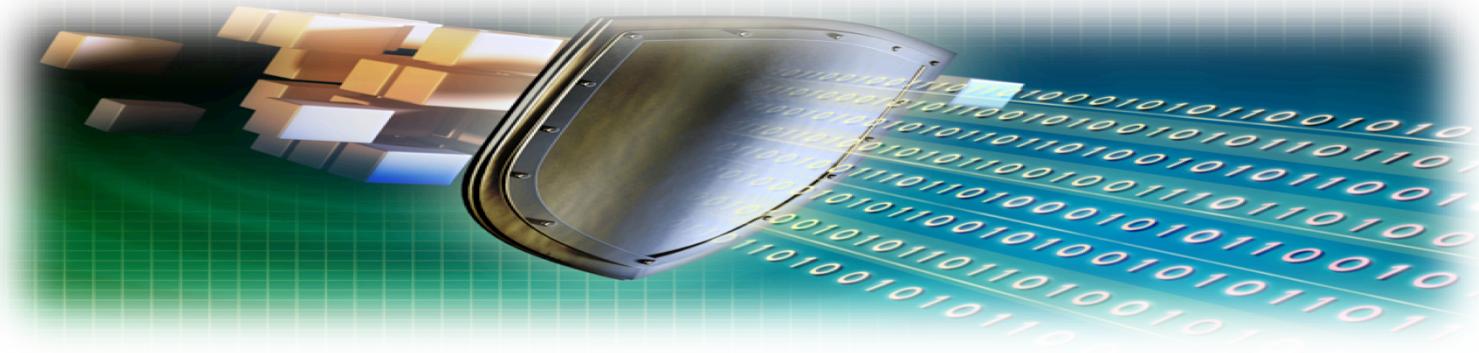




Working Together to Build Confidence

Towards a common OMG Risk Metamodel

Dr. Nikolai Mansourov, CTO KDM Analytics





Who we are, what we do

- Security Assurance company
 - Security risk assessments
 - Top-down, in the context of DoDAF views
 - Bottom-up, from source or binary code
 - Emphasis on automation
 - Emphasis on information sharing
 - OMG System Assurance Ecosystem
 - Systematic, repeatable methodology
 - FORSA
 - Efficient tool support
 - KDM Blade
 - Cameo Risk Analyzer, integrated with NoMagic Cameo Enterprise Architect



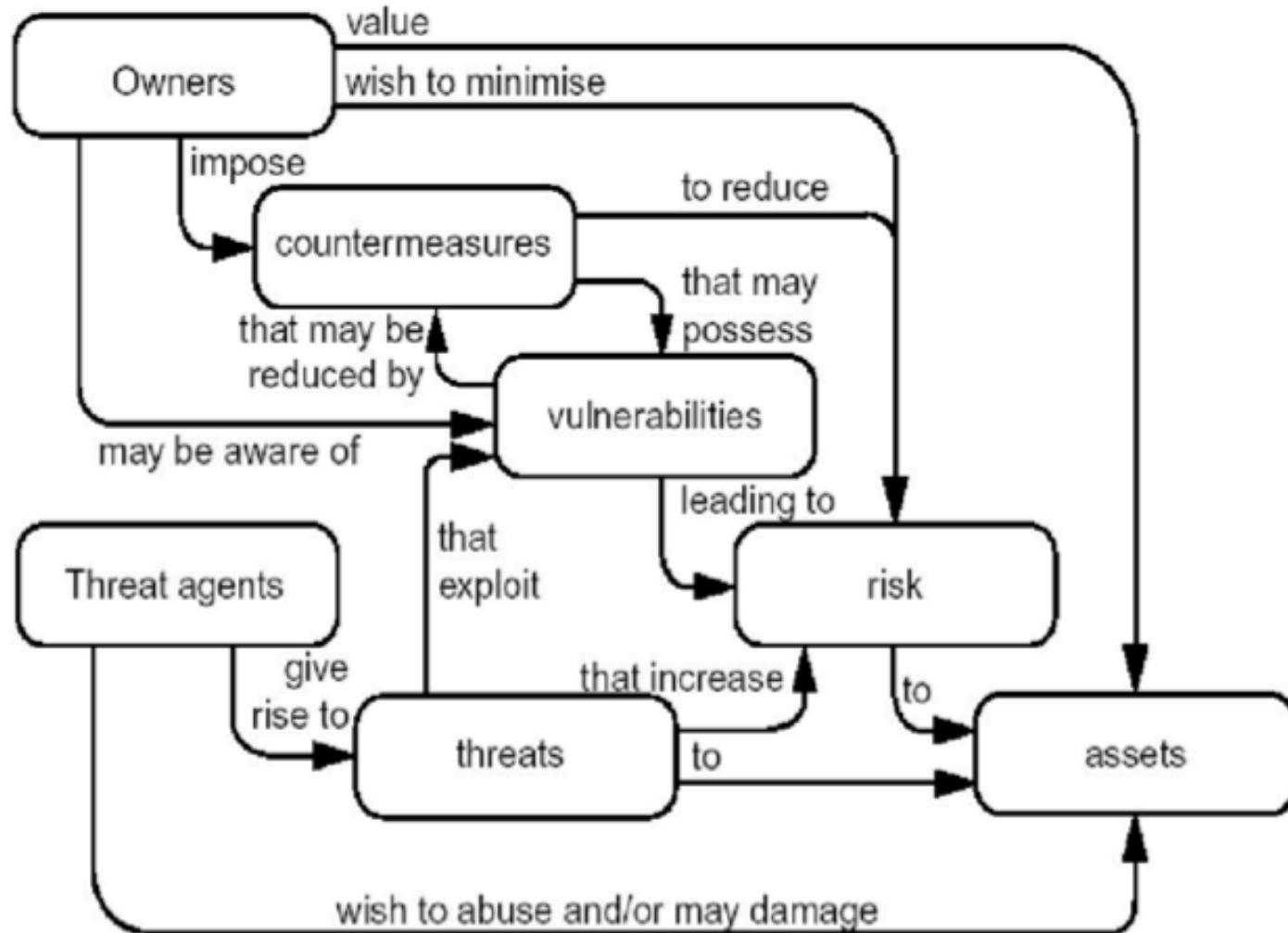


Tools, Interoperability, “Automated Everything”





What is security risk ? (ISO 15408)





Existing Threat and Risk Analysis methodologies

- ISO/IEC 13335
- ISO/IEC 15408
- ISO/IEC 15443
- ISO/IEC 27001
- CRAMM (UK)
- EBIOS (France)
- Mehari (France)
- Magerit (Spain)
- HTA (Canada)
- NIST SP-800-30 (US)
- Octave (SEI CMU)
- RiskAn (Czech Rep)
- Microsoft Threat Analysis Methodology
- Open Group FAIR
- & others

Challenges:

- 1) no interoperability;
- 2) few approaches deal with discernable concepts
- 3) few approaches are systematic enough to provide assurance



Failing to understand ALL risks ...



JUSTIFIABLE RISK ASSURANCE = RISK MANAGEMENT + ASSURANCE CASE

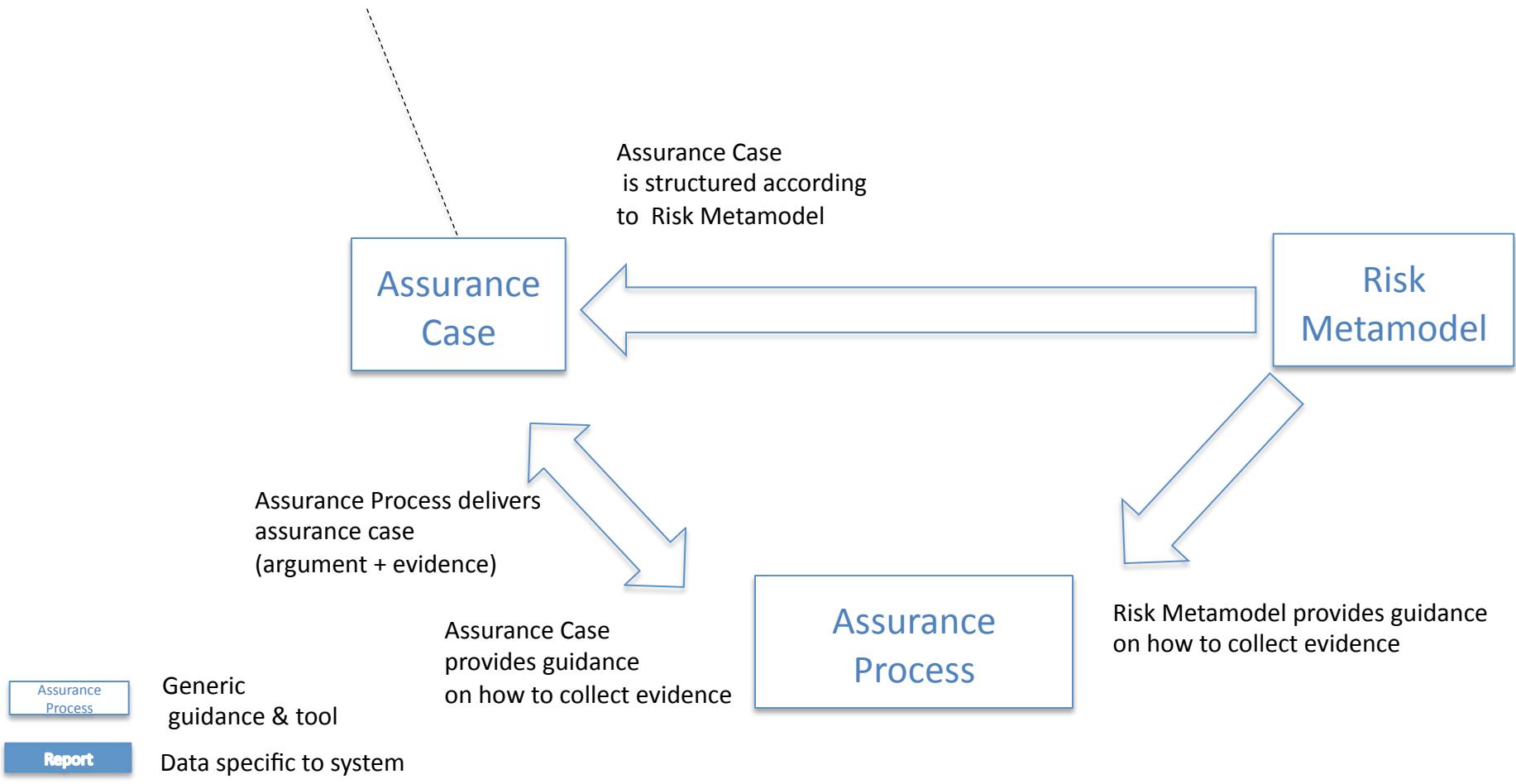
Brief first pass, more details later, time permitting





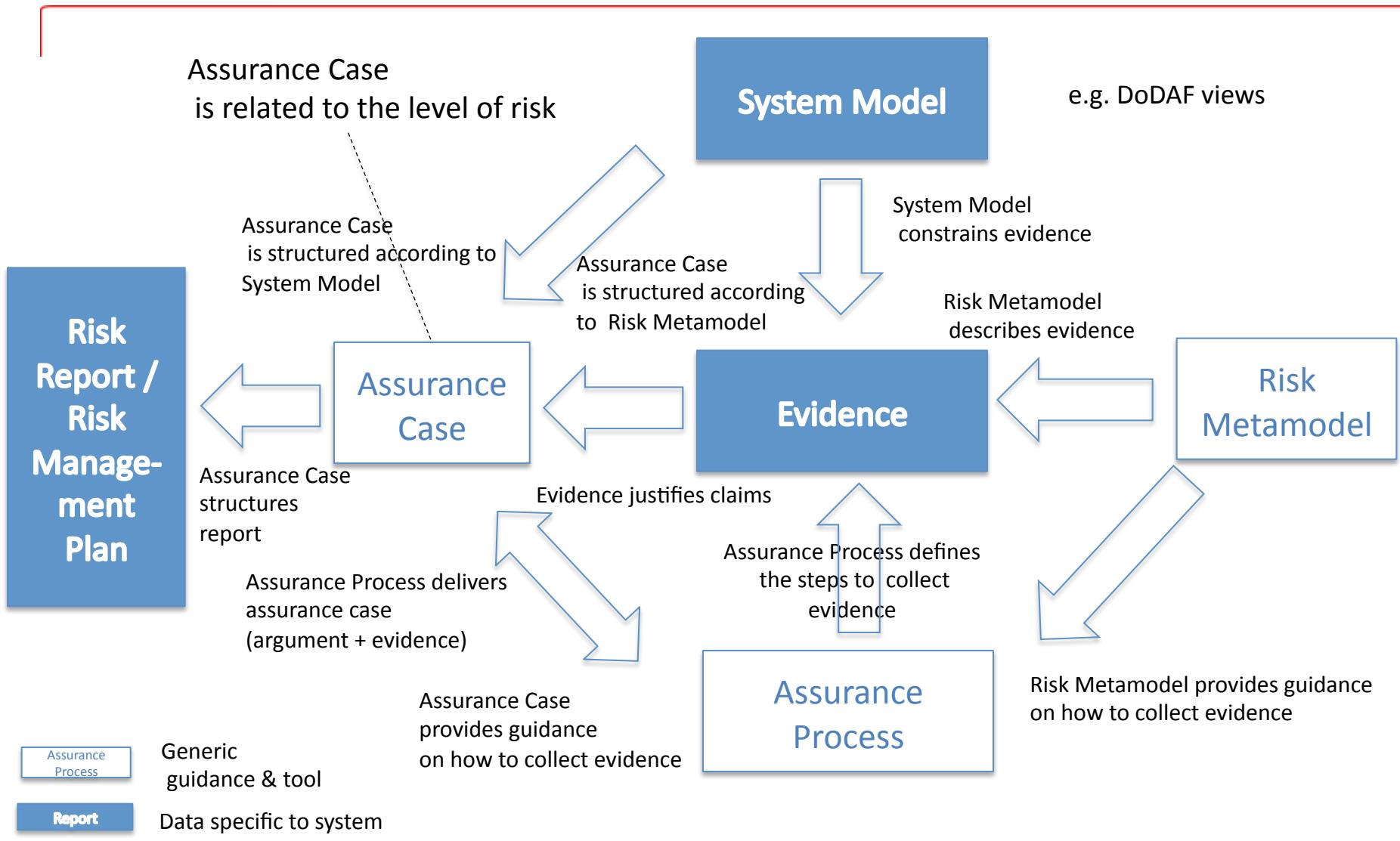
Justifiable Risk Assurance

Assurance Case
is related to the level of risk





Justifiable Risk Assurance





Our FORSA methodology

FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis

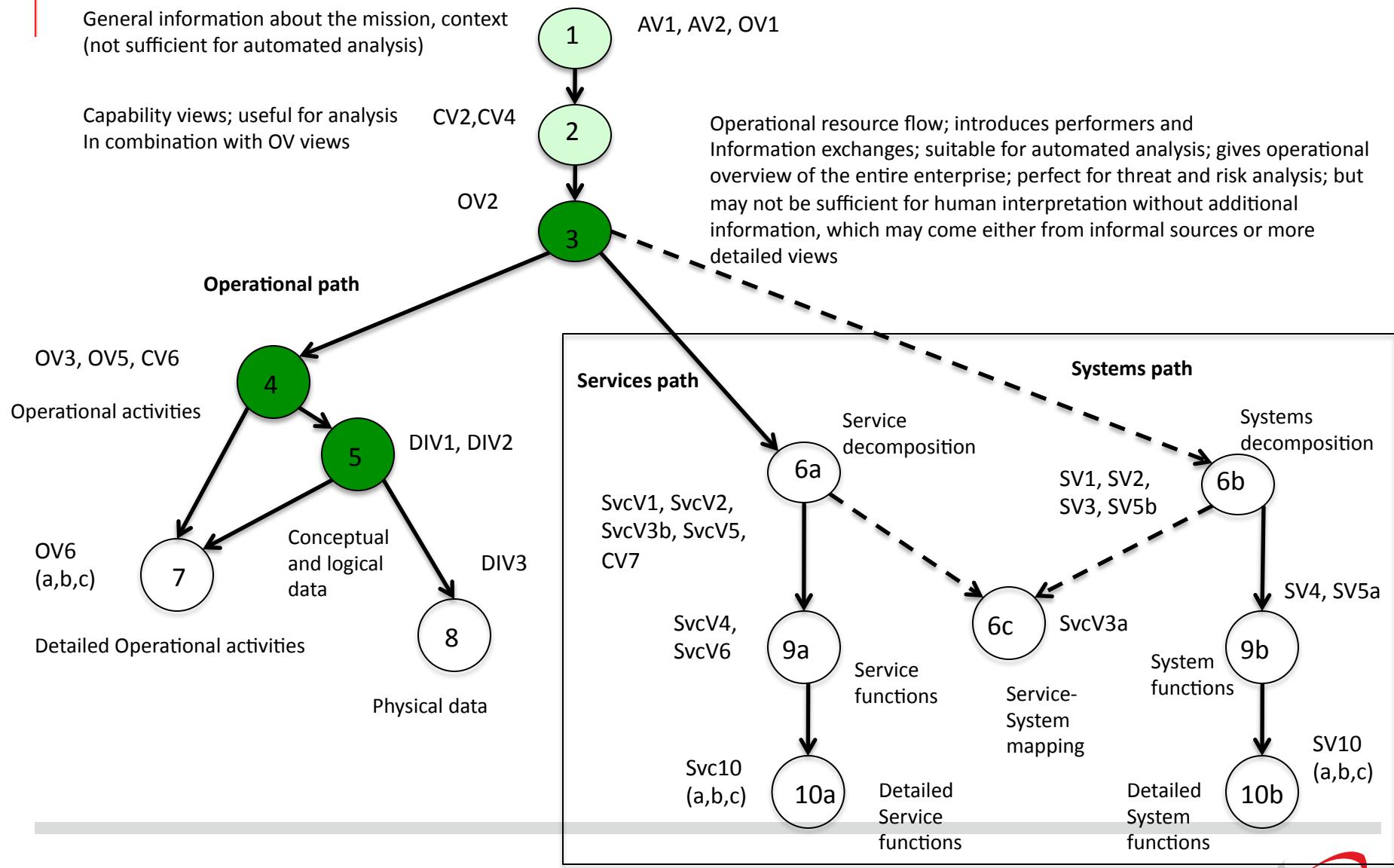
FORSA:

- Fact Oriented
- Repeatable
- Security
- Assessment

The sequence of steps is designed to increase *confidence*, and therefore increase *assurance*



Operational Risks and DODAF 2.0

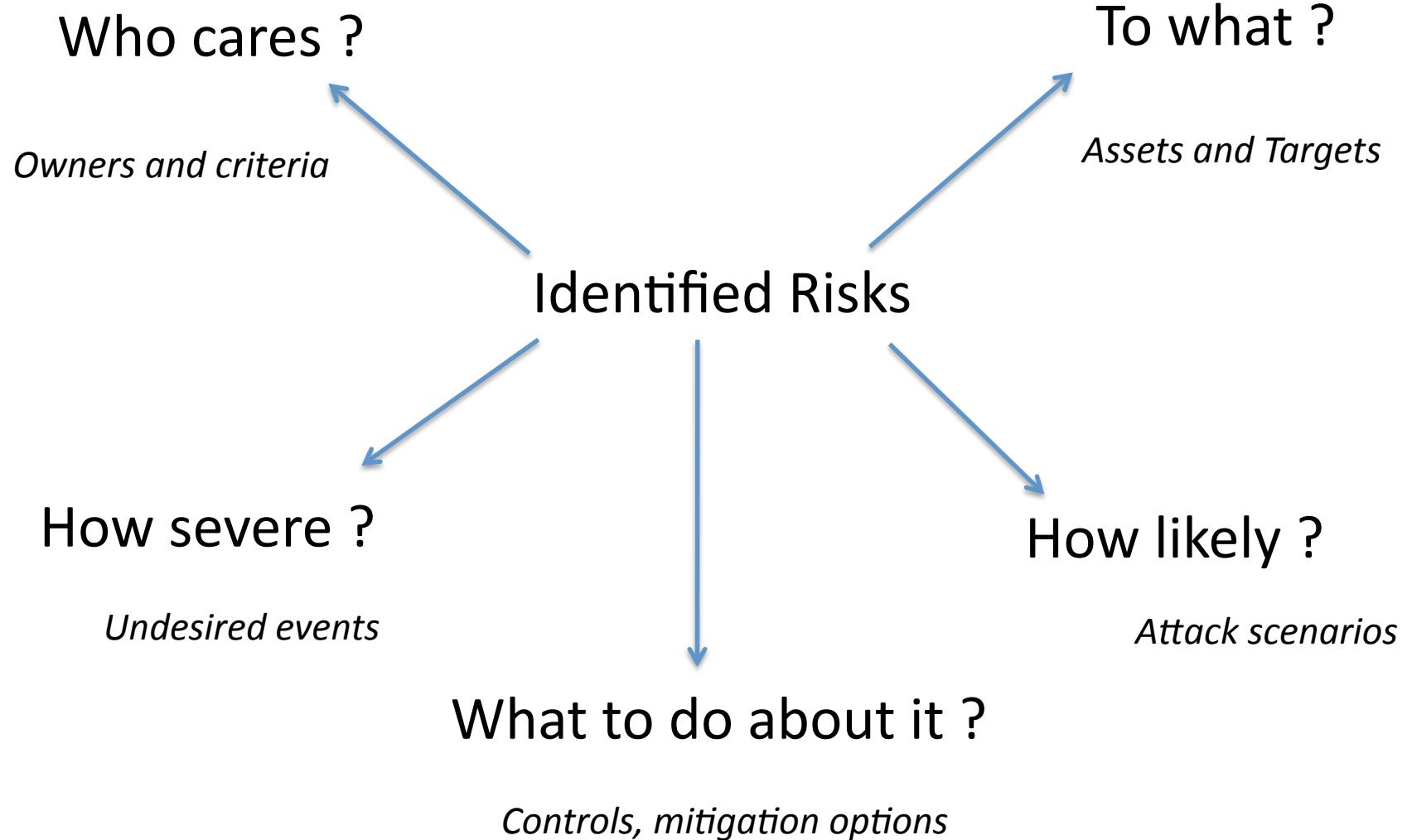


OVERVIEW OF THE RISK METAMODEL FOR JUSTIFIABLE RISK ASSURANCE



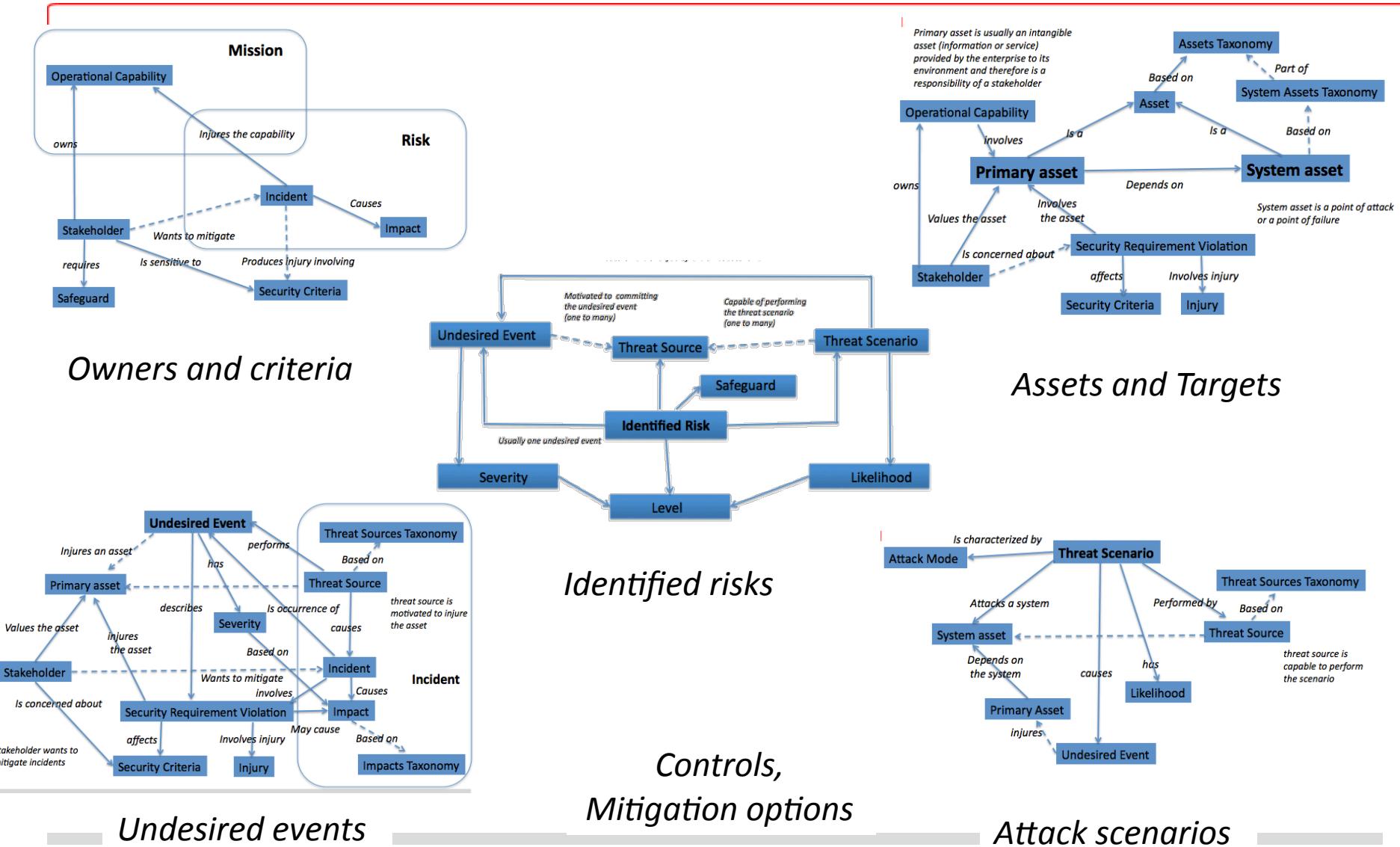


Overview of the Risk Metamodel





Overview of the Risk Metamodel



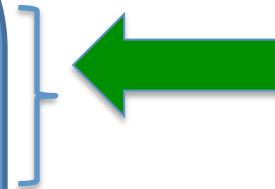
PART 1: THE OPERATIONAL CONTEXT





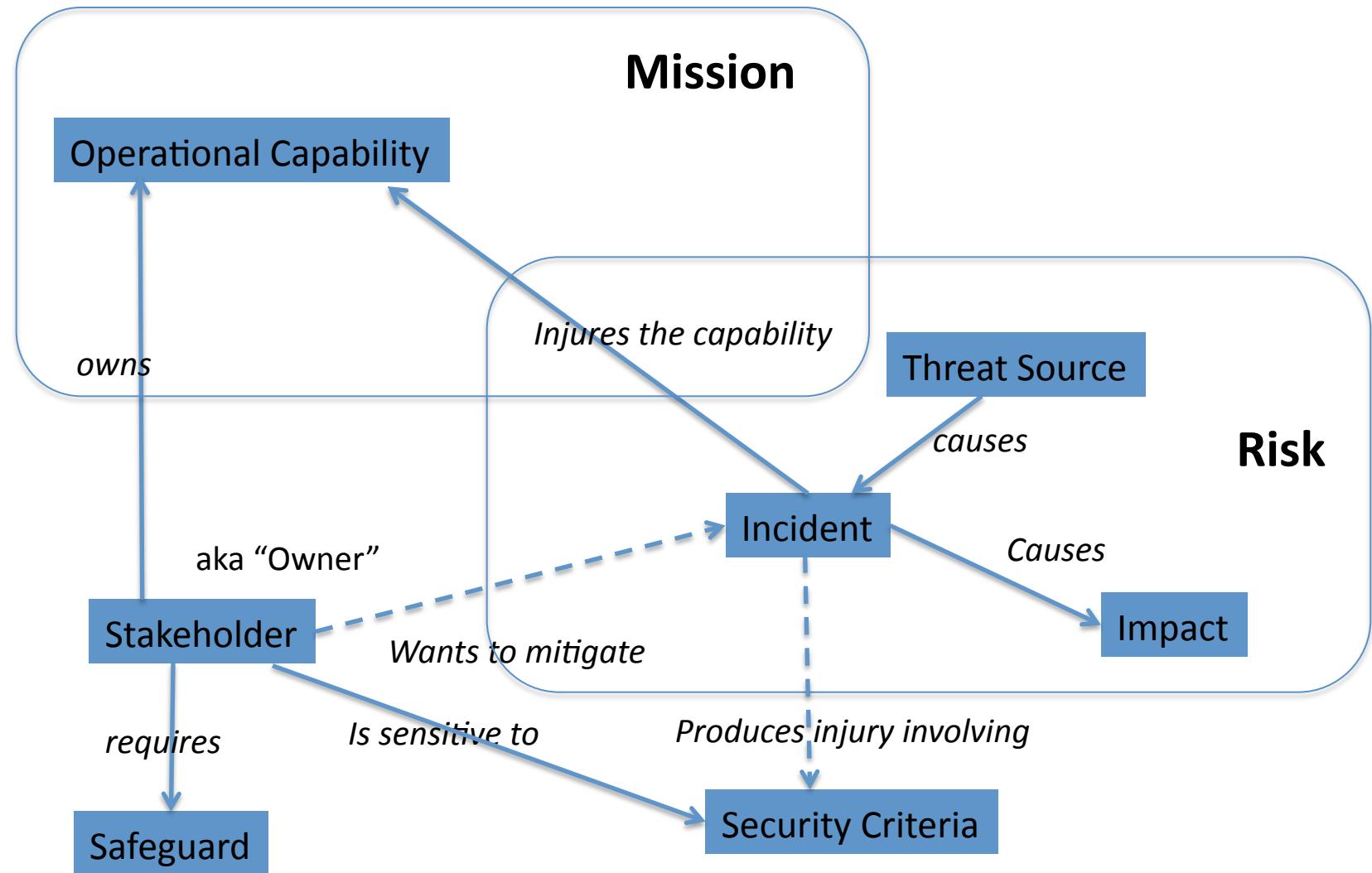
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis



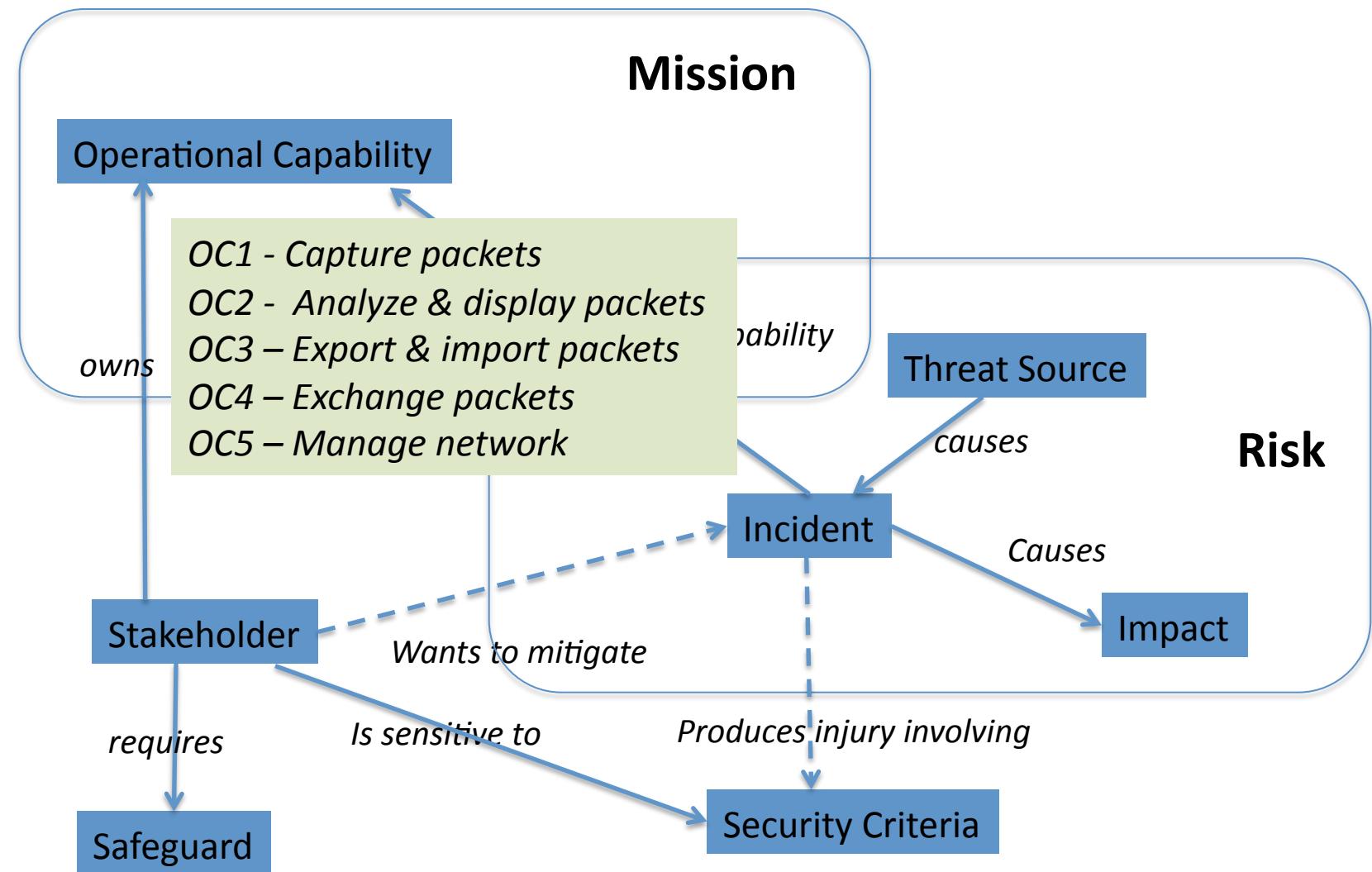


Analysis of the operational context is based on the following model



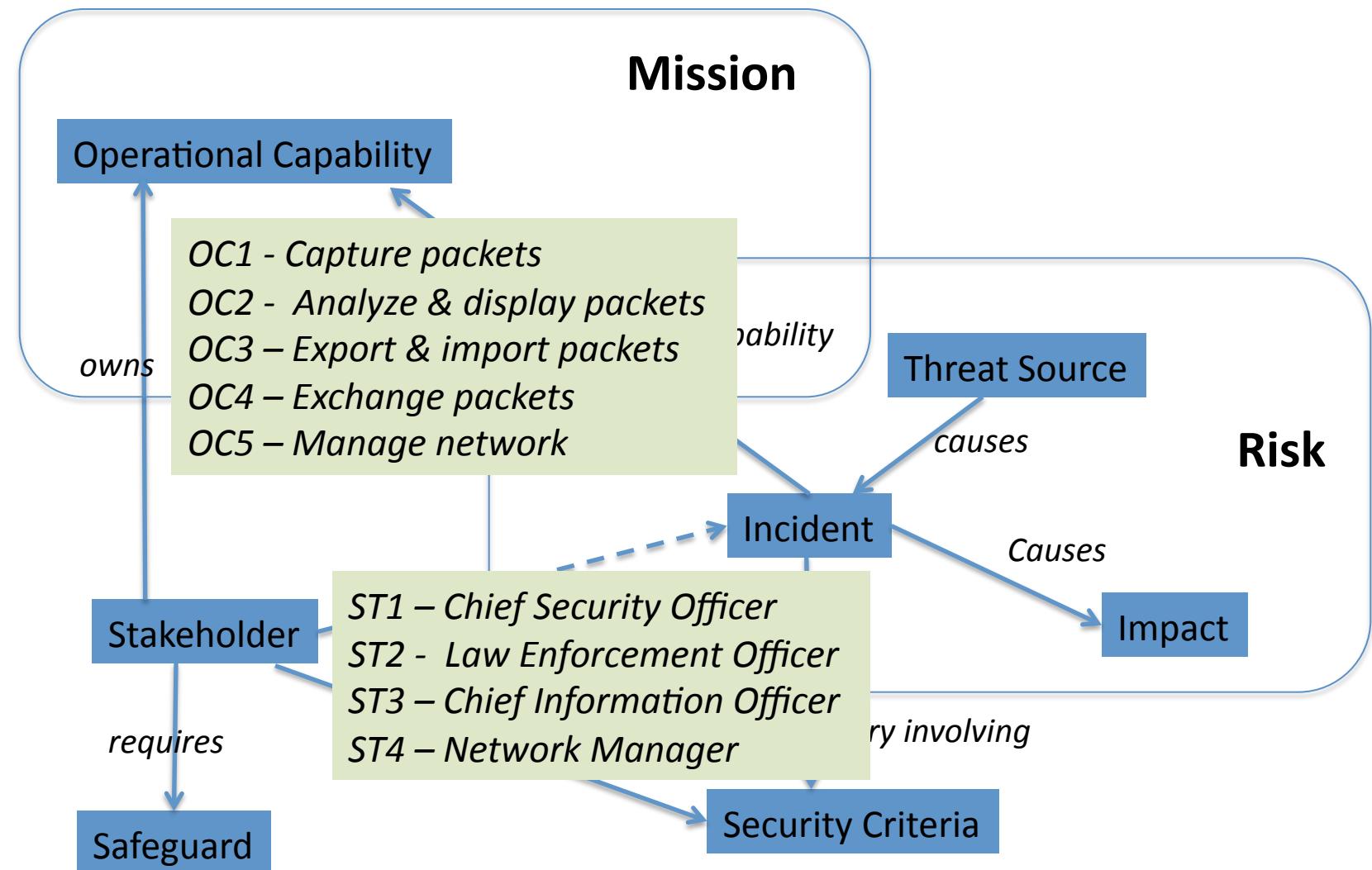


Analysis of the operational context is based on the following model



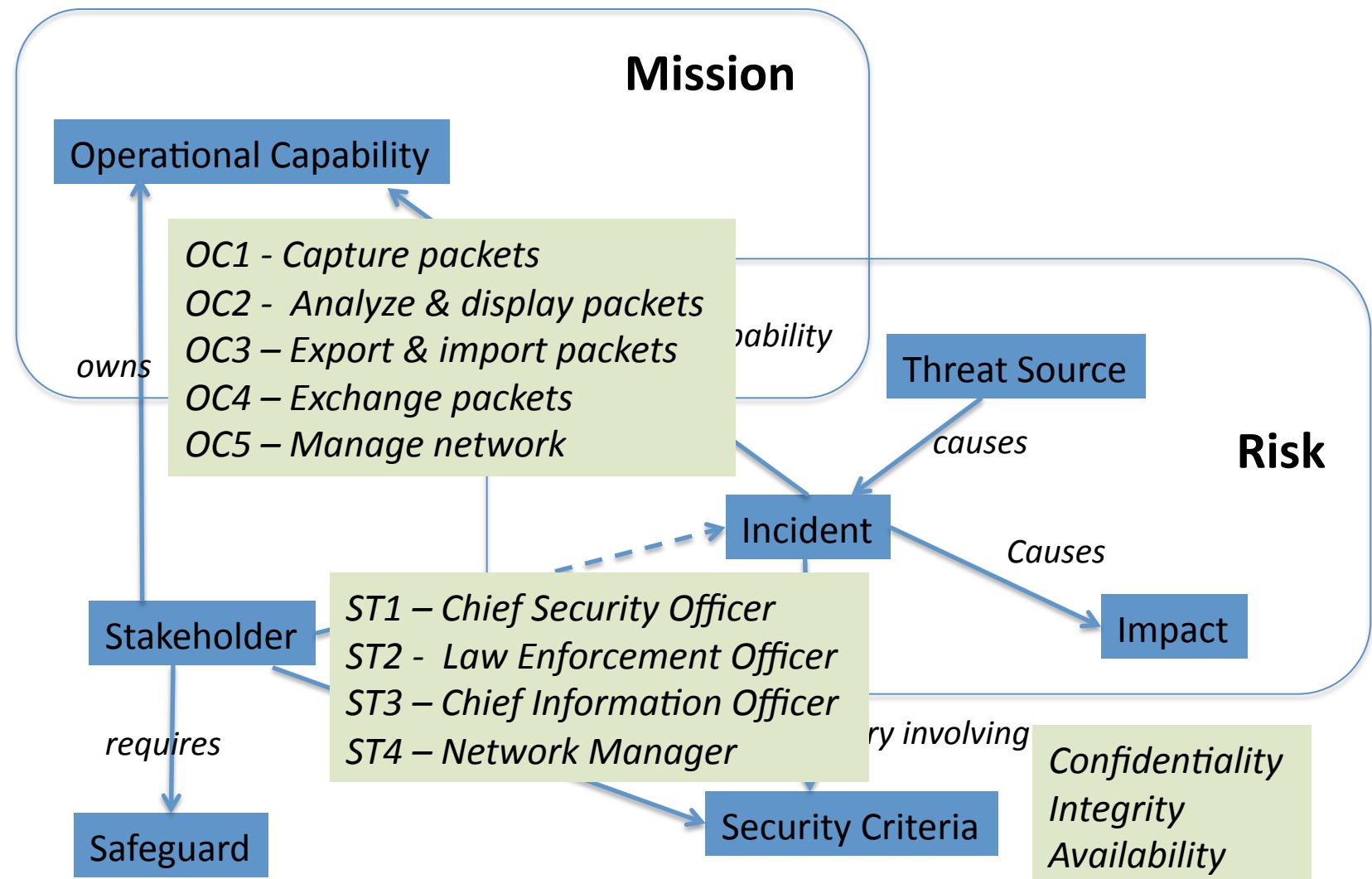


Analysis of the operational context is based on the following model



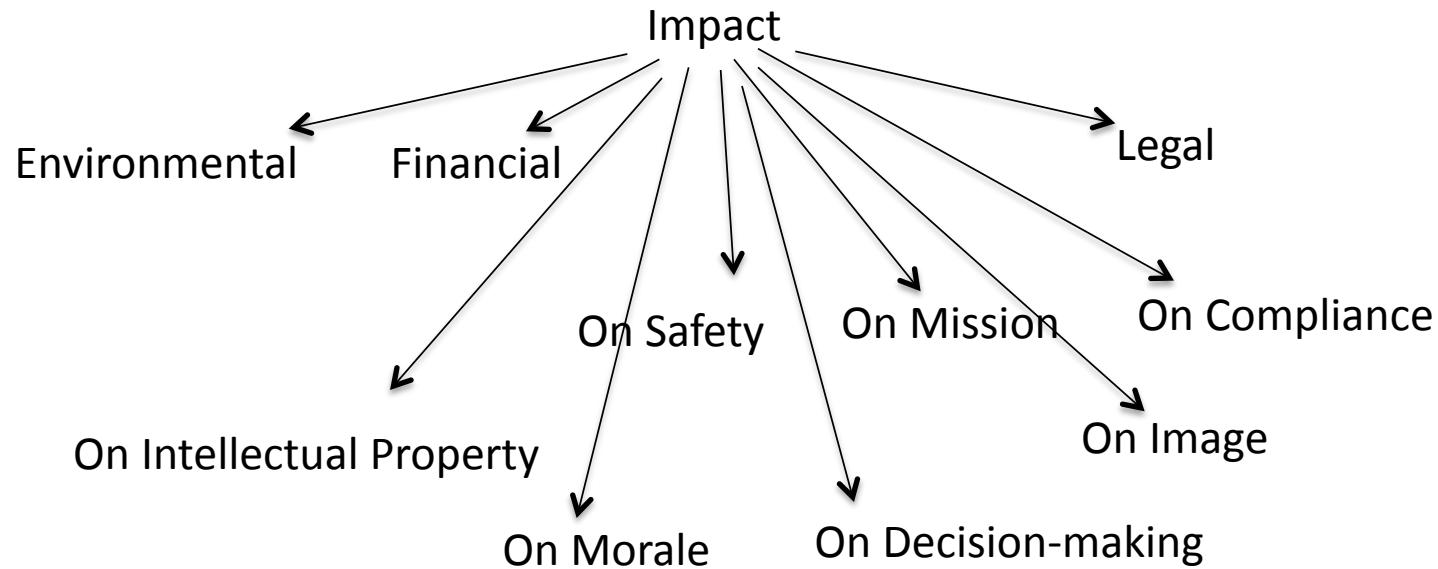


Analysis of the operational context is based on the following model





“Standard” Taxonomy of Impacts



Impacts are related to:

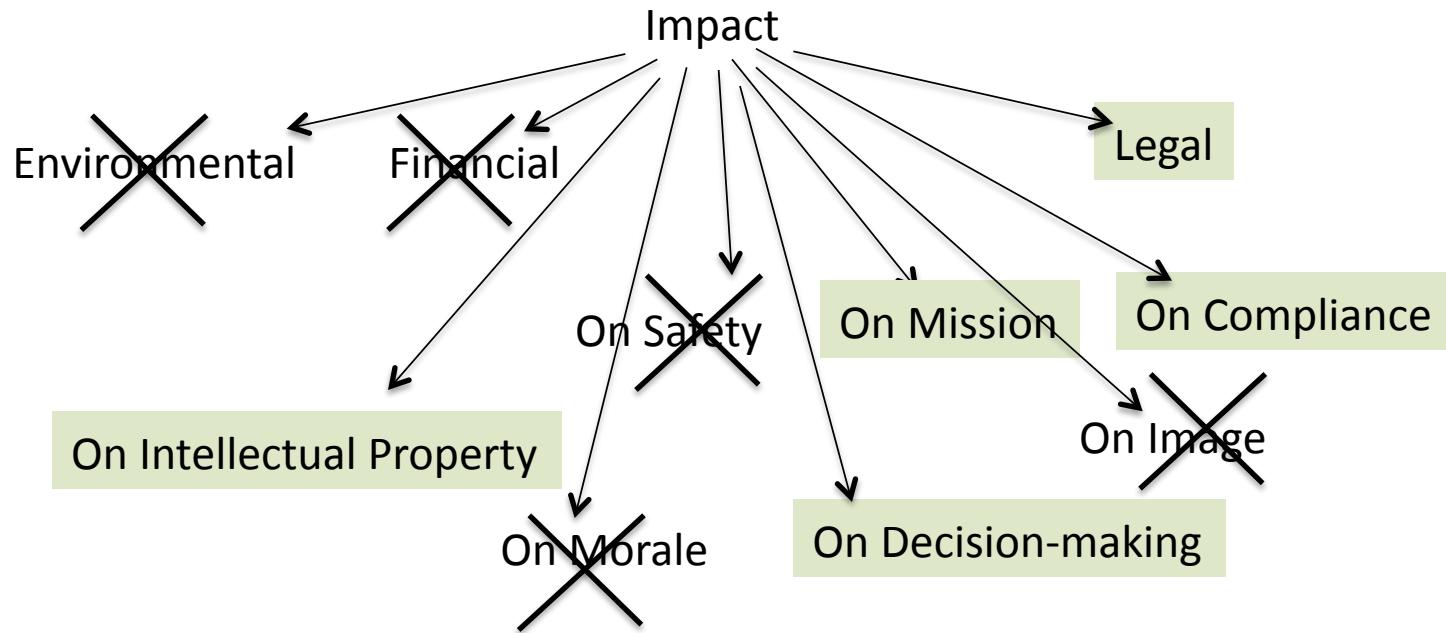
- Identification of the primary assets
- Injury and undesired events

Based on EBIOS and HTRA





Taxonomy of Impacts in scope



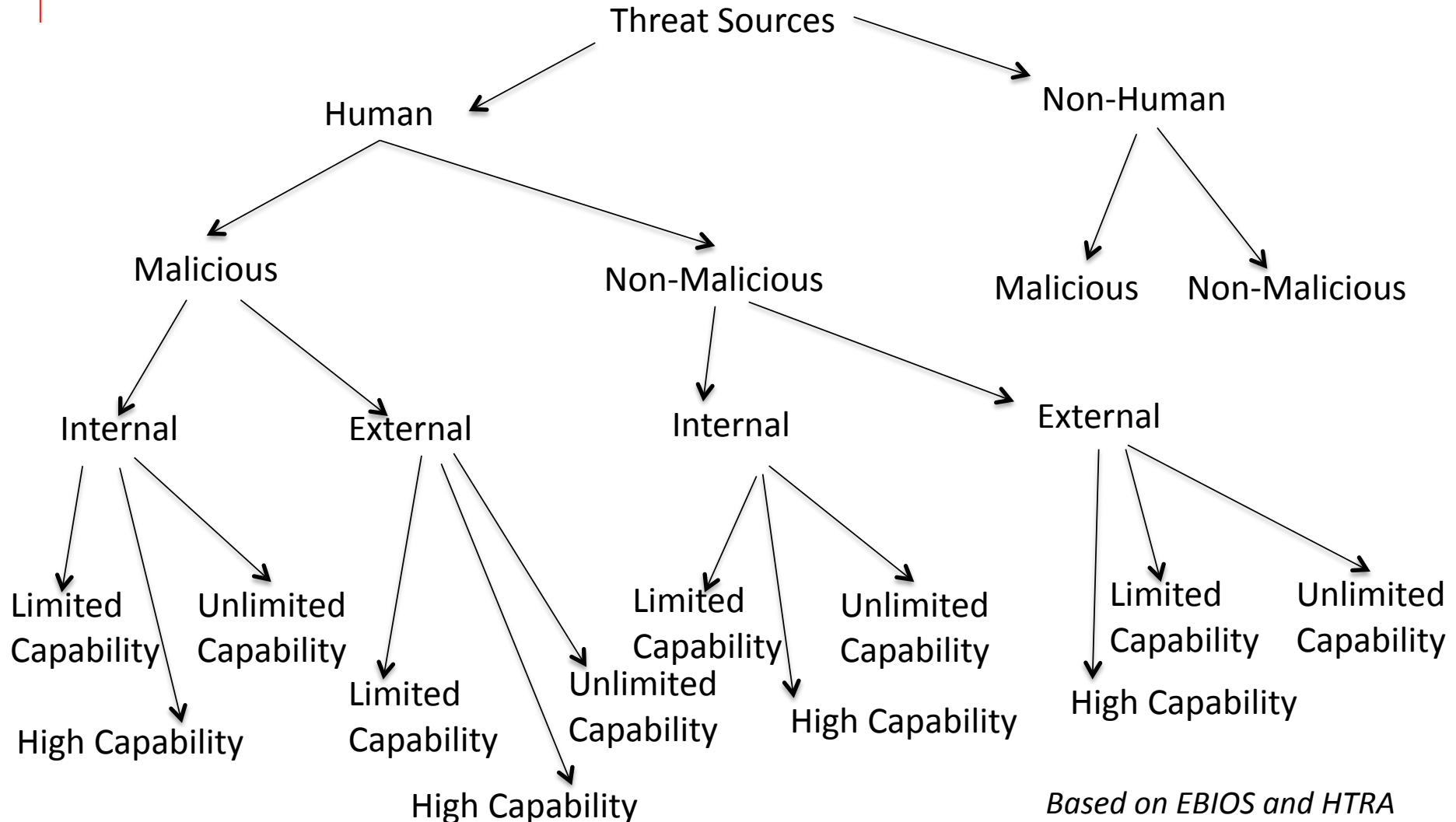
Impacts are related to:

- Identification of the primary assets
- Injury and undesired events



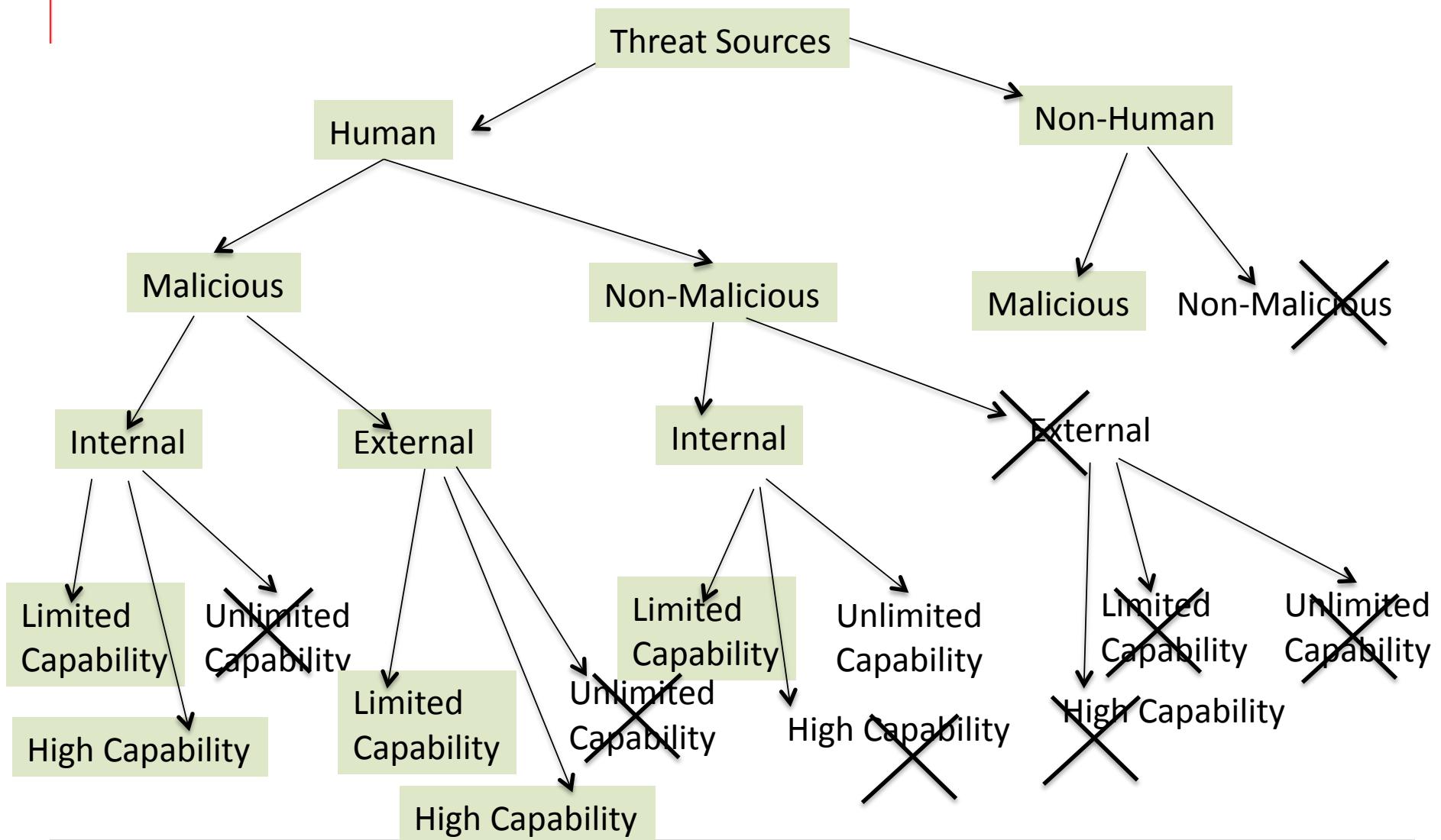


“Standard” Taxonomy of threat sources





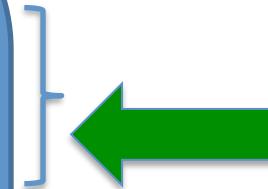
Taxonomy of threat sources in scope





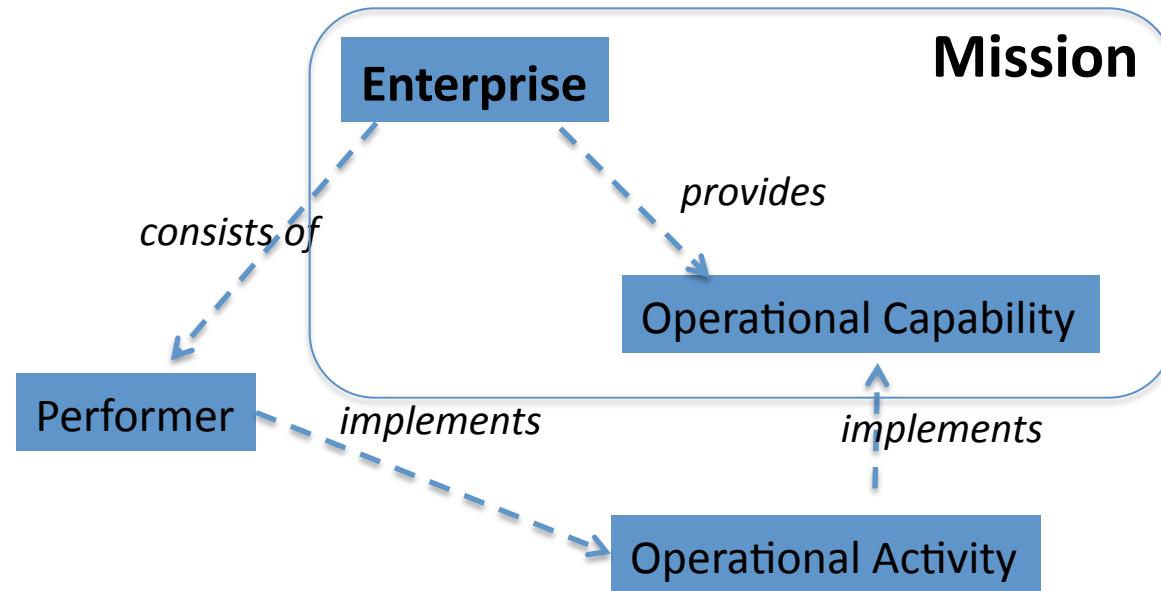
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Threat Scenario Identification
6. Threat Scenario Analysis
7. Risk Identification
8. Safeguard Identification
9. Vulnerability Analysis
10. Risk Analysis



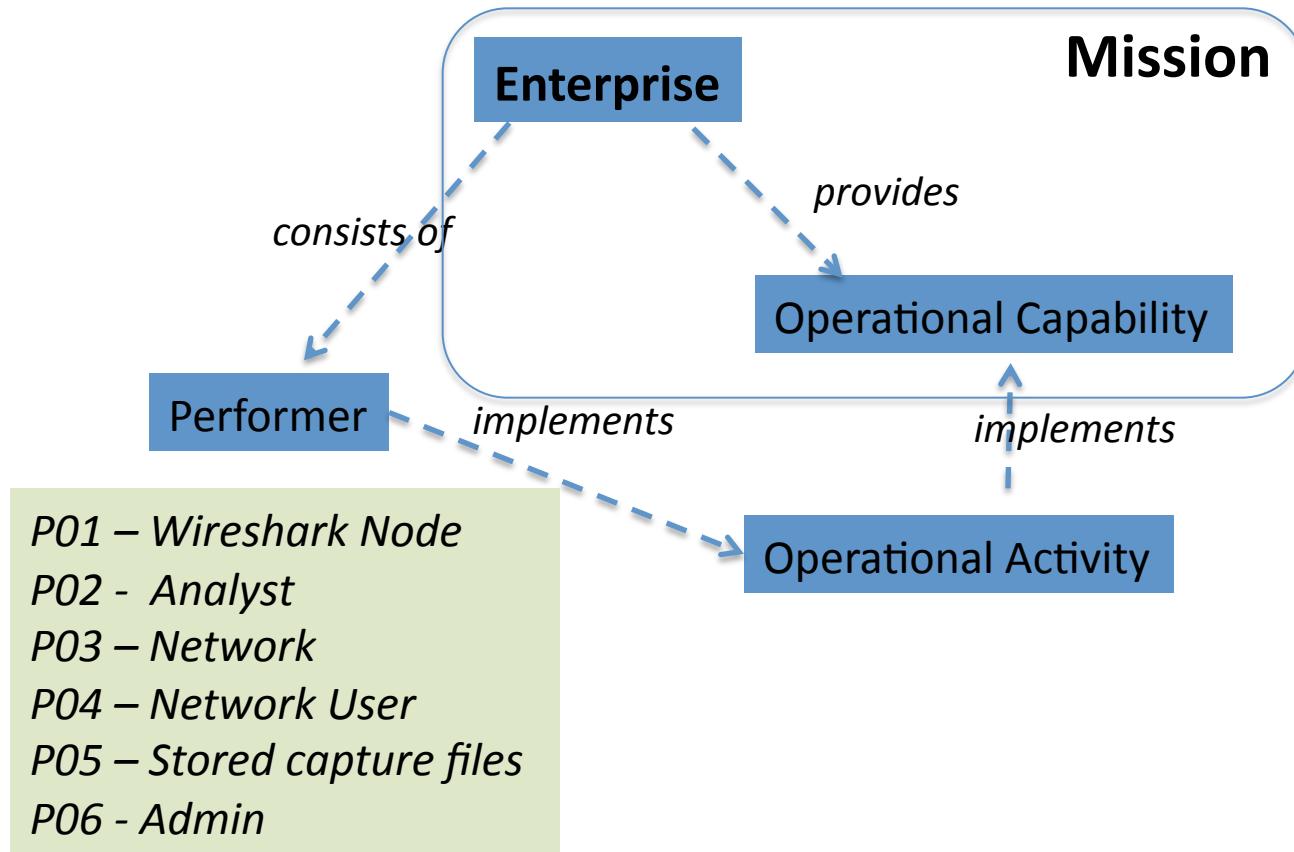


Analysis of System Facts is aligned with Business Models



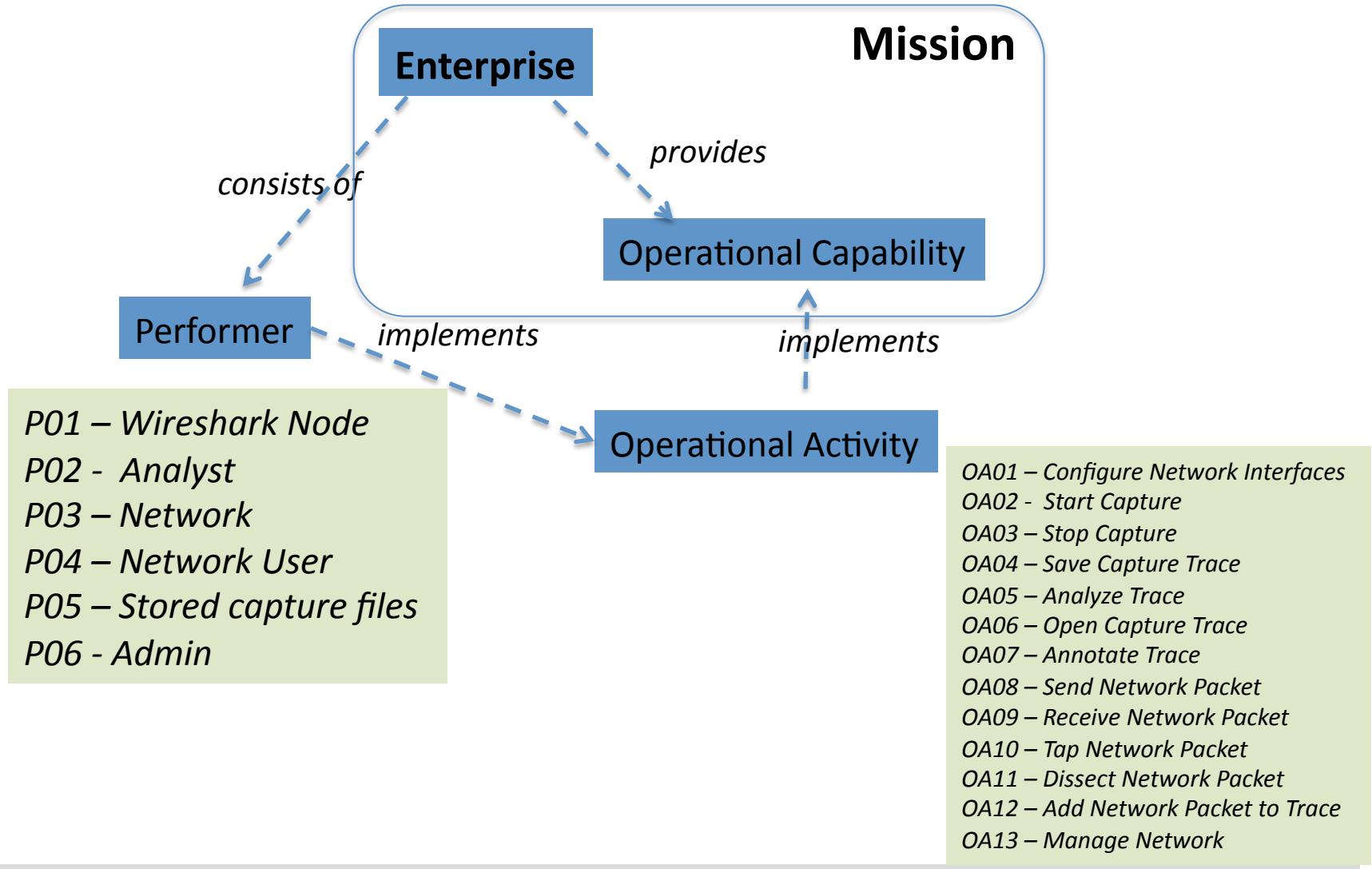


Analysis of System Facts is aligned with Business Models





Analysis of System Facts is aligned with Business Models



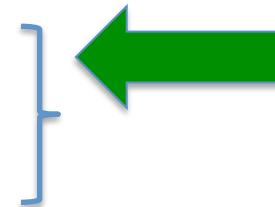
PART 2: THE EFFECT ANALYSIS





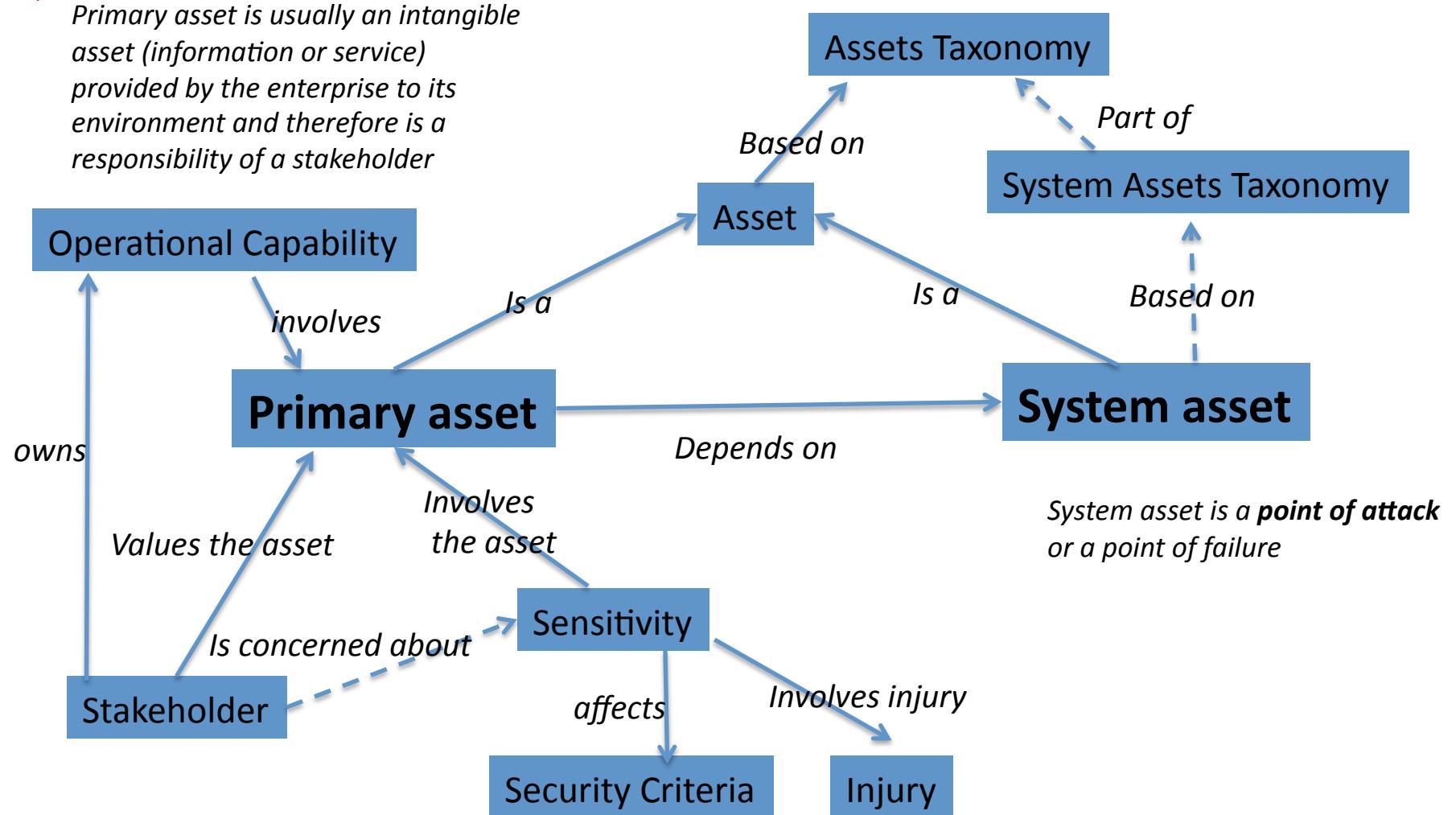
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis



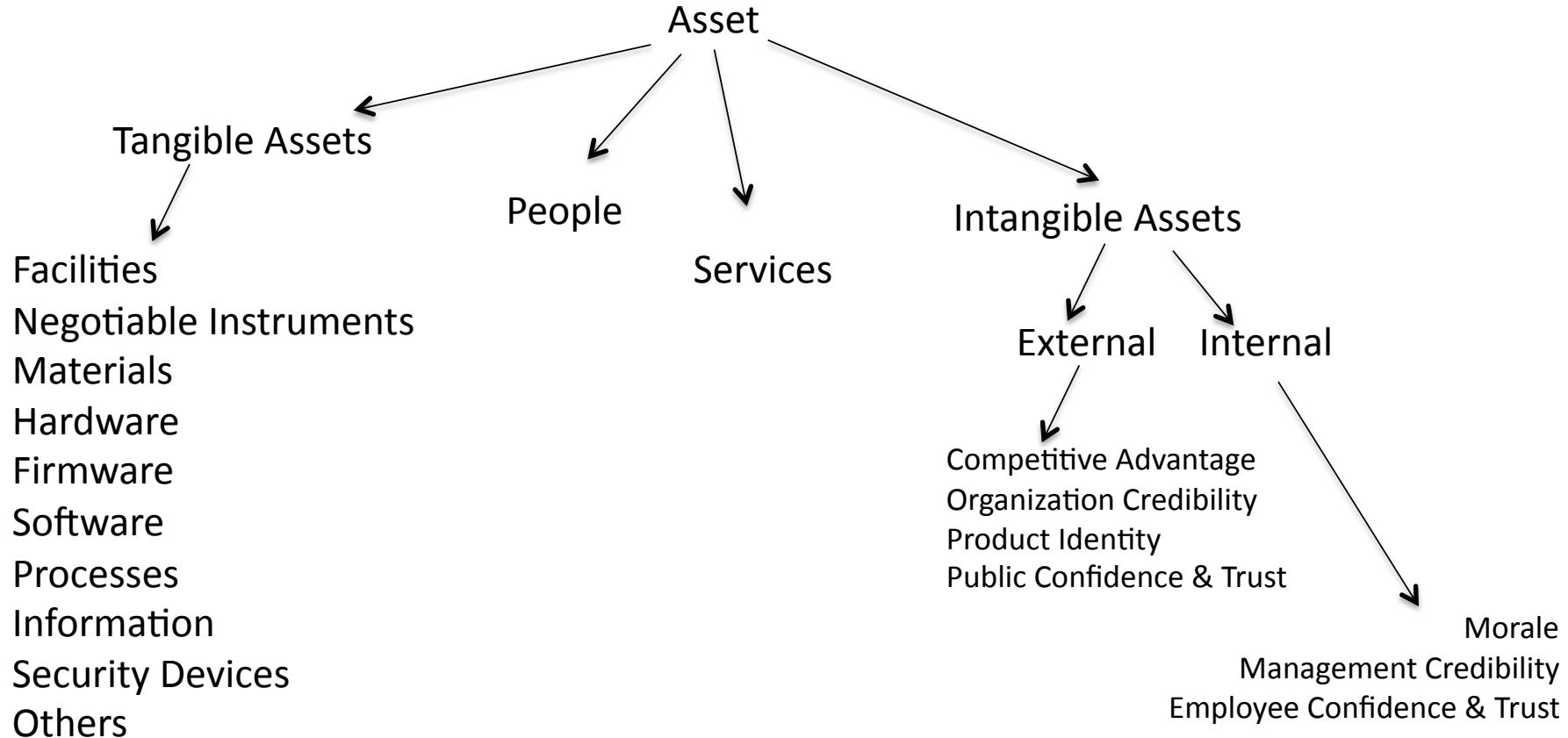


Analysis of Assets is based on the following model





Taxonomy of Assets

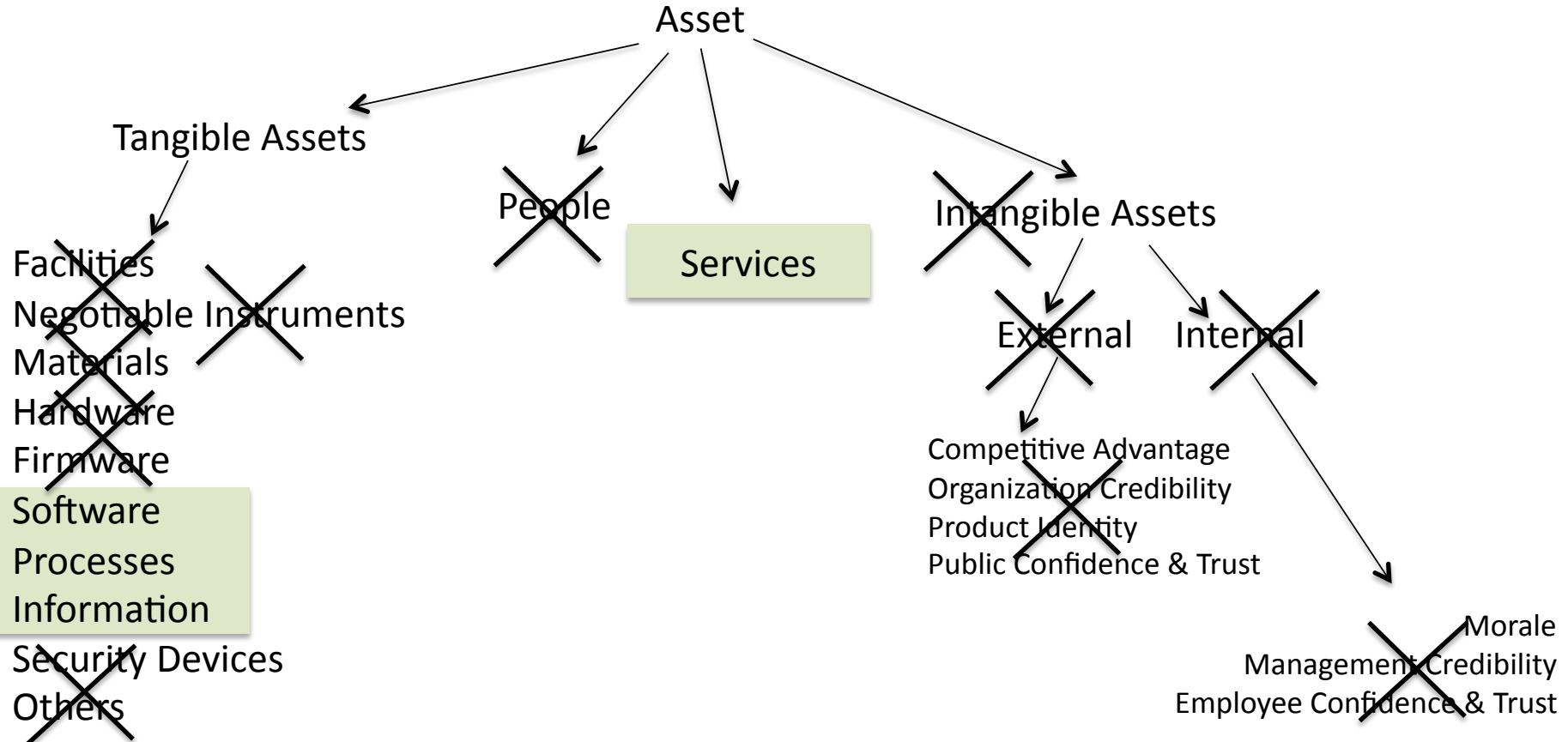


Based on HTRA



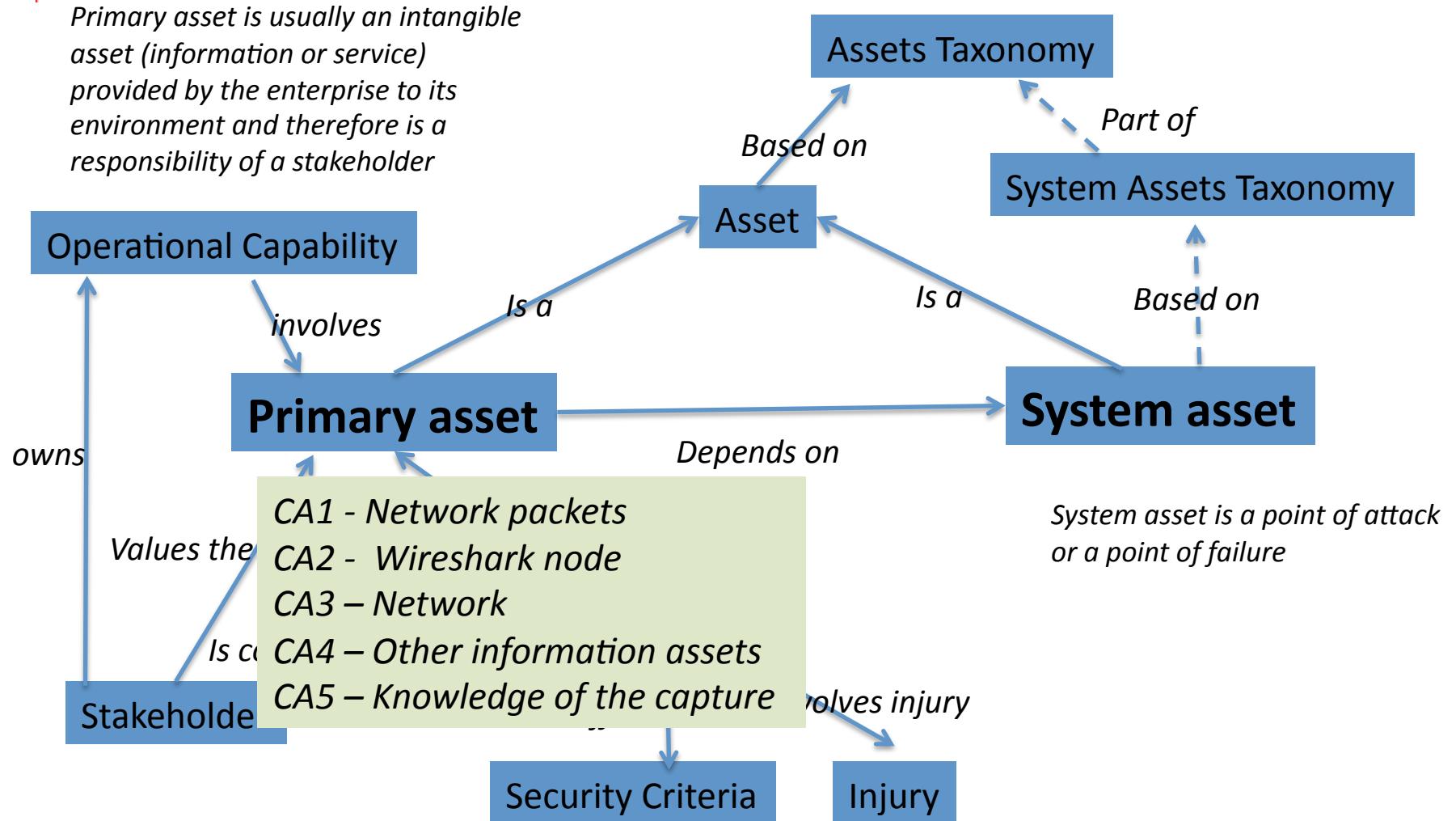


Taxonomy of Assets in scope



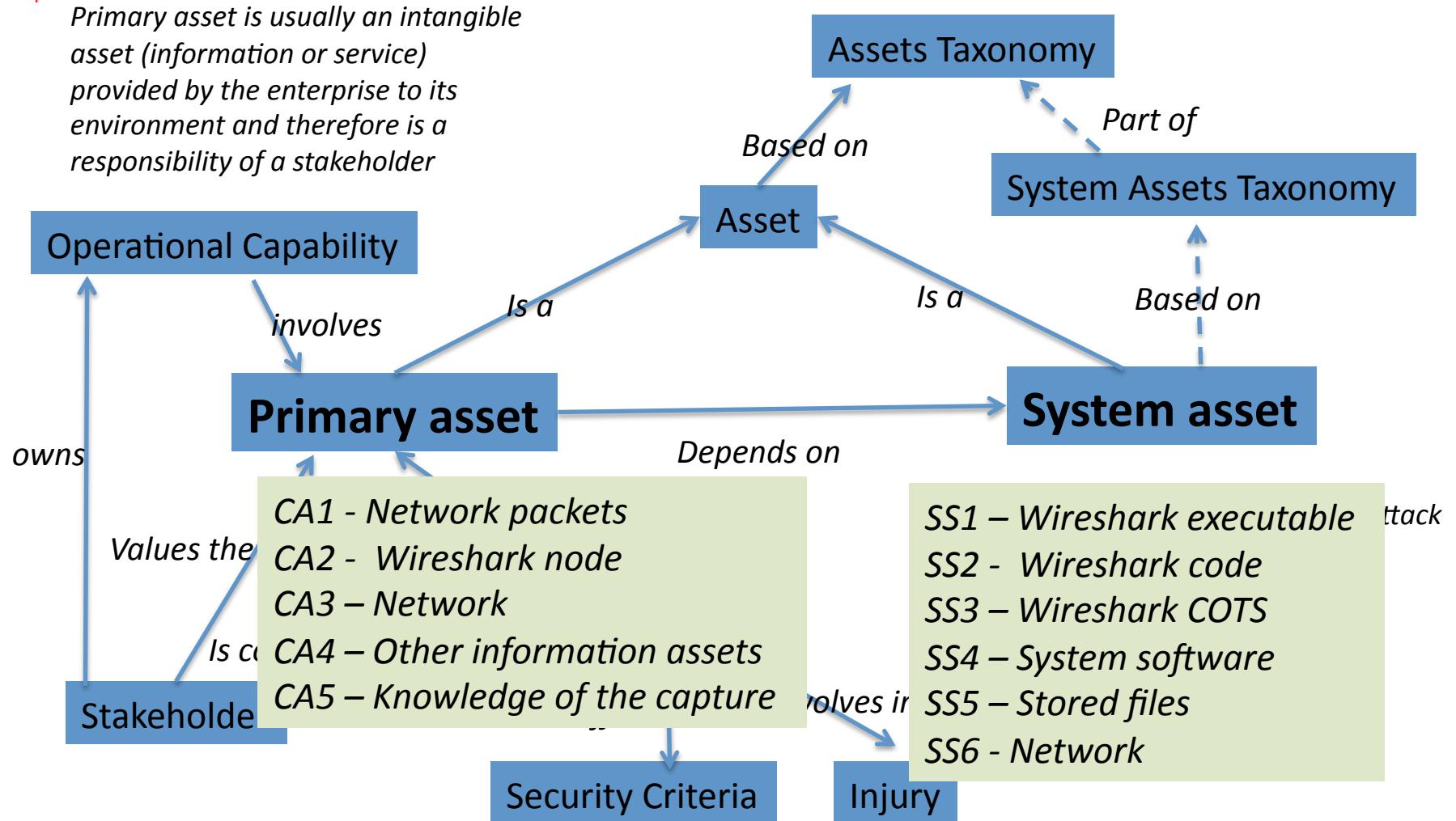


Analysis of Assets is based on the following model





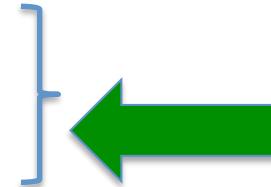
Analysis of Assets is based on the following model





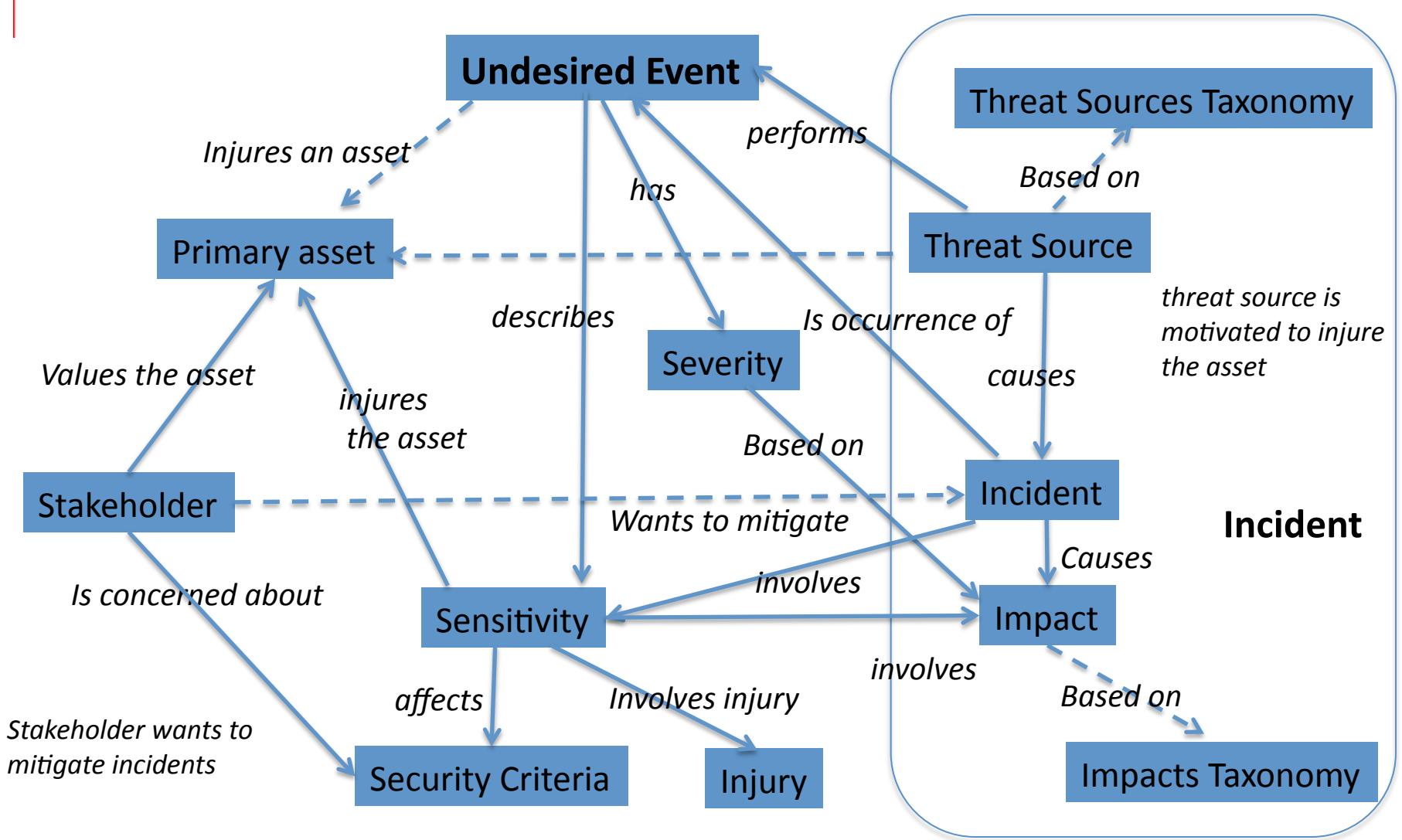
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis



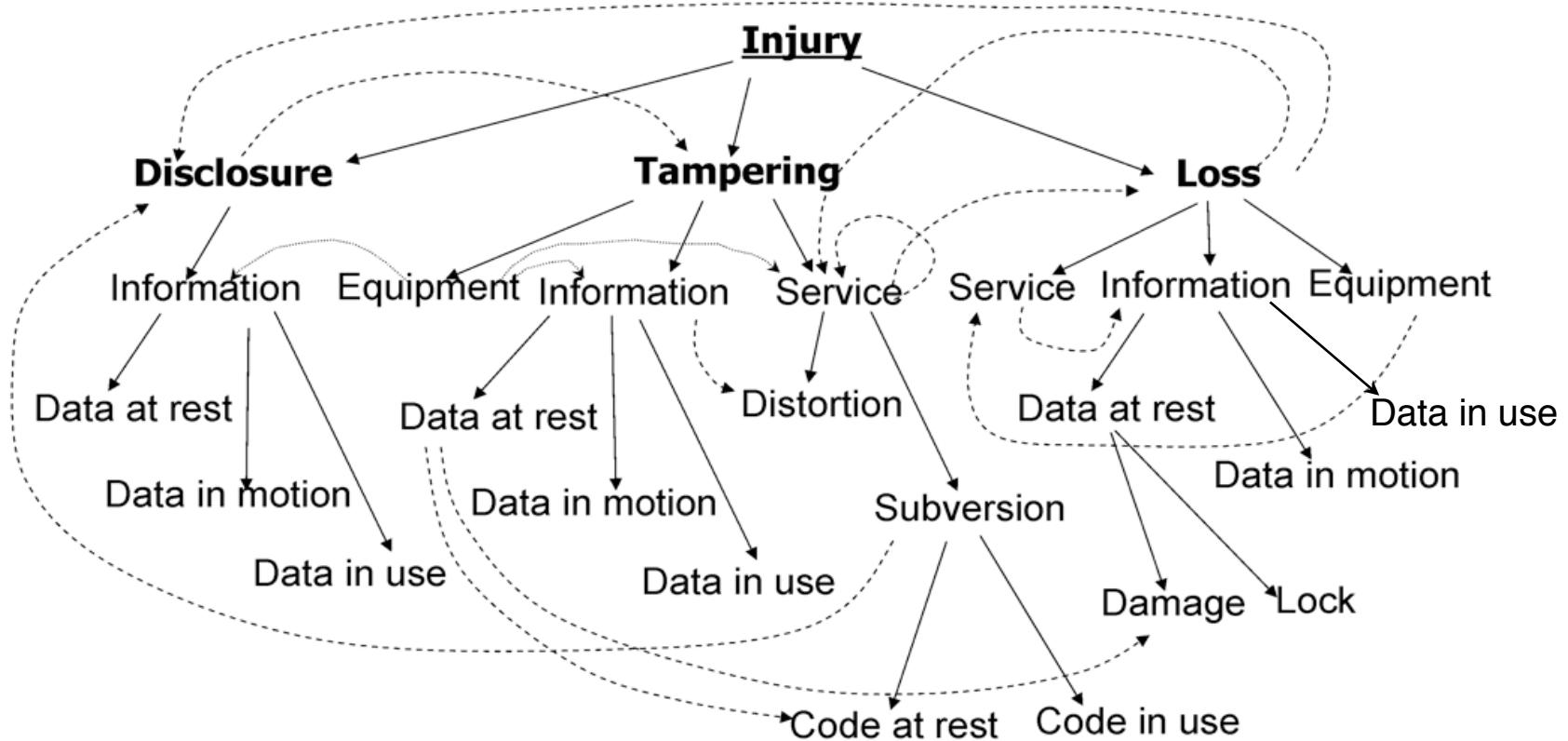


Analysis of Undesired Events is based on the following model



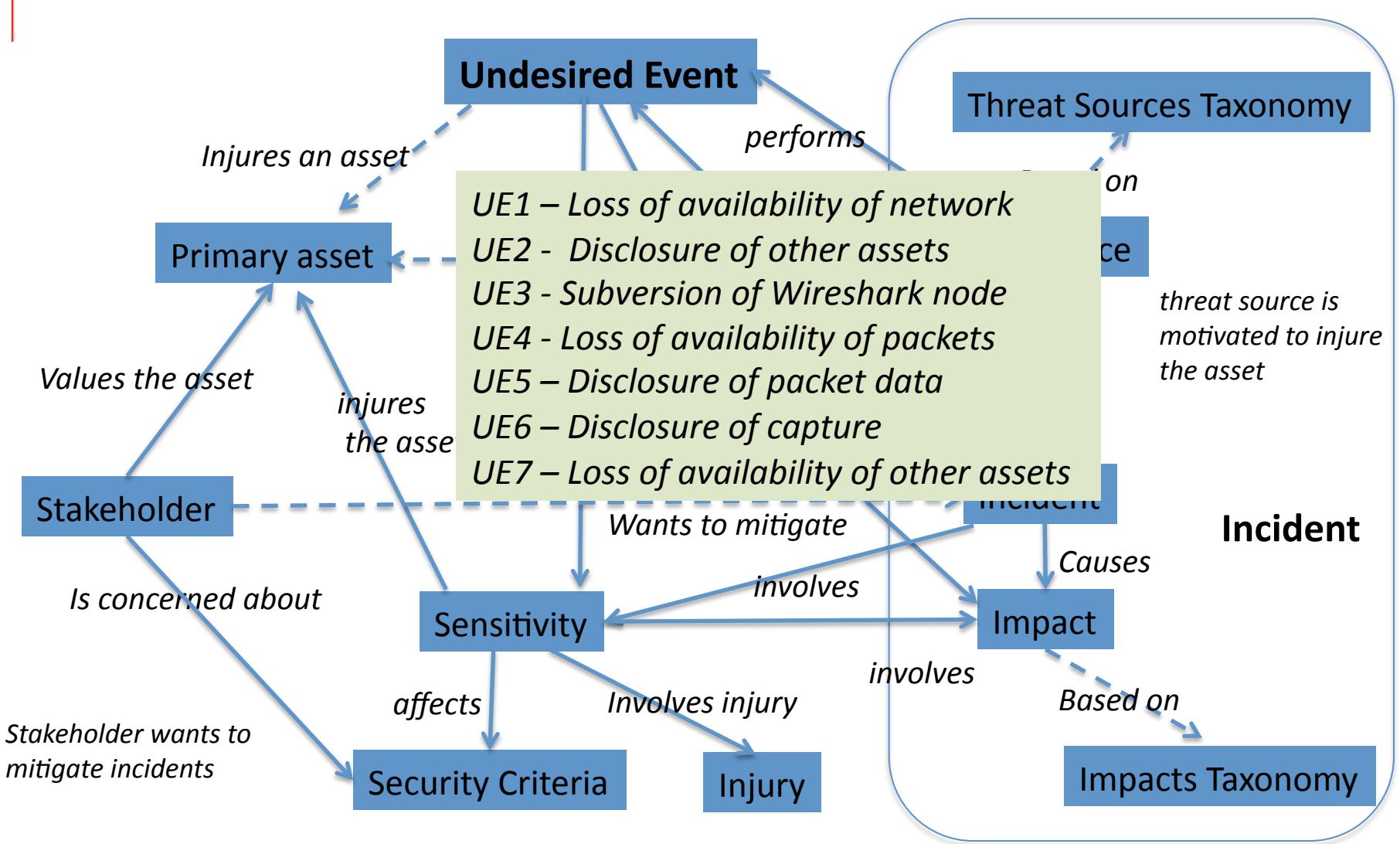


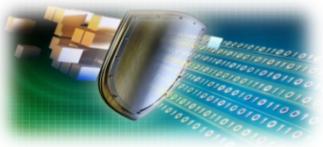
Taxonomy of injuries for cyber security





Analysis of Undesired Events is based on the following model





FORSA: *The Effect analysis*

FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis

} Mostly import (if possible) or interviews

+ validation & verification }

+ validation & verification }

At this point we can justify that we understand ALL classes of Undesired Events that can occur, and justify their severity



PART 3: THE CAUSE ANALYSIS

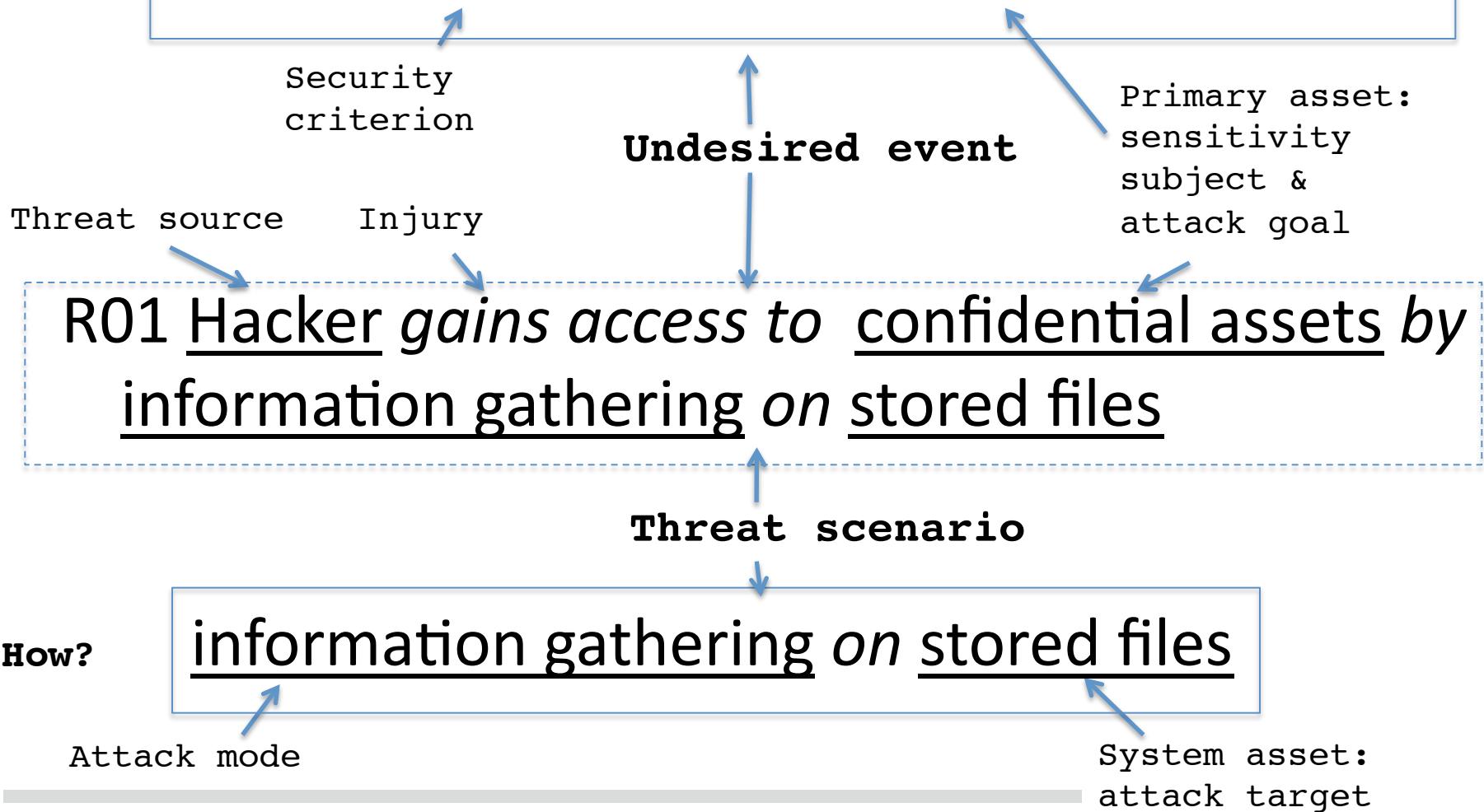




Cause and effect in a risk statement

what?

Loss of confidentiality of confidential assets

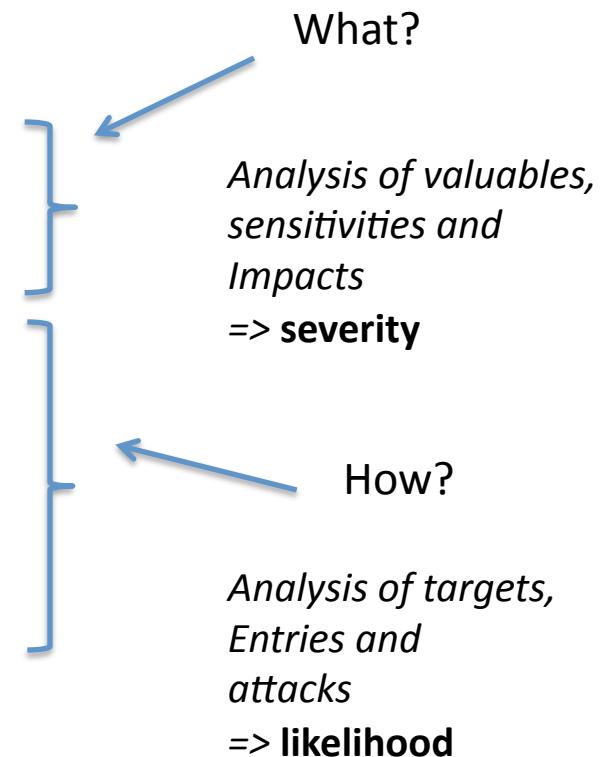




The corresponding FORSA steps

FORSA STEPS

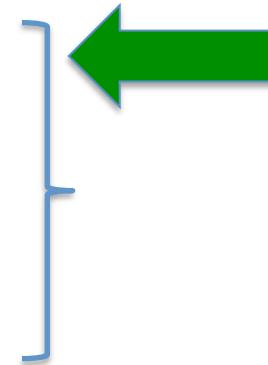
1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis





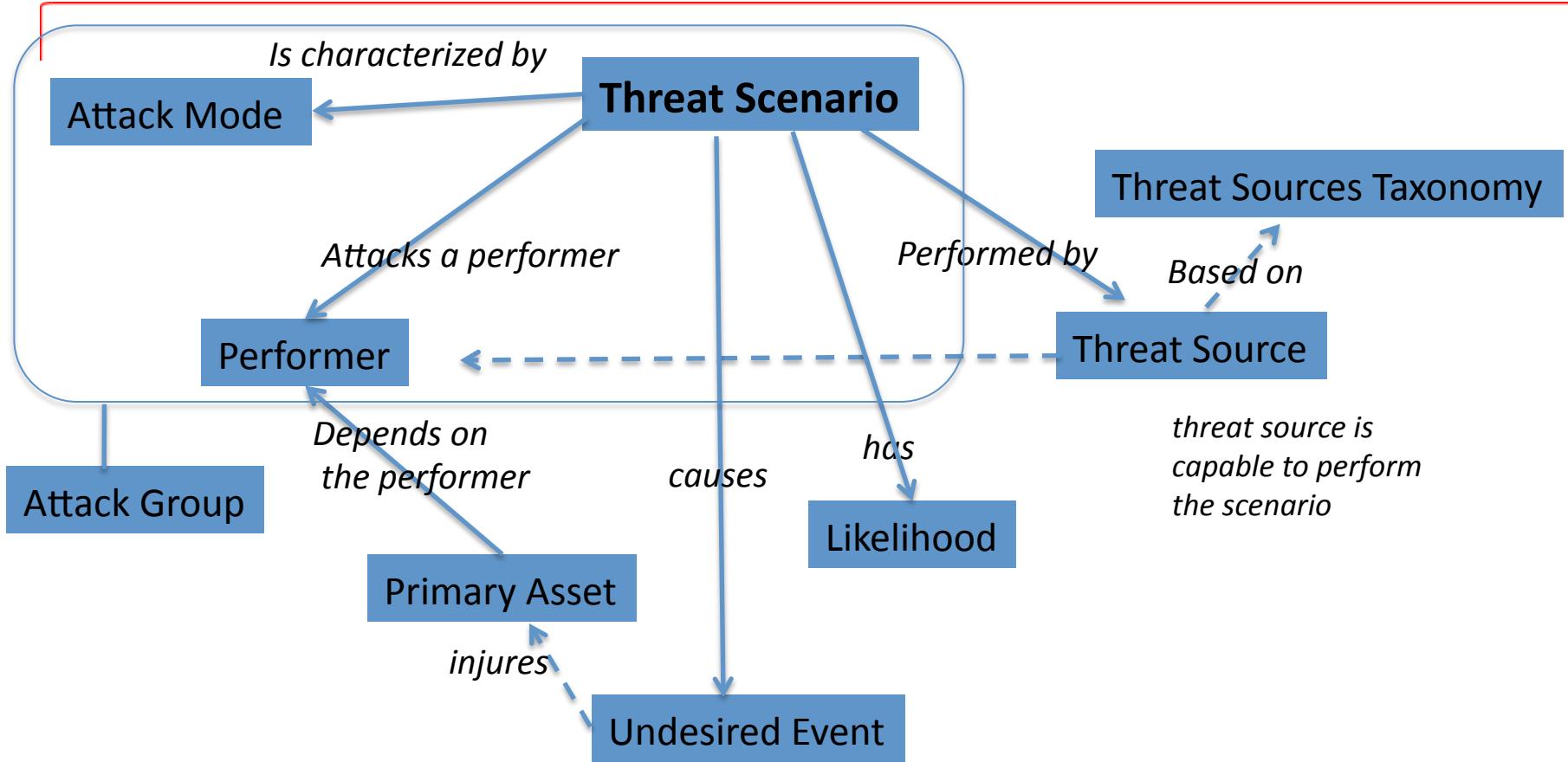
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis





Analysis of Attack Groups is based on the following model



Attack Group considers a single entry point; This is a class of attacks

Threat Scenarios within the Attack Group describe various multi-stage attacks;
In a simple case Attack Group involves a single Threat Scenario





Attack Groups

Attack Groups

Attack modes

- Abuse
- Exceeding capacity
- Damage
- Loss
- Modification
- Information Gathering

- Abuse of Wireshark node
- Damage to the Wireshark node
- Exceeding capacity of the Wireshark Node
- Modification of the Wireshark Code
- Information Gathering on Wireshark Code
- Information Gathering on Stored Files
- ...

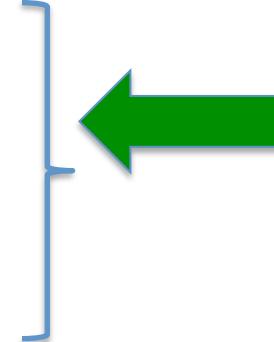
Note: Attack Groups can be systematically enumerated as a product of attack modes and systems (performers, entry points);
this is a controlled brainstorming approach





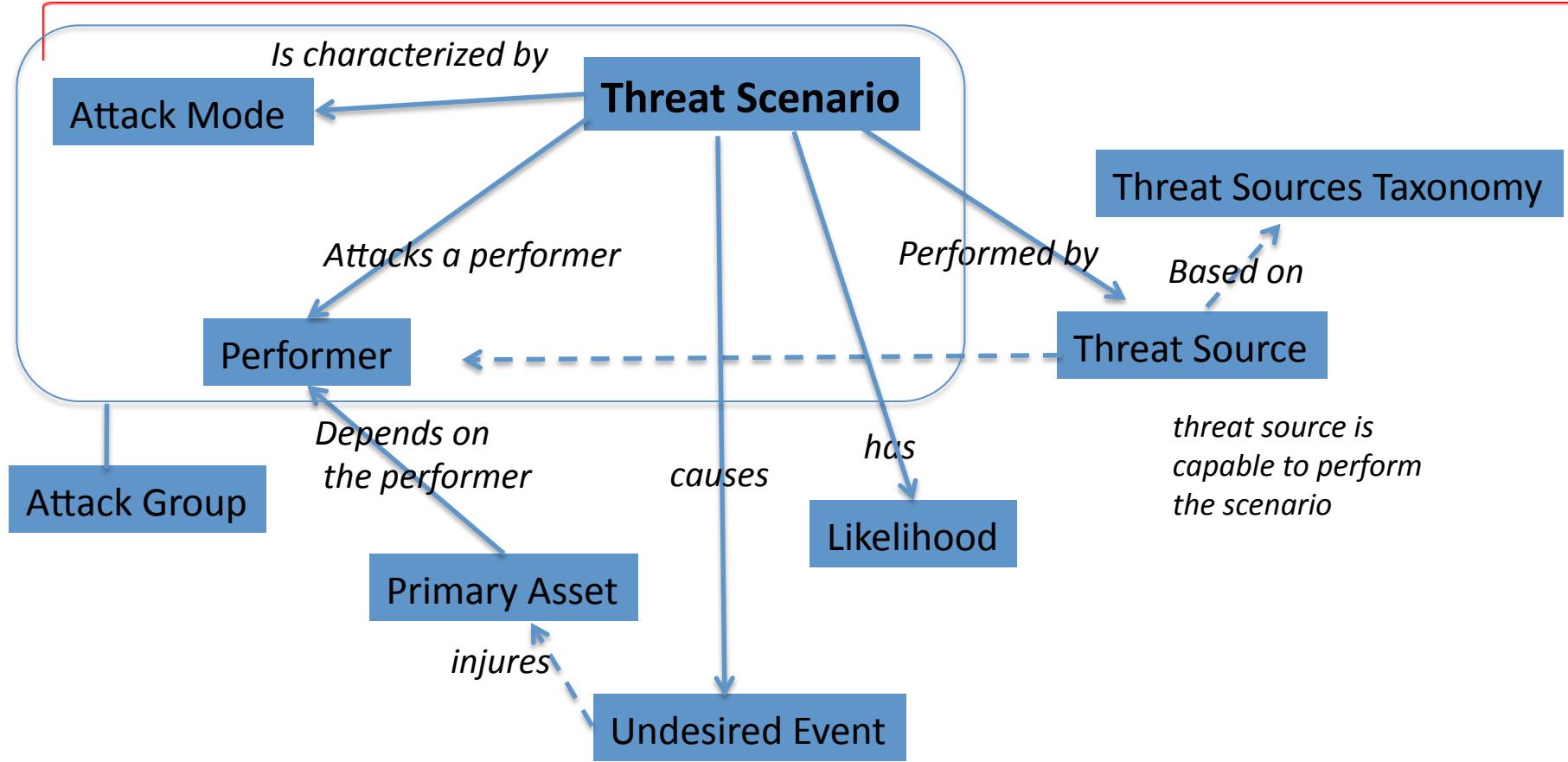
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis





Analysis of Threat Scenarios is based on the following model



Attack Group considers a single entry point; This is a class of attacks.

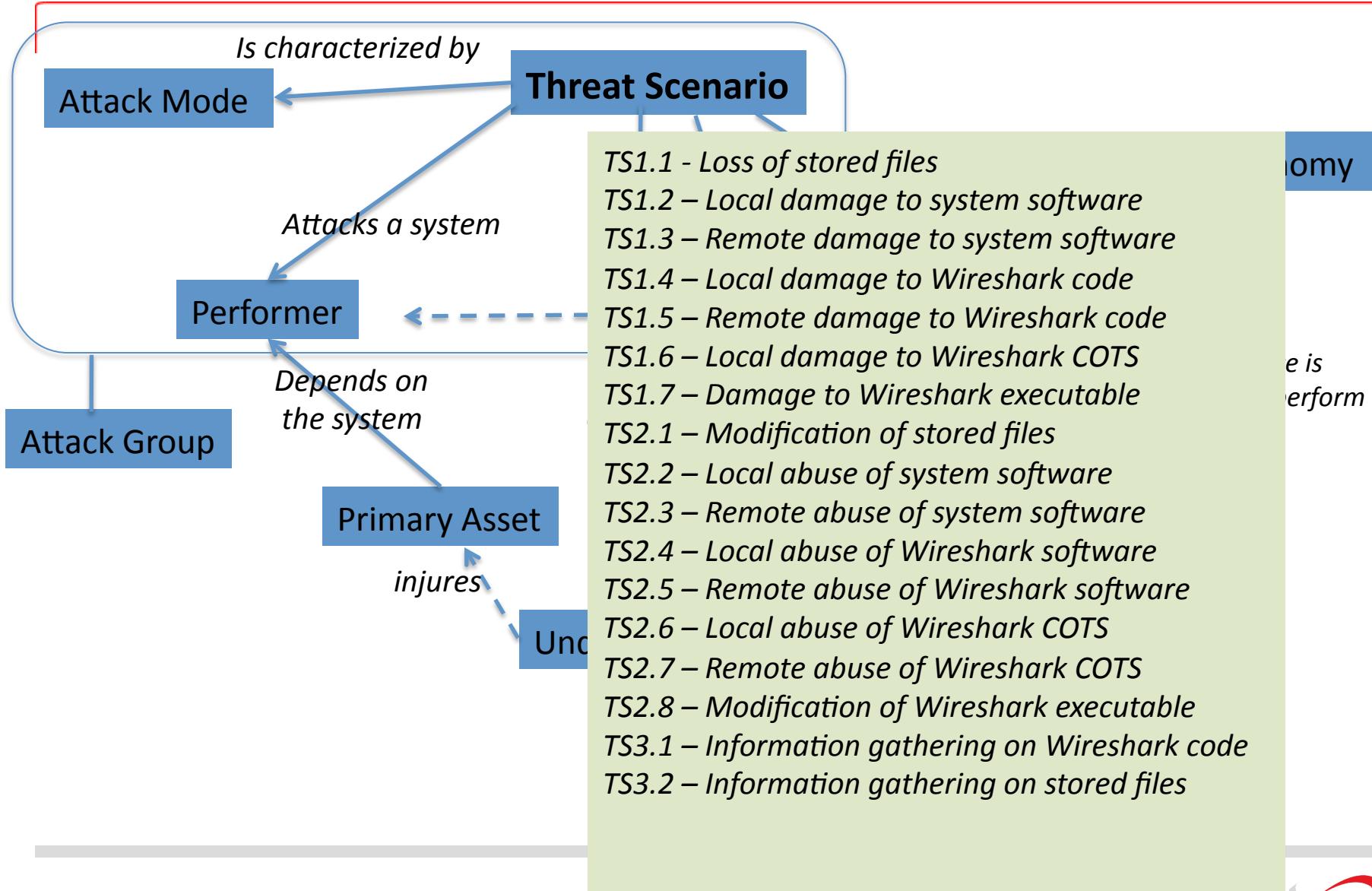
Threat Scenarios within the Attack Group describe various multi-stage attacks;

Analysis of Threat Scenarios is about connecting to impacts (the “How” to the “What”)



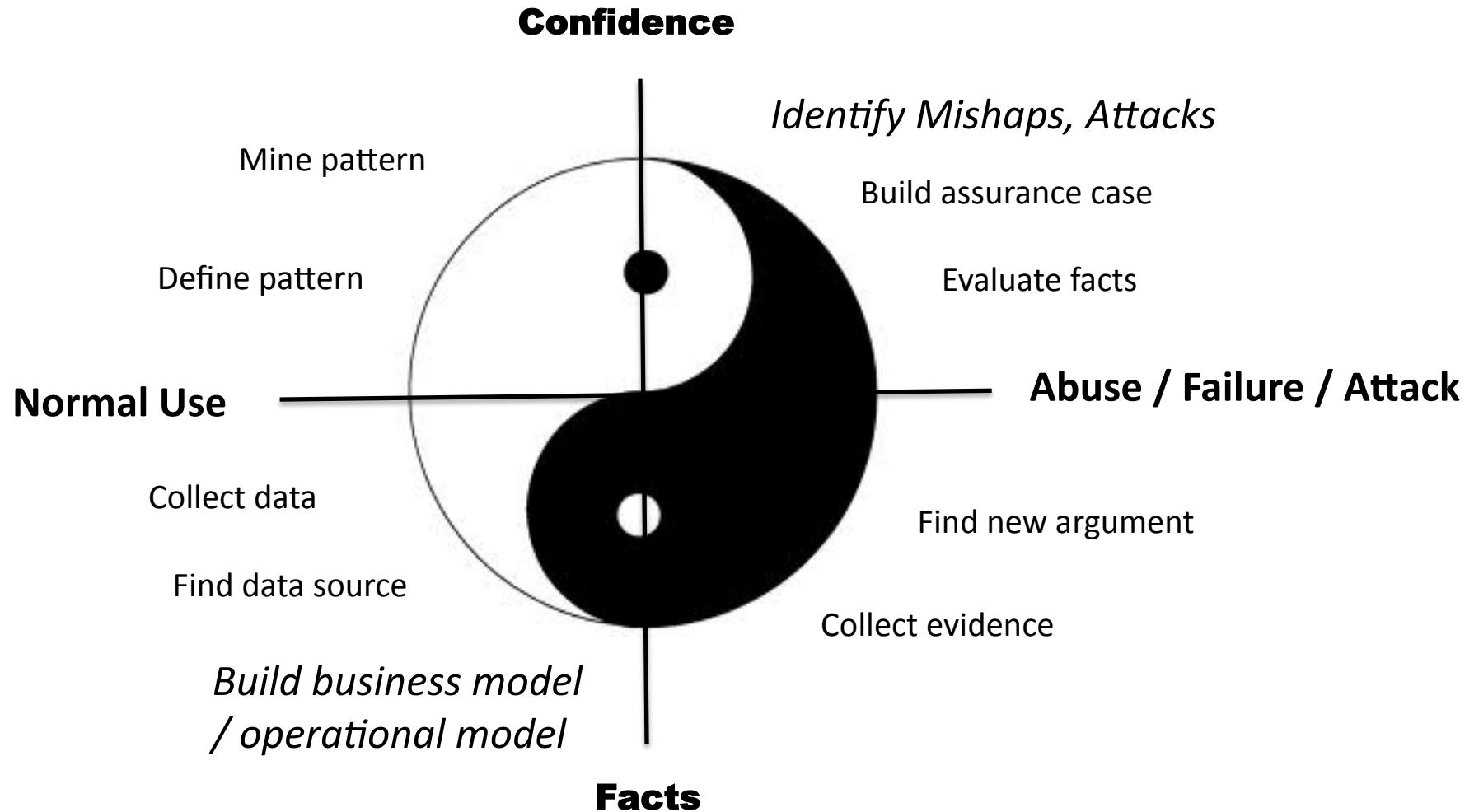


Analysis of Threat Scenarios is based on the following model





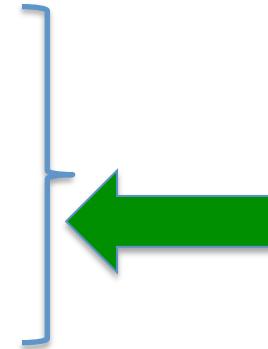
The Yin and Yang of Security Assurance





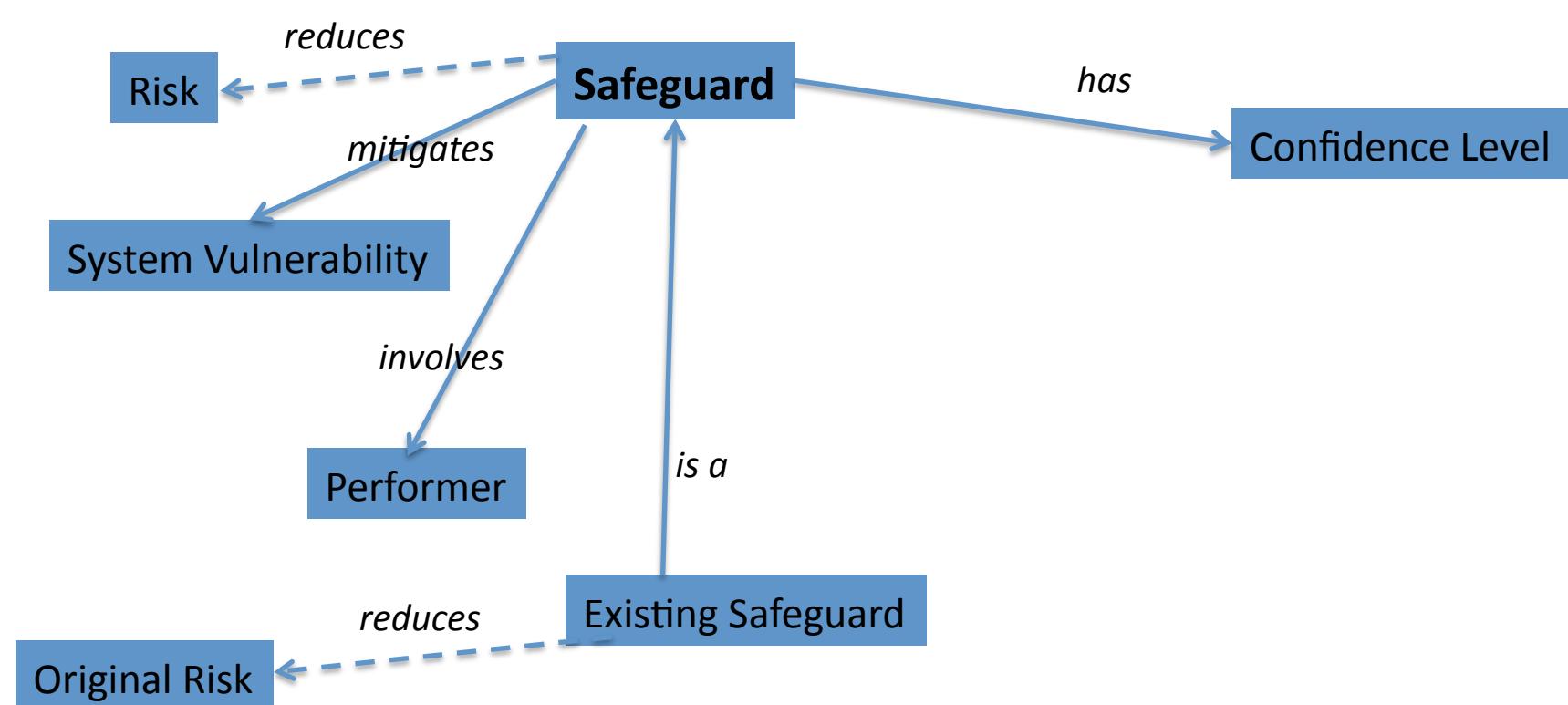
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis





Analysis of Safeguards is based on the following model



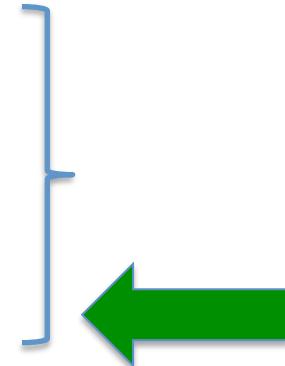
Threat Scenario within an Attack Group describes a multi-stage attack that involves multiple Performers;
A Safeguard prevents an attack from succeeding;
A System Vulnerability is a condition involving a certain Performer that
enables the attack and permit it to propagate and eventually cause an undesired event





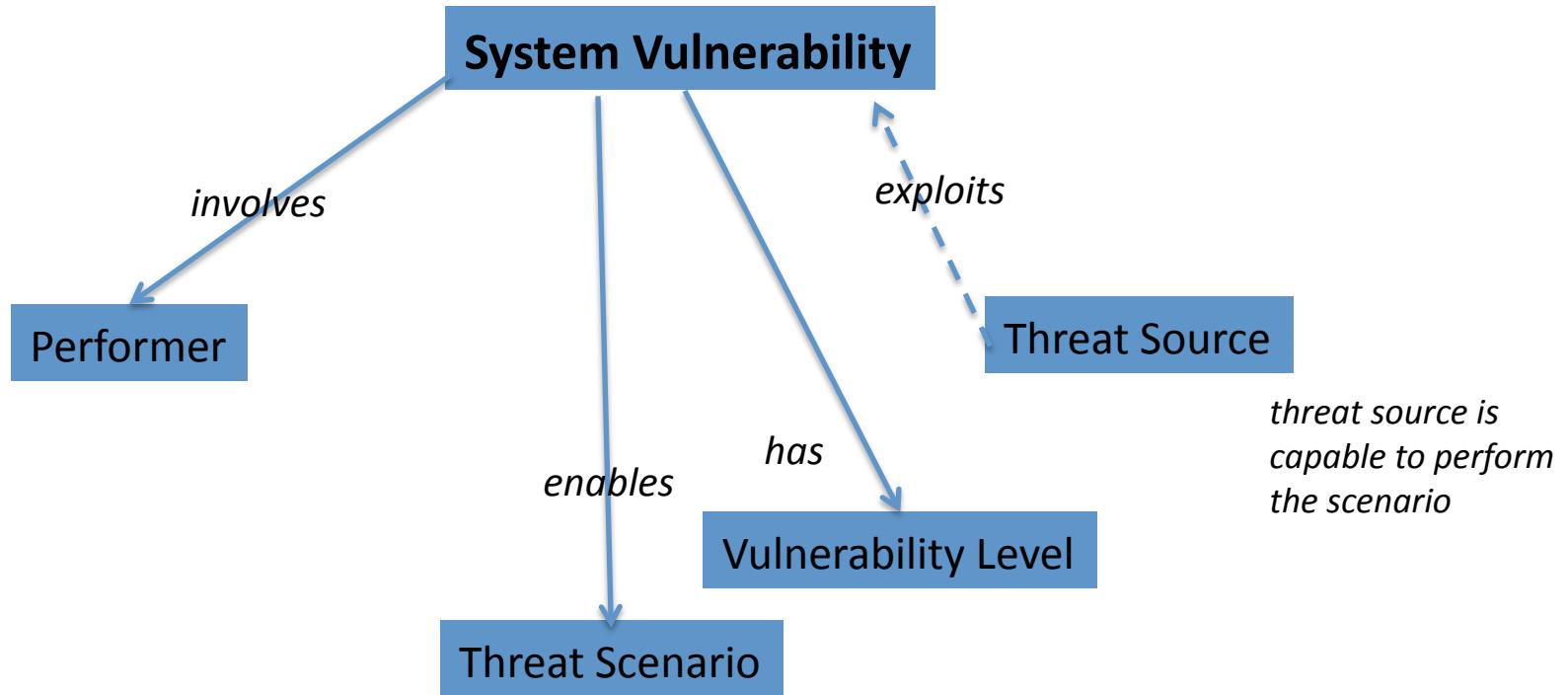
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis





Analysis of System Vulnerabilities is based on the following model



Threat Scenario within an Attack Group describes a multi-stage attack that involves multiple Performers;
A System Vulnerability is a condition involving a certain Performer that enables the attack and permit it to propagate and eventually cause an undesired event





FORSA: The Cause analysis

FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis

At this point we can justify that we understand ALL classes of attacks on the system and justify their likelihood; and justify the level of vulnerability

+validation & verification

+validation & verification

+validation & verification

+validation & verification

PART 4: RISK ANALYSIS & MITIGATION





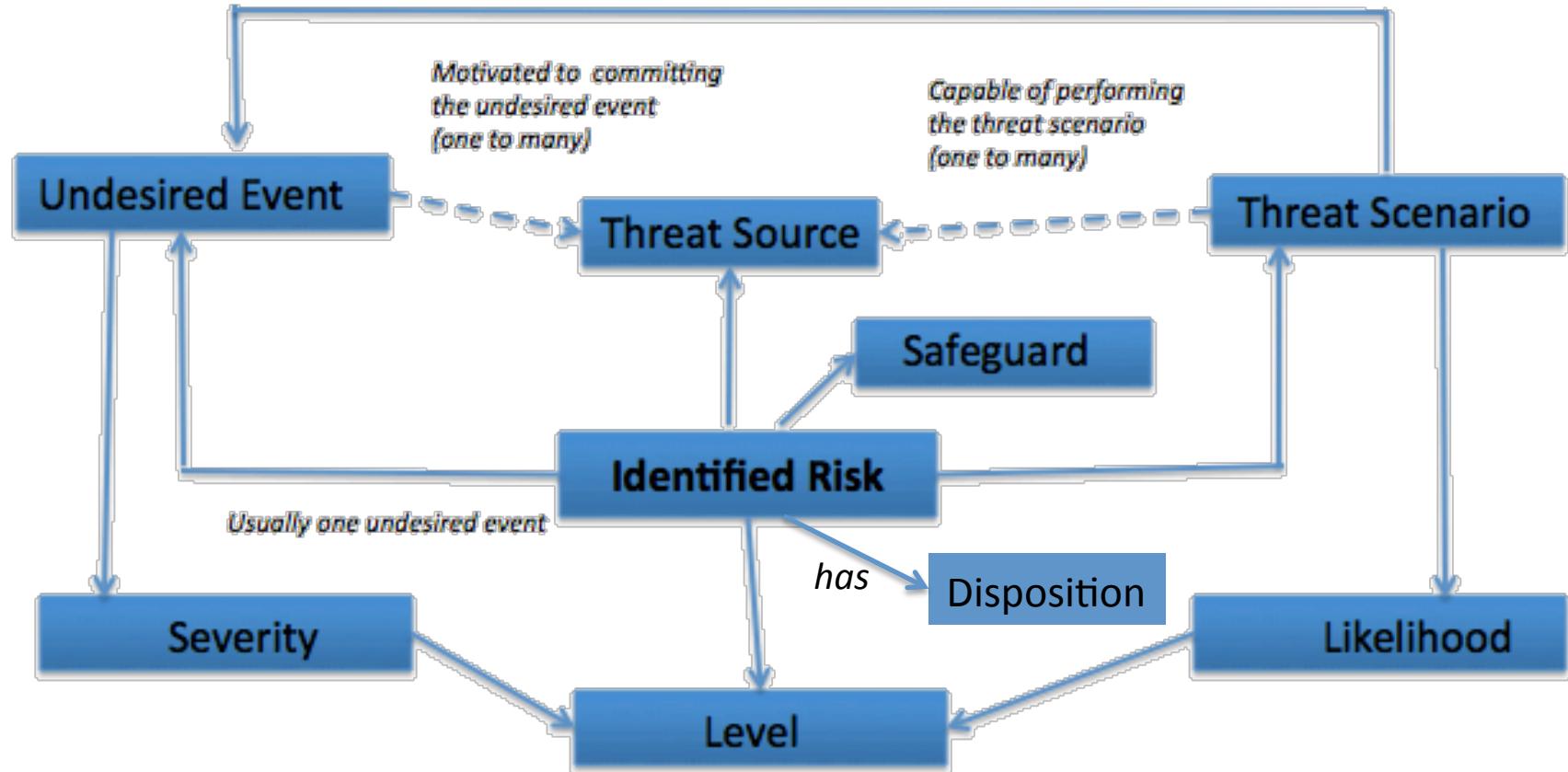
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis

} Analytics, recommendations,
Mitigation option analysis

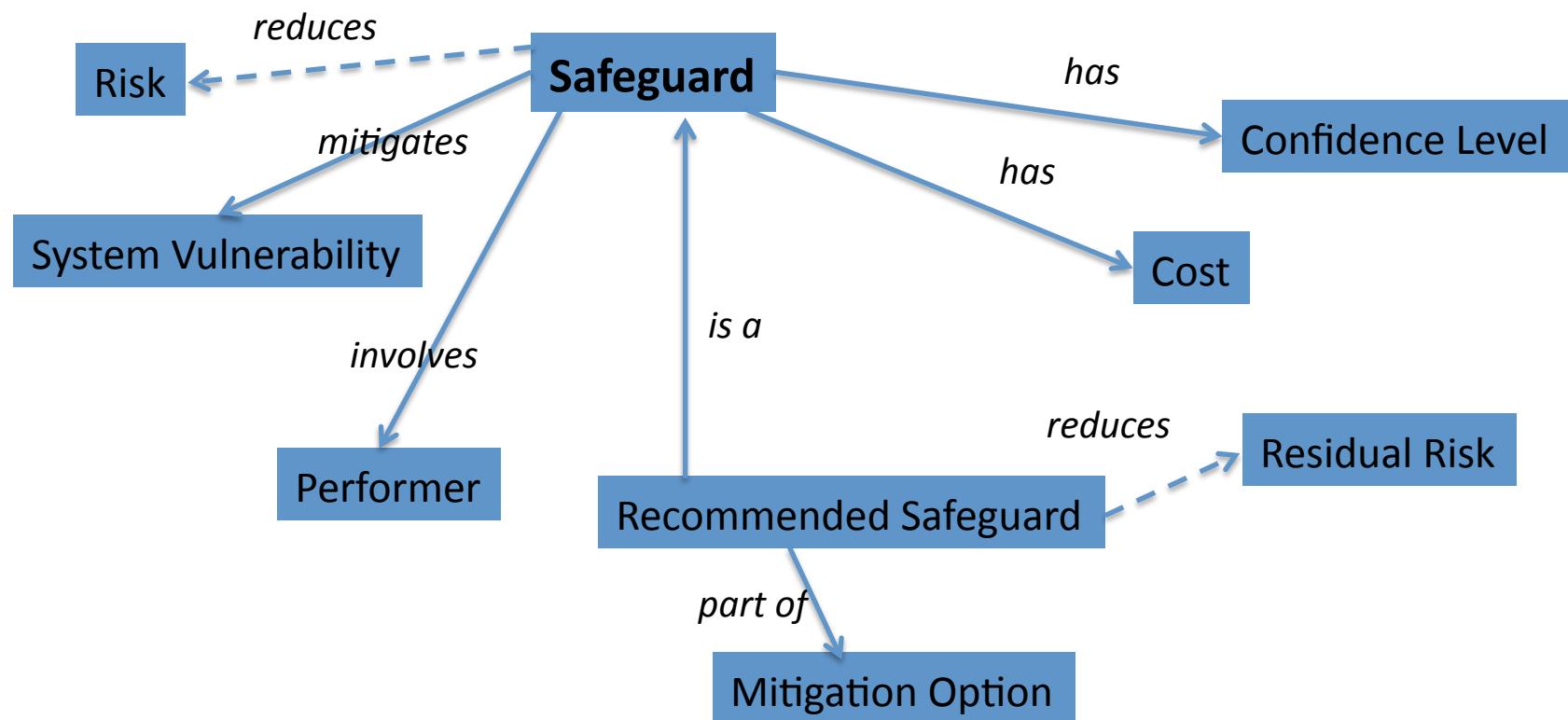


Analysis of Risks is based on the following model





Risk Mitigation Analysis is based on the following model



Threat Scenario within an Attack Group describes a multi-stage attack that involves multiple Performers;
A Safeguard prevents an attack from succeeding;
A System Vulnerability is a condition involving a certain Performer that
enables the attack and permit it to propagate and eventually cause an undesired event





KDM BLADE TOOL

Now integrated with NoMagic tools as Cameo Risk Analyzer





KDM Blade GUI

File Edit Navigate Project Vulnerabilities Analysis List Report TRA Report NVD Window Help

Blade Navigator X Machine Resources Posix Overview Model Threat Scenario Entry Point Exit Point Entry Point Identified Risk X 1 KDM Blade

Blade Navigator

- wireshark-v3_03
 - Assessment Criteria
 - Code Model
 - F01 Operational Context
 - F02 System Facts
 - F03 Asset Identification
 - F04 Undesired Event Identification
 - F05 Attack Group Identification
 - F06 Threat Scenario Analysis
 - F07 Safeguard Identification
 - F08 Vulnerability Analysis
 - F09 Risk Identification
 - F10 Risk Analysis
 - S01 Vulnerability Types
 - S02 Software Facts
 - S03 Evidence
 - S04 Vulnerability Findings
 - S05 Path Analysis Results
 - S06 Attack Analysis
 - extractor
 - reports
- Blade Notes X

Identified Risk (17 of 17)

type filter text All Categories

Instance	Category
R01 - Hacker gains access to confidential assets by information gathering	
R02 - Targeted virus or timebomb affects integrity or availability of network assets	
R03 - Hacker subverts wireshark node by remote attack exploiting vulnerability	
R04 - Hacker subverts wireshark node by remote attack exploiting vulnerability	
R05 - Criminal learns about forensic activity by attacking wireshark executable	
R06 - Targeted virus or timebomb affects availability of other assets by a	
R07 - Malicious user subverts wireshark node by locally attacking wireshark	
R08 - Malicious user subverts wireshark node by locally attacking system	
R09 - Criminal forces wireshark to miss packets by attacking wireshark e	

Main Threat Analysis Vulnerability Analysis

Overall System Vulnerability Level Not Set

Vulnerabilities (9)

Name	Note	Category	Level
V01 - Incorrect permissions on stored trace		Misconfiguration	Not Set
V02 - Local access to stored traces		Access control	Not Set
V03 - Remote access to stored traces		Access control	Not Set
V05 - Abuse of system software		Admin	Not Set

Capable Threat Sources (0)

Name	Note	Category
------	------	----------

Details X KDM List Properties are not available.

0 items selected

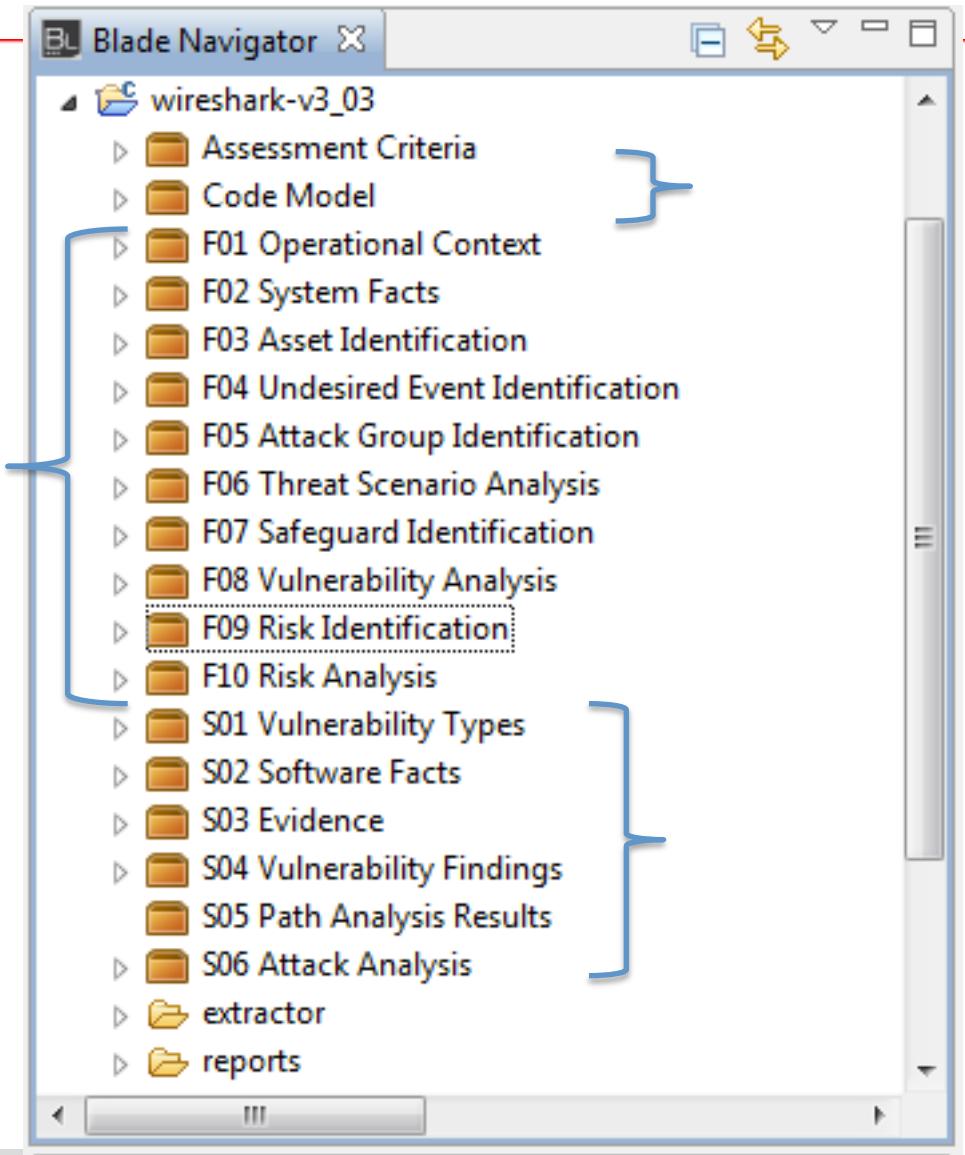




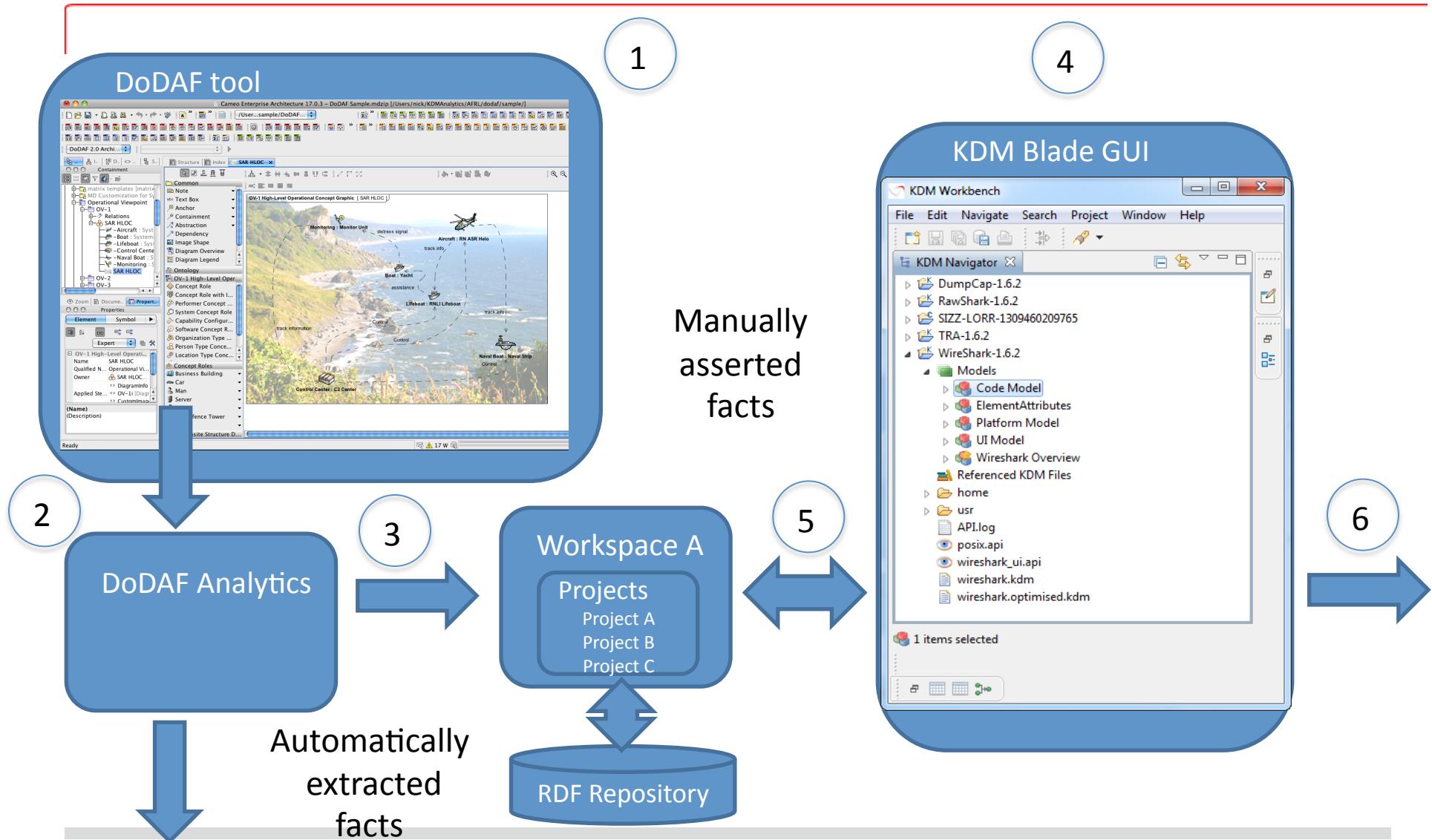
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis
11. Evidence Analysis

Blade Navigator

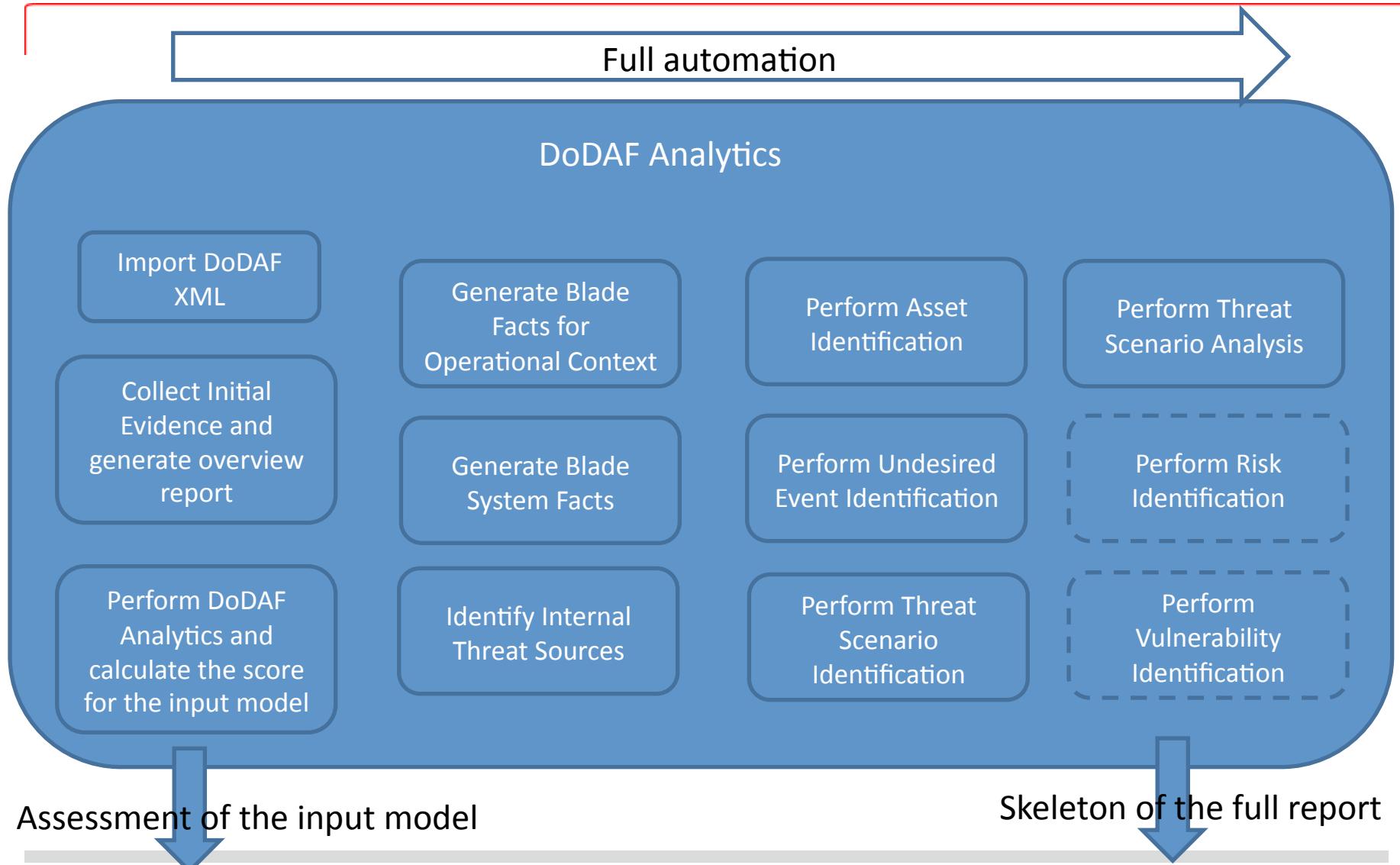


Sources of Facts in KDM Blade





DoDAF Analytics: “Automated Everything”



QUESTIONS ?



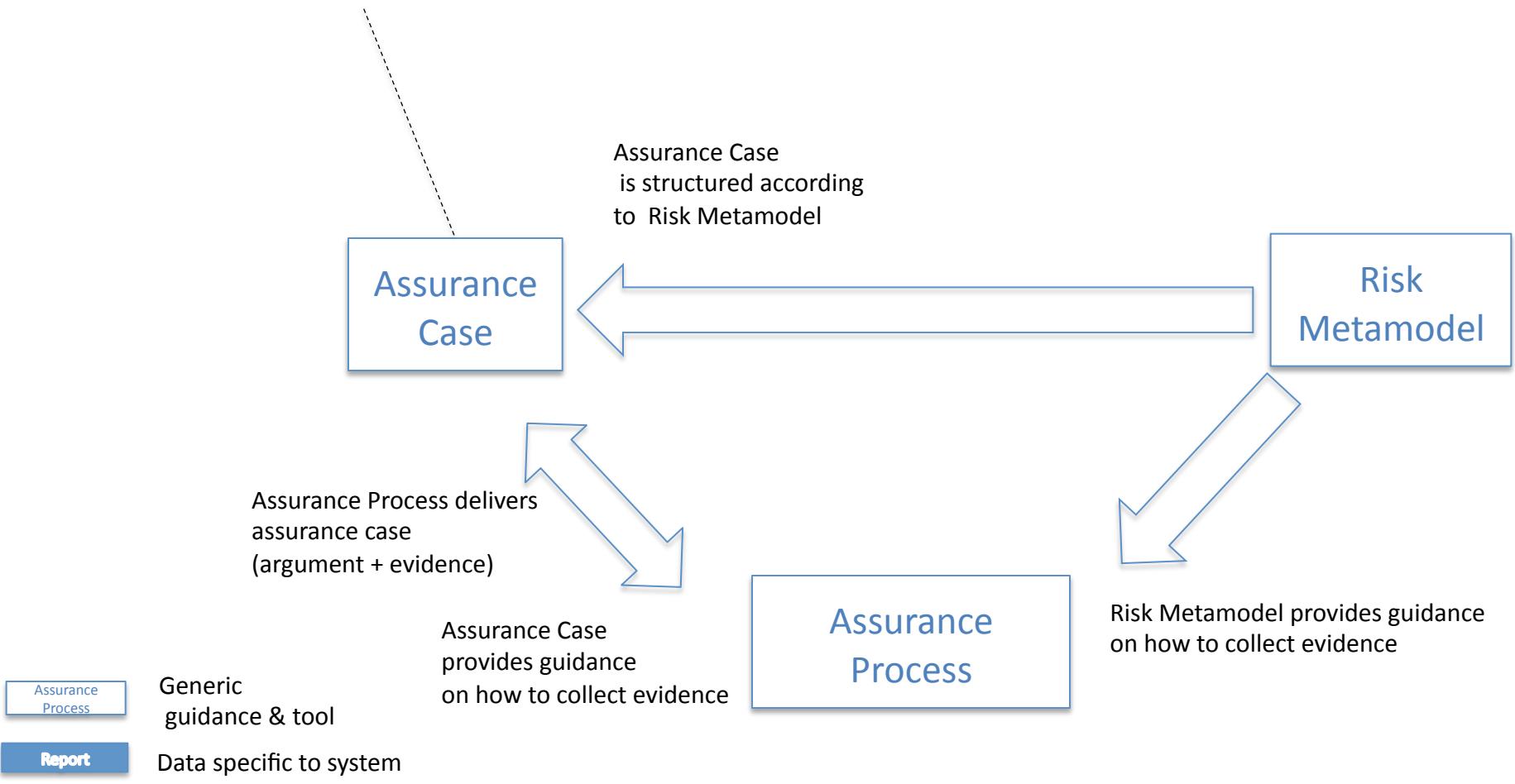
***JUSTIFIABLE RISK ASSURANCE =
RISK MANAGEMENT + ASSURANCE
CASE***





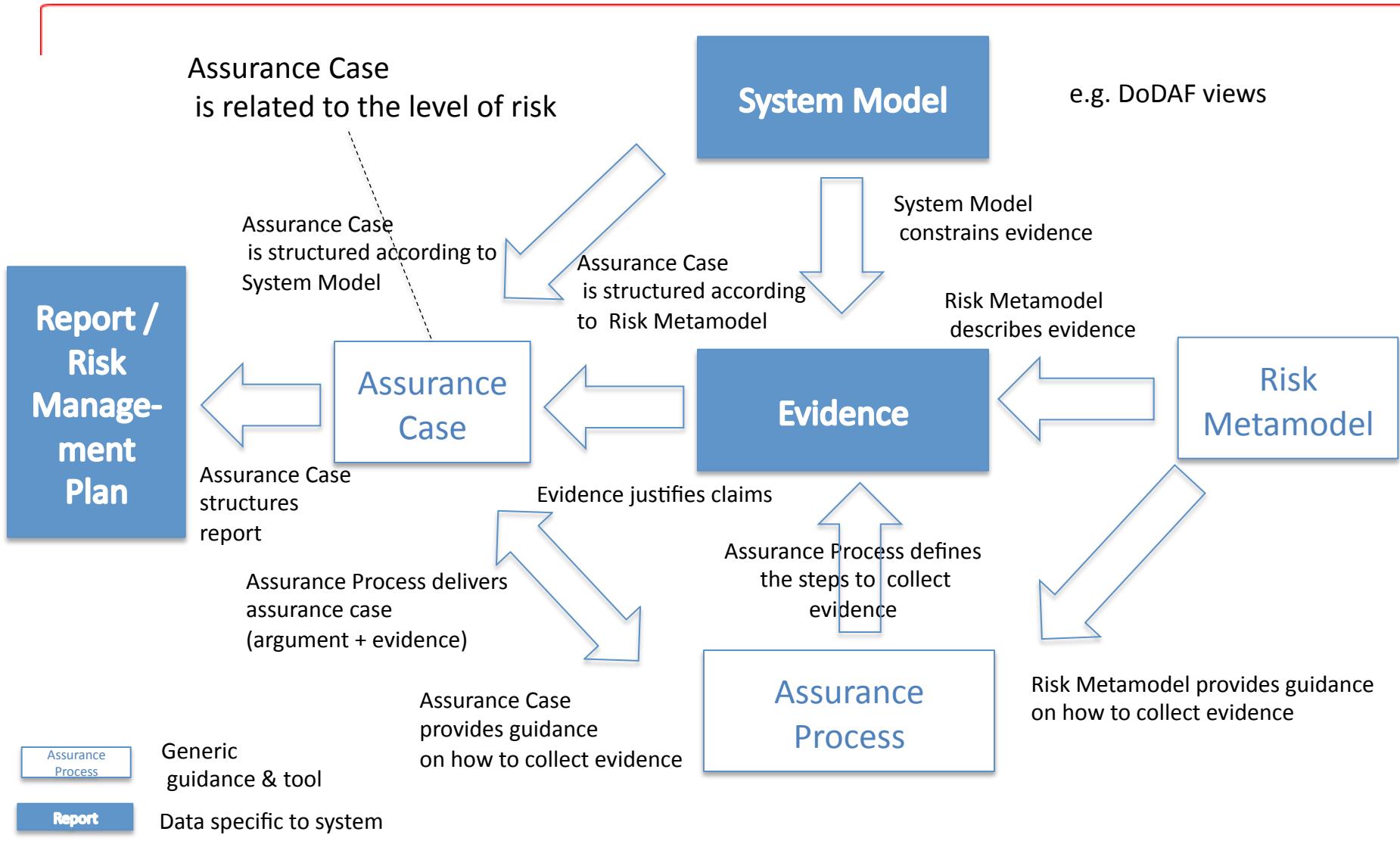
Justifiable Risk Assurance

Assurance Case
is related to the level of risk





Justifiable Risk Assurance





The key outcome is a justifiable list of risks

FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis

Steps leading to systematic identification of risks





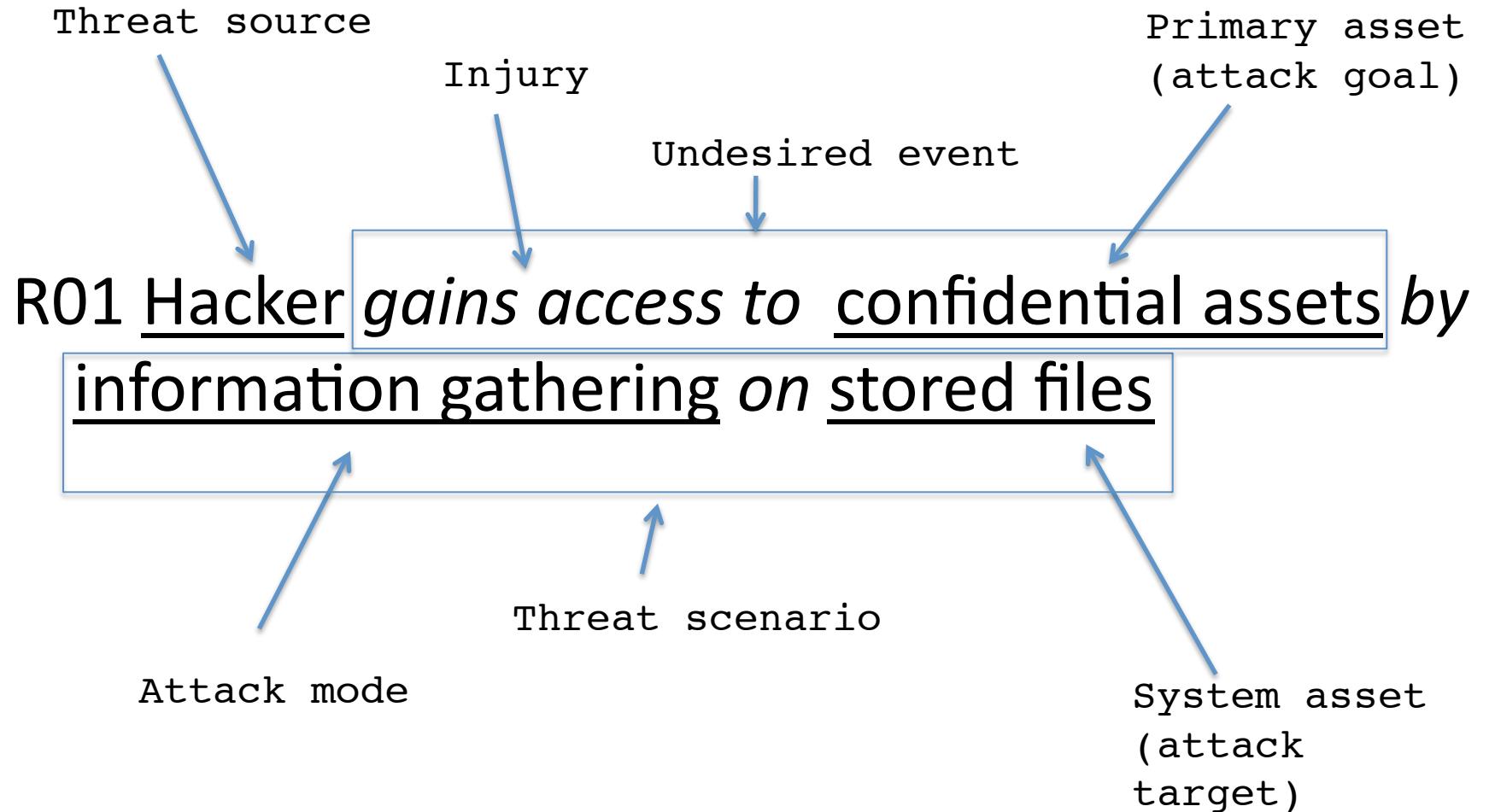
Results of justifiable risk analysis (1 of 2)

ID	Description	Severity	Likeli-hood	Level	Resi-dual	Confi-dence
R01	Hacker gains access to confidential assets by information gathering on stored files	high	high	high	low	80%
R02	Targeted virus or timebomb affects integrity or availability of network by attacking wireshark executable	high	high	high	low	80%
R03	Hacker subverts wireshark node by remote attack exploiting vulnerabilities in Wireshark code	high	medium	high	low	80%
R04	Hacker subverts wireshark node by remote attack exploiting vulnerabilities in system software on wireshark node	high	medium	medium	low	80%
R05	Criminal leans about forensic activity by attacking wireshark executable	medium	high	medium	low	80%
R06	Targeted virus or timebomb affects availability of other assets by attacking wireshark executable	medium	high	medium	low	80%
R07	Malicious user subverts wireshark node by locally attacking wireshark code	medium	low	medium	low	70%
R08	Malicious user subverts wireshark node by locally attacking system software on wireshark node	medium	low	medium	low	70%
R09	Criminal forces wireshark to miss packets by attacking wireshark executable	medium	high	medium	low	70%





Anatomy of a risk statement

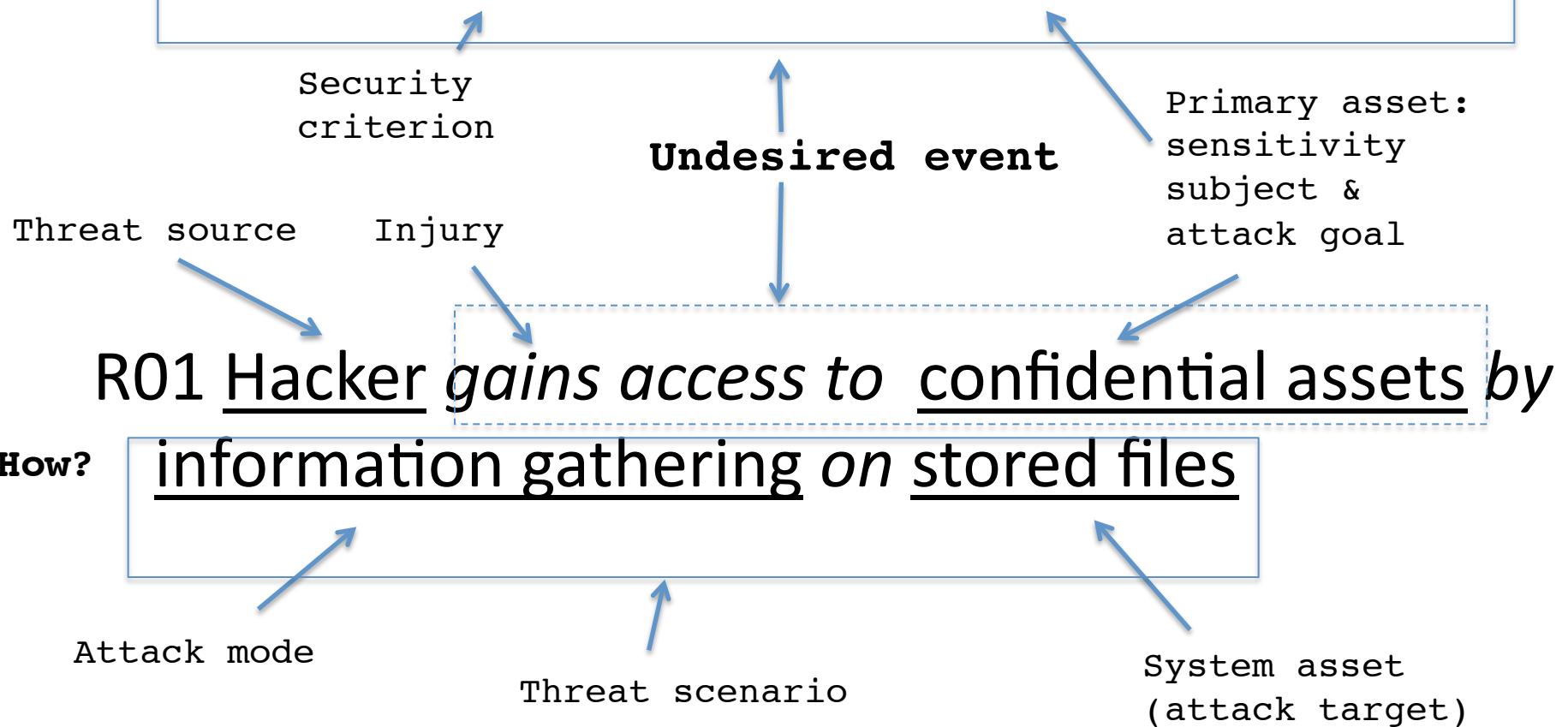


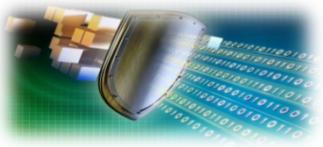


Cause and effect in a risk statement

what?

Loss of confidentiality of confidential assets

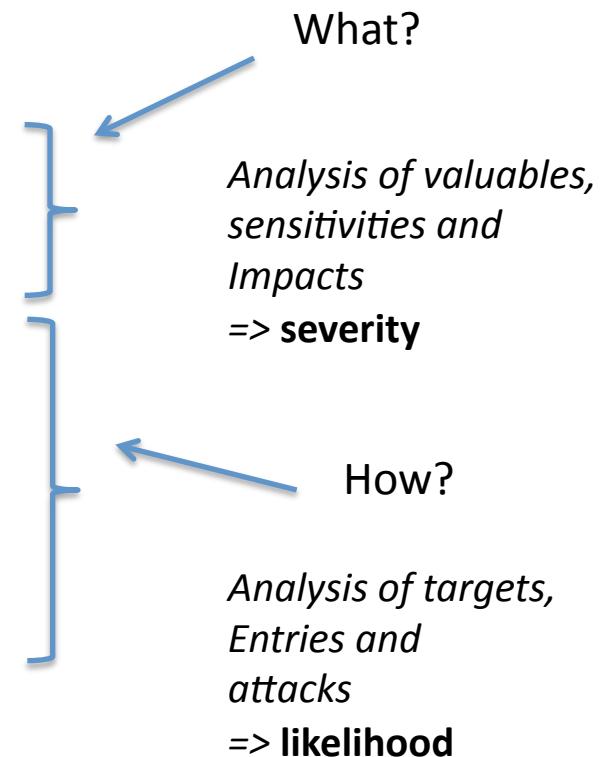




The corresponding FORSA steps

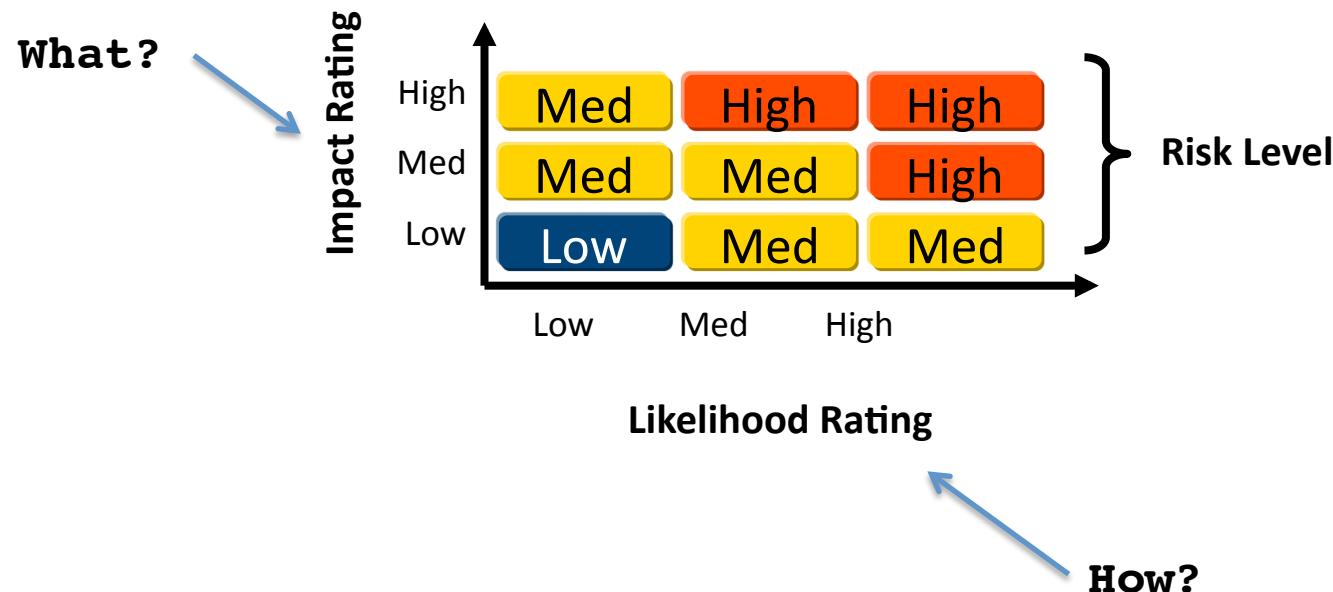
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis





Risk analysis



$$\text{Risk} = f(\text{Severity}, \text{Likelihood})$$



FROM RISK TO CLAIMS & EVIDENCE THROUGH PATTERNS

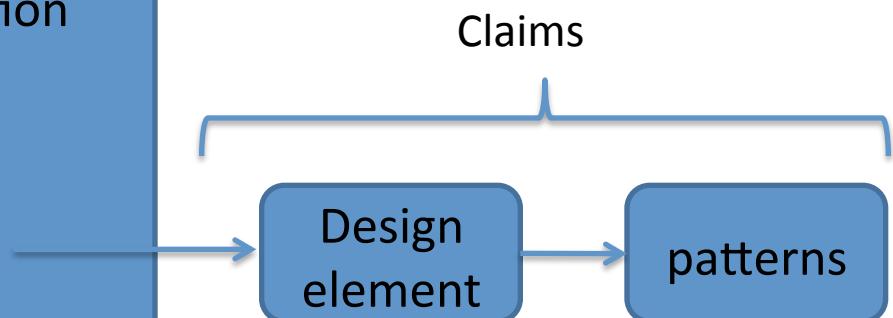




Evidence collection planning

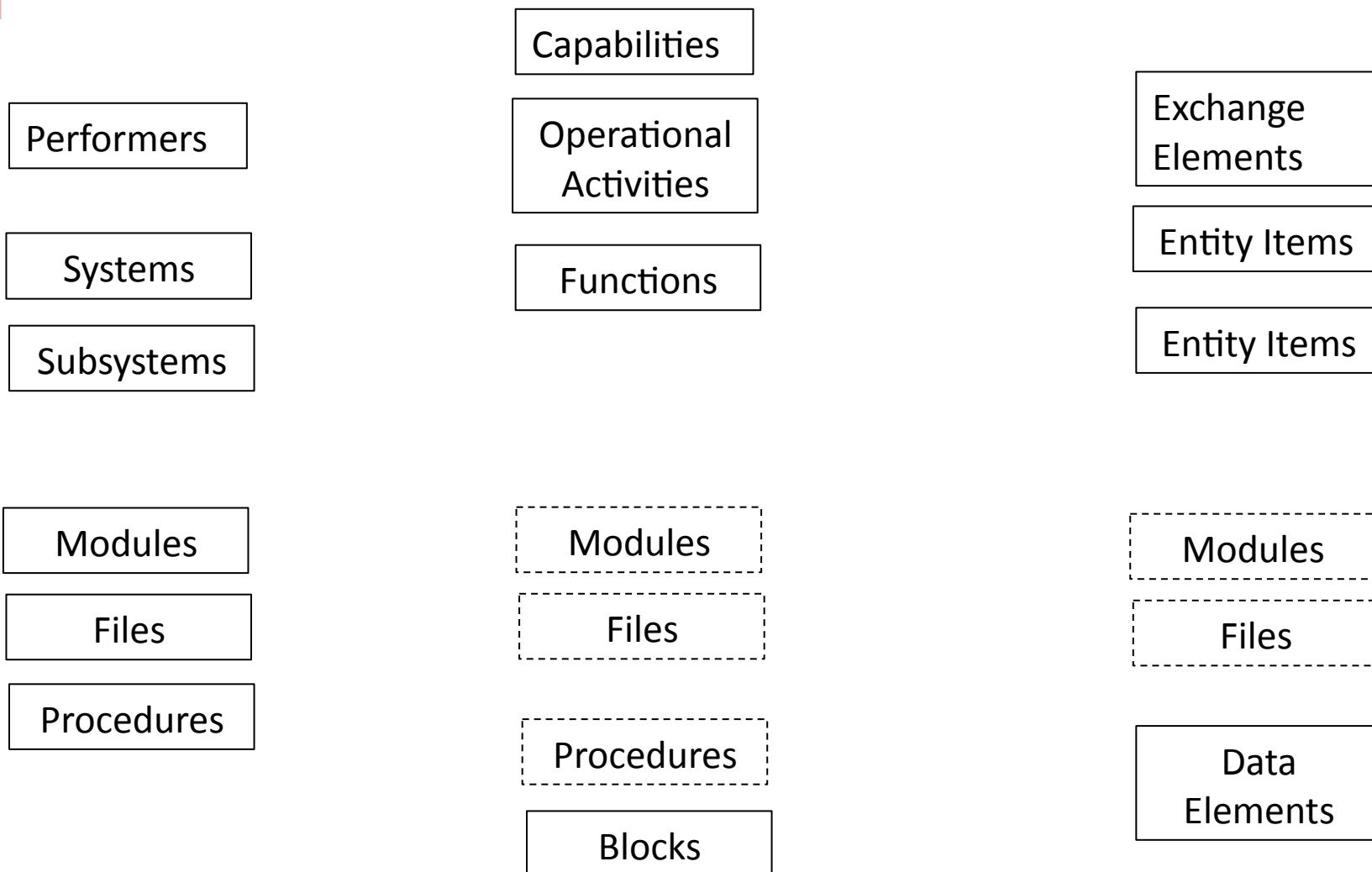
FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis





Business Models -> SysML -> Code

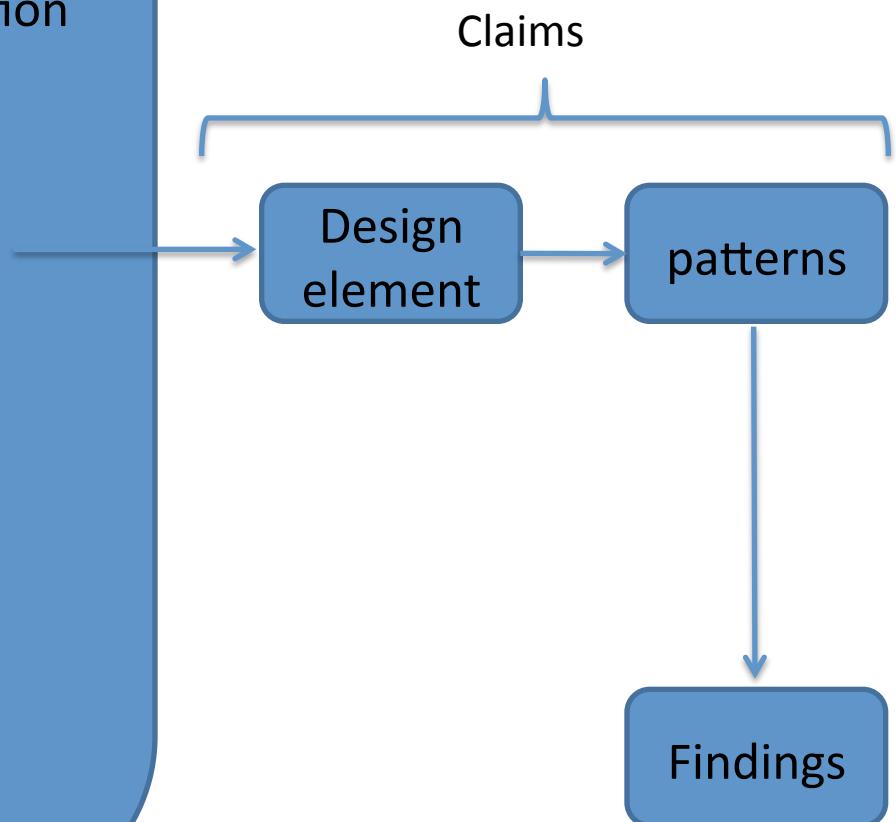




Evidence collection

FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis

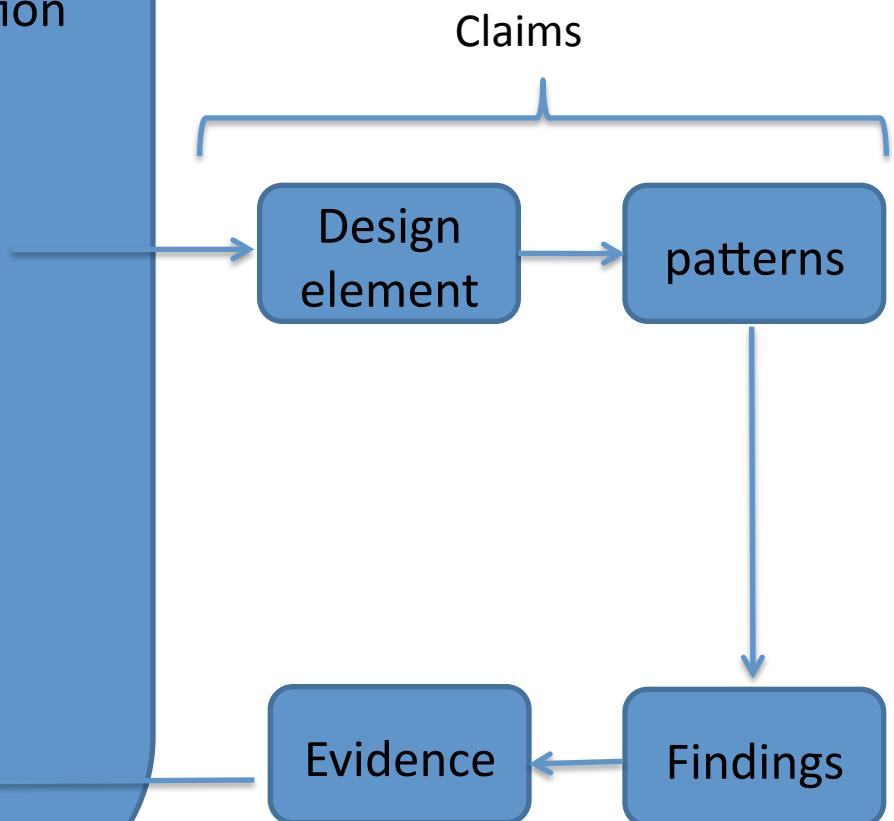




Evidence analysis

FORSA STEPS

1. Operational Context Identification
2. System Facts
3. Asset Identification
4. Undesired Event Identification
5. Attack Group Identification
6. Threat Scenario Analysis
7. Safeguard Identification
8. Vulnerability Analysis
9. Risk Identification
10. Risk Analysis
11. Evidence Analysis





Undesired Events -> Claims -> Patterns

- We start with an enumeration of undesired events (something happens; an *injury*)
 - Usually the injury happens *to an asset*
 - There is a *design element (piece of code)* that causes the injury when executed
 - Can we identify all necessary pieces of code for the specific injury ?
- We make *claims* regarding all possible necessary conditions of an injury
- As the result we get the *patterns* to identify the corresponding design elements
- Some patterns are *common* vulnerability patterns
- Others are application-specific patterns



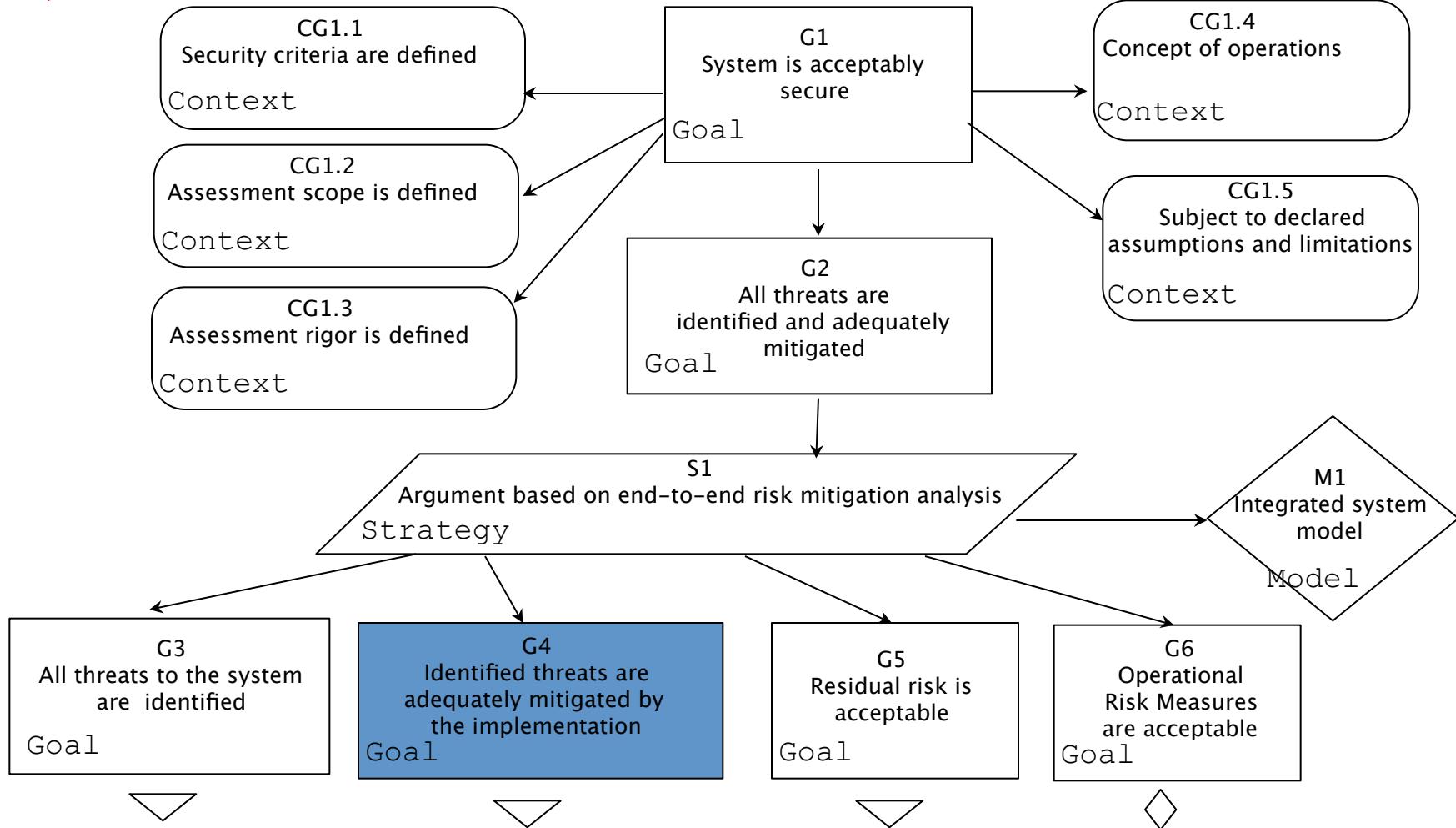
ASSURANCE CASE FOR JUSTIFIABLE RISK MANAGEMENT

uses OMG Structured Assurance Case Metamodel (SACM)



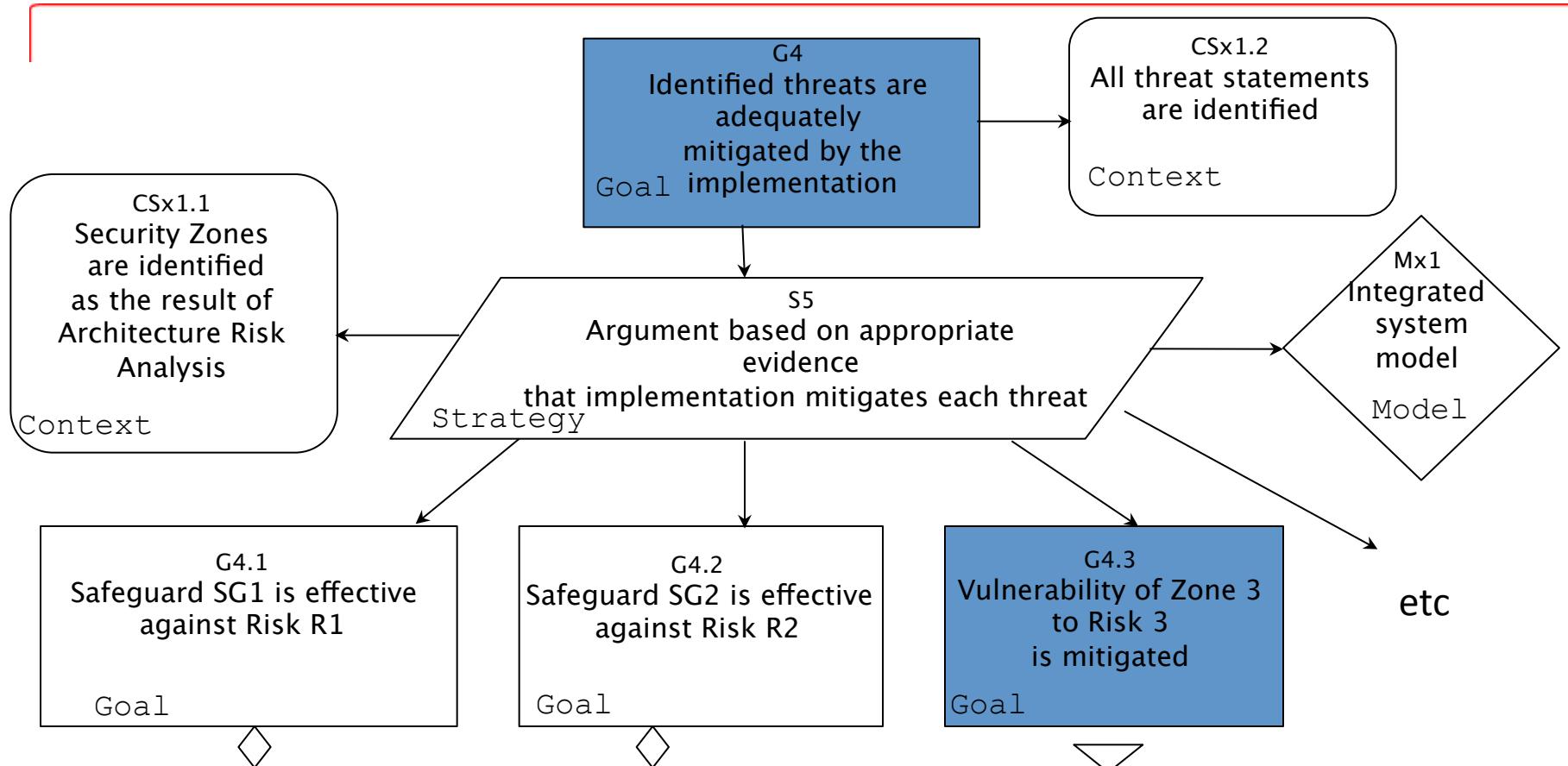


Security Assurance Case (top)





Mitigation argument



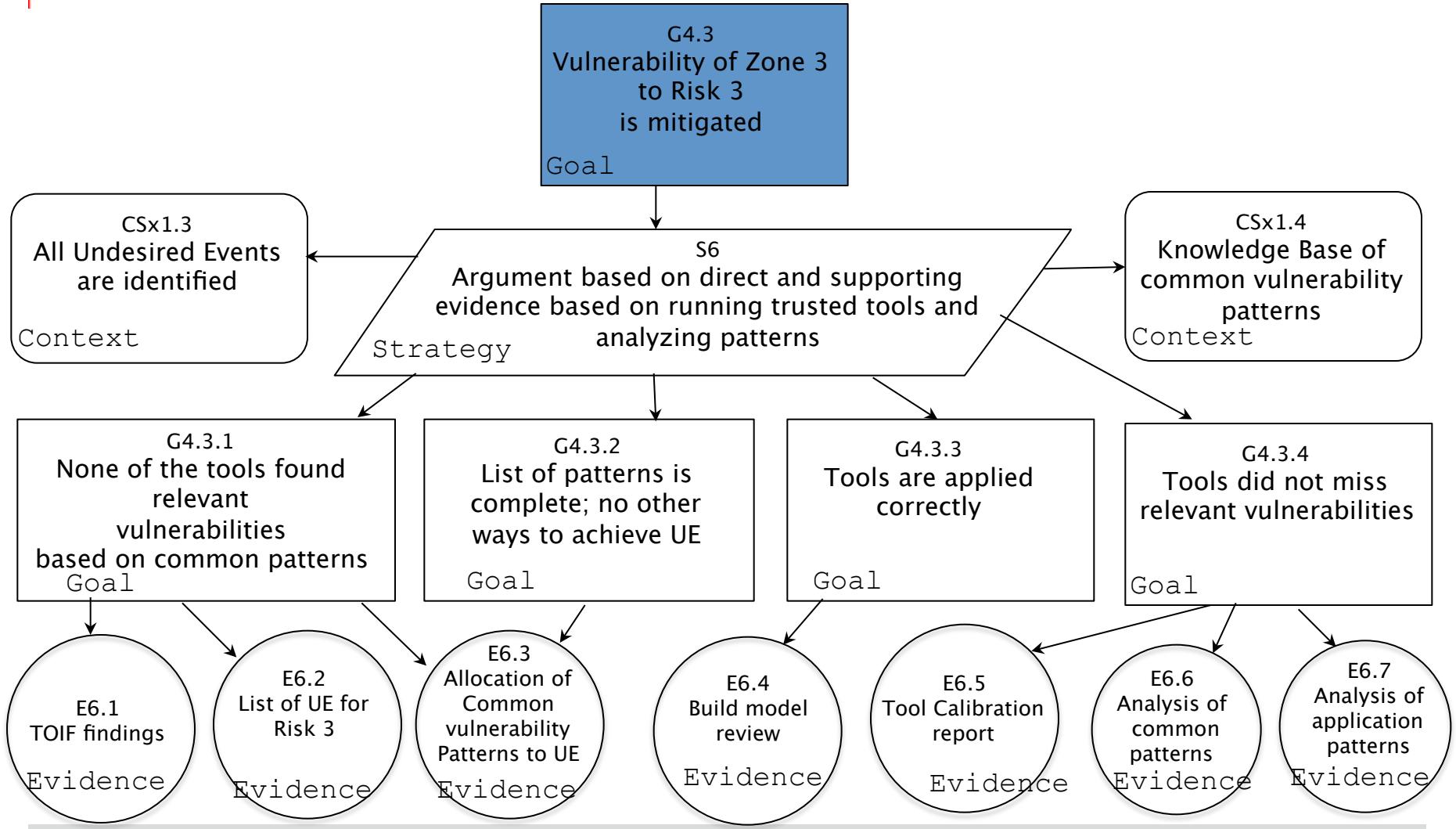
Specific argument:
Claims and evidence

Specific argument:
Claims and evidence



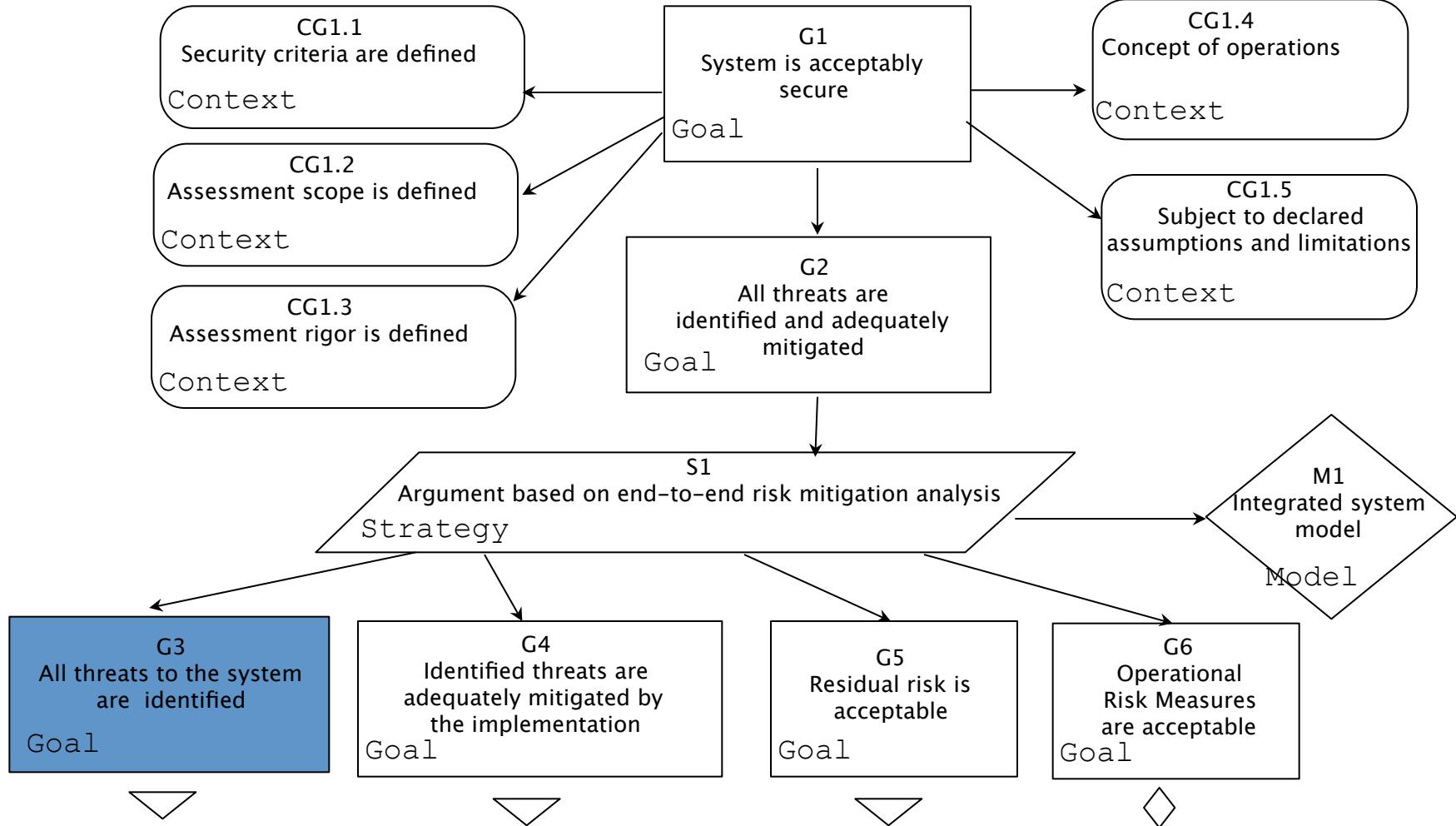


Vulnerability Mitigation Argument



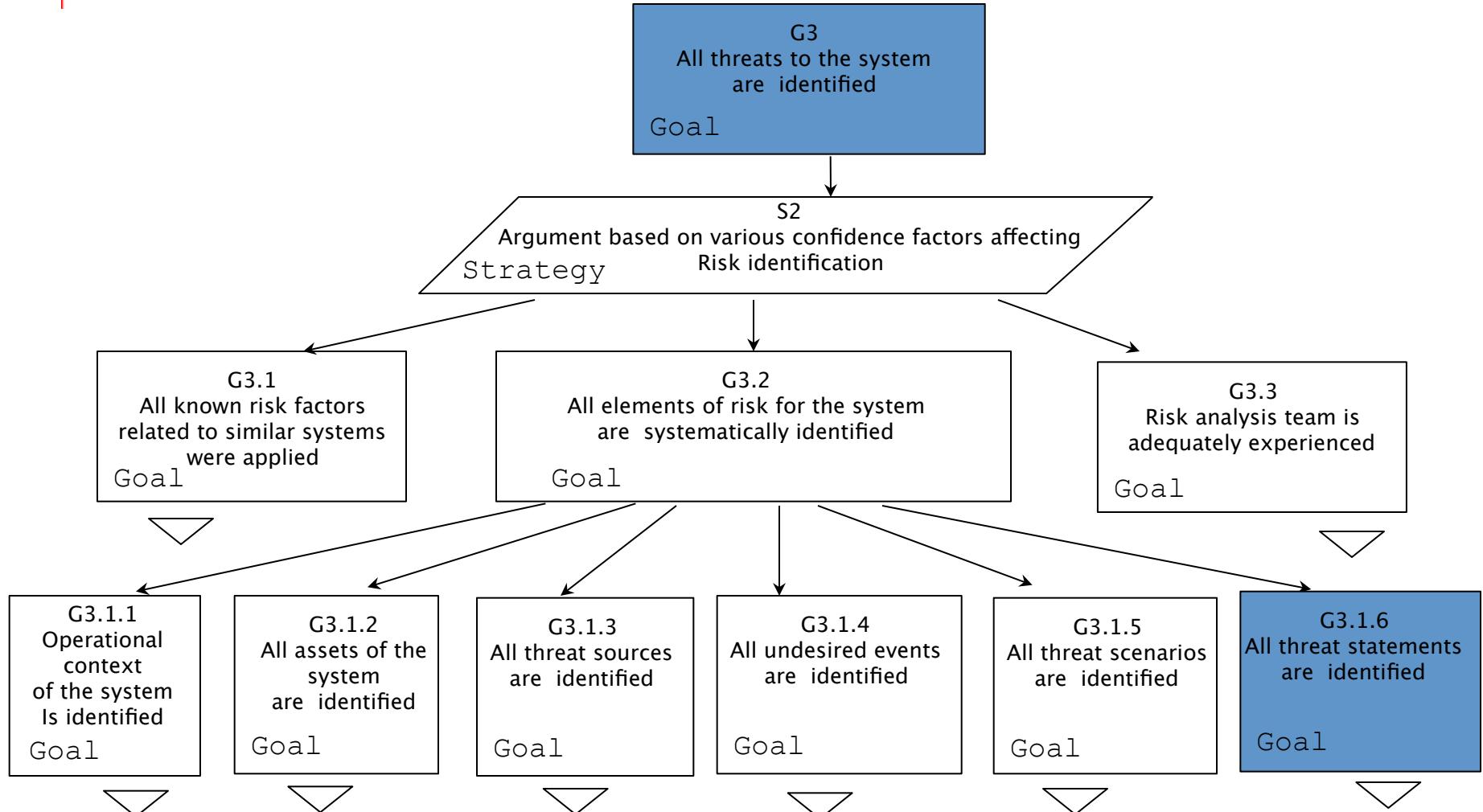


Security Assurance Case (back to the top)



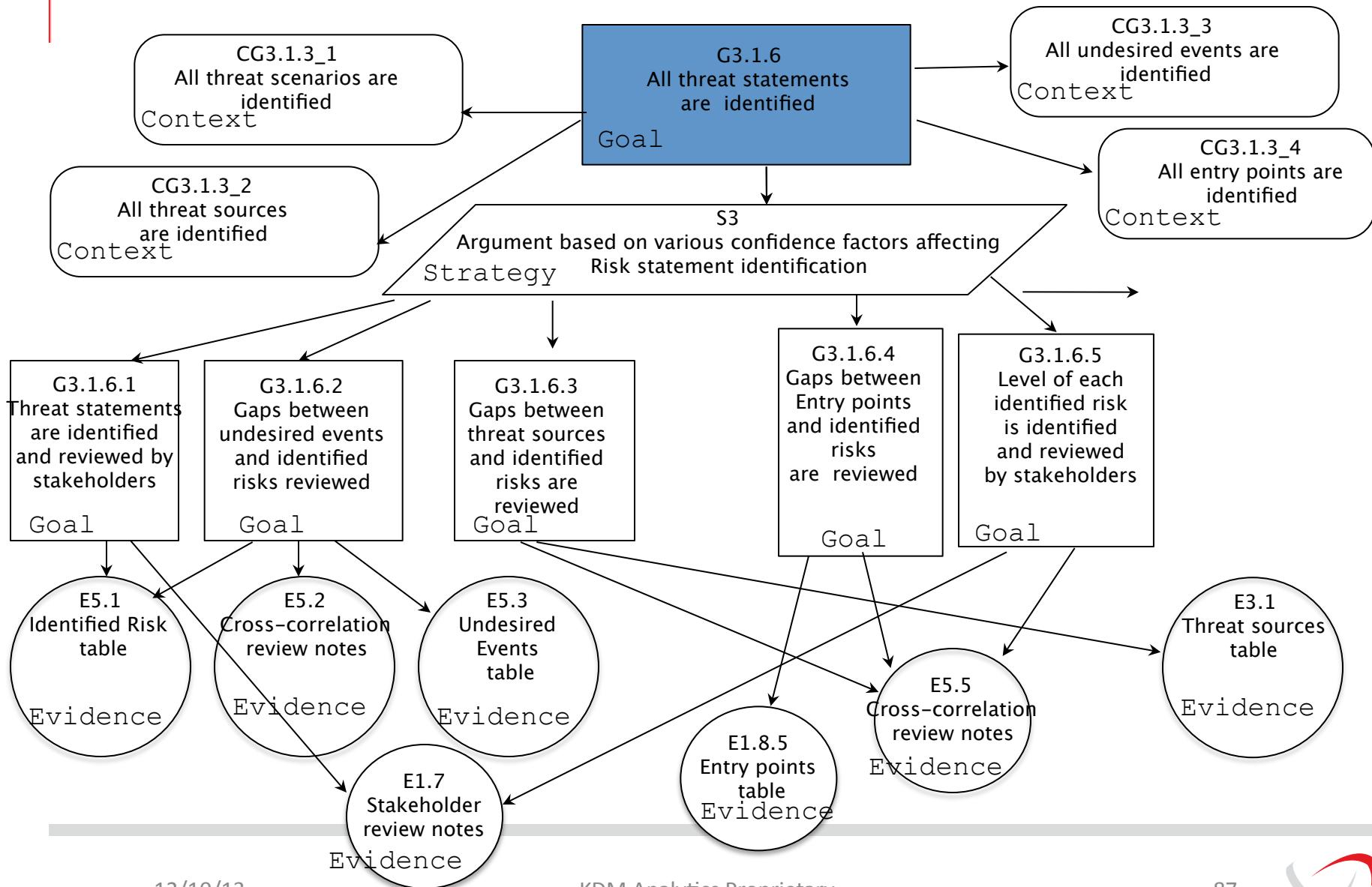


Threat identification argument





Threat identification argument (cont'd)





Evaluation of confidence



Confidence = $\sqrt{(\text{Importance of Claim}, \text{Strength of Evidence})}$



QUESTIONS ?

