International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(03 November 2020)

XSTR-USM
Unified security model (USM) – A neutral integrated system approach to cybersecurity

Summary

This Technical Report serves as a one-stop live document to regroup all the related work conducted on a neutral integrated approach to cybersecurity called the unified security model.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Keywords

Evaluation criteria, residual risk, risk, risk management.

Table of Contents

Technical Report ITU-T XSTR-USM

Unified security model (USM) – A neutral integrated system approach to cybersecurity

1 Background

The total global economy in 2018 was estimated to be $86 Trillion[1]. As of June 2019, it is estimated[2] that there are 4,536,248,808 people connected to the Internet. The Internet has spread to 58.8% of a population of 7,716,223,209. The Global Risks Report 2019[3] outlines the greatest risks facing the world, listing cyber threats as the fourth most significant societal risk in terms of severity of impact. As the world accelerates into the Fourth Industrial Revolution, according to the ITU Global Cybersecurity Index 2018 [4], 73% of the Internet connected world today is unprotected while the remaining 27%, who think they are protected, spend 80% of the global security spending, estimated to be $300B by 2023[5].

2 The problem and solution approach

In the simplest of terms, the problem is communication and what it takes to convey security in unique and unambiguous ways across a heterogenous global environment. In order to communicate one has to articulate what is to be communicated,and that is where the problem begins. The "what" to be communicated in this case is "all matters security," defined as all significant data, information and knowledge contained about relationships between targets, threats, and countermeasures. The "what" is vast, heterogenous, fragmented, and non-interoperable making it very complex and costly to track and manage. In most cases, eliminating all of the risks is neither possible nor necessary. Thus, the objective of risk management is to reduce risks to an acceptable level for the owner.

Most of the security knowledge outside of the brains of experts is predominantly in worded form contained in structured and unstructured files organized in lists and frameworks, a form difficult to consume by humans. The work is being done by all individually and separately in pockets, and redoing the work again and again, never demanding better.

The sheer number of potential targets, methods of exploitation unique to the vulnerability of each target, and countermeasures against each is far beyond the human ability to track and associate using current methods and tools; let alone manage, demonstrate compliance or contribute to an active incident response. All those matters are urgent ones that should have been addressed in the past.

The ability to detect and identify attack patterns applicable to a potential specific target and quickly access effective countermeasure patterns is essential to protection. Current visibility limitations and difficulty in connecting the dots in real time makes this impossible. This temporal chasm must be closed. Managers and practitioners must have quick, easy and persistent access to a single truth of situational awareness over the state of a complex set of relationships between target elements of the network performing business functions; others performing security functions; threat vectors and how all this fulfils control compliance requirements.

[1] The $86 Trillion World Economy in one chart, https://howmuch.net/articles/the-world-economy-2018

[2] June 2019 World Internet Usage & Population Statistics https://www.internetworldstats.com/stats.htm

[3] http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[4] Global Cybersecurity Index (GCI) 2018 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[5] https://www.gminsights.com/pressrelease/cyber-security-market

The unified security model and architecture presented here is a universal "all matters security" architecture, that is neutral and agnostic. It has the potential to facilitate security control mass interoperability and security response automation.

3 Definitions

This Technical Report uses the following terms defined elsewere:

3.1 **risk** [b-ISO 31000]: Effect of uncertainty on objectives.

NOTE 1 – An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.

NOTE 2 – Objectives can have different aspects and categories, and can be applied at different levels.

NOTE 3 – Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

3.2 **risk management** [b-ISO 31000]: Coordinated activities to direct and control an organization with regard to risk.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AS	Attack Surface
CAPEC	Common Attack Pattern Enumeration and Classification
CP	Certification Profile
CCP	Compliance and Certification Profile
DV	Digital Value
EC	External Control
IC	Internal Control
SA	Security Asset
SAP	Security Asset Profile
SPP	Security Policy Profile
TP	Threat Profile
TV	Threat Vector
USA	Unified Security Architecture
USM	Unified Security Model
VA	Value Asset
VP	Value Process
VP-E	Value Process Ecosystem

5 Unified security model

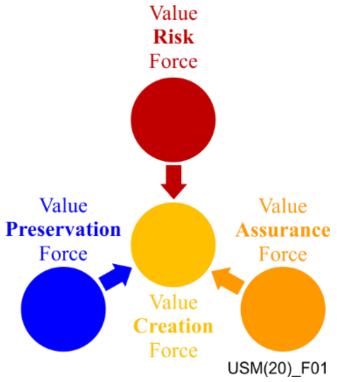


Figure 1 – Digital value forces

As illustrated in Figure 1, the unified security model (USM) is based on four forces that act on digital value (DV), which first must be created, then threatened, then protected with confidence.

The USM forces are colour coded in order to achieve the use of iconography, essential for the ease of comprehension.

- **Value creation force**: At the genesis of the USM in the centre is the value creation force, represented by the colour gold.
- **Value risk force**: Since by nature any value will be threatened, the second is the value risk force, represented by the colour red.
- **Value preservation force**: Since the value is at risk, fiduciary stakeholders fulfil their duty-of-care by investing in security, the third is value preservation force, represented by the colour blue.
- **Value assurance force**: In order to ensure that value is protected and meeting expected norms of risk acceptance, the fourth force is value assurance, represented by the colour orange.

The USM is general enough to allow different residual risk and risk acceptance models to exist. The focus of this Technical Report is on the architecture that would feed the data required to conduct a reliable risk analysis. Selecting the most appropriate controls involves balancing the potential benefits derived in calculation of the value of targeted assets against costs of controls, opportunity of threats, and outcomes of the risk when realized. The residual risks evaluated from the model should be compared with risk owners' acceptable level of risks. Since the implementation of selected controls can also introduce new risks that need to be managed, the procedures might be iterated until the residual risks are accepted by the risk owners.

In addition to the use of colour, the use of shapes is introduced to achieve enhanced simplicity of the expression of activity, as illustrated in Figure 2.

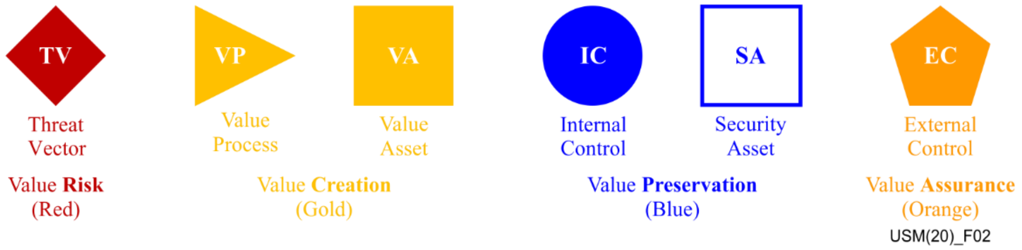


Figure 2 – Digital value force actors

The use of colour coded forces and now shapes taking on those colours allows for the creation of a set of actors each with a very specific role and relationship to each other.

- **Value creation force** is represented by:
  - **Gold triangle**: Value process (VP) that generates value
  - **Gold solid square**: Value asset (VA) enables the value process (VP) to generate value.
- **Value preservation force** is represented by:
  - **Blue circle**: An internal control (IC) defines the full and appropriate security policy objectives to be achieved to provide protection to the value asset (VA).
  - **Blue hollow square**: A security asset (SA) is any process or technology that delivers security value to a value asset (VA).
- **Value risk force** is represented by:
  - **Red diamond**: A threat vector (TV) is a malicious exploit attacking the vulnerability of a value asset. An attack exploit such as those that can be found in the common attack pattern enumeration and classification (CAPEC) (https://capec.mitre.org/).
- **Value assurance force** is represented by:

Orange pentagon: An external control (EC) is a security control that originates from an external authority and is published as either a "Shall" security control to be fulfilled by regulation or is published as a "Should" security control to be fulfilled by a recommended Standard.The USM in Figure 1 is updated in Figure 3 where actors are now engaged in driving their intrinsic force properties.

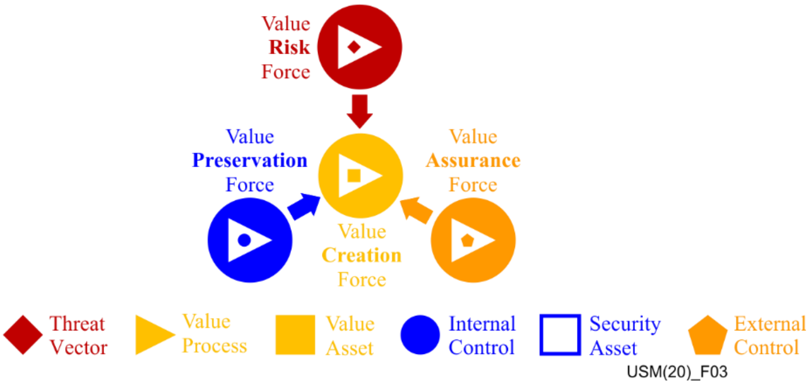


Figure 3 – Digital value force and their actors

6 Unified security architecture

Technically the unified security architecture (USA) is a relationship-based reference architecture that integrates using links "all matters security," including cyber-threats, cyber-targets, cyber-security and cyber-assurance into one unified measurement system. At the centre of the USA is a kernel that acts as a singular and complete "relationship expression" that can model all possible security scenarios by actors.

The kernel illustrated in Figure 4 is referred to as the "*Ruler*" involves six (6) actors engaged in five (5) relationships, each between two (2) actors.

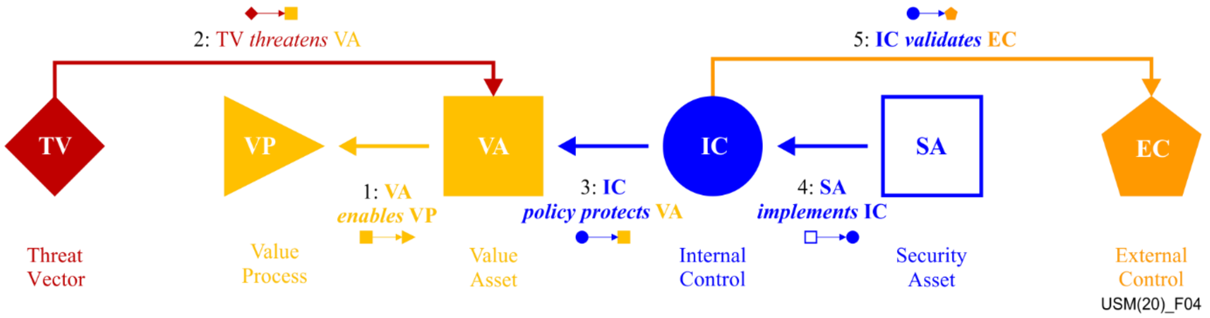
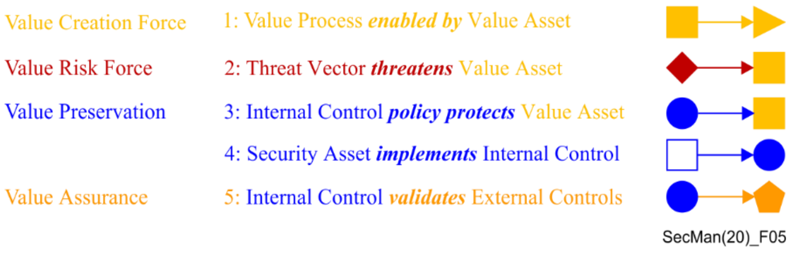


Figure 4 – Digital value force actor role expression

The ruler "reads" as follows, sequentially following the numbers in Figure 4 and starting with the value asset as the starting anchor.

- A value asset **enables** a value process (1). This relationship allows business criticality and data sensitivity to be quantified. How important is the value asset? What is the impact if compromised? The objective is to adequately protect the most critical assets of the most valuable value process in sequential order, starting with the asset with highest exposure, followed by the second highest, and so on.
- Threat vector **threatens** the value asset (2). Likelihood is unique to the value asset's vulnerability and location in the value process network.
- Internal control **policy** **protects** value asset (3). Based on value asset criticality and sensitivity, what security protection is defined by policy and management funding commitment.
- Security assets **implements** internal control (4). People, process and technology collectively referred to as security assets deliver the protection to the value asset.
- Internal controls **validates** external control (5). The justification, artefacts and evidence used to substantiate internal control fulfilment is used to substantiate external control fulfilment.

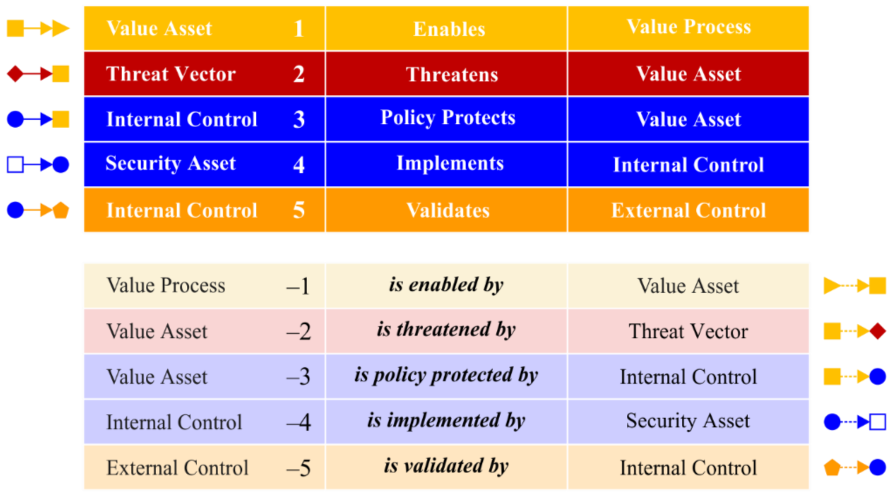
Figure 5 illustrates the visual icon representation of each dual actor role. The icons can now replace words for immediate cognitive recognition.



Value Creation Force	1: Value Process ***enabled by*** Value Asset	■→▶
Value Risk Force	2: Threat Vector ***threatens*** Value Asset	◆→■
Value Preservation	3: Internal Control ***policy protects*** Value Asset	●→■
	4: Security Asset ***implements*** Internal Control	□→●
Value Assurance	5: Internal Control ***validates*** External Controls	●→⬟

Figure 5 – Actor-actor role relationships

The table in Figure 6 provides not only the direct relationship ***tenses*** but also their reverse complements that also exist by default. This is the notion of observing the same relationship from opposite ends.



■→▶	Value Asset	1	Enables	Value Process
◆→■	Threat Vector	2	Threatens	Value Asset
●→■	Internal Control	3	Policy Protects	Value Asset
□→●	Security Asset	4	Implements	Internal Control
●→⬟	Internal Control	5	Validates	External Control

Value Process	–1	*is enabled by*	Value Asset	▶→■
Value Asset	–2	*is threatened by*	Threat Vector	■→◆
Value Asset	–3	*is policy protected by*	Internal Control	■→●
Internal Control	–4	*is implemented by*	Security Asset	●→□
External Control	–5	*is validated by*	Internal Control	⬟→●

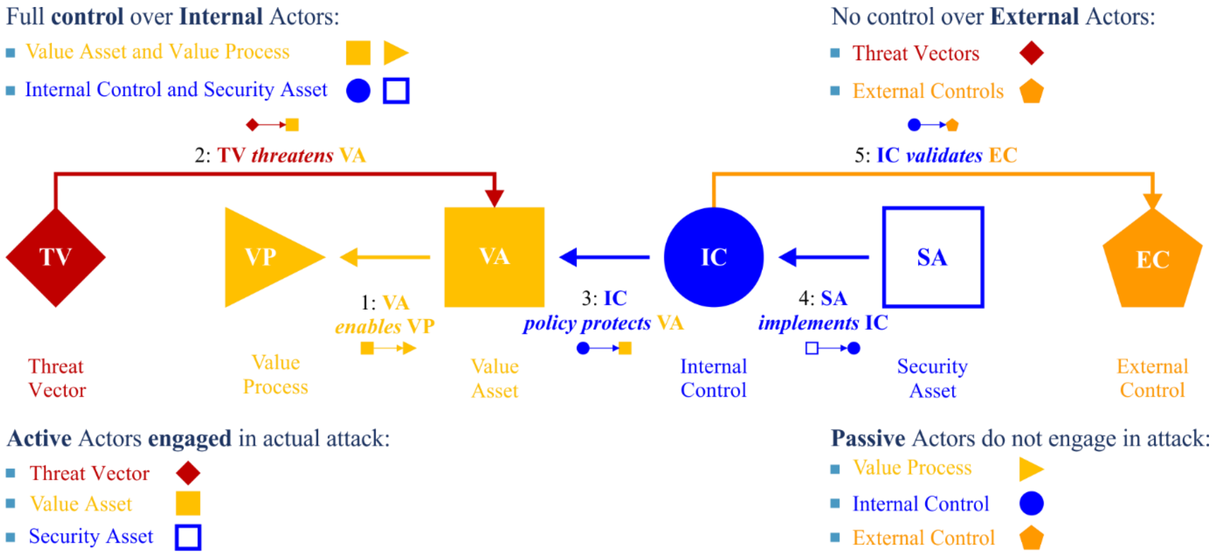
SecMan(20)_F06

Figure 6 – Ruler kernel direct and indirect relationships

The actors align towards two aspects of risk management. The left side of the ruler involves threat vectors and value process and value assets generating value. These actors enable a value impact analysis where value asset criticality and sensitivity can be accounted for.

- **Risk-to-value**: the left side of the diagram represents the value asset criticality and sensitivity based on its role in the value process. Note: Criticality – business importance; Sensitivity – Data sensitivity
- **Protection-to-value**: the right side of the diagram represents security assets delivering security defined by internal control policy.

In addition, actors can be characterized as illustrated in Figure 7 as either internal, where full control over them can be exercised or external, where no control over them can be exercised. Actors are either active and directly involved in the attack or passive and not directly involved in the attack.



SecMan(20)_F07

Figure 7 – Actor characteristics

As the name implies, the ruler is a measurement construct. The "Ruler" is a role-based decomposition of the USM where the four (4) digital value forces are modelled by six (6) actors engaged in five (5) relationships. It is asserted that

"any specific security scenario" involving "all matters security" can be modelled by this Ruler.

The ruler illustrated in Figures 4 and 7 define a **single instance** scenario ruler anchored to one vulnerability of one value asset involved in a value process. Once the value asset is specified as the anchor, all other actors are constrained in available options. That is, actor choices and options are heavily interconnected and interdependent.

In a similar way that the value asset anchors the ruler to a single instance of a security scenario, the value process defines the assessment scope of all possible value asset threat scenarios to be accounted for.

Figure 8 illustrates a "**profile measurement system**" that stores all the ruler unique scenarios and relationships for all vulnerabilities of all value assets involved in one value process involved in an ecosystem.

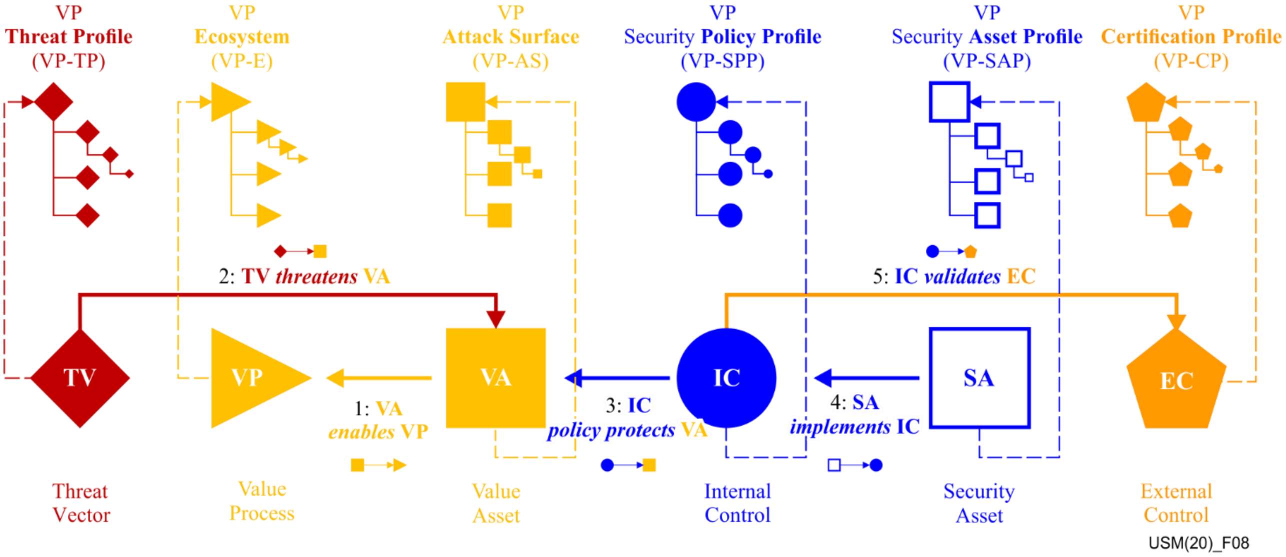


Figure 8 – VP threat profile, attack surface, policy, security, and compliance profiles

By systematically going through each potential vulnerability of each value asset of the value process, and linking potential threats and countermeasures, six value process profiles are generated. The specific number and type of value assets involved in the value process defines the unique nature of the profiles.

- **VP threat profile**: Contains a profile of all threat vectors linked to all value assets involved in the value process.
- **VP attack surface profile**: Contains a profile of the cumulative attack surface of all the value assets involved in the value process.
- **VP policy profile**: Contains a profile of all of the cumulative security policies related to commitment to protect all value assets enabling the value process.
- **VP security profile**: Contains a profile of all security assets, people, process and technology involved in meeting the internal control requirements.
- **VP compliance profile**: Contains a profile of all external security controls that govern the value process.

7 Unified security architecture modelling and analysis

Figure 9 illustrates the complete upper model of the unified security architecture from the ruler aggregating up into profiles and then into risk model.

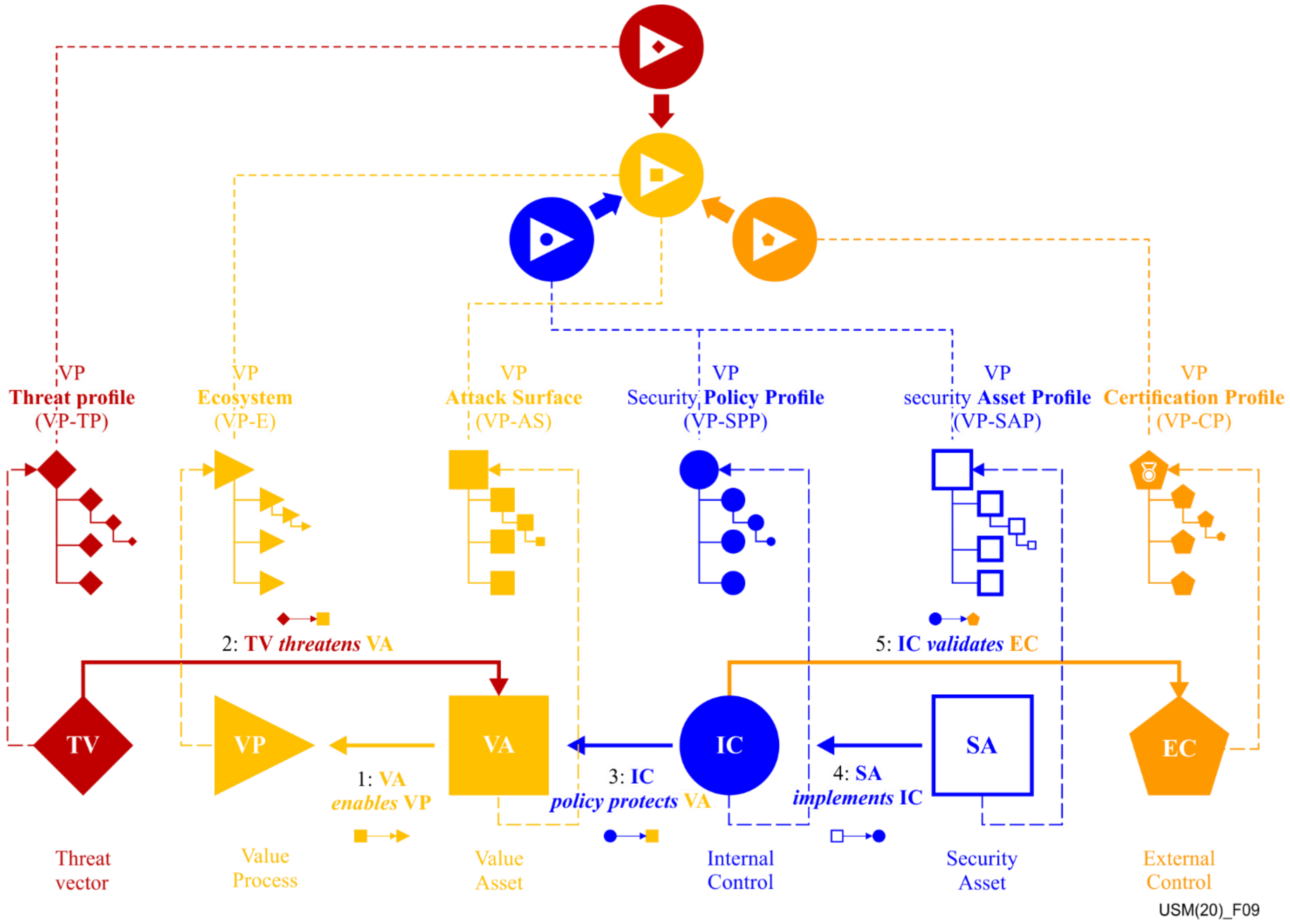


Figure 9 – Unified security architecture

In order to demonstrably protect a value process to a reasonable level and to an acceptable level of assurance, all countermeasures to all threats to all value assets involved in the value process must be identified, documented, analysed and reasonable protection designed, applied and validated.

The profile measurement system enables each actor and their relationships to be modelled independently. The aspects of threat and protection modelling are as follows and illustrated in Figure 10.

- **Value creation modelling**: the ability to model the value creation process (value process) and analyse the value of the IT assets by which it is enabled (value assets). Lines of value creation and value processes are modelled in order to identify the value asset types that must be secured.
- **Value threat modelling**: the ability to instantly obtain and visualize the applicable threat vectors that may exploit vulnerabilities in each of the value assets involved in the value process. All threat vectors are unique to the value asset or target vulnerability.
- **Value protection modelling**: the ability to analyse and design the reasonable security policies (internal control) and select, implement and evaluate potential security assets that could meet the control requirements
- **Value assurance modelling**: the ability to demonstrate compliance to an external control using performance evaluation results previously measured by all security assets involved in fulfilling the requirements of the internal controls.

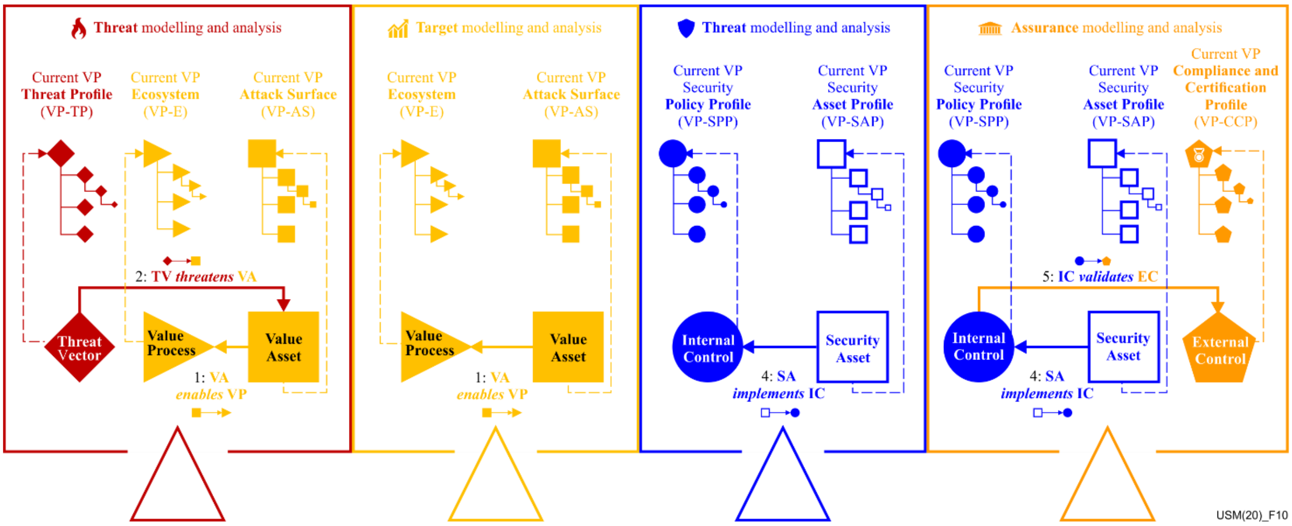


Figure 10 – USA threat | Target | Security | Assurance modelling and analysis

8 Unified security architecture – Decompose down

Illustrated in Figure 11 is the complete unified security architecture illustrating six levels. The kernel ruler defines the core as level 0: role expression. Starting from the ruler as level 0, one can aggregate up towards residual risk and decompose down towards the actual assets involved in an attack. Decomposition level below the ruler are indicated with negative integers and above the ruler as positive integers.

To evaluate the residual risk, the rule or criteria of measuring the amount of risk according to the type of the risk should be defined. How to measure the entire risks of all the rulers, how to measure the risk of a ruler considering the effect of relationships between the components and the values of amounts of components in the rule should be defined, since the entire risk of the specific systems is the integrated result of all the rulers in the system's architecture. Also, when components of different rulers are overlapped, for example, a threat affects several assets and/or an asset targeted from several threats, as well as a control protecting several assets from several threats, it should be defined how to measure the combinations and sequences of multiple risks of the related rulers.

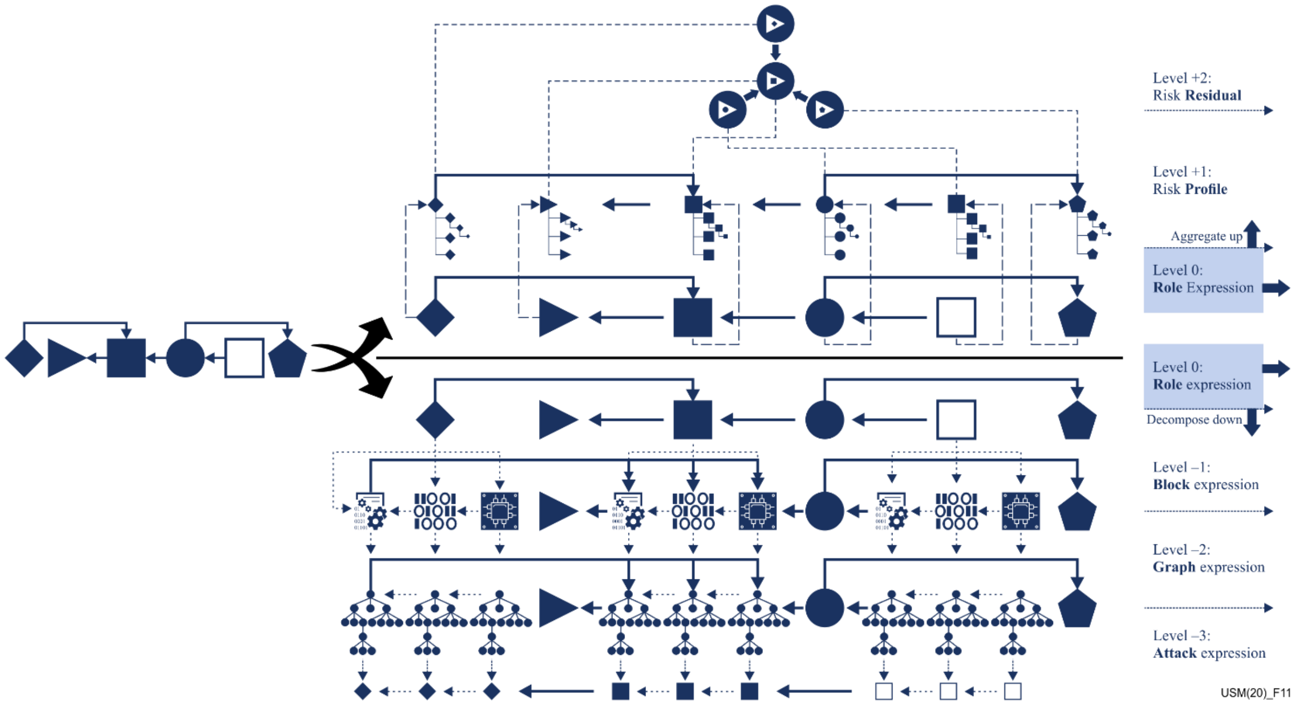


Figure 11 – Unified security architecture

It is not the intention of this document to describe the USA downward decomposition, to the actual assets involved in an attack. The use of graphs creates security knowledge expressions that greatly improve the outcome of machine learning and is the precursor to automation.

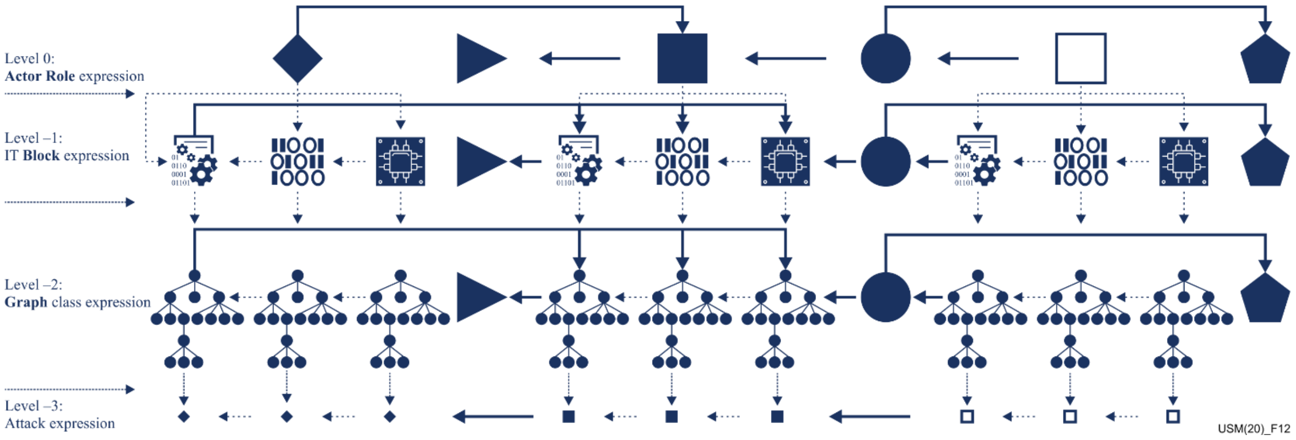


Figure 12 – Unified security architecture lower half – Decompose down

Bibliography

[b-ISO 31000] ISO 31000:2018(en) Risk management – Guidelines