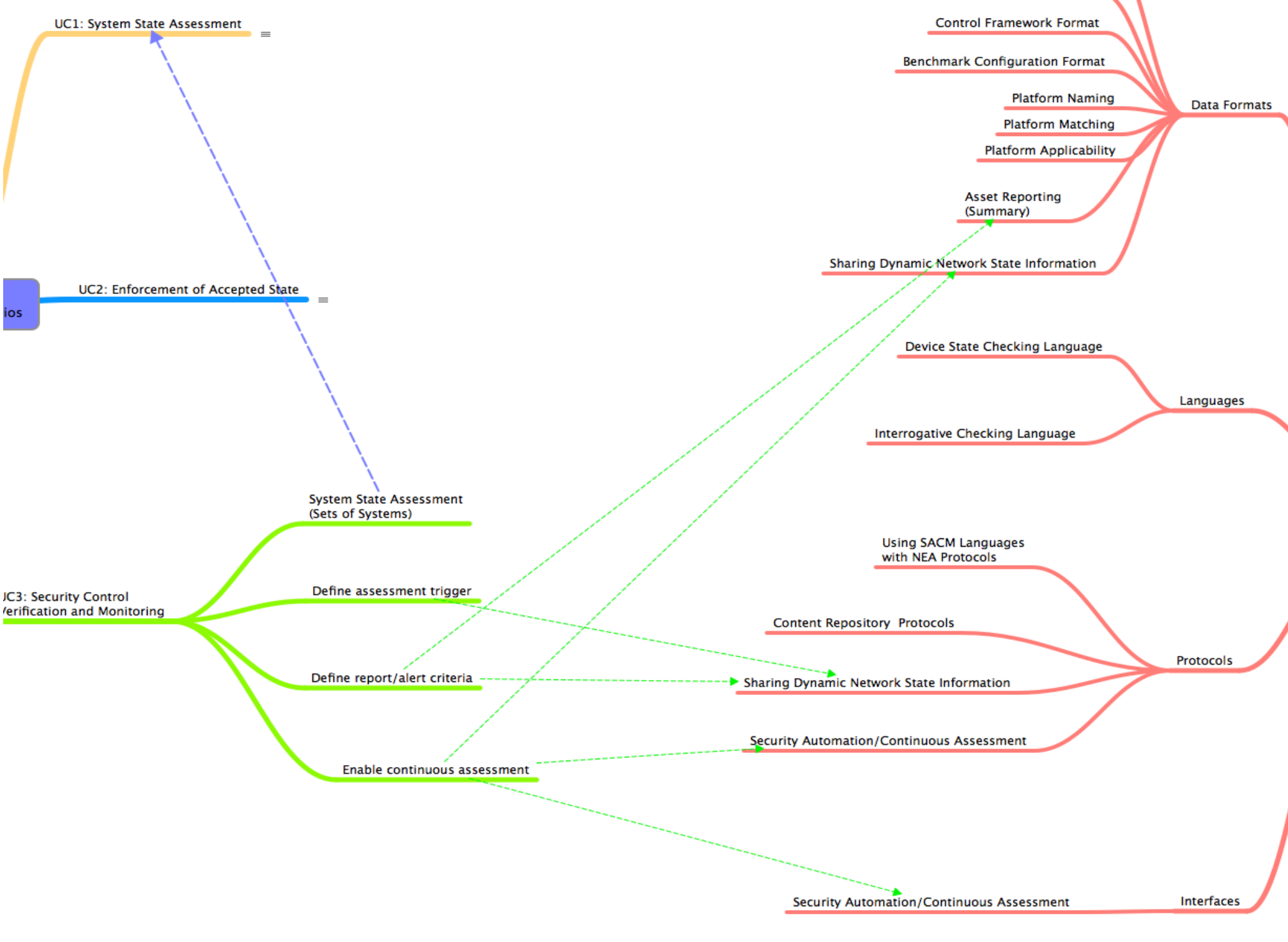

Asset Description Format
Asset Identification
Control Framework Format
Benchmark Configuration For
Define target system
Data Formats
System State Assessment
Platfor Applicability
ata collection instructions
Asset Reporting (Summary)
Sharing Dynamic Network State Information
Compare ac
Interrogative Checking L
System State Assessment (Single System)
Use Case Success Scenarios
UC2: Enforcement of Accepted State
Evaluate compliance level
Languages
Potential Standards Track
Identified I-D Documents
Content Repository Protocols
Protocols
System State Assessment (Sets of Systems)
Sharing Dynamic Network State Inform
Security Automation/Continuous Assessment
UC3: Security Control Verification and Monitoring
Define assessment trigger
Define report/alert criteria
Security Automation/Continuous Assessment
Interfaces
Enable continuous assessment
Checking System Guideline
Informational


System State Assessment
Enforcement of Acceptable State
Protocols
Use Case Success Scenarios
Define target system
able state policy
ata collection instructions
Collect actual state values
Compare actual state values
System State Assessment (Single System)
level
System State Assessment (Sets of Systems)
Define assessment trigger
Define report/alert criteria
Enable continuous assessment
UC3: Security Control Verification and Monitoring
Asset Description Format
Asset Identification
Control Framework Format
Benchmark Configuration Format
Platform Naming
Platform Matching
Platform Applicability
Asset Reporting (Summary)
Data Formats
Sharing Dynamic Network State Information
Device State Checking Language
Interrogative Checking Language
Languages
Using SACM Languages with NEA Protocols
Content Repository
Sharing Dynamic Network State Inform
Security Automation/Continuous Assessment
Security Automation/Continuous Assessment
Interfaces
Checking System Guideline
Informational
Potential Standards Track
Identified I-D Documents


System State Assessment
Data Formats
Languages
Protocols
Interfaces
Security Control Verification and Monitoring
Use Case Success Scenarios
Potential Standards Track
Identified I-D Documents
Asset Description Format
Asset Identification
Control Framework Format
Define target system
Collect actual state values
Compare actual state values
Device State Checking Language
System State Assessment (Single System)
Evaluate compliance level
Content Repository Protocols
Security Automation/Continuous Assessment
Enable continuous assessment
Checking System Guideline
Informational


Asset Description Format
Asset Identification
Control Framework Format
Benchmark Configuration Format
Platform Naming
Platform Matching
Platform Applicability
Asset Reporting (Summary)
Sharing Dynamic Network State Information
Data Formats
Define target system
Select acceptable state policy
Retrieve data collection instructions
Collect actual state values
Compare actual state values
UC1: System State Assessment
Device State Checking Language
Interrogative Checking Language
Languages
UC2: Enforcement of Accepted State
Using SACM Languages with NEA Protocols
Content Repository Protocols
Protocols
Sharing Dynamic Network State Information


Sharing Dynamic Network State Information
UC1: System State Assessment
Device State Checking Language
Languages
Interrogative Checking Language
System State Assessment
(Single System)
UC2: Enforcement of Accepted State
Using SACM Languages
with NEA Protocols
Evaluate compliance level
Content Repository Protocols
Protocols
Sharing Dynamic Network State Information
Security Automation/Continuous Assessment


UC1: System State Assessment
UC2: Enforcement of Accepted State
ios
UC3: Security Control
Verification and Monitoring
System State Assessment
(Sets of Systems)
Define assessment trigger
Define report/alert criteria
Enable continuous assessment
Control Framework Format
Benchmark Configuration Format
Platform Naming
Platform Matching
Platform Applicability
Asset Reporting
(Summary)
Sharing Dynamic Network State Information
Data Formats
Device State Checking Language
Interrogative Checking Language
Languages
Using SACM Languages
with NEA Protocols
Content Repository Protocols
Sharing Dynamic Network State Information
Security Automation/Continuous Assessment
Protocols
Security Automation/Continuous Assessment
Interfaces