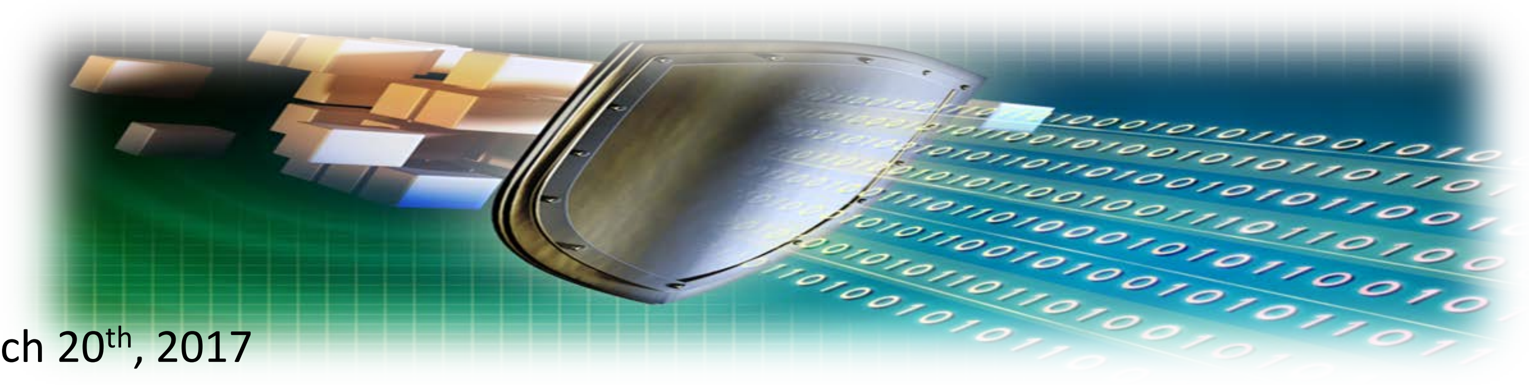
KDMAnalytics

Prioritize, Measure and Quantify Cyber Security Risk

Cybersecurity and Risk Management

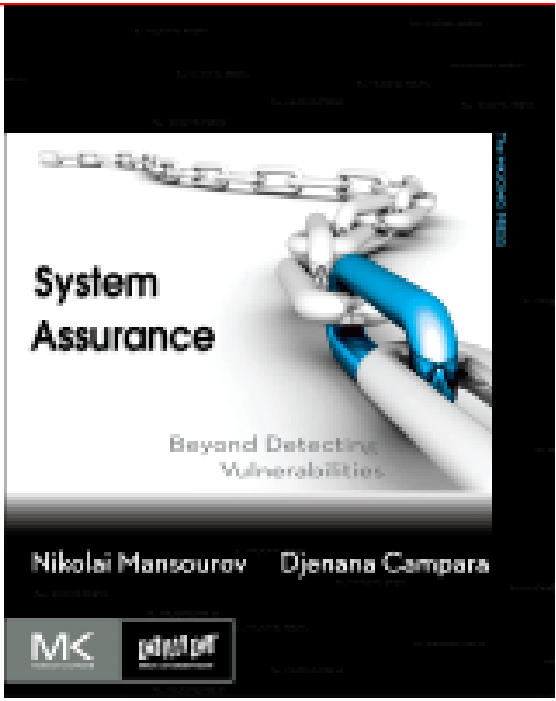
Dr. Nikolai Mansourov, CTO



March 20th, 2017

Who we are

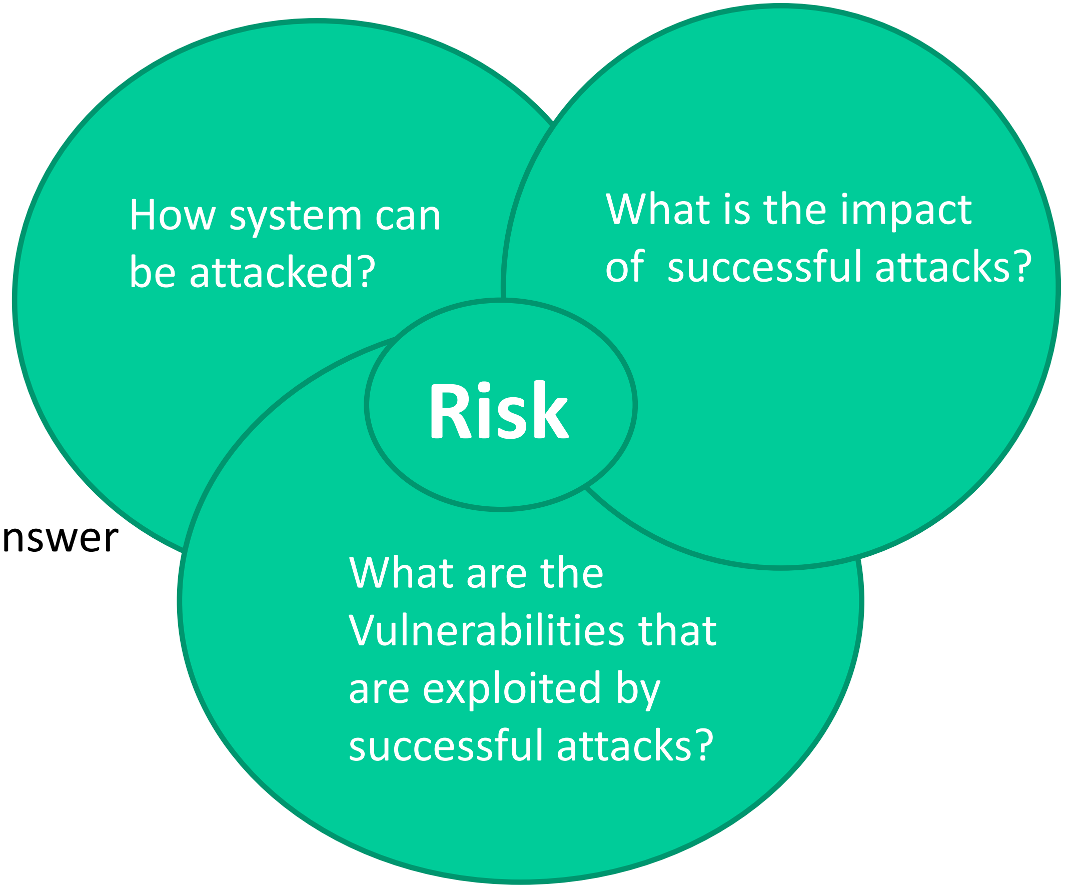
- KDM Analytics:
- We provide solutions to automate cybersecurity assessments
- Leaders in Model-based Cybersecurity Assessment (MBCA)
- http://www.kdmanalytics.com



What is the challenge ?

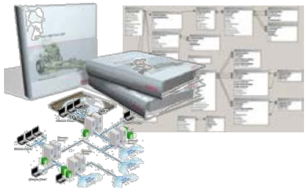
Goal:
Risk Assessment Methodology within the Risk Management Framework (RMF) that is systematic, objective and allows automation and that can answer a tough question:

How do we *know* that *all* threats have been addressed


How system can be attacked?
What is the impact of successful attacks?
Risk
What are the Vulnerabilities that are exploited by successful attacks?

Towards automation

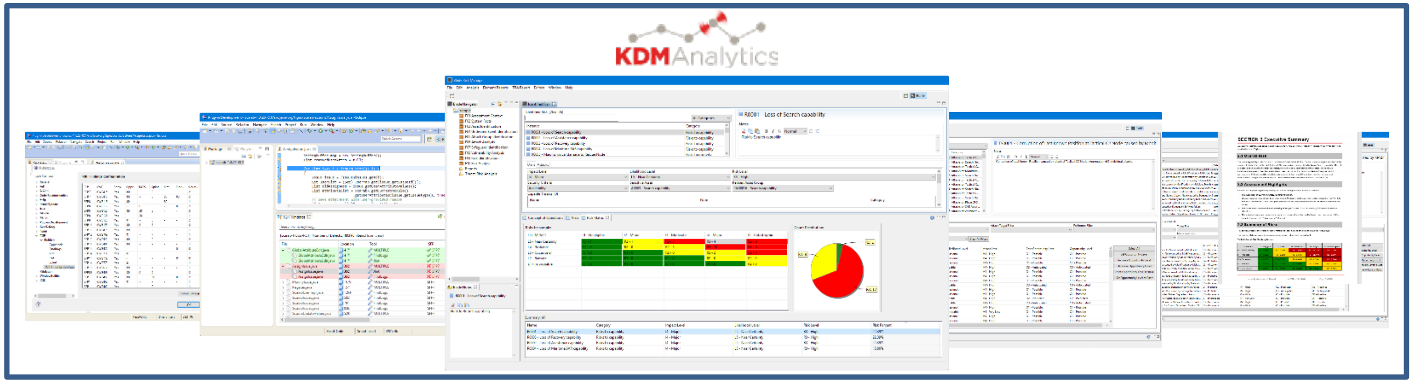
CONOPS



Cybersecurity Knowledge

- National Vulnerability Database
- Compliance Specifications
- Fault Patterns
- Code Security Defects
- Threat-Risk Analysis models

Software System



Threat Risk Analysis Reports

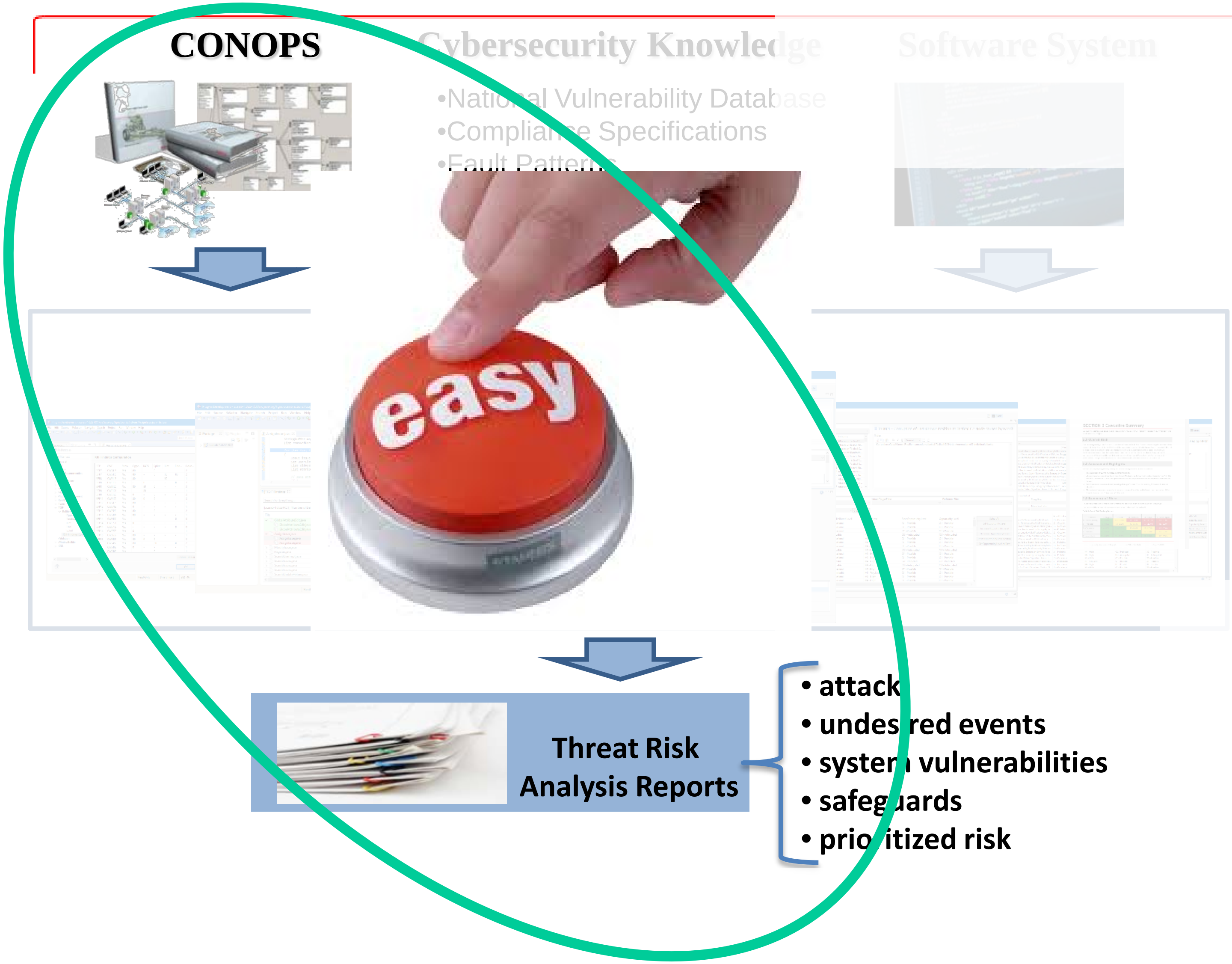
- **attack**
- **undesired events**
- **system vulnerabilities**
- **safeguards**
- **prioritized risk**

A top-down, automated operational risk analysis including multi-stage attack analysis producing a quantitative risk report, including risk distribution by component, business assets and threats; associated vulnerability characteristics

A bottom-up, targeted vulnerability analysis producing a quantitative residual risk focused on deep analysis of the riskiest components identified/prioritized in the top-down risk report

Effective measurement, prioritization and mediation of the assurance risks posed by system vulnerabilities

Automated top-down risk assessment


CONOPS
Cybersecurity Knowledge
•National Vulnerability Database
•Compliance Specifications
•Fault Patterns
Software System
easy
Threat Risk Analysis Reports

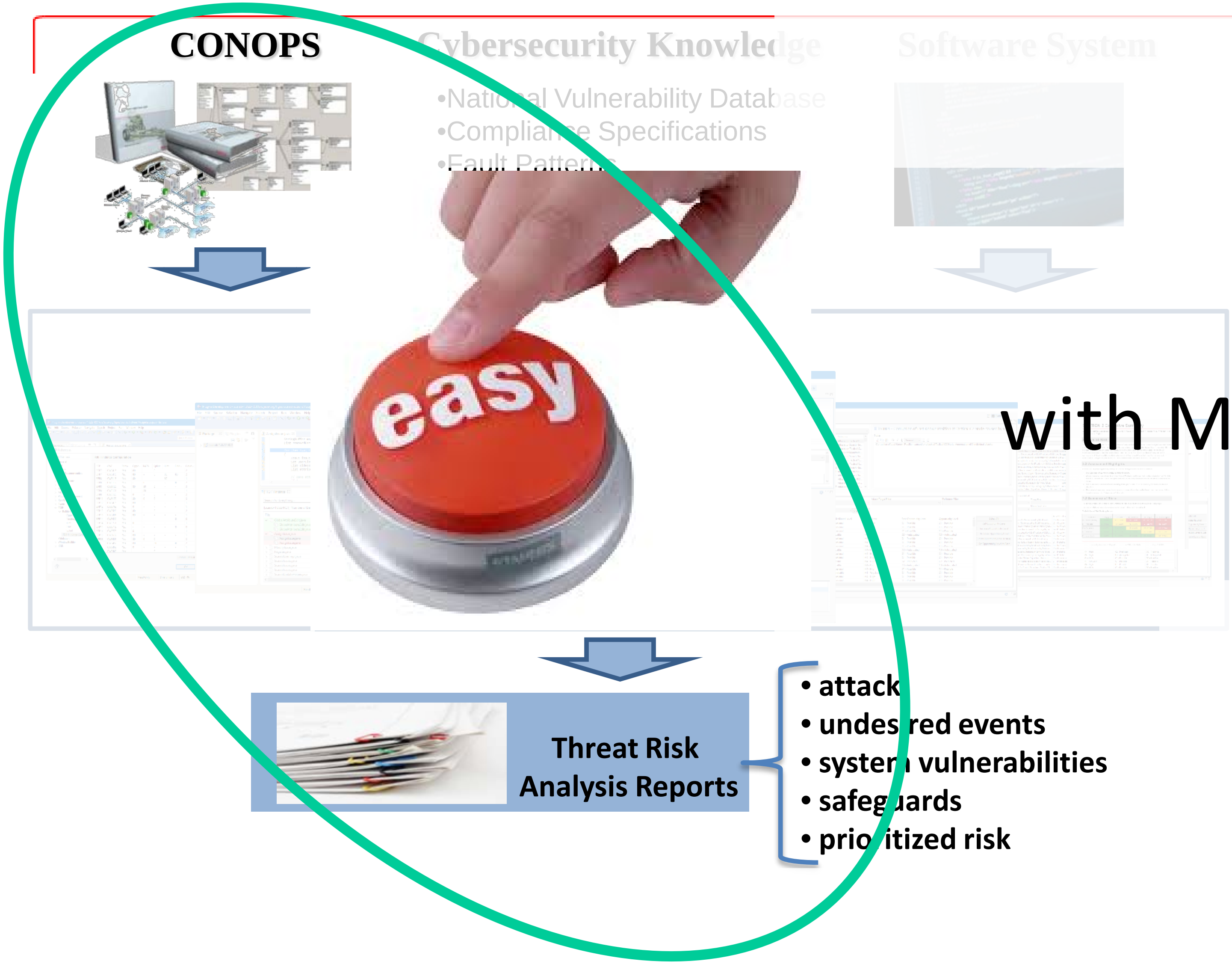
- attack
- undesired events
- system vulnerabilities
- safeguards
- prioritized risk

Collection of facts

A top-down, automated operational risk analysis including multi-stage attack analysis producing a quantitative risk report, including risk distribution by component, business assets and threats; associated vulnerability characteristics

A bottom-up, targeted vulnerability analysis producing a quantitative residual risk focused on deep analysis of the riskiest components identified/prioritized in the top-down risk report

Easy – with MBCA



- National Vulnerability Database
- Compliance Specifications
- Fault Patterns

Threat Risk Analysis Reports

- attack
- undesired events
- system vulnerabilities
- safeguards
- prioritized risk

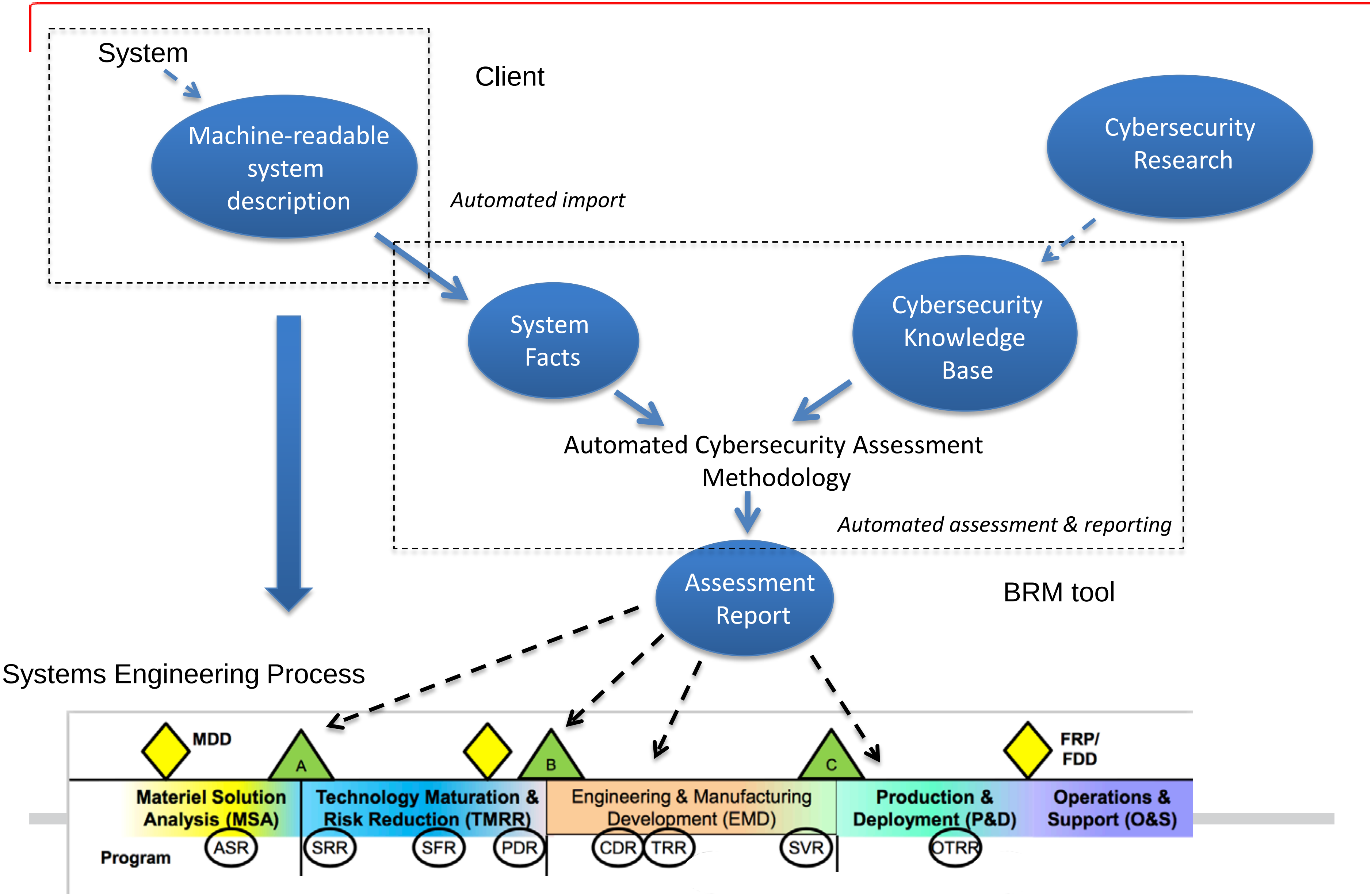
with MBCA

Collection of facts

A top-down, automated operational risk analysis including multi-stage attack analysis producing a quantitative risk report, including risk distribution by component, business assets and threats; associated vulnerability characteristics

A bottom-up, targeted vulnerability analysis producing a quantitative residual risk focused on deep analysis of the riskiest components identified/prioritized in the top-down risk report

Model-Based Cybersecurity Assessment



System

Machine-readable system description

Client

Cybersecurity Research

Automated import

System Facts

Cybersecurity Knowledge Base

Automated Cybersecurity Assessment Methodology

Automated assessment & reporting

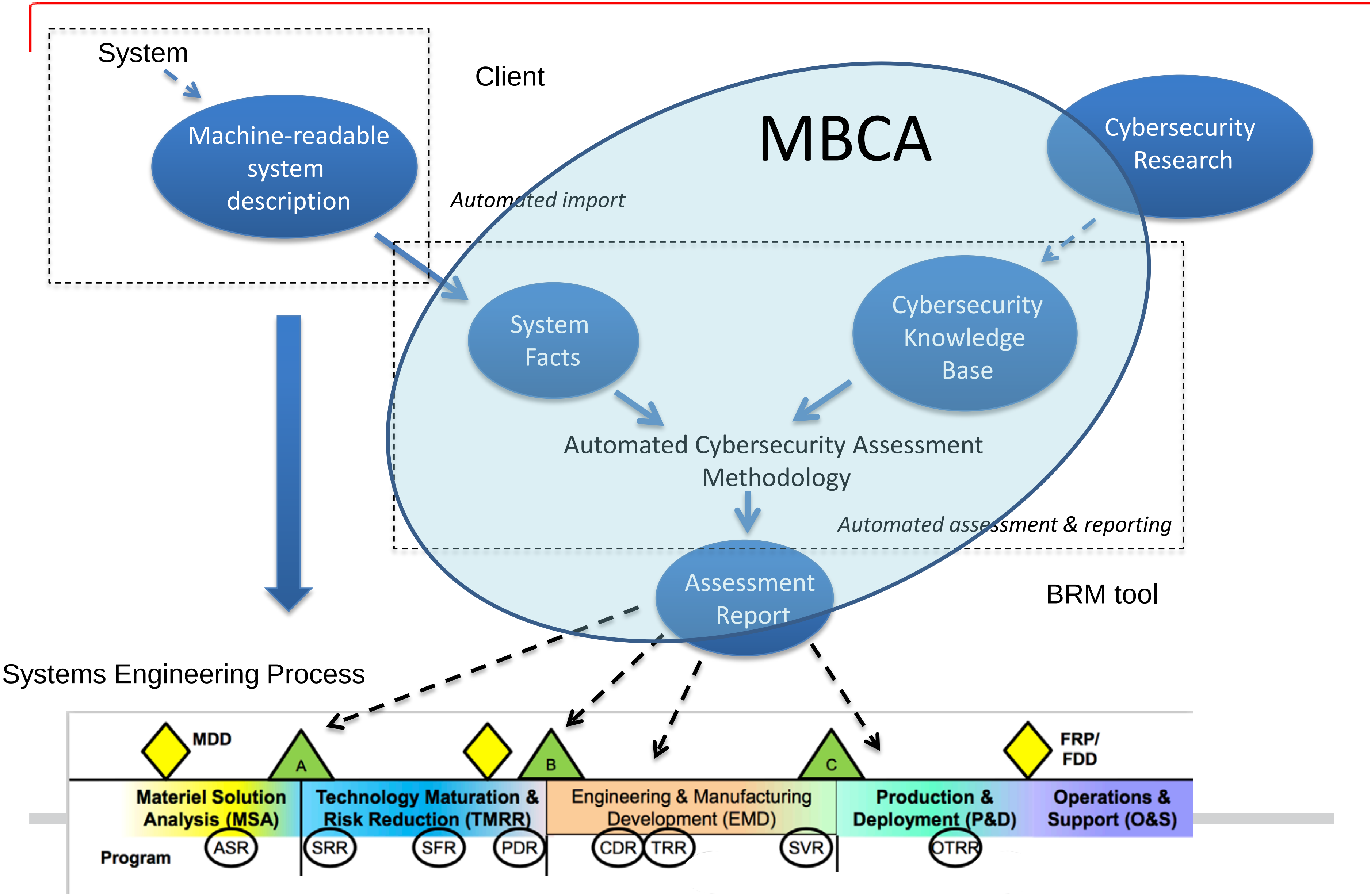
Assessment Report

BRM tool

Systems Engineering Process

MDD
A
B
C
FRP/ FDD
Materiel Solution Analysis (MSA)
Technology Maturation & Risk Reduction (TMRR)
Engineering & Manufacturing Development (EMD)
Production & Deployment (P&D)
Operations & Support (O&S)
Program
ASR
SRR
SFR
PDR
CDR
TRR
SVR
OTRR

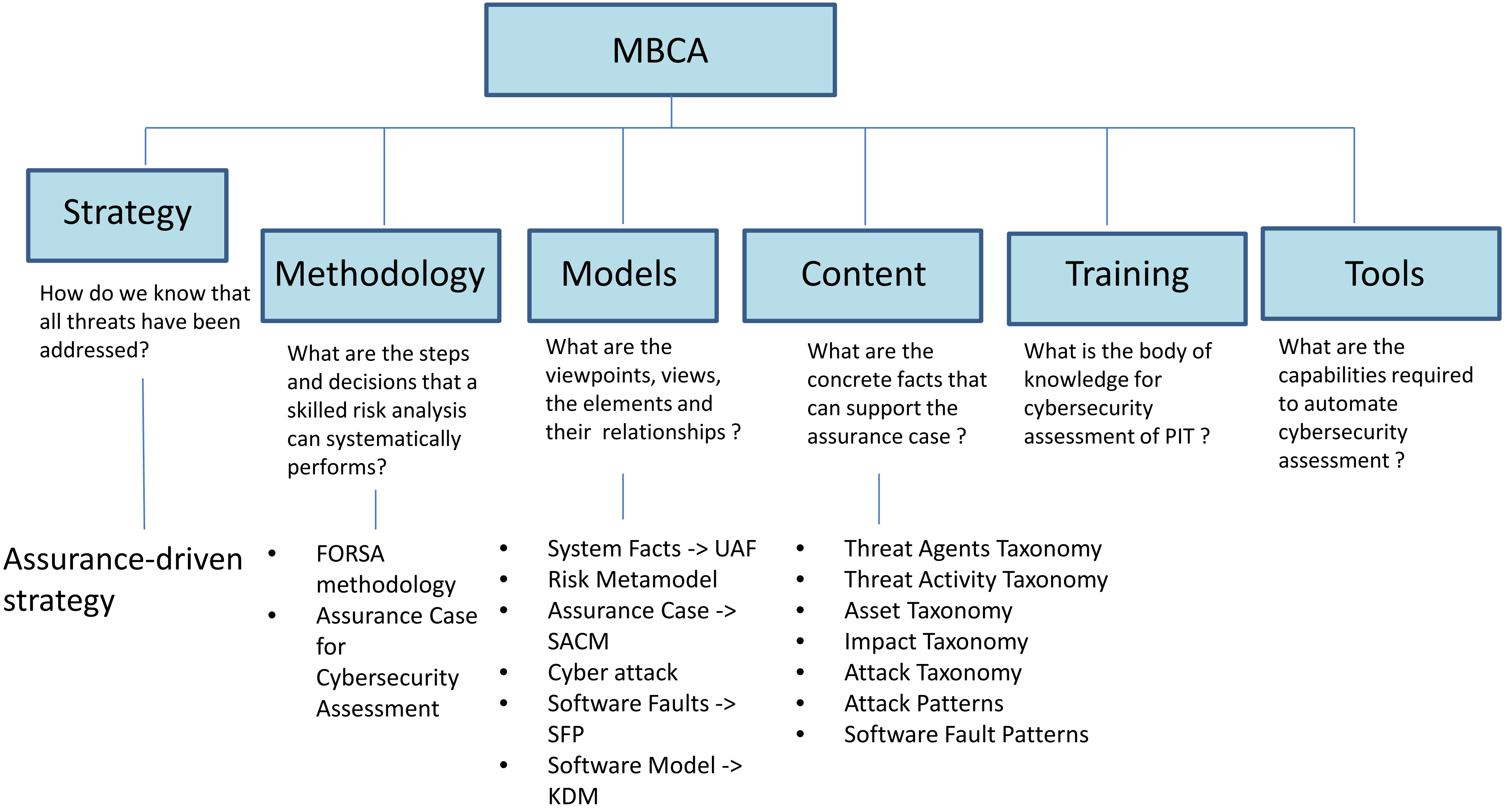
Model-Based Cybersecurity Assessment


System
Machine-readable system description
Client
MBCA
Cybersecurity Research
Automated import
System Facts
Cybersecurity Knowledge Base
Automated Cybersecurity Assessment Methodology
Automated assessment & reporting
Assessment Report
BRM tool
Systems Engineering Process
MDD
A
B
C
FRP/ FDD
Materiel Solution Analysis (MSA)
Technology Maturation & Risk Reduction (TMRR)
Engineering & Manufacturing Development (EMD)
Production & Deployment (P&D)
Operations & Support (O&S)
Program
ASR
SRR
SFR
PDR
CDR
TRR
SVR
OTRR

Why model?

- Benefits of a model-based approach:
  - Adapt to various input formats
  - Adapt to various reporting formats
  - Adapt to cybersecurity content
  - Separate analytics from system facts
  - Foundation for inferences
  - Link to internal assurance case

Components of MBCA



MBCA

Strategy

How do we know that all threats have been addressed?

Assurance-driven strategy

Methodology

What are the steps and decisions that a skilled risk analysis can systematically performs?

- FORSA methodology
- Assurance Case for Cybersecurity Assessment

Models

What are the viewpoints, views, the elements and their relationships ?

- System Facts -> UAF
- Risk Metamodel
- Assurance Case -> SACM
- Cyber attack
- Software Faults -> SFP
- Software Model -> KDM

Content

What are the concrete facts that can support the assurance case ?

- Threat Agents Taxonomy
- Threat Activity Taxonomy
- Asset Taxonomy
- Impact Taxonomy
- Attack Taxonomy
- Attack Patterns
- Software Fault Patterns

Training

What is the body of knowledge for cybersecurity assessment of PIT ?

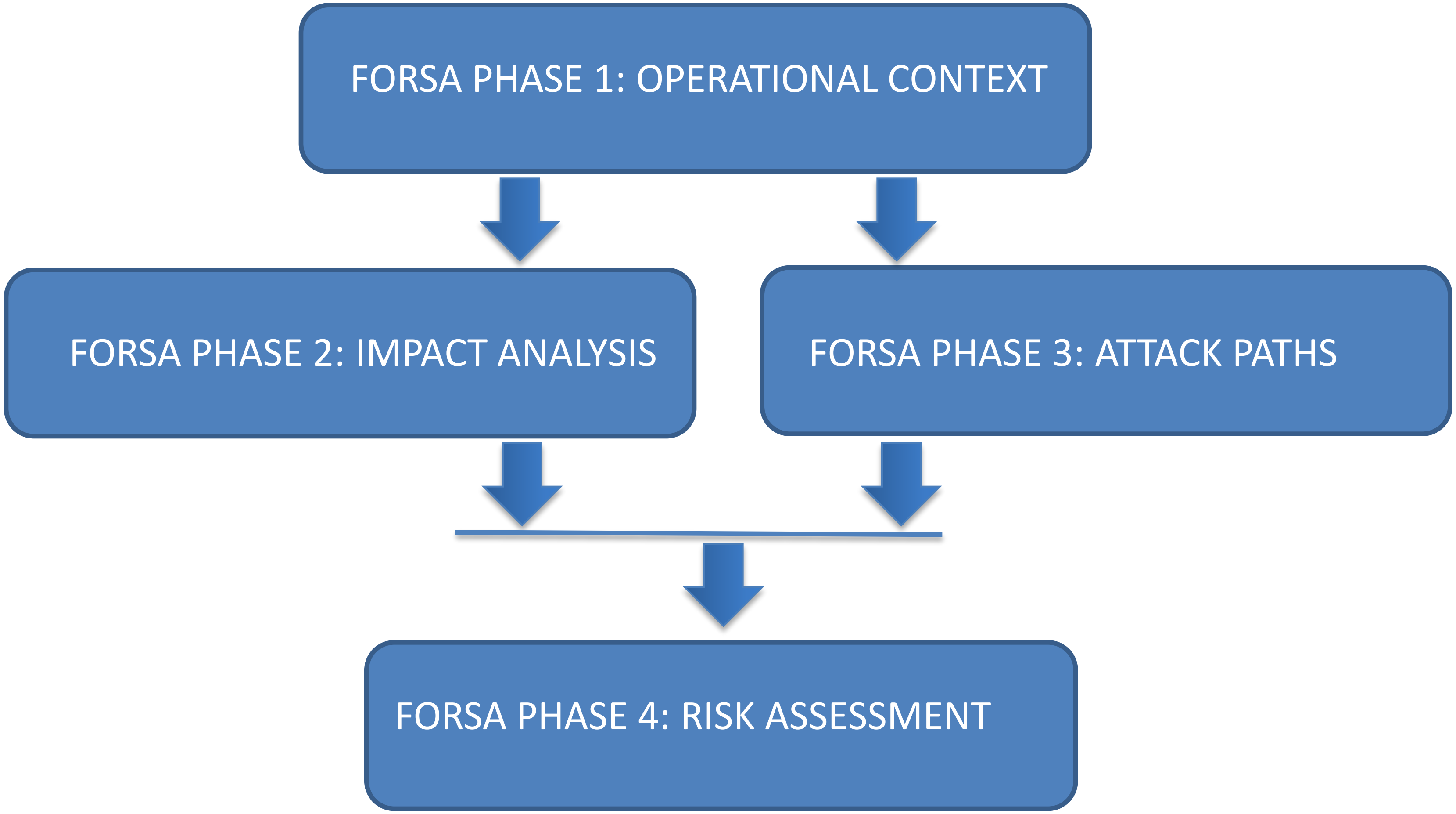
Tools

What are the capabilities required to automate cybersecurity assessment ?

Why new strategy?

- Because if the strategy does not guarantee that all threats have been addressed, the resulting process is not systematic and repeatable, relies on human expertize/brainstorming, and can not be automated
- Traditional Strategies
  - Historically: compliance-based
    - Risk assessment, but not cybersecurity assessment
  - Popular: Vulnerability-based using software tools
  - Threat-based
  - Entry-point based
  - NIST
    - Asset-based
    - Impact-based
    - Threat-based
- Assurance-based strategy
  - Perform steps in the order that maximizes assurance
  - Provide internal assurance case
  - Addresses the key question: how do we know that all threats have been addressed

Overview of the FORSA methodology



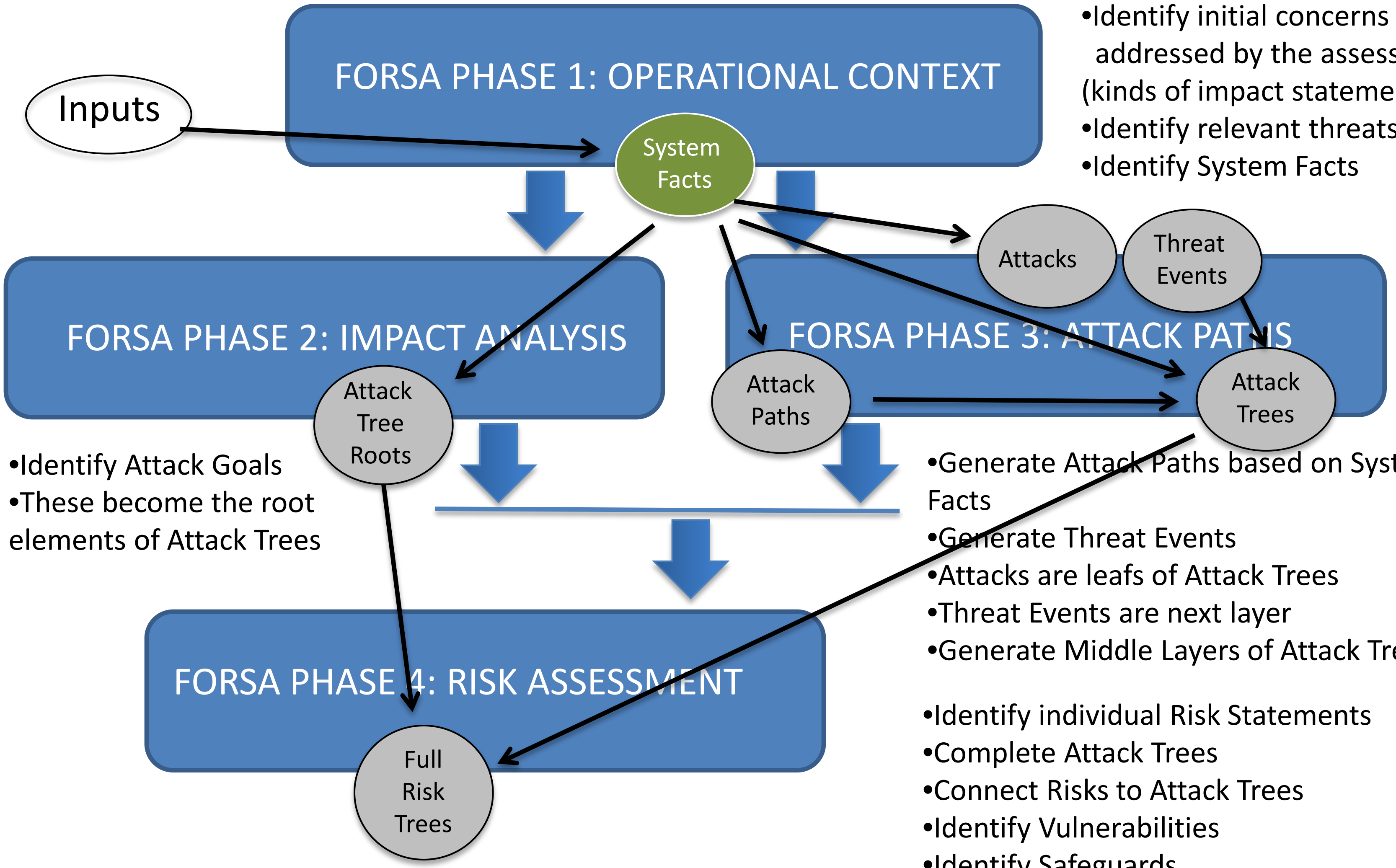
FORSA PHASE 1: OPERATIONAL CONTEXT

FORSA PHASE 2: IMPACT ANALYSIS

FORSA PHASE 3: ATTACK PATHS

FORSA PHASE 4: RISK ASSESSMENT

Overview of the FORSA methodology



Inputs

FORSA PHASE 1: OPERATIONAL CONTEXT

System Facts

- Identify initial concerns to be addressed by the assessment (kinds of impact statements);
- Identify relevant threats;
- Identify System Facts

Attacks

Threat Events

FORSA PHASE 2: IMPACT ANALYSIS

Attack Tree Roots

- Identify Attack Goals
- These become the root elements of Attack Trees

FORSA PHASE 3: ATTACK PATHS

Attack Paths

Attack Trees

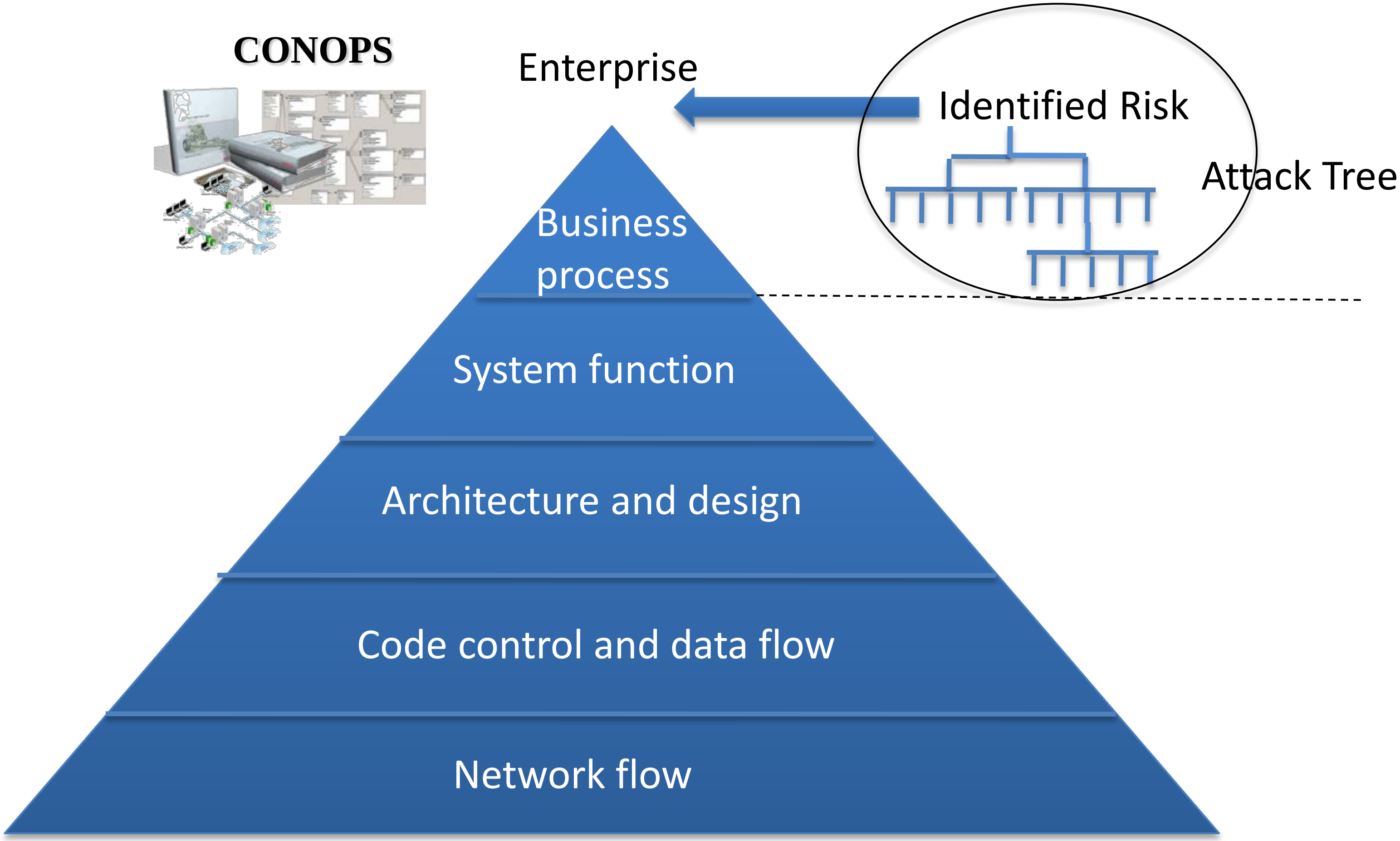
- Generate Attack Paths based on System Facts
- Generate Threat Events
- Attacks are leafs of Attack Trees
- Threat Events are next layer
- Generate Middle Layers of Attack Trees

FORSA PHASE 4: RISK ASSESSMENT

Full Risk Trees

- Identify individual Risk Statements
- Complete Attack Trees
- Connect Risks to Attack Trees
- Identify Vulnerabilities
- Identify Safeguards

Key model: Attack Tree



CONOPS

Enterprise

Identified Risk

Attack Tree

Business process

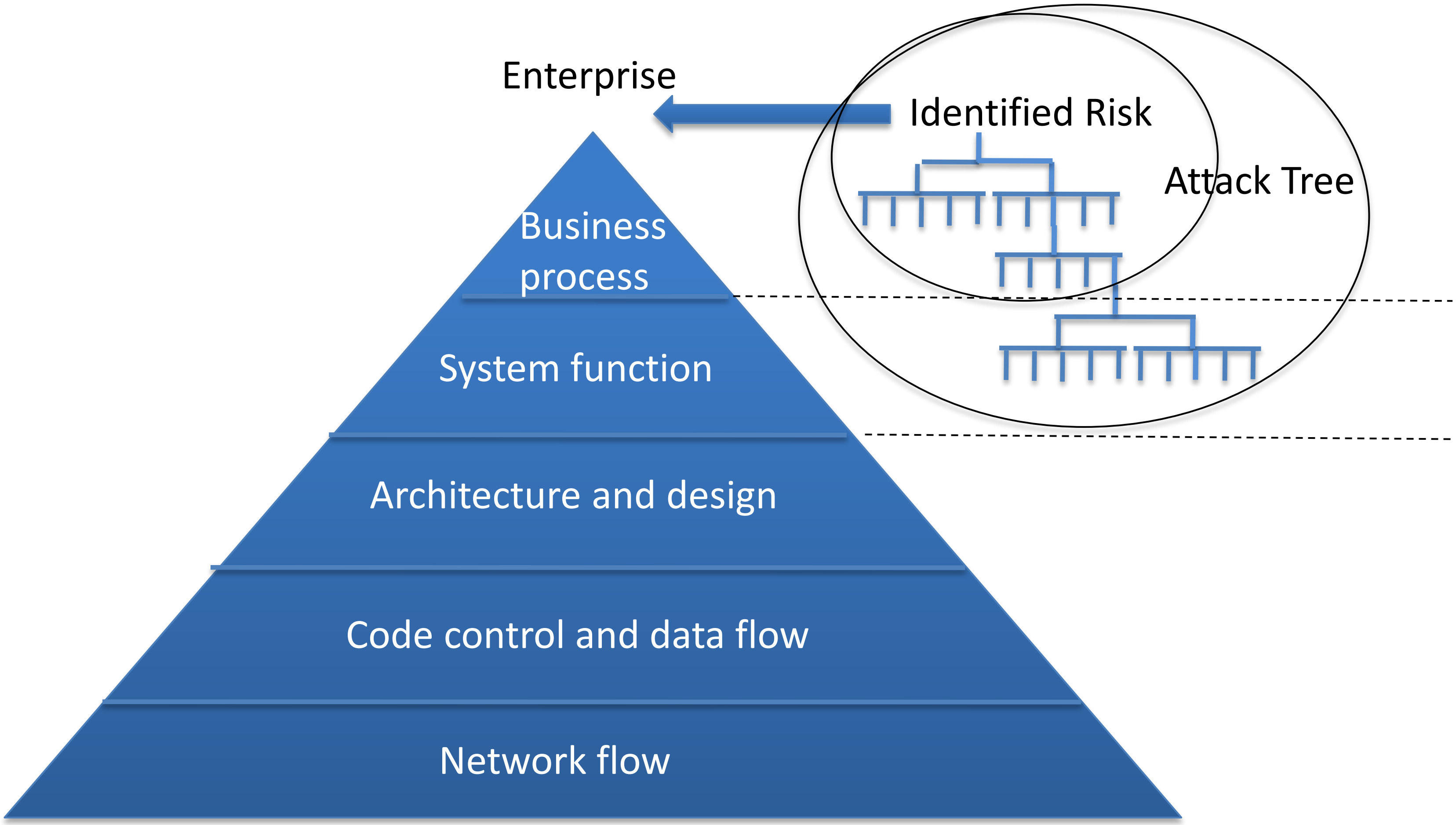
System function

Architecture and design

Code control and data flow

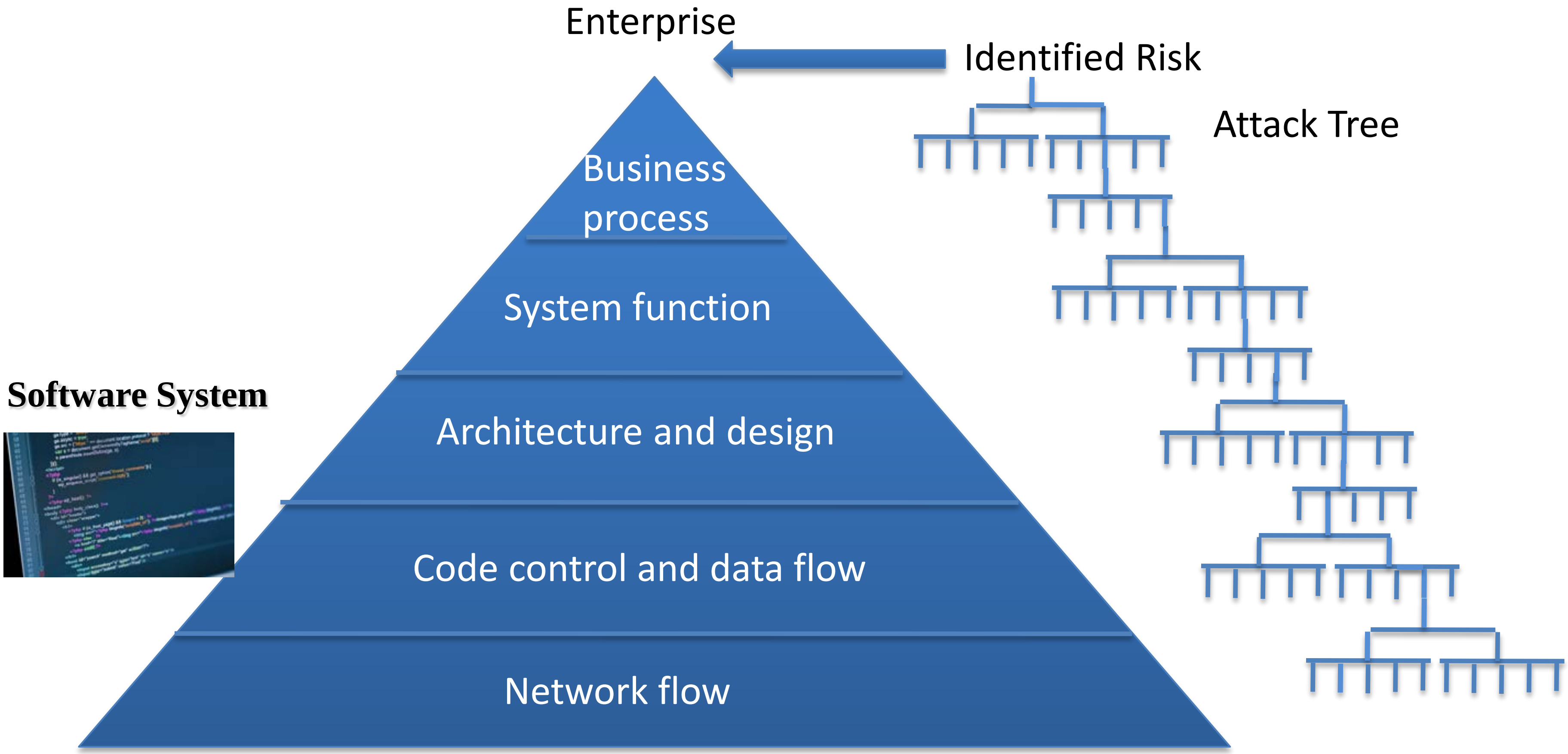
Network flow

Attack Tree can be seamlessly extended

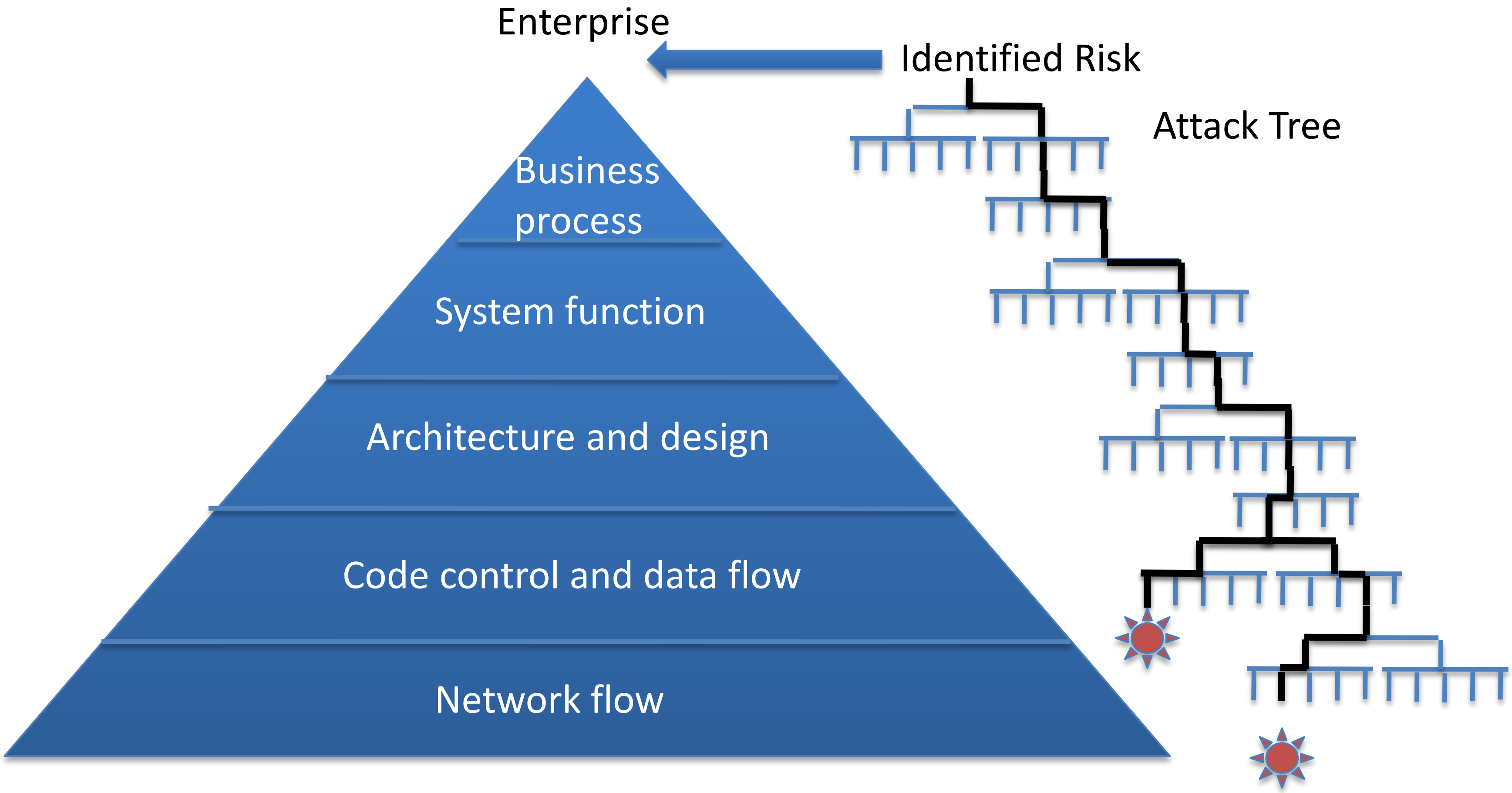


KDMAnalytics

All the way down to the implementation

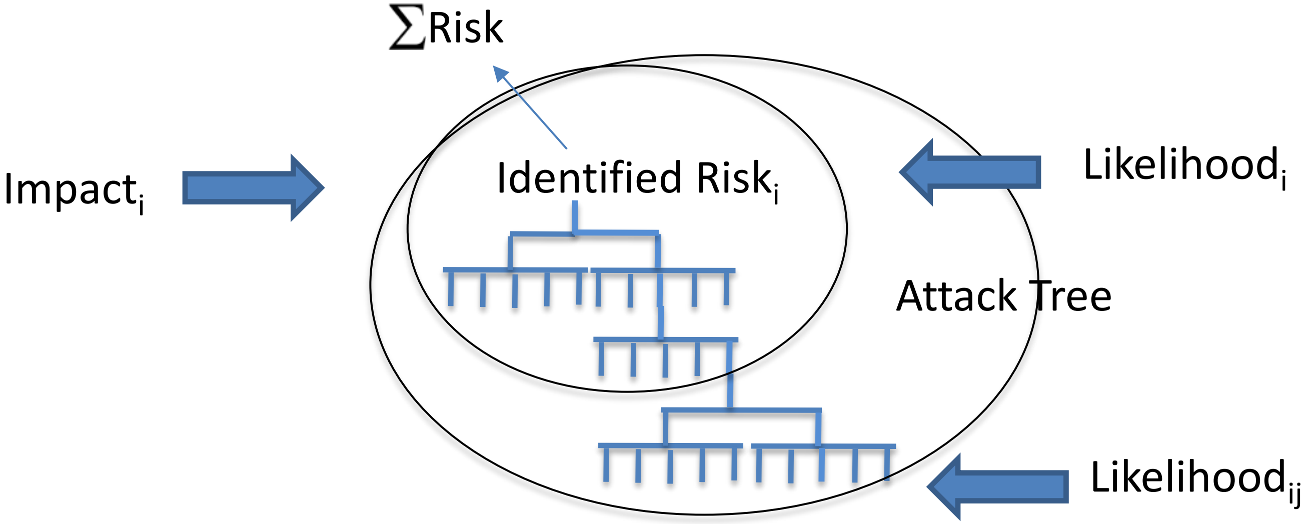


So that vulnerability findings can be traced to identified risks

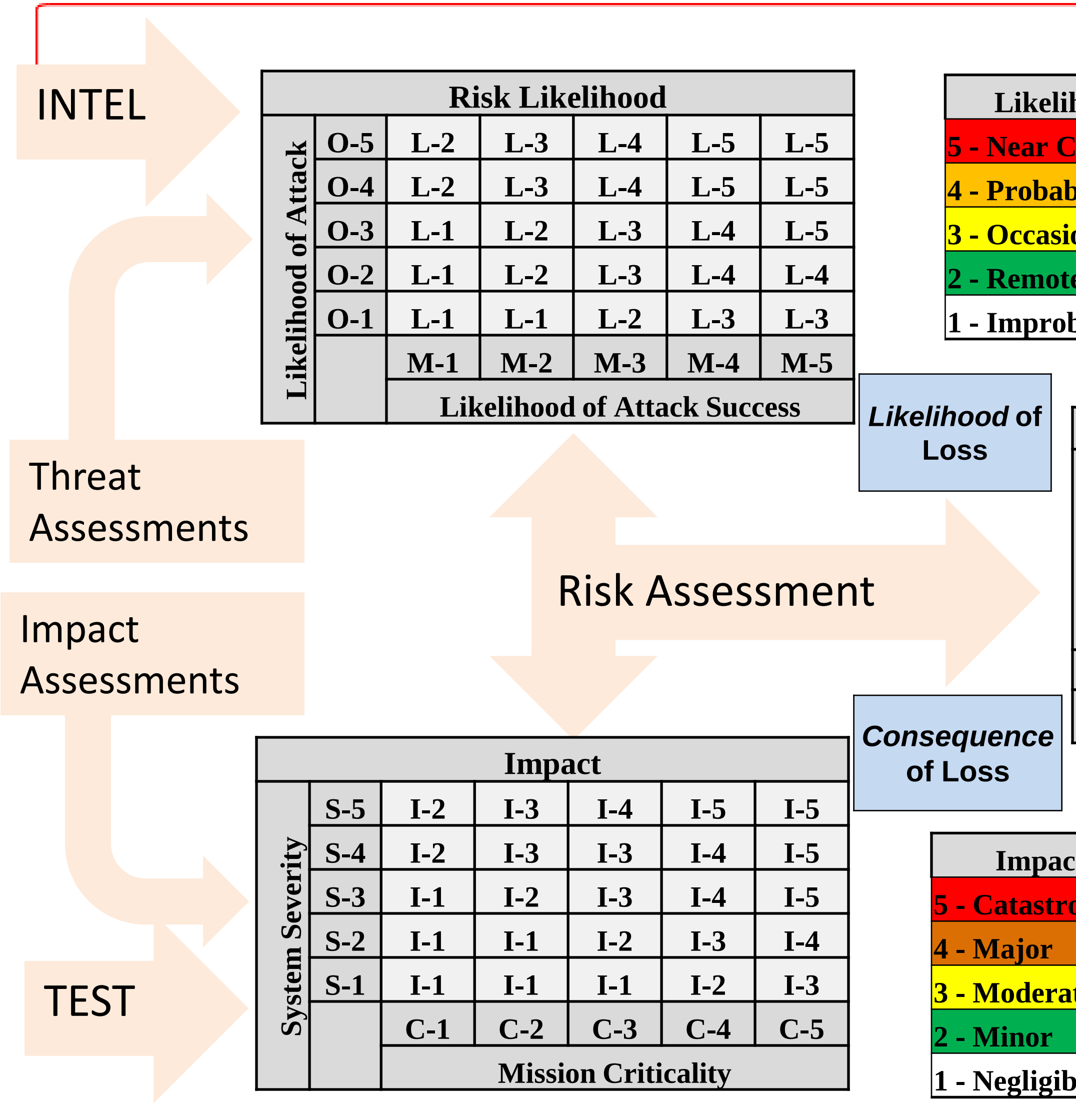


Attack Tree is used to calculate risk

$$\textbf{Risk} = \sum_{i \text{ in Enumeration Strategy}} \textbf{Risk}_i \quad \text{where } \textbf{Risk}_i = \textbf{Impact}_i \times \textbf{Likelihood}_i$$



5x5 risk calculation schema



Risk Likelihood

Likelihood of Attack					
O-5	L-2	L-3	L-4	L-5	L-5
O-4	L-2	L-3	L-4	L-5	L-5
O-3	L-1	L-2	L-3	L-4	L-5
O-2	L-1	L-2	L-3	L-4	L-4
O-1	L-1	L-1	L-2	L-3	L-3
	M-1	M-2	M-3	M-4	M-5
	Likelihood of Attack Success				

Impact

System Severity					
S-5	I-2	I-3	I-4	I-5	I-5
S-4	I-2	I-3	I-3	I-4	I-5
S-3	I-1	I-2	I-3	I-4	I-5
S-2	I-1	I-1	I-2	I-3	I-4
S-1	I-1	I-1	I-1	I-2	I-3
	C-1	C-2	C-3	C-4	C-5
	Mission Criticality				

Likelihood
🟥 5 - Near Certainty
🟧 4 - Probable
🟨 3 - Occasional
🟩 2 - Remote
1 - Improbable

Overall Risk Factor Matrix

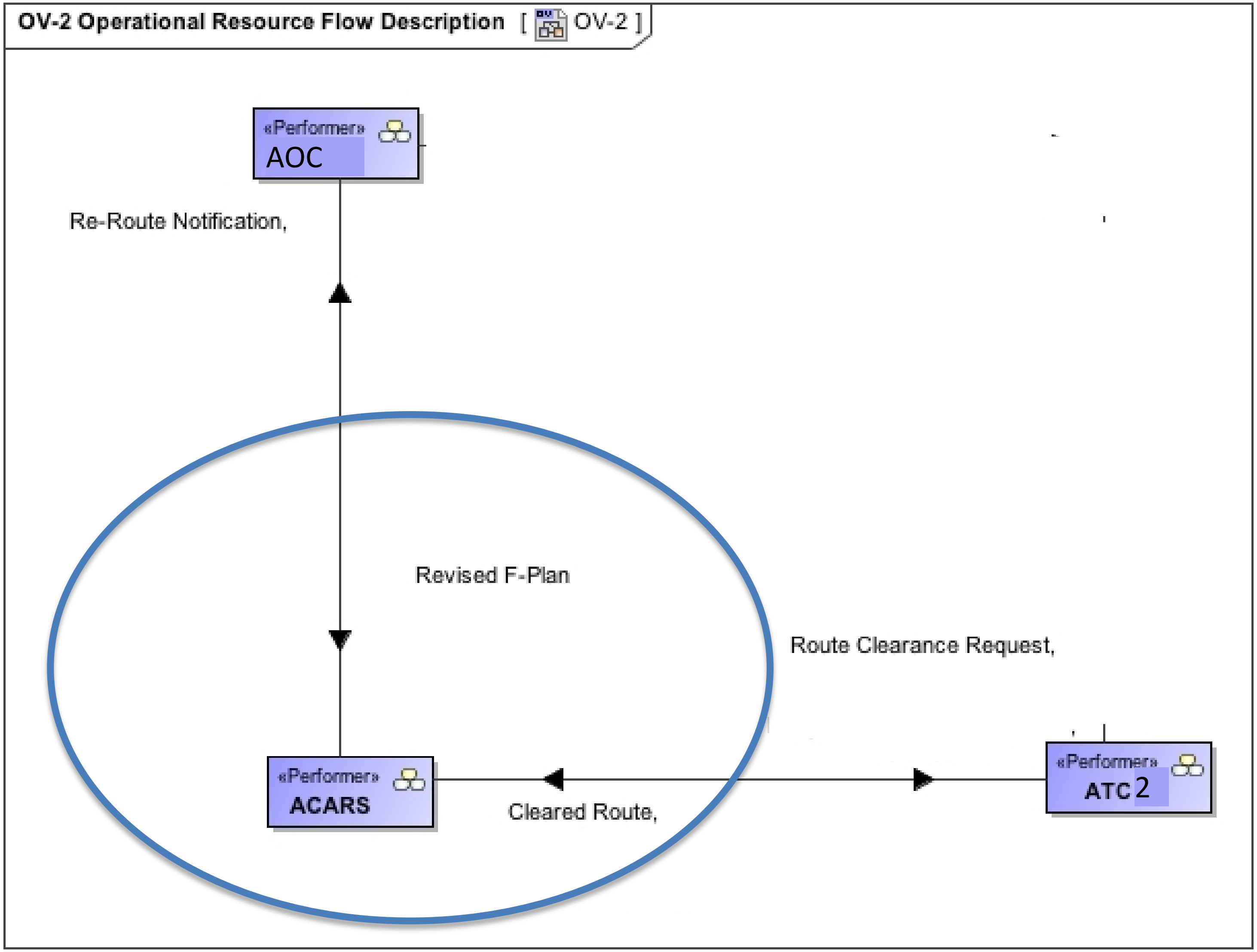
LIKELIHOOD					
L-5	🟩	🟨	🟥	🟥	🟥
L-4	🟩	🟨	🟨	🟥	🟥
L-3	🟩	🟩	🟨	🟨	🟥
L-2	🟩	🟩	🟩	🟨	🟨
L-1	🟩	🟩	🟩	🟩	🟨
	I-1	I-2	I-3	I-4	I-5
	IMPACT				

Impact
🟥 5 - Catastrophic
🟧 4 - Major
🟨 3 - Moderate
🟩 2 - Minor
1 - Negligible

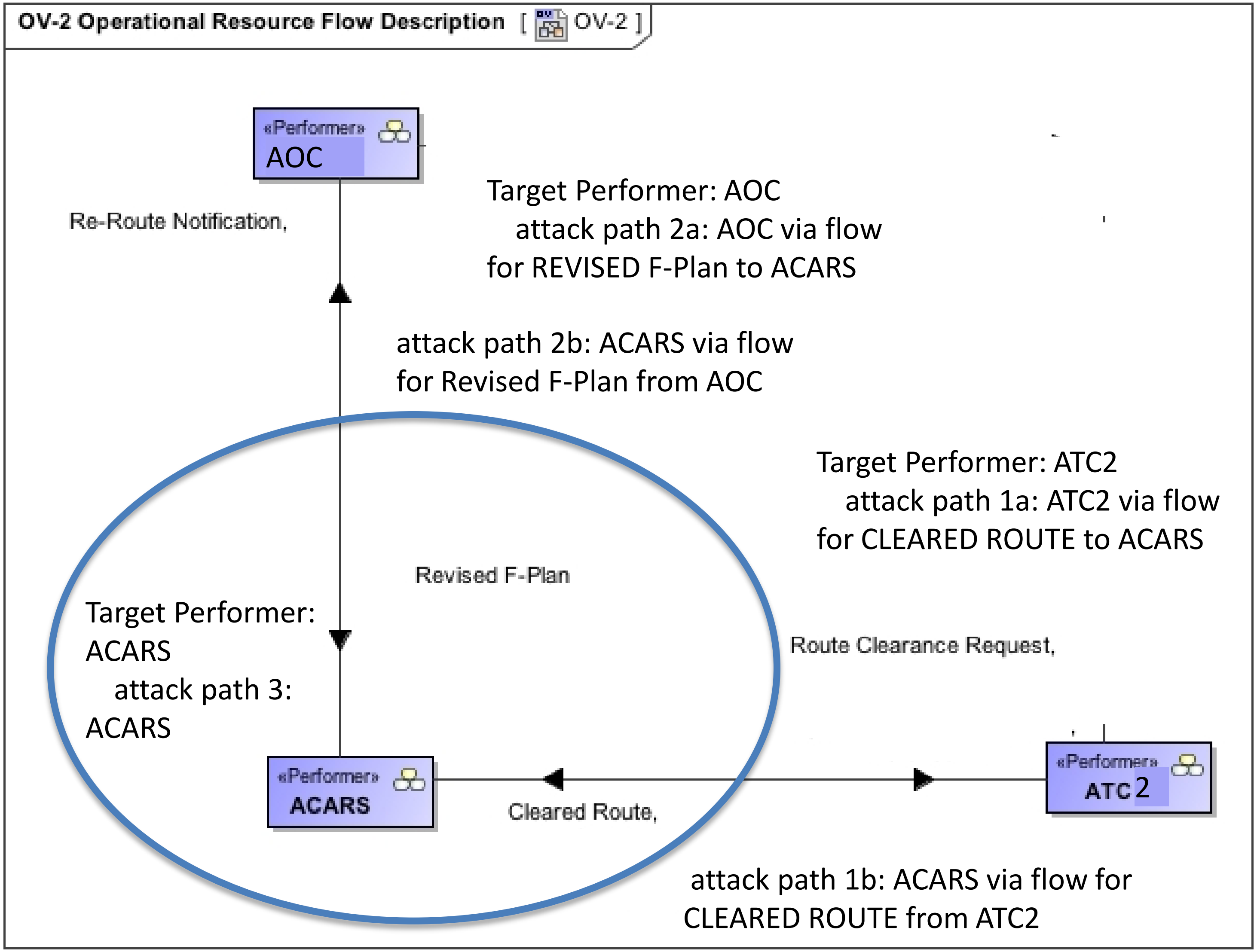
Risk
🟥 High
🟧 Moderate
🟩 Low

Derived from:
NIST 800-30 Risk Assessment
DOD Risk Management Guide

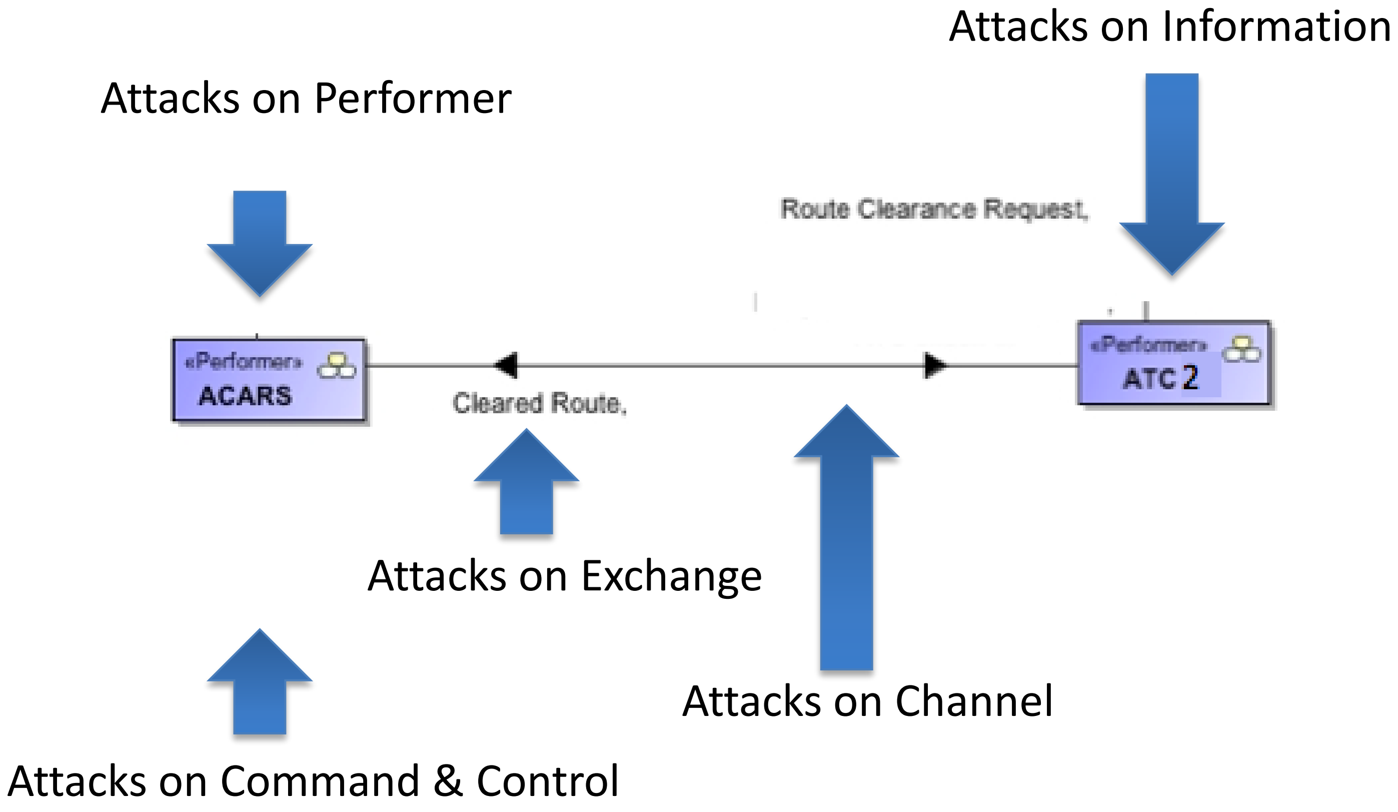
OV-2 with system boundary



Identified 5 basic Attack Paths


OV-2 Operational Resource Flow Description [OV-2]
«Performer»
AOC
Re-Route Notification,
Target Performer: AOC
attack path 2a: AOC via flow for REVISED F-Plan to ACARS
attack path 2b: ACARS via flow for Revised F-Plan from AOC
Target Performer: ATC2
attack path 1a: ATC2 via flow for CLEARED ROUTE to ACARS
Revised F-Plan
Target Performer: ACARS
attack path 3: ACARS
Route Clearance Request,
«Performer»
ACARS
Cleared Route,
«Performer»
ATC 2
attack path 1b: ACARS via flow for CLEARED ROUTE from ATC2

Attack Category



Attacks on Information

Attacks on Performer

Attacks on Exchange

Attacks on Channel

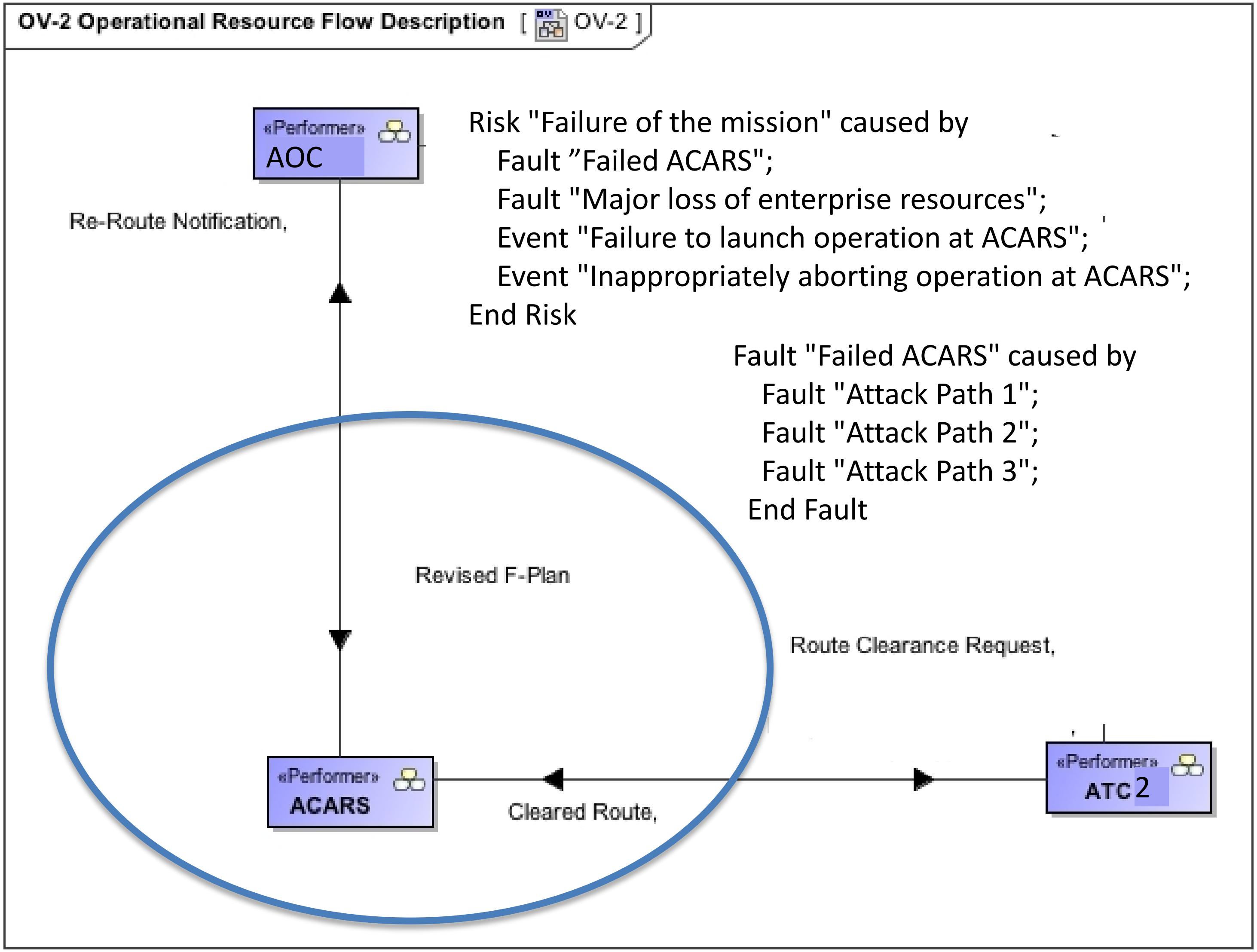
Attacks on Command & Control

Full "attack space" has multiple dimensions

- "Dimensions" of the attack space:
  - Attack category
  - Internal/External
  - Cyber/Physical
  - Attack mode
- This gives us 5x2x2x6=120 cells

- Attack Tree- A branching, hierarchical data structure that represents a set of potential approaches to achieving an event in which system security is penetrated or compromised in a specified way (CNSSI 4009)
  - A complete collection of a systems attack paths.

Sample Identified Risk



Risk "Failure of the mission" caused by
Fault ”Failed ACARS";
Fault "Major loss of enterprise resources";
Event "Failure to launch operation at ACARS";
Event "Inappropriately aborting operation at ACARS";
End Risk

Fault "Failed ACARS" caused by
Fault "Attack Path 1";
Fault "Attack Path 2";
Fault "Attack Path 3";
End Fault

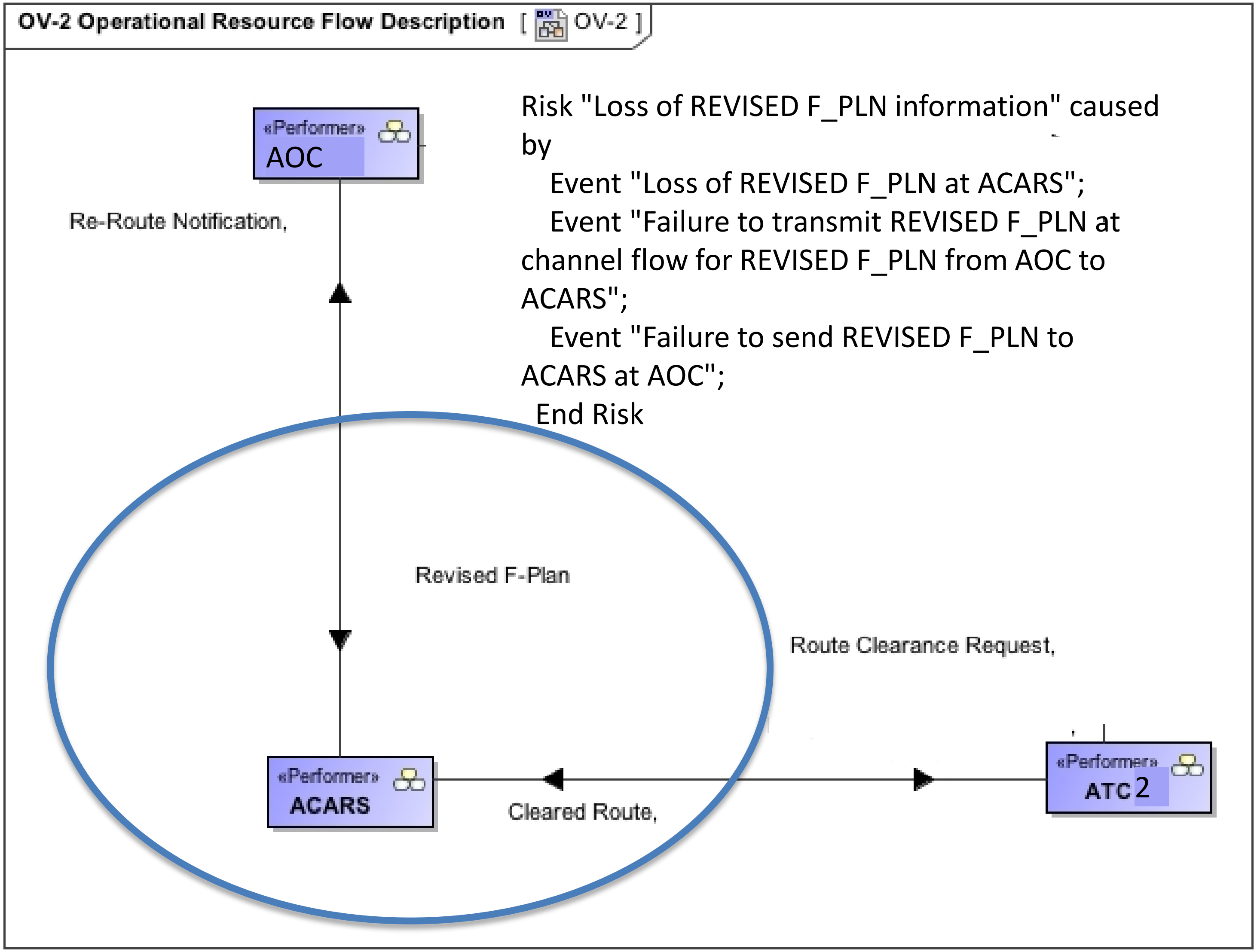
Multi-stage attacks for ACARS

```
Fault "Attack Path 1" caused by
  Event "Sending inappropriate CLEARED ROUTE to ACARS at ATC2",
    Condition "Multi-stage attack on ACARS causes mission failure";
  Event "Sending fake CLEARED ROUTE at channel flow for CLEARED ROUTE from ATC2 to ACARS",
    Condition "Multi-stage attack on ACARS causes mission failure";
 End Fault

 Fault "Attack Path 2" caused by
  Event "Sending inappropriate REVISED F_PLN to ACARS at AOC",
    Condition "Multi-stage attack on ACARS causes mission failure";
  Event "Sending fake REVISED F_PLN at channel flow for REVISED F_PLN from AOC to ACARS",
    Condition "Multi-stage attack on ACARS causes mission failure";
 End Fault

Fault "Attack Path 3" caused by
  Event "Major failure at ACARS",
    Condition "Major failure at ACARS causes mission failure";
  Event "Failure to perform activity at ACARS",
    Condition "Operational failure at ACARS causes mission failure";
 End Fault
```

Another Identified Risk



Risk "Loss of REVISED F_PLN information" caused by

Event "Loss of REVISED F_PLN at ACARS";

Event "Failure to transmit REVISED F_PLN at channel flow for REVISED F_PLN from AOC to ACARS";

Event "Failure to send REVISED F_PLN to ACARS at AOC";

End Risk

KDMAnalytics

Prioritize, Measure and Quantify Cyber Security Risk

Questions ?