Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Enterprise Transformation Projects-The Role of The Polymathic Security Learn Processes (ETP-PSLP)

Antoine Trad [a]*

[ac]Dr., 5 rue Carle Hebert, Courbevoie, 92400, France.
[a]Email: antoine.trad@ibistm.org

Abstract

This article illustrates the role and how to design and implement an Enterprise Transformation Projects (ETP) in-house Polymathic Security Learn Process (*Concept*) that can use the previous ETP's Holistic Security Concept (ETP-HSC) [1] with a major change, that includes a generic and holistic transcendent Artificial Intelligence (AI) based ETP-PSLP Concept (simply the *Concept*). The *Concept* includes interfaces to practically all AI and related technology domains, like Author's AI modules, Machine Learning (ML), Deep Learning (DL), Big Data (BD), Data Sciences (DS), and others (simply *Intelligence*). The *Concept* uses the author's Polymathic transformation framework and methodology that in this article focuses on ETP's security by using Polymathic Learning Processes (PLP) [2]. ETPs are complex and have very high level of failure rates (at about 95 percent), and due to this fact, adding difficulties that are related to Security frameworks, Interfaceable AI products, inexistent PLP approaches, can result in a siloed and unmaintainable ETP's integration. Such a transformation becomes unmanageable. The *Concept* ensures enterprise's (simply an *Entity*) security, business long-term sustainability, and operational excellence, by applying the PLPs to solve encountered problems. ETP's main problem is in the acceptance of a PLP and *Concept* [2]. The *Concept* shows how an ETP integrates PLP based *Intelligence* to support and resolve *Entity's* security breaches. The PLP is supported by the author's (today usable) Applied Holistic Mathematical Model (AHMM) for PLP based AI (AHMM4AI). The AHMM4AI is the result of many years in research and development in the fields of security, AI, business, financial and organizational engineering, and applied mathematical models. This article is cross-functional research and on an authentic mixed-research method, the Heuristic Decision Tree (HDT) that is ETP's internal decision-making motor [3,7]. The AHMM4AI based

Concept supports: 1) A mixed-method empirical Decision-Making System (DMS); 2) A well-established Action Research (AR) (ideal for PLPs) method for *Concept*; and 3) A framework for a successful finalization of secured ETPs. The *Concept* is a new block in the author's Research and Development Project (RDP) and is a continuation with the aim is to offer an example of an In-House Implemented (IHI) Transformation Framework (IHITF). The *Concept* includes many of the author's research works on the applications of ETPs (simply a *Project*), security concepts, AI, Cloud Services (CS), and Mathematical Models (MM).

Keywords: Security Learn Process; Artificial Intelligence; Polymathics; Enterprise Security; Enterprise architecture; Enterprise Transformation Projects; Natural Languages; Mathematical Models; Requirements; Strategic and Critical Business Systems; Performance Indicators; and Strategic Visions.

Citation: A. Trad, "Enterprise Transformation Projects: The Role of The Polymathic Security Learn Processes (ETP-PSLP)", *ARIS2-Journal*, vol. 3, no. 2, pp. 34–65, Dec. 2023.

DOI: https://doi.org/10.56394/aris2.v3i2.34

---

* Corresponding author. Email address: antoine.trad@ibistm.org

1. Introduction

The *Concept* is based on empiric security PLPs, specialized security cases, and resulting experiences, which can be described by using a Natural Language Programming (NLP) in the form of scripts. Such scripts can be used in the context Enterprise Architecture (EA), that are stored in the Knowledge Management System (KMS) (that also a part of *Entity's Intelligence*) in the form of applicable PLPs.

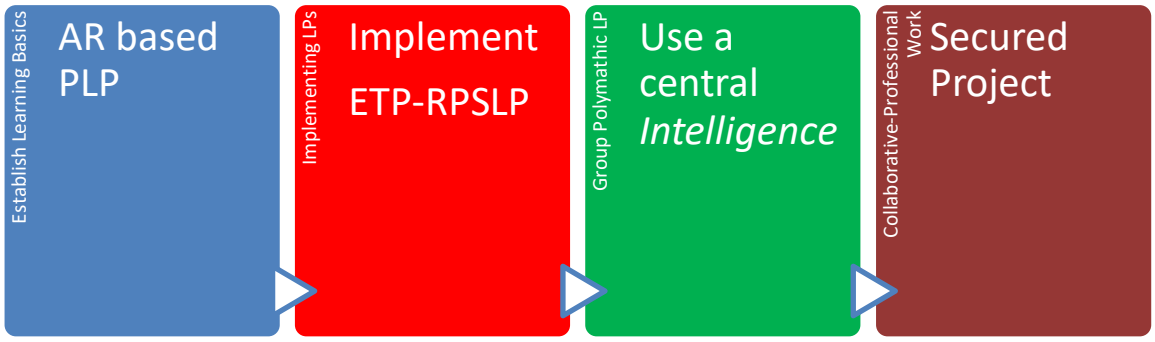

Figure 1: The integration of the PLP in a Project.

AR based HDT solves problems and the solutions (and their paths to actions) are persisted in PLPs; and can be hammered in the *Entity's* security strategy. The *Concept* offers sets of solution patterns, recommendations, and an example of an IHITF that includes PLP, EA for secured *Entities*, security engineering, managerial, and technical propositions. The *Concept* can be used by executive (or ETP) managers, security architects/analysts, and infrastructure engineers to enable solutions to transform the *Entity*. The RDP adopts a Polymathic approach and is interdisciplinary, which includes ETP-HSC, IHITF, (Re)Organization concepts, Project Management (PM), Information and Communication Systems (ICS), secured ICS (sICS), EA, geoeconomics/geopolitical analysis, and other domain. This article is linked to all the author's works and previous RDP's findings; which implies that previous blocks are included in this article. The *Concept* uses the ETP-HSC that includes already analysed security mechanisms like: Managing Passwords, Firewalls, Secure Development and Operations, Antivirus, Wireless Fidelity, Malware, Security Monitoring and Log**s…** [4,5]. PLP relates to: 1) An evolutive learning approach; 2) Enhances the IHITF and avoids simplistic quantitative locked-in products; 3) Avoids siloed security solutions, products, and concepts; 4) Uses methodological and empirical approach that combines EA, sICS, security domains, and AI; and 4) A PLP Work Team (PLPWT) to be used by *Project's* implementation and security teams [4,5] to implement the *Entity's Intelligence*. The PLPWT is used to implement, modify, and integrate PLPs as shown in Figure 1. *Concept*'s integration uses: Critical Success Areas (CSA), Critical Success Factors (CSF), Key Performance Indicators (KPI), Concrete sICS VARiables (VAR). *Project's* CSAs, CSFs, KPIs, and VARs are known as *Project's* Factors. The PLP uses the HDT and Factors to support *Intelligence*, where PLPs absorb problem-solving experiences from encountered (and solved) *Project's* security problems. The *Concept* can be based on existing standard frameworks like: 1) EA which can support PLPs [6]; 2) An IHITF and associated MMs like the AHMM4AI [3,7]; 3) Unbundling *Entity's* resources, security mechanisms, and services pool [8,9]; 4) AI domains [10,11]; 5) A scalable ICS and an agile PLPWT [12]; 6); Problem solving supported by *Intelligence* [13]; 7) Sherwood Applied Business Security Architecture (SABSA) [44]; 8) The Committee of Sponsoring Organizations of the Treadway Commission (COSO); and many others.

2. Concept's Characteristics

A Project has various Viewpoints, like "O" for organizational, "A" for EA, "S" for Security … In this article the Viewpoint "C" (which combines all Viewpoints and where "S" is the central one) that uses a PLP approach.

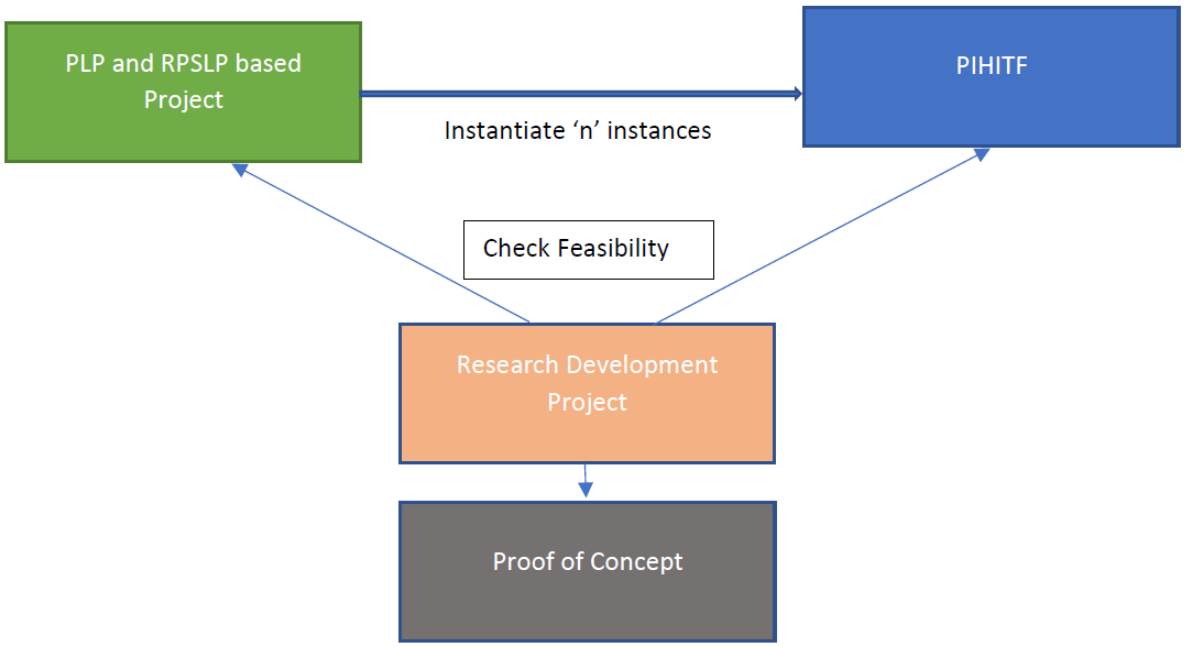

Figure 2: The interaction between the *Project*, RDP, and PLP/Concept.

This article uses an IHITF or the author's Transformation Research Architecture Development framework (*TRADf*) that includes: 1) sICS, PLPWT, and corresponding PLP patterns; 2) *Intelligence*; 3) *Concept* generators; and 5) An RDP evolutive strategy, which is the 1st CSA and its heading is in fact the initial set of CSFs.

3. The RDP for AI and PLP

3.1. AHMM's Generic Basic Elements

This article uses the generic basic elements that were already defined in the ETP-HSC [1] and other author's works; these elements assess security risks, and some of the basic elements are:

- ***a*** for atomic
- ***m*** mapping operator
- **….**
- *REQ* *is an ETP* ***requirement***
- ….
- *GAP* *is a* ETP ***gap*** that results from *Concept*.
- ….

3.2. AHMM4AI's Nomenclature

The *Concept* uses AHMM4AI' basic elements to construct its nomenclature that has two major parts: 1) ICS basics; and 2) The applied security requirements, as shown in Figure 3:

Requirements:

mcREQ	= ***m*** KPI	(R1)
mcMapping mcArtefact/mcREQ	= mcArtefact + ***m*** mcREQ	(R2)
FTR	= mcREQ	(R3)
PRB	= ***m*** PRB	(R4)
REQ	= ***m*** CSF = ⋃ mcREQ	(R5)
REQ	= ⋃ FTR + ⋃ RUL + ⋃ CNT + ⋃ DIA + ⋃ REL	(R6)

Figure 3: AHMM4AI's nomenclature.

Where a PLP is the choreography of a set of actions that were used to solve a security problem or requirement.

3.3. A Polymathic Projects' and Concept's Approaches

The ETP-HSC and hence the *Concept* use the Unbundling and Securing Process (USP) to defragment the *Entity's* legacy organizational units (simply Unit), which in general have heterogenous methodologies/structures, (s)ICSs, and security concepts. As shown in Figure 4, the *Concept* (and the underlying ETP-HSC) focuses on transforming and securing Unit's resources and applying Viewpoint "C",. Viewpoint "C"'s has the following structure [1]:

- sMA = ∑ aBB + ∑ sBB + ∑ aMVC (C1)
- sBB = ∑ UP+ ∑ sMA + ∑ sOPM (C2)
- sCBB = ∑ sBB + ∑ sABB + ∑ SBB (C3)
- sIBB = ∑ sCBB (C4)
- Unit = ∑ sIBB (C5)
- PLP = ∑ Unit-modifications' actions (C6)
- …
- sUnit = ∑ sSUPL (C10) … secured Unit (sUnit)
- PSLP(i) = ∑ sUnit-modifications' actions (C11)
- *Entity*(C) = ∑ PSLP(i) (C12)

The *Concept* supports the refinement and securing sUnit's platform components.

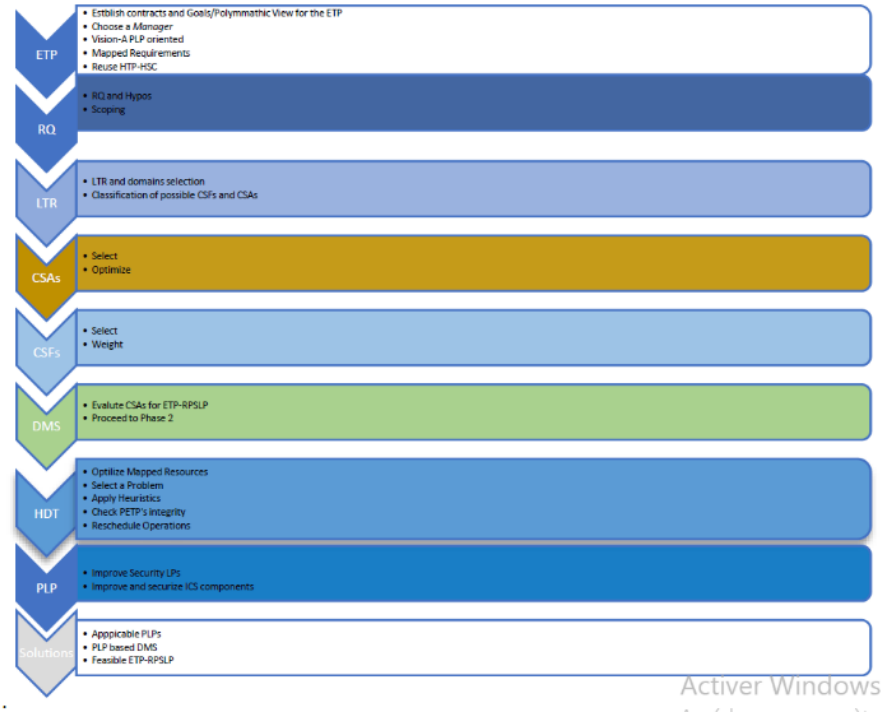

Figure 4: *Concept*'s approach.

The RDP presents *TRADf* which relates the selected Applied Case Studies (ACS) and the PoC, which are based on a concrete transformation initiative labelled the EUBank (a concrete ETP). Figure 5 shows the Polymathic-holistic approach used by the *Concept*. And the first step established the Research Question (RQ) and initiated an in-depth Literature Review Process (LRP).

3.4. The RQ and LRP

The RDP's RQ is: "Can the *Concept* support the implementation of secured Units; and thus, apply PLPs for a secured Entity?". Where this article's auxiliary RQ is: "How can PLPs accumulate Project's experiences?". The RDP uses: AI related PLPs, EA/ADM inspired Transformation Development Method (TDM), AHMM4AI, Factors' Management System (FMS), HDT, and *Intelligence*. LRP's processing and analysis showed that there are no similar concepts, frameworks, and approaches; and that *TRADf*, has a clear lead in Polymathic Transformation Research. Where *TRADf* was developed to show how to implement an IHITF. But there are some siloed and marginal industry and scholar usable resources that are related learning processes-based security concepts, but unfortunately they are limited to well-defined scopes and are not Polymathic; like the case of The Open Group Architecture Framework (TOGAF) that is usable framework, but unfortunately is a very limited cookbook, and tackles superficially ETP topics. Therefore, *TRADf*, ETP-HSC based *Concept*, and AHMM4AI based RDP (and other author's works), are pioneering, innovative and cover a significative *Projects'* gap(s). Project related gaps and their very high failure rates (~95%) were confirmed by the LRP [14]. These failures are due to siloed approaches, an excessive commercial attitude, and the lack of a Polymathic approach to *Projects* and the *Concept*. The LRP used the following resources: 1) Articles and resources related to AR/PLPs, ETP-HSC, Secured ICS reengineering, EA/TDM, and *Projects*; 2) The existing author's RDP/LRP works, and *TRADf*; 3) *Concept*'s feasibility; 4) Initial sets of Factors and the FMS; and 5) RDP's use of the Empirical Engineering

Research Model (EERM); and as shown in Figure 6, the next Project's step is to select and classify the sets of Factors in the FMS [15].

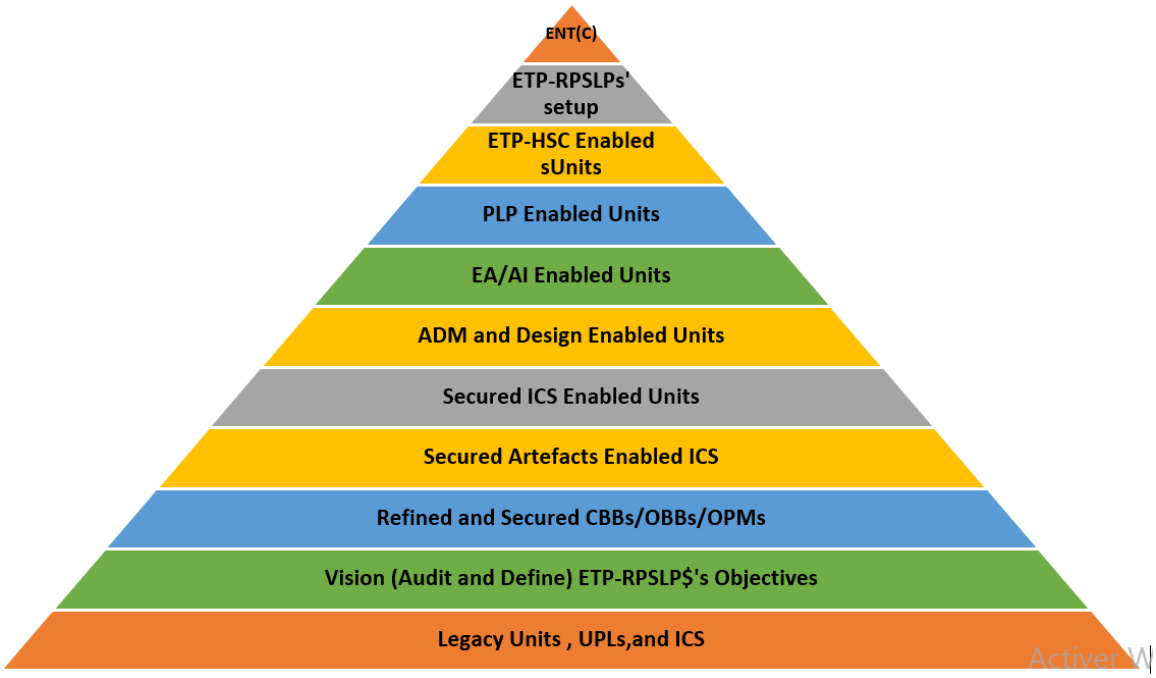

Figure 5: *Concept*'s Evolution.

3.5. CSAs and CSFs Management System

A FMS contains CSAs and a CSA contains a set if CSFs, where in turn a CSF is a set of Key Performance Indicators (KPI). A KPI maps (or corresponds) to a unique Project or PLP requirement or feature [15]. For a given requirement (or a problem), *TRADf* selects initial sets of Factors, to be used by the HDT based *Intelligence*. A CSF maps to a requirement(s), PLP… [16]. The Rating and Weighting Concept (RWC) evaluates Factors. *Intelligence's* requests are served as shown in Figure 6. KPIs are linked to concreted VARs [16,17,18]. RDPs' phases are: 1) Phase 1 (represented in Decision-Tables, DT), forms the empirical part of the RDP, DTs check CSAs; and 2) Phase 2, tries to solve a concrete problem by using the HDT and RWC.

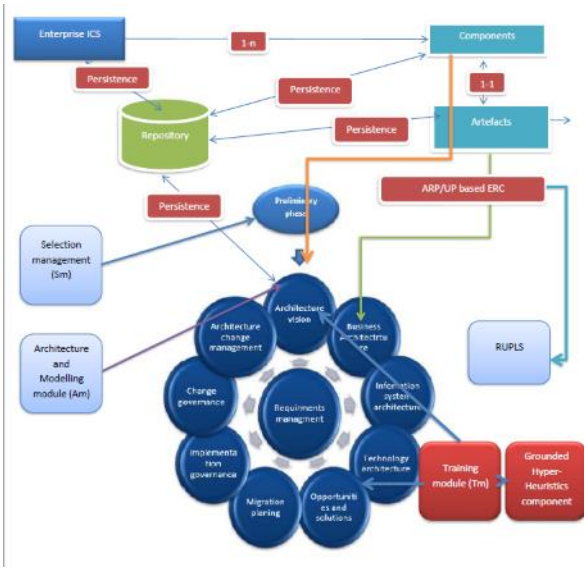

Figure 6: The *Concept* and FMS' integration with the RDP [20].

3.6. The RWC

TRADf (or an IHITF) needs an internal and open/generic RWC and Weightings (WGT) or it can use an external commercial one. *TRADf's* RWC proposes the following rules and definitions:

- The weighting for each CSA is CSA_WGT ϵ { 0.00% … 100.00% } are floating point percentage values, which are derived from DTs (One CSA has one DT and a set of CSFs).
- A weighting is defined for each *Concept*'s CSF, and a rating for each KPI.
- The selected corresponding weightings for CSFs is CSF_WGT ϵ { 1 … 10 } are integer values.
- The selected corresponding ratings to KPI KPI_RAT ϵ { 0.00% … 100.00% } and is derived from: 1) An ICS application/module variable(s) (simply VAR); or 2) Estimated by the IHITF or a domain specialist.
- The AHMM4AI applies the HDT, which uses the RWC.
- RWC (Project-iteration i) = ∑CSA*CSA_WGT.
- CSA_WGT = ∑CSF*CSF_WGT.
- CSF_WGT = ∑KPI*KPI_RAT.
- KPI_RAT = ∑VAR*VAR_RAT.
- Otherwise the RWC can use standard external solutions like:
- Like the one proposed by the Object Management Group's (OMG) (OMG, 2022): 1) The Decision Model and Notation (DMN); 2) The DMN can be used for implementing business decisions and business rules; and is optimal for Project's status checking; and 3) The DMN can be used for Tables' evaluation and HDT's operations.
- The weighted criteria matrix is a *Intelligence* that can evaluate Projects; and is based on the evaluation criteria (that has weighted by ratings). By evaluating alternatives based on KPIs with respect to defined criteria.
- The *Concept* uses the HDT which is mainly qualitative method and has specific calls to quantitative methods. And such complex artefacts need an EERM.

3.7. EERM's Usage

The EERM is optimal for the RDP and *TRADf* (because they apply the multi-level mixed-research HDT) that is unconventional [16,17,19], and it includes: 1) A heuristics reasoning approach; 2) Quantitative Analysis for AI (QNT4AI); 3) Qualitative Analysis for AI (QLT4AI) research method that supports a mixed approach; and 4) A PLP based on the HDT [16]. The EERM checks if the RDP's outcome is acceptable and tries to convince the

reader(s) that the recommendations are feasible. In engineering, a PoC is a software prototype of a testable RQ where a Factor (or independent variables, in theoretical research) is processed to evaluate its effects on RDP's dependent variables. *Concept*'s author's related works are: 1) The ETP-HSC, on which the *Concept* is built [1]; 2) Polymathic learning articles, which support PLPs [4,5]; 3) Business Transformation Projects-The Role of a Transcendent Software Engineering Concept (RoTSEC) [21]; 4) Business Transformation Projects-The Role of Requirements Engineering (RoRE) [22]; 5) Business Transformation Projects based on a Holistic Enterprise Architecture Pattern (HEAP)-The Basic Construction [23]; 6) Integrating Holistic Enterprise Architecture Pattern-A Proof of Concept [24]; 7) A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Project-Intelligent atomic building block architecture [25]; 8) A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-An Information System's Atomic Architecture Vision [26]; 9) Organizational and Digital Transformation Projects-A Mathematical Model for Building Blocks based Organizational Unbundling Process [27]; 10) Organizational and Digital Transformation Projects-A Mathematical Model for Enterprise Organizational Models [28]; 11) Organizational Transformation Projects-The Role of Global Cyber Security and Crimes (RoGCSC) [72]; and 11) Using Applied Mathematical Models for Business Transformation [20]; 2) Applied Holistic Mathematical Models for Dynamic Systems (AHMM4DS) [20]. The *Concept* is complex and causes resistances and failures, therefore there is the need for Transformation Readiness Checks (TRC).

3.8. The TRC

Project's complexities are the main cause of their failures; and *The Chaos Report*, edited by the Standish Group assert that: … *only about 29% of transformations come in on time and budget*… [29,30]. The TRC offers [31]: 1) *Business Transformation Readiness Assessment* capacities; 2) TDM's executions; 3) *Concept* execution capacities; 4) PLP accumulates experiences; and 4) Use an IHI Methodology, Domain, and Technology Common Artefacts Standard (MDTCAS).

3.9. RDP's CSFs

Table 1: This CSA has the average of 9.25.

Critical Success Factors	KPIs	Weightings
CSF_RDP_Polymathic_Approach	Proven	From 1 to 10. **10 Selected**
CSF_RDP_Factors_FMS_Integration	Proven	From 1 to 10. **10 Selected**
CSF_RDP_RWC_Integration	Complex	From 1 to 10. **08 Selected**
CSF_RDP_EERM	Feasible	From 1 to 10. **09 Selected**
CSF_RDP_TRC	Feasible	From 1 to 10. **09 Selected**
CSF_RDP_AHMM	Feasible	From 1 to 10. **09 Selected**
CSF_RDP_IHI_TRADf	Possible	From 1 to 10. **09 Selected**
CSF_RDP_LTR	Proven	From 1 to 10. **10 Selected**

valuation

Based on the AHMM4AI, LRP and *Intelligence*, this CSA's CSFs/KPI were evaluated with the RWC and the results are shown in Table 1. This CSA's result of 9.20, which is high, is due to RDP's and *TRADf's* maturity [27]. As the RDP's CSA presented positive results, the next CSA to be analyzed the role the sICS and technology.

4. The Role of the sICS and Technology

4.1. The Role of Digital Transformation and Strategy

Today there are many ICS and security tools and frameworks, and they apply siloed ICS-models. The ETP-HSC based *Concept*: 1) Supports the automation of security architecture, design, and integration operations; 2) Its controls uses networked secured Building Blocks (sBB) that originate from various domains like finance, governance and other; 3) It tries to detect sICS problems, financial crimes, business disruptions and corruption; and 4) Implements Cybersecurity mechanisms. Cybersecurity is responsible to avoid security related dangers and threats; and to support an sICS. To deliver an sICS, the *Concept*'s first-step is to successfully implement a Digital Transformation (DT) that offers a common platform for secured Services (sSRV) and resources. DTs are strategic for *Projects*, because they support high-adoption rate of sICS/digital technologies. DTs use TDM and secured MDTCAS (sMDTCAS) to integrate digitized Application Domain (APD) models [32,33]. An Entity must offer an all-inclusive DT based on ETP-HSC/*Concept* and sMDTCAS.

4.2. The sMDTCAS

A *Project* has an IHI sMDTCAS, as shown in Figure 7, which is a common-denominator of existing methodologies and practices. The sMDTCAS can include: Object Oriented (OO) Methodology (OOM); Structure Analysis and Structured Design (SA/SD); Unified Modelling Language (UML); TOGAF/ADM based TDM; Modelling languages, like ArchiMate; Decision Making Notation (DMN); Entity Relationship Diagrams (ERM); Business Process Models (BPM)… sMDTCAS can interface various methodologies by using OOM/UML which are the fundaments of all methodologies [34].

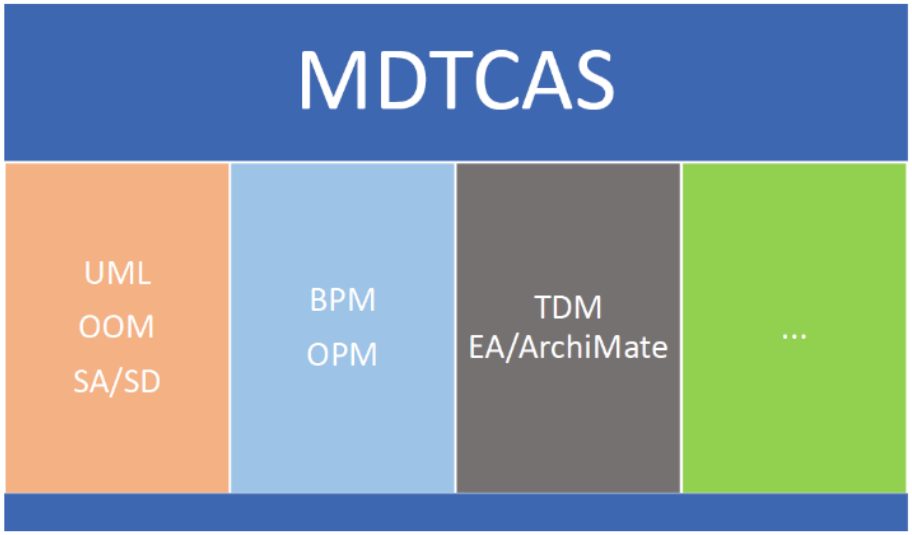

Figure 7: sMDTCAS' implementation.

The *Concept* use PLPs to incorporate analyzed APDs' scenarios and how they solve related problems (from the functional and technical perspectives). PLPs contain the used *Application Services* and sMDTCAS diagrams that represent *Concept's* behavior. The PLP incorporates also APD competencies, and related *Business Architecture* and sICS architectures for APDs like Finance, Human Resource, Supply chain, … A PLP incorporates a holistic

overview across all *Project's* CSAs to localize, inter-relate or predict security breaches/problems [34]. A PLP also includes secured BPMs (sBPM) as one of its most important bricks.

4.3. The sBPM

To monitor sBPMs with TDMs, sBBs, and Units, the PLP must incorporate: 1) Common and generic sBBs; 2) sMDTCAS' interaction; 2) Business Process Architecture (BPA) usage; 3) EA/TDM synchronization; 4) Test/detection sBPMs/scenarios' management; 5) Persisting best practices and Return on eXperiences (ROX); 6) Units' problem solving procedures; and 9) An *Entity* Security concept [35]. The PLP supports a security concept that is measurable to mitigate security Risks (sRisk); and also, to ensure *Project's* successful evolution. For that goal the *Project* needs to define a focused vision.

4.4. A Focused Vision

The *Concept* and TDM need a focused vision on how to manage PLPs and must establish a PLP based Architecture Vision (PPAV), as shown in Figure 8.

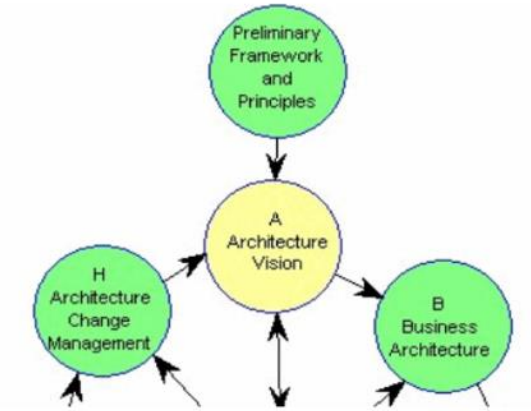

Figure 8: TDM's vision phase.

A PLP depends on resources like sBBs, sSRVs, secured Model View Control (sSRV); and *TRADf* relates PPAVs to Factors, activates Viewpoint "C", and associates PPAV with the following CSFs:

- Coalition to Support the Vision (CSF_PROJECT_VIS_CSV).
- PPAV's Adoption (CSF_PROJECT_VIS_CVA).
- PLP's Capacities (CSF_PROJECT_VIS_PLC).
- Time for Execution (CSF_PROJECT_VIS_T4X).
- Tooling ADoption (CSF_PROJECT_VIS_TAD).
- sBB's concept adoption (CSF_PROJECT_VIS_SBB).
- sMVC adoption (CSF_PROJECT_VIS_MVC).
- sBPM Control and Monitoring adoption (CSF_PROJECT_VIS_BPM).
- Transaction Capability Adoption (CSF_PROJECT_VIS_TCA).
- Strategy for PSLP (CSF_PROJECT_VIS_RPS).
- PoC's capabilities (CSF_PROJECT_VIS_PCC).

To support such a PPAV there is the need to execute the USP to deliver sets of refined artefacts like sBBs.

4.5. The USP and Unbundled Artefacts

A set of sBBs is persisted in secured Compound BBs (sCBB) that are managed by the TDM [36] and they are built from IHI resources. The TDM ensures that the PPAV is respected to provide a conceptual and logical view(s) of sCBBs and sSRVs (simply SRV) used across APDs. A sSRV corresponds to a secured APD Transaction (sATR) or secured Cybertransaction. The TDM manages requirements, sSRVs, and sATRs which can be registered in PLPs to solve future APD problems [37,38]. The USP unbundles legacy Unit's components into classified sSRVs based sATRs. The USP applies the *architecture & modeling extraction techniques*, which can fail because of bad design; and the generated sets of sSRVs can be used in sBPMs. sSRVs map to different types of *Project's* and PLP constructs [31], which needs the adoption of the PBA and sMDTCAS to interface distributed BBs and Data sBBs (DBB) [27,39]. The USP extracts also data structures/patterns to form DBBs, like the 1) Business Data or Interaction Modeling Patterns that is the basis of the *Business Knowledge Management Pattern* (BKMP) [39,40]; The BKMP by the PLP, sSRVs and the Project's repository [31,37]. The PLP and *Concept* support the organization and classification of sSRVs in *Projects* [41], to avoid that a the USP generates a sSRV hairball, for that aim it uses the PBA and sMDTCAS to model the usage of sSRVs [34,39,40], taking into account possible sRisks.

4.6. Possible sRisks

The AHMM4AI based *Project* uses various mathematical domains to deliver a unique model [20]. The Project must have an sRisk mitigation concept, and the PLP must include the following: 1) sRisk avoidance and prediction mechanisms; 2) sRisk reduction; 3) Adapted actions; 4) Transfer sRisks to third parties; and 5) sRisk acceptance concept [20,39]. As shown in Figure 9 the symbol Σ indicates summation of all the relevant AHMM's members, while the indices and the set cardinality have been omitted.

The Generic AHMM's Formulation

TDM	*is a **Transformation Development Method**, which can be ADM based…*	
AHMM	$= \bigcup$ TDMs + $\bigcup$ DMMs	(G1)

AHMM's Application and Instantiation for a Domain

Domain	$= \bigcup$ APD	(G2)
AHMM4(*Domain*)	$= \bigcup$ TDMs + DMMs(*Domain*)	(G3)

Figure 9: The AHMM4AI main formulas.

The *Concept* interfaces are based on the TDM and uses services to enable the Polymathic transformation model. The AHMM4AI based TDM is the combination of TDM and AHMM4AI as shown in Figure 9.

4.7. The Polymathic Transformation Model

The AHMM4AI based TDM model:

AHMM4AIbTDM = AHMM4AI(TDM) (G4).

The Polymathic transformation model is the combination of an AHMM4AI based TDM, and *IterationGap* that can be modelled using the following formula:

Project = AHMM4AIbTDM(*IterationGap*) (G5).

The *Project* is based on the extraction and management of PLPs. The extracted PLPs are based on the HDT that uses sSRVs. The AHMM4AI is composed of large number of interconnected nodes, to solve defined problem types.

4.8. The sICS' and Technology CSFs

Based on the AHMM4AI, LRP and *Intelligence*, for this CSA's CSFs/KPI were weight and the results are shown in Table 2. This CSA's result of 8.50, which is low, and that is due to the fact that the DT, USP, and sRisks' mitigation processes are complex; but this CSA has a limit value and might be feasible.

Table 2: This CSA's average is 8.50.

Critical Success Factors	AHMM4AI enhances: KPIs	Weightings
CSF_sICS-Tech_DT_Implementation	Complex	From 1 to 10. **08 Selected**
CSF_sICS-Tech_sMDTCAS_sBPM	Possible	From 1 to 10. **09 Selected**
CSF_sICS-Tech_PPAV	Possible	From 1 to 10. **09 Selected**
CSF_sICS-Tech_USP_SRV	Complex	From 1 to 10. **08 Selected**
CSF_sICS-Tech_sRisks	Complex	From 1 to 10. **08 Selected**
CSF_sICS-Tech_Security_Strategy	Possible	From 1 to 10. **09 Selected**

valuation

The sICS and related technologies can support the *Concept* and PLP based *Projects*…

5. PLP BASED PROJECTS

5.1. PLP's Basics

AR's main advantages to be used by the PLP are [59,60]: 1) It is optimal for learning and PLPs, because it adopts an empirical approach that enriches reflective practices and practical experiences; and delivers the sets of applied actions that corresponds to the HDT based *Concept*; 2) Tackles sICS, business, and other *Project*'s concrete problems in participatory, collaborative, and cyclical ways in order to produce practical knowledge that can stored in PLPs for future use; and 3) Can be: Positivist, Interpretive, and Critical; and supports basic PLP operations that are shown in Figure 10 [58].

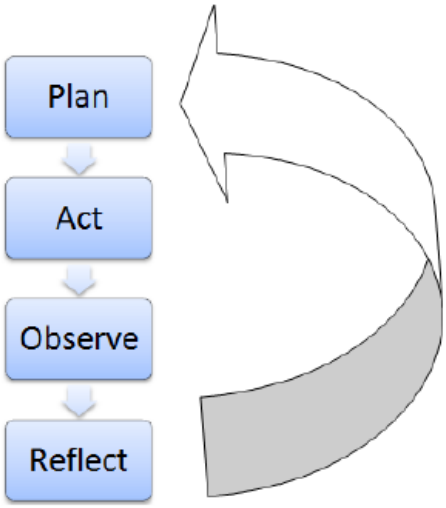

Figure 10: AR's basic operations [58].

5.2. A Qualitative Approach

AR's Qualitative/Heuristics reasoning approach emerged as an *Intelligence/AI* field in the middle of the 20th century; and in 1950, Alan Turing developed a fundamental test for automated machine logic, which is known as the *Turing Test*. The term AI was coined in the proposal for a seminal AI domain's conference that took place at Dartmouth in 1956 [53].

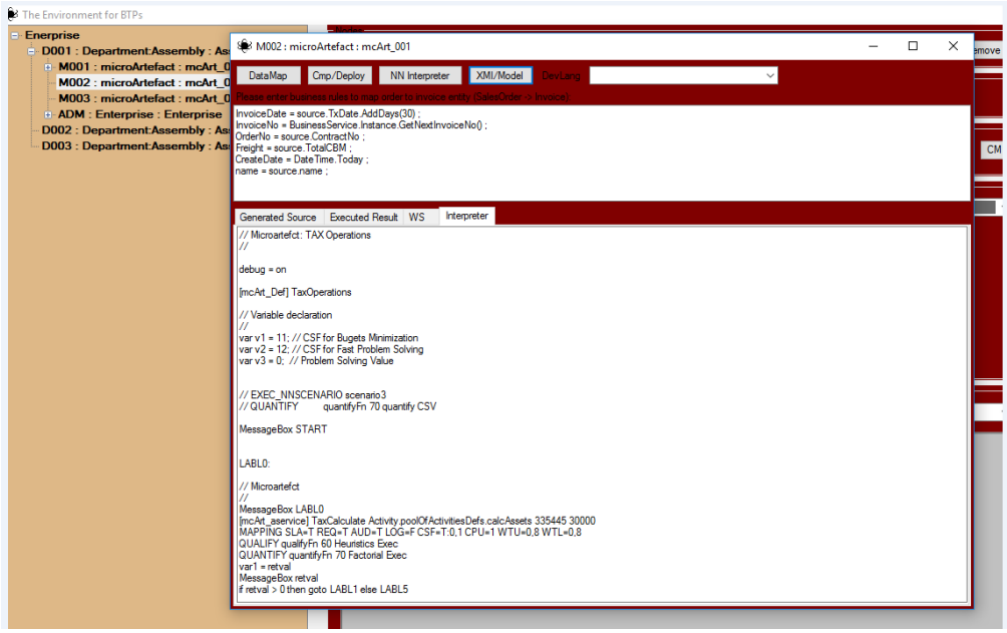

Figure 11: NLP's integration.

Qualitative *Intelligence* is a: 1) Cognitive process that uses an HDT, where an HDT launches IHI NLP scripts, as shown in Figure 11; 2) Sequential set of actions that starts from an initial state to a solution-state(s) that are persisted in PLPs; 3) Set of actions to find solution(s) (or a goal state); 4) HDT process that has root-node; 4) Interface to RWC; and 5) Solution-node that include Security changes that are stored in a PLP [52]. AI tries to

simulate the functions of the human-brain in a qualitative manner, which is a pure empirical concept and not the popular and simplistic quantitative approach that has a marketing only objective. Therefore, a PLP adopts a qualitative approach and is based on beam-search and AR, which are dedicated for education and learning processes, and are represented in *TRADf's* HDT [7]. It is recommended to select the evolution of *Intelligence*, that is based on qualitative based PLPs (and not simplistic quantitative concepts), because such an approach is capable of solving complex problems, like *Project's* sICS/Security problems. PLPs depend on *Project's* sICS/Security situation/context/status with respect to finance, history/experiences, real-time events. HDT's integrated NLP processor (that interprets actions-based scenarios) searches for sICS/Security problem's best-solution(s). Where best solutions depend on selected Factors, RWC, and Objective Functions (OF). The *Concept* uses NLP scripts to interface the HDT to solve problems and enhance/modify PLPs. The PLPWT supports NLP's script development and PLPs' modifications, as shown in Figure 11. PLPs correspond to business and sICS/Security architectural model(s) that is abstracted by the sMDTCAS that offers inter-operability capabilities.

5.3. Intelligence Interfacing and Inter-operability

The *Concept* is supported by a predictive *Intelligence* to solve sICS problems, which can be the source of sRisks and failures... Problems can be measured and weighted by the RWC, where sRisks are not easy to measure. Intelligence delivers a set of possible actions. *Intelligence* uses the HDT to solve problem(s) and controls PLPs improvements. The PLP uses sSRVs-based sBPMs to describe the process and delivers constructs for future problem solving, which means that it learns from gained experiences [31]. The PLP is generic and its interface with the TDM supports legacy-components refinement, mapping, and integration; which all enables APD's PLPs integration and offers the following inter-operability characteristics: 1) Supports the integration of *Project's* components like sSRVs…; 2) Inter-resources operability; 3) Usage of sBPMs and the *business interaction matrix,* which maps sSRVs, PLPs, and functional domains; 4) PLPs and inter-operable resources support sUnits' reorganization; and 5) Respects Polymathic constraints.

5.4. Polymathic Constraints

Projects need to integrate, and enhance PLPs; where a PLP needs continuous modifications [46]; and that requires: 1) Evolutive PLP focused quality concept; 2) Enhancements' concepts; 3) Polymathic implementation's cookbook; 4) Use of PLP Patterns (PLPP); and 5) PLPP and sICS bridging; 5) sICS' security evolution roadmap; 6) Building an *Entity* and *Concept* metamodels; 7) FMS' interface with the ADM/TDM [47]; 8) To support concurrent PLPs; and 9) Adapting the sMDTCAS for TDM. The *Concept* aligns: 1) PLPs implementation and usage visions or PPAV; 2) Supports PLP's modelling principles; 3) PLPs management; 4) Interfacing external PLPs; 5) Defining PLP's granularity and Unit of Work (UoW); 6) Persisting Project's experiences; and 7) Abstracting concrete problems and complexity. To manage complexities the *Concept* offers an IHI Security Related Complexities Management Strategies (SRCMS) [48]. The SRCMS inter-relates various sICS, PLPP, and security domains which can be abstracted by the use of the *Global Simplicity Index (GSI).* A PLPP has a GSI, which shows the level of its complexities' reduction. The SRCMS uses the HDT for problem-solving and hence for the improvement of PLPPs [49,50]. The *Concept* uses inter-operability to [51]: 1) Be used as a systemized module; 2) Include APD problem-solving capacities, as shown in Figure 12; and 3) Includes physical, logical, and human Factors.

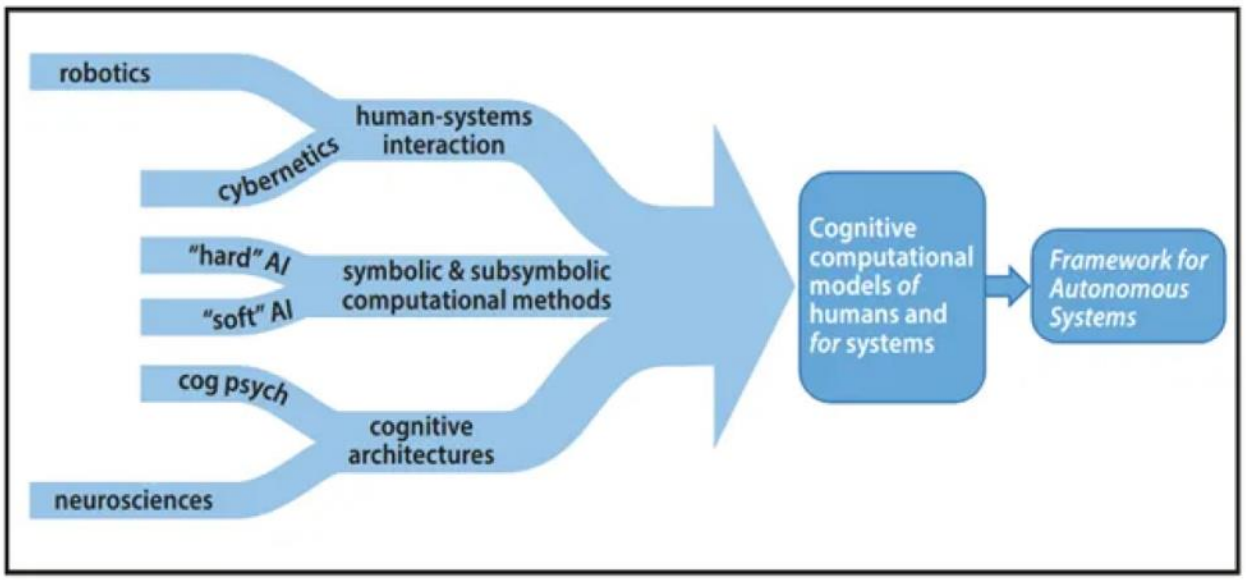

Figure 12: The *Concept* is an autonomous sub-system [51].

Projects' complexities and ever evolving security and AI, have generated a new transformational shift which has imposed the *Concept and an AI approach*.

5.6. The Concept as an AI (and Intelligence) Main Construct

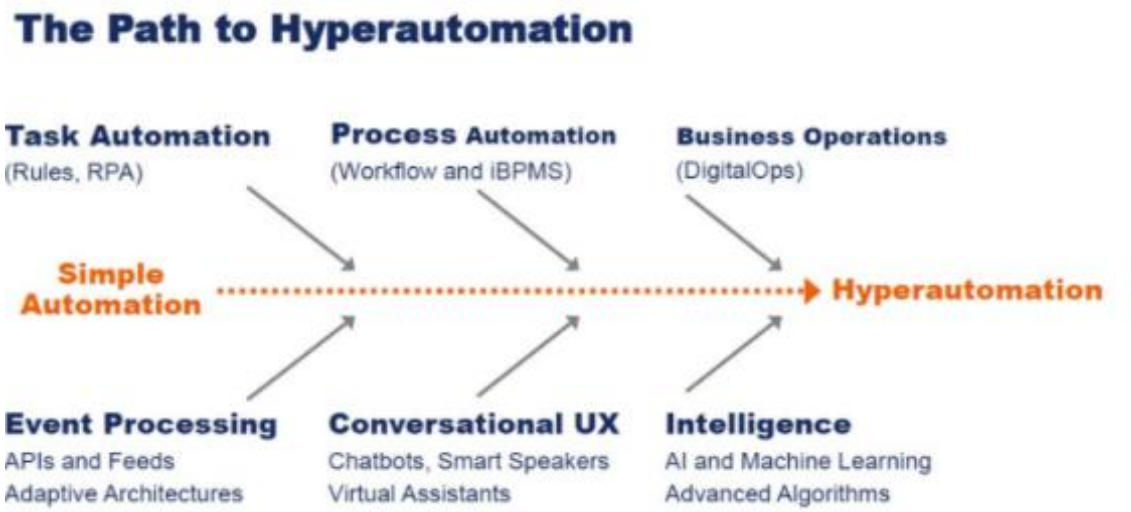

Figure 13: PLP's interfaces AI/OR Hyperautomation [54].

The *Concept* offers a PLPWT based-interface to implement AI/*Intelligence* domains like Operation Research (OR), ML/ DL, and many others. These AI domains can be generalized by using the generic PLPPs and HDT processors; these processors are supported by: 1) the *Concept* and TDM modelling; 2) Implementing generic PLPP interfaces for ML, OR … to support hyper-automation as shown in Figure 13; 3) *Intelligence'*s Polymathic integration; 4) A PLP abstracts OR, ML…; and 5) Using complex algorithmics? Domains like OR, has important advantages as shown in Figure 11. The *Concept* abstracts complexities in interfacing various AI domains as shown in Figure 14. The *Concept* uses OFs to optimize and store results in PLPs which can help reorganization [54,55].

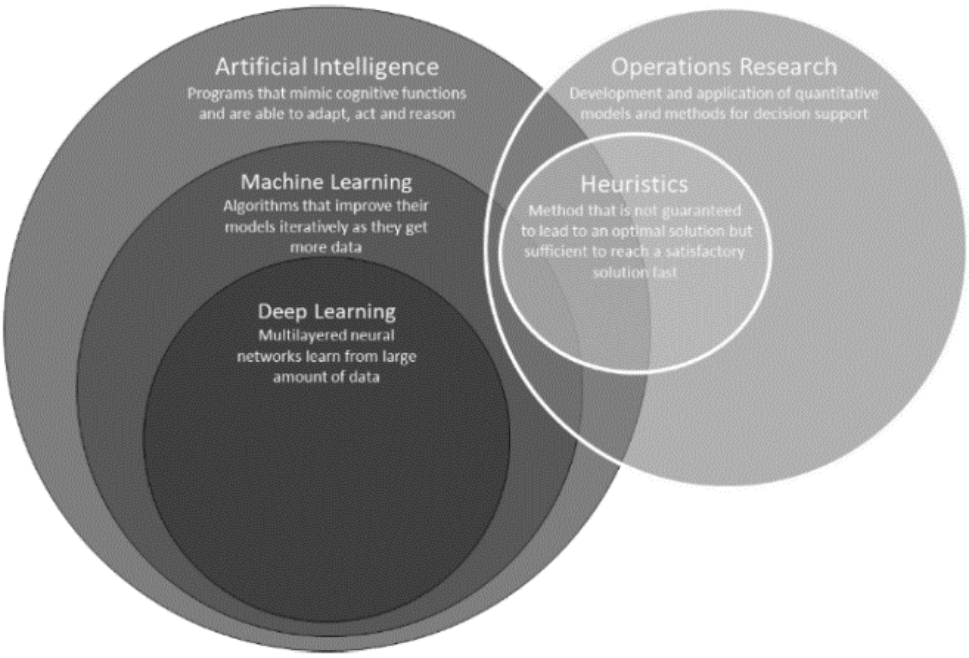

Figure 14: Various AI domains [56].

5.7. sUnit's Reorganization

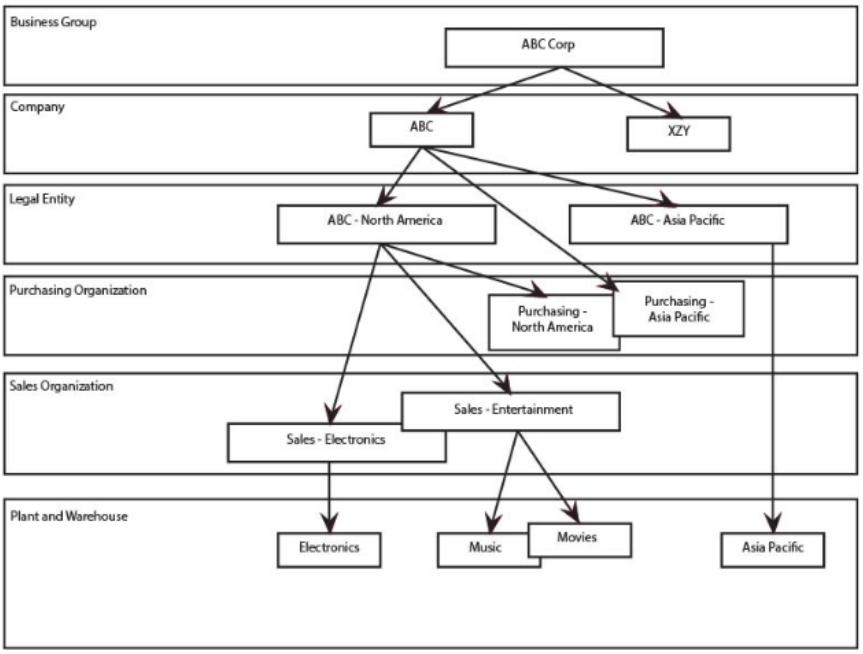

Figure 15: Typical sUnit's reorganizational model [43].

PLPs and related sBPMs can prove inconsistencies and use *Intelligence* to deliver actions to reorganize sUnits and hence the *Entity*. Using PLPs' sequence of actions can improve *Project's* success rates; these actions are based on *organizational routines* or *known actions*, knowing that there are various types of reorganizational models (or sBPMs) [42,43]. sUnits reorganization improve *Entity's* security which worst problem is Resistance to Change (R2C); where R2C can be evaluated in all TDM's phases, and PPAV can preview that in principles. The *Concept*

(re)organizational model include [53]: 1) Use classifications and unbundling; 2) PLPs' interfaces with AI domains and HDT's usage; 3) The use of the IHITF to support the Project and *Concept*. Polymathic models use the HDT and the RWC [57]. This part (or CSA) shows clearly that the Entity has to establish a PLP based Polymathic Entity Metamodel (PEM) and its variant PEM for Security (PEM4S) to facilitate *Concept*'s integration in *Projects*.

5.8.PLP Based Projects' CSFs

Based on the AHMM4AI, LRP and *Intelligence*, for this CSA's CSFs/KPI were weight and the results are shown in Table 3. This CSA's result of 7.20, which is low, and that is due to the fact that inter-operability, and constraints' management are complex tasks and can be feasible. All the presented CSAs can be verified in the PoC's implementation.

Table 3: This CSA's average is 8.60.

Critical Success Factors	AHMM4ERC: KPIs	Weightings
CSF_PLP-Projects_Qualitative	Feasible	From 1 to 10. **09 Selected**
CSF_PLP-Projects_Inter_Operability	Complex	From 1 to 10. **08 Selected**
CSF_PLP-Projects_Constraints	Complex	From 1 to 10. **08 Selected**
CSF_PLP-Projects_AI_Modules	Feasible	From 1 to 10. **09 Selected**
CSF_PLP-Projects_sUnits	Feasible	From 1 to 10. **09 Selected**

valuation

6. IMPLEMENTING THE CONCEPT IN PROJECTS

6.1. Concept's Needed Skills

The needed set of skills are [68,69]: 1) Polymathic Security architecture; 2) Interfacing of EA and Security architectures; 3) Detailed AI and PLPs modeling and integration; 4) Interfacing AI components; 5) *Concept* related application's sBPMs and sSRVs; 6) Security and common requirement engineering; 7) Standardized sICS integration; 8) TDM/EA, sMDTCAS, and related Business, Data, Application, and Technology Architectures; 9) Generic skills like leadership and audit; 10) Business and organizational engineering; 11) PM technics; 12) ICS IDE technologies; 13) Business use cases design sBPMs integration; 12) Standard frameworks; 13) Building PEMs*;* and other.

6.2. Implementing a PEM and PEM4S

There are many approaches for building a PEM and PEM4S (simply a *MetaModel*), where a *MetaModel* is crucial for *Projects* and for their Security; which might take many years to finalize. To avoid *Entity's* locked-in commercial sICS/Security and AI products, a recommended way is to apply a Relational DataBase (RDB) based *MetaModel*. An RDB-based *MetaModel* can be implemented by using *Entity's* sICS/data-storage and RDB Security concepts and mechanisms; without the need for continuous massive investments in siloed-commercial products. A *MetaModel* supports a *Project*, because the RDB is normally used in all sICS' and Security subsystems. RDB's primary advantage is that they contain all the essential security requirements, information,

structures, integrity-checking controls, and applied MM constraints/constructs [61]. Another possibility is to use an Asset Management (AM) based *MetaModel,* in which a Project can use the Holistic Project Asset Management Concept (HPAMC) to support a *MetaModel*. The HPAMC manages and secures *Entity's* assets that includes all its resources/assets: 1) Business cases, requirements, and processes; 2) Financial and real-estates assets; 3) Software, RDBs, sICS components; and other types of assets [6]. The *MetaModel* delivers a transcendent and generic approach which is usable by the sMDTCAS.

6.3. *The MetaModel and sMDTCAS*

The *Concept* is an AI driven-concept that offers PLP templates and PLPPs to support *Entity's Intelligence* and also is coupled with the *MetaModel* and sMDTCAS. The *MetaModel* and sMDTCAS support the mapping concept for the common, business and Security *Project's* requirements. The *MetaModel* and sMDTCAS need a successful USP... The USP generates sSRVs which contain *Intelligence* and application services and for that there is the need to apply the "1:1" mapping concept. The *Concept* use *MetaModel* and sMDTCAS interfaces to interact with various NLP scripts which's main aim is: 1) To find HDT based solutions; 2) Locate fallouts; 3) Interface different sICS-languages and IDEs; 4) Security components; and 5) Accesses *MetaModel's* dictionaries and registries. PLPs and related NLP scripts use traditional Universal Description, Discovery and Integration (UDDI) or Application Programming Interface (API) to manage accesses to sSRVs and sBPMs catalogues. Registries link *Intelligence*, sBPMs and their interaction with sSRVs, which are registered by active PLPs. The *MetaModel* uses the registry and dictionary to interface *Entity's* ICS and Security components. The *MetaModel* can be used to access high-level management tools based on SWOT to evaluate the effectiveness of *Concept's* integration. A *MetaModel* can used to apply SWOT based analysis, where its elements relate to Factors by using the interface *Concept* for Security Specific Factors (Concept2SSFAC) class-structure type. Each CSA contains related Security Specific CSFs and in turn KPIs where each KPI links to an sICS variable (VAR, which is a sSRV's attribute(s) and is represented as sSRV.VAR) [63,64], an the various structures are shown in Figure 16.

```
SWOT2CSA
{
        S_Value          = HDT.eval( CSA.S_Value );
        W_Value          = HDT.eval(  CSA.W_Value );
        O_Value          = HDT.eval(  CSA.O_Value );
        T_Value          = HDT.eval(  CSA.T_Value );
};

CSA2CSF
{
        S_Value          = HDT.eval(  CSF.S_Value );
        W_Value          = HDT.eval(  CSF.W_Value );
        O_Value          = HDT.eval(  CSF.O_Value );
        T_Value          = HDT.eval(  CSF.T_Value );
```

```
};

CSF2KPI
{
        S_Value         = HDT.eval(  KPI.S_Value );
        W_Value         = HDT.eval(  KPI.W_Value );
        O_Value         = HDT.eval(  KPI.O_Value );
        T_Value         = HDT.eval(  KPI.T_Value );
};
```

Interfacing to sCBBs with KPI elements relate VARs by using the KPI2VAR structure:

```
KPI2VAR
{
        S_Value         = HDT.eval(  BB.VAR.S_Value );
        W_Value         = HDT.eval(  BB.VAR.W_Value );
        O_Value         = HDT.eval(  BB.VAR.O_Value );
        T_Value         = HDT.eval(  BB.VAR.T_Value );
};
```

Figure 16: Concept2SSFAC's structures.

6.4. Interfacing sICS Implementation Environment

The *MetaModel*, *Concept*, and Concept2SSFAC, interface the sICS environment's components to persisted PLPs, by:

- Security concepts and architecture guidelines.
- Behaviour Driven Development (BDD) that is accessed by NLP scripts .
- Modelling languages like UML, OOM, and ArchiMate which include behavioural and structural elements (and a wide-range of relationships) [35].
- Application cartography refinement tools and extracted diagrams, like TOGAF's Application Communication Diagram (ACD) that depicts all used ICS and Security models; with their mappings related to communication between secured applications and accesses sCBBs.
- API's Management (APIM) tools [65].
- Test Driven Development (TDD) is a programming approach and a concept where software developers design the test first concept.
- Acceptance Test-Driven Development (ATDD) that is applied to test the collaboration of business clients, *Project* engineers, *Project* testers and software engineers to finalize a subsystem [66].
- A secured PLP Test (sPLPT) that combines TDDs, ATDDs and is based on developing tests where tests represent the results of the requirement's behaviour of a set of NLP scripts.
- Requirements' implementation uses NLP scripts and methodologies like UML.
- *MetaModel*'s and sMDTCAS' capabilities to interface PLP based *Intelligence*.
- PLP accumulated Implementation Development Environments (IDE) and Development and Operations (DevOps) experiences.
- The *Concept* consults Security specialists, executive directors, Project-members, and is designed to identify EA and Security risks [71].
- Integrating standards ²frameworks, like risk frameworks; like the popular COSO which is presented in Figure 17.

COSO defines basic components, a common language and a roadmap for *Project's* sRisk management. sRisks' mitigation and management objectives are: 1) Strategic; 2) Operations; 3) Reporting; and 4) Compliance. And related Factors are [70]: 1) Organizational; 2) *Concept's* interfacing; 3) sRisks' assessment; 4) Determining

sRisks' possibilities; 5) Identifying sRisk responses and actions; 6) Communication of sRisk results and storing them in PLPs; 7) Monitoring; and 8) Integrating the Digital Forensics and Incident Response (DFIR) Concept (DFIRC).

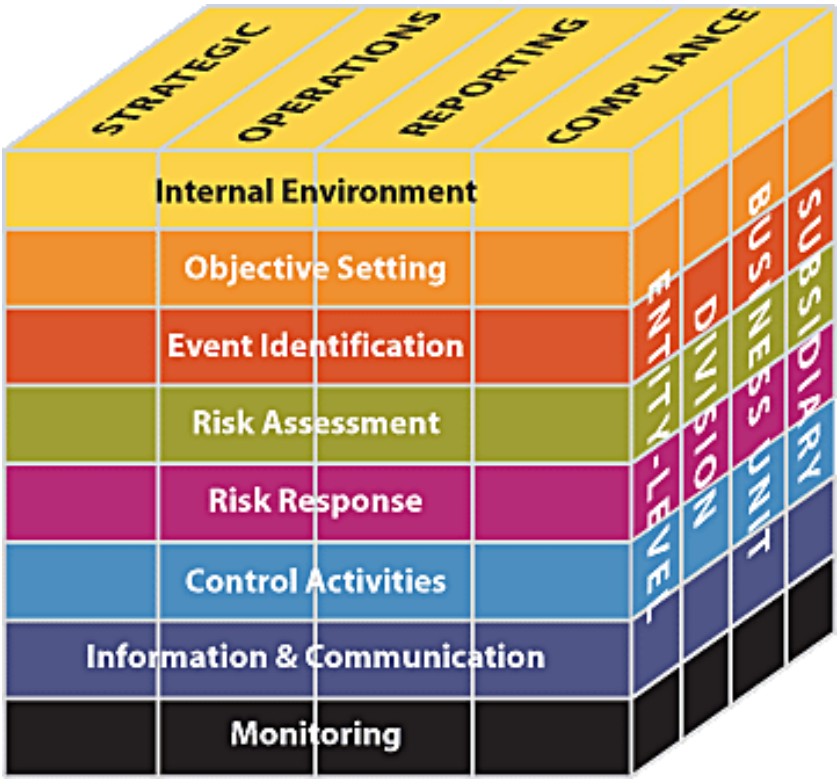

Figure 17: The COSO framework [70].

The *Concept* can interface frameworks like COSO which include common components, a common language and offers a roadmap for risk-management, which modifies and enhances PLPs.

6.5. The Concept, Global Cybersecurity and Crimes

The *Concept* includes Cybersecurity and governance of sRisks and related Factors, which can be mitigated, to ensure *Entity's* global evolution and to predict (and eventually) block Cyber (or traditional) crimes/misdeeds. *Entity's* and its partners Cyberspace's resilience, control, and security concepts are siloed, insufficient, chaotic, and concentrate only on sICS/technical-platforms' infrastructural characteristics, which can be fed in PLPs. *Entities* are aggressed by Cybercrimes that are based on Cybersecurity weaknesses and violations that are difficult to detect. Secured *Projects* and hence *Entities* are very complex to secure, because of various sICS and APD problems, and they depend on the *Entity's* structure and PLPs management. The *Entity's* structure depends on sSRVs and sICS which are used to (re)organize sUnits. The *Concept* uses sMDTCAS and TDM to integrate standard methodologies, like TOGAF and SABSA [44,45]. The sICS related *Projects* use TDM's cyclic phases, which includes USPs. Figure 18 shows sBPMs' Security roadmap, which can be integrated in PLPs. Using sBPMs in PLPs enables: 1) The reduction of PLPs complexities; 2) Parallel development of sBPMs using secured DevOps (DevSecOps); 3) Valuation and allocation of Security controls to sICS elements, sSRVs, …; 4) Optimizing

interdependencies between sBPMs and Security controls; 5) *Entity* wide Security monitoring, optimization and improvement of PLPs using DevSecOps. [72,73].

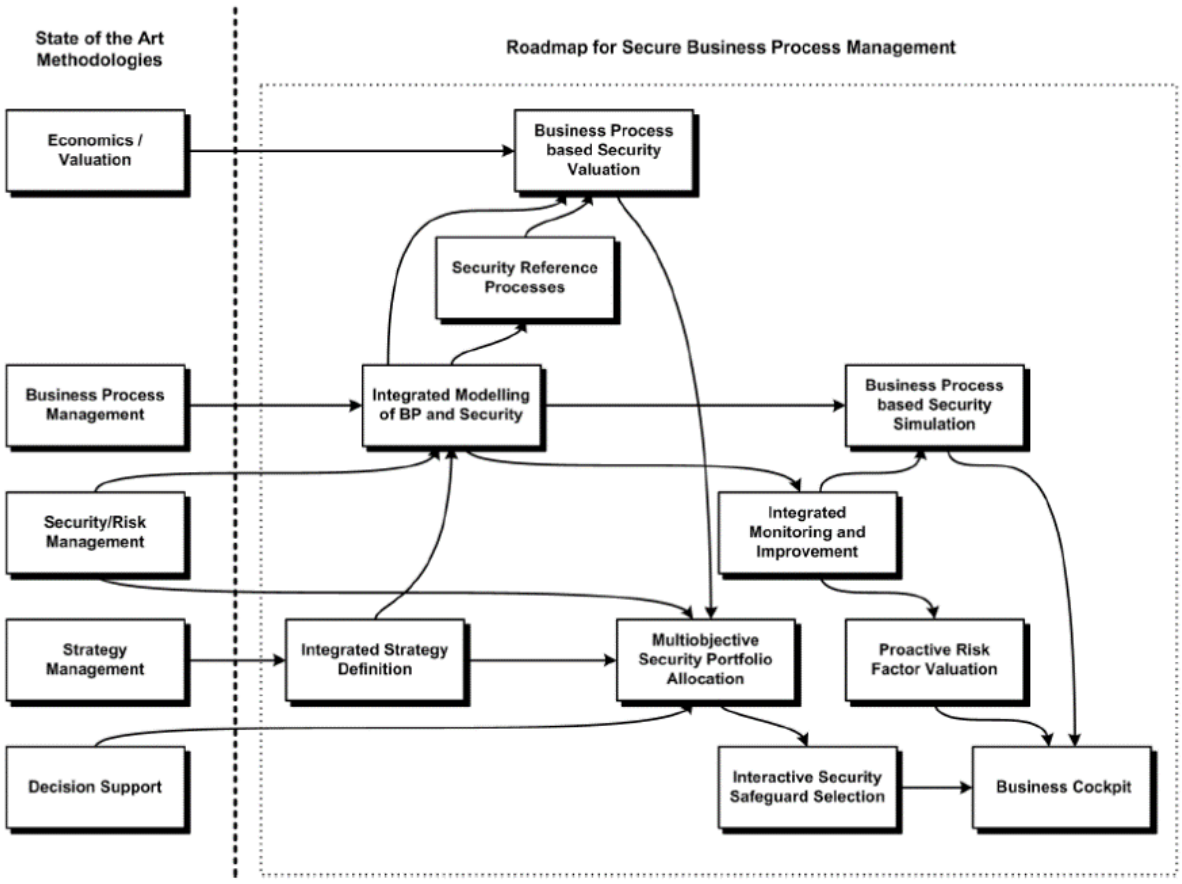

Figure 18: Roadmap for secured sBPMs for PLPs [73].

6.6. The Use of DevSecOps

DevSecOps manages: 1) *Project's* IDEs, developers, operations and security specialists; 2) Is controlled by a *Entity* Secured Control and Logging Infrastructure (ESCLI), which feeds PLPs; and 3) PLPs editing. Cyberbusiness platforms are not *Project* and APD agnostic but can offer: 1) Better performance; 2) Reliability; and 3) Cybersecurity/Tracing in PLPs. sUnits are controlled/monitored in real-time by the ESCLI which is optimal for monitoring and support PLPs' presentation, sorting, and tuning. An ESCLI can used to analyse, collect and store in PLPs. An *Entity* can also build an IHI secured Cloud (sCloud) to avoid locked-in situations and important security breaches. The *Concept* uses EA/TDM to support interfacing market risk frameworks like COSO, which is shown in Figure 19 [72].

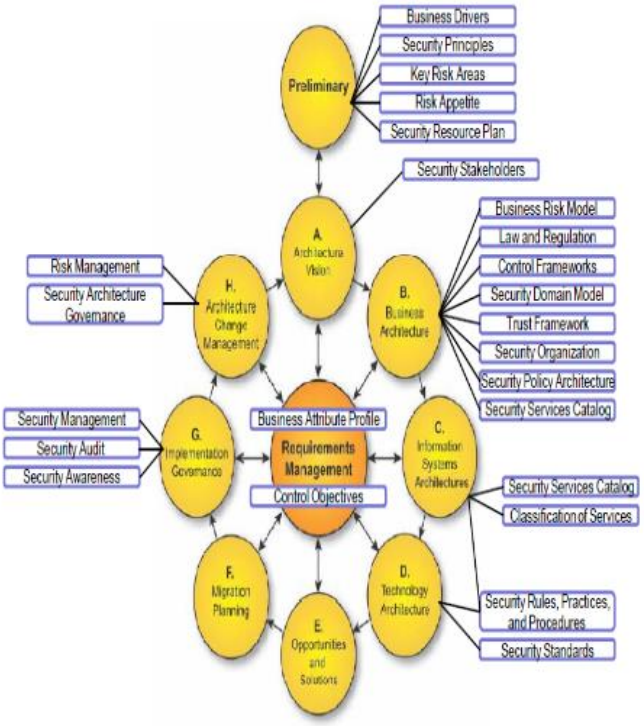

Figure 19: Integration of SABSA with the *Concept* [45].

Entity(S/C) needs the *Concept* to combine many security fields where Cybersecurity is the central issue. Therefore, the *Concept* needs the TDM, which interfaces frameworks like ADM, SAFe, COBIT, CISA… Unfortunately, today, we are just tackling isolated fields like Software security, Network Security… As shown in Figure 20.

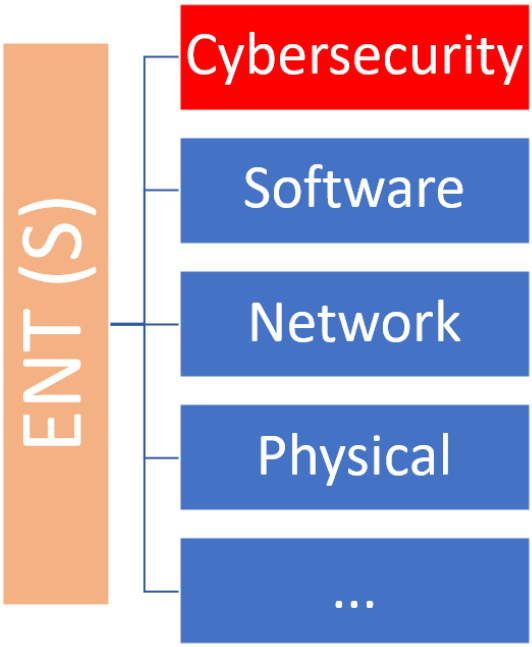

Figure 20: *Entity*'s ETP-HSC Approach [1].

6.7. Concept's CSFs

Based on the AHMM4AI, LRP and *Intelligence*, for this CSA's CSFs/KPI were weight and the results are shown in Table 4. This CSA's result of 9.0, which is high, and that is due to the fact that the *Concept* is built on mature

components and previous RDP findings; so the *Concept* CSA is implementable. As previously mentioned all presented CSAs are verified in the PoC's implementation.

Table 4: This CSA's average is 7.20.

Critical Success Factors	AHMM4AI enhances: KPIs	Weightings
CSF_Concept_Projects_Skills	Proven	From 1 to 10. **10 Selected**
CSF_Concept_Projects_MetaModel	Possible	From 1 to 10. **09 Selected**
CSF_Concept_Projects_HighLevel_Interfacing	Proven	From 1 to 10. **10 Selected**
CSF_Concept_Projects_Cybersecurity	Complex	From 1 to 10. **08 Selected**
CSF_Concept_Projects_DevSecOps	Possible	From 1 to 10. **08 Selected**

valuation

7. THE POC'S IMPLEMENTATION

7.1. Concept's Basic Preparations

The first step is to reuse ETP-HSC's PoC [1] and then to prepare environment by setting-up the PPAV, sMDTCAS/TDM, and the PLPs storage for EUBank, as shown in Figure 21 [27].

Figure 21: PoC's preparations sequences [1].

This PoC uses various *TRADf* modules, like the USP and *Concept*, which focus on the extraction and securing of sSRVs [27], that can support EUBank's secured sATR.

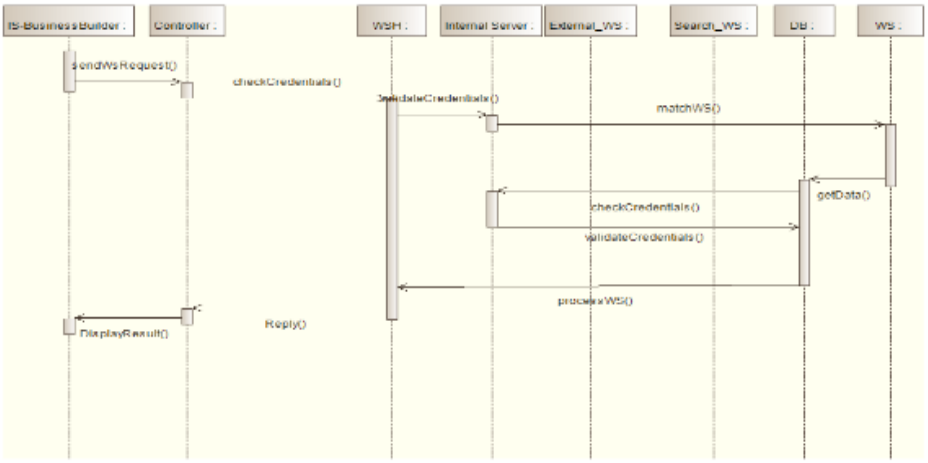

Figure 22: The sATR's activity diagram.

sCBBs are assembled to build sSRVs' based sBPMs/scenarios and sATRs, which need the optimal level/approach of granularity that respects the "1:1" mapping mechanism [45,46]. A logical view of a series of sSRVs based sATRs is presented in Figure 22, and their consumption of SRVs, in the form of an sMDTCAS' variant of the activity diagram. where events are managed by the sICS node-servers, that require ETP-HSC encryption which is managed by the TDM. The sATR uses a set of sCBBs which are presented in Figure 23. The ADM/TDM phases B,C, and D, implement the needed sATRs; and at last update PLPs.

USP-APD Environnement	Provide APD sSRVs
Controller	Passes a SRV request
Find sSRV	Execute
Data Source	Return information and update PLPs

Figure 23: sATR's elements.

7.2. Concept's Design and Implementation

PoC's essential constraint is to use existing sICS and security standards in a reduced form, what corresponds to sMDTCAS' main objective. In this case the sMDTCAS transcendent sSRVs, and diagrams are used. These standards include sSRVs to be used to integrate sBPMs and HDT scenarios in the existing sUnits. To identify the initial sets of CSAs' CSFs and test whether the RQ's of CSFs affect *Concept's* (including the or ETP-HSC) integration. The PoC uses the HDT based mixed qualitative and quantitative method. The PoC in the beginning uses Phase 1 that is mainly based on the HDT DTs, which uses the RWC. Phase 1 is used to weight the relative importance of CSAs and CSFs for the usage of *Concept* or ETP-HSC and that is done using a DTs [47].

7.3. PoC's Phase 1

RDP's LRP outcome proves the existence of an important research-knowledge gap and it's (or Phase 1's) outcome supports the RQ's credibility, by the use of the LRP and *TRADf*'s archive or knowledge-base, of an important set of references, previous author's IHITF, articles, works, documents, and links.

Table 5: PoC's phase 1 outcome is (rounded) 8.40.

/

CSA Category of CSFs/KPIs	Project/Concept Capability	Average Result	Table
RDP's Integration	Usable-Mature	From 1 to 10. 9.25	1
sICS/Technology	Transformable-Possible-Difficulties	From 1 to 10. 8.50	2
PLP based Projects	Transformable-Possible-Difficulties	From 1 to 10. 8.60	3
Concept's Integration	Heterogenous-VeryComplex	From 1 to 10. 7.20	5
Evaluate First Phase			

After selecting the needed *Concept*'s Factors, they are linked to various HDT's NLP scenarios. The PoC is based on the CSFs' binding to specific RDP resources, where the *Concept* was prototyped using *TRADf*. The HDT represents the relationships between this RDP's RQ and *Project* requirements, sSRVs, PLPs, and selected Factors. PoC's interfaces were achieved using Microsoft Visual Studio .NET environment and *TRADf*. The *Concept* uses calls to resulting sSRVs, to execute HDT actions related to *Concept* security requests. CSFs were selected and evaluated (using WGTs, HDT, and *Intelligence*) and the results are illustrated in Table 5, which shows that the *Concept* is a central phase and not an independent undertaking. In fact, it is essential for the *Project's* risk concept. HDT's main constraint is that CSAs having an average result below 7.5, will be ignored. This fact, leaves the *Concept*'s CSAs (marked in green) effective for RDP's conclusion(s); and drops the CSAs marked in red. Phase 1, shows that the *Concept* part of the *Project* will probably fail and is a very complex one because of the *Concept*'s complex security operations. The PoC can proceed to Phase 2.

7.4. PoC's Phase 2

Starts with sMDTCAS/TDM's, PLPs storage's setup and Factors selection. Phase's 2 setup includes: 1) Sub-phase A or the PPAV and Architecture Vision phase's goals, establishes a *Concept* approach and goals; 2) Sub-phase B or the Business Architecture phase establishes *Concept's* target TDM/EA and related PLPs' activities; 3) Sub-phase C shows and uses the Application Communication Diagram to describe *Concepts*' activities; 4) Sub-phase D or the Target Technology Architecture shows the needed *Concept* and ETP-HSC's optimal infrastructure landscape; and 5) Sub-phases E and F, or the Implementation and Migration Planning, presents the transition PPAV based architecture, which proposes intermediate situation(s) and evaluates *Concept*'s status. sSRVs and HDT based *Intelligence* has mappings to *Entity's* resources and the *Concept* defines relationships between sSRVs, *MetaModel*/sMDTCAS, PLPs, and Problems (PRB).

7.5. PRBs Processing in a Concrete HDT Node

The *Intelligence* solves *Concept's* PRBs, where Factors link to specific *Concept* PRB type and has a set of actions that are processed in a concrete HDT node. For this goal, the action *CSF_Concept_or_ETP-HSC_Extraction_Procedure* was called and delivered SOL(s). Solving PRBs involves the selection of actions and possible Solutions (SOL) for multiple *Project* activities. The HDT is on mixed quantitative/qualitative and has a dual-objective that uses the following steps:

- In Phase 1, *TRADf's* interface implements HDT scripts to process the selected CSAs. And then relates PoC's resources to *CSF_Concept_or_ETP-HSC_Extraction_Procedure*.
- The *Intelligence* is configured to weight and tuned to support the HDT.
- Link the selected node to HDT to deliver the root node.
- The HDT starts with the *CSF_Concept_or_ETP-HSC_Extraction_Procedure* and proposes SOL(s) in the form of *Concept* actions/improvements.

HDT scripts support AHMM4AI's instance that are processed in the background to deliver *Concept* or ETP-HSC risk procedures and value(s). The AHMM4AI based *Intelligence* uses sSRVs to deliver *Concept* operations; which are a set of *Concepts* actions that are stored in PLPs.

7.6. Interfacing High-Level Methods and PLPs

Using Factors to interface SWOT as shown in Figure 24 and *Concept* executes the following steps:

- Use *TRADf's* variant of SWOT, the SWOT based Transformation's Organizational Risks' Management (STORM) [x64].
- Linking *Concept* to STORM.
- Factors tags are linked to various STORM scenarios.
- Links Factors to structures, like CSA2CSF…
- Intelligence and its HDT NLP scripts to deliver SWOT's output/solutions.
- Output/solutions are persisted in PLPs.

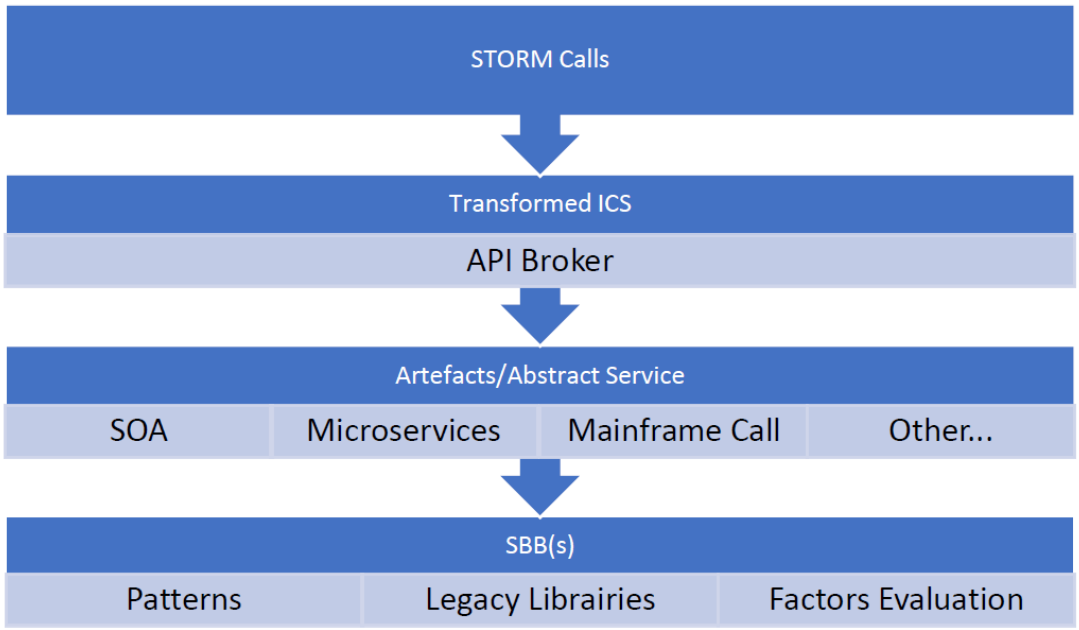

Figure 24: Interacting SWOT/ STORM.

The used SWOT/ STORM are: Concept2SSFAC, CSA2CSF, CSF2KPI, and KPI2VAR; and then IHITF's frontend mapping actions are activated by: 1) Selecting HDT nodes that contains *Concept's* Factors, and 2) Selecting the security problem to be solved. SWOT/ STORM uses Intelligence to generate needed actions to solve a request and store the results in PLPs.

8. CONCLUSION AND RECOMMENDATIONS

The *Project* must use the USP to transform the legacy ICS and deliver an sICS and the pool of sSRVs; the USP is very complex and can be the cause of *Projects'* failures and success rates can be improved by using an IHITF, *Concept*/ETP-HSC, and PPAVs based related strategies. PPAVs uses an optimal security and PLP based approach and the PoC proved *Concep's* complexities [36,19]. The *Concept* supports sICS, sSRVs and sBPMs based PPAVs concept to facilitate the transformation of sUnits. The proposed PLP management approach is an optimal for the *Concept* which supports *Project's* security related PLPs management; and the LRP presented an important knowledge gap, that is mainly due to the fact that are no similar IHITF, *Concept*, *Metamodel*/sMDTCAS approaches and that there is an extreme lack of a Polymathic-holistic approaches. There are siloed and limited manual security tools and methods, but the *Concept* presents the possibility to implement an IHITF and an *Entity* specific *Concept* [44].

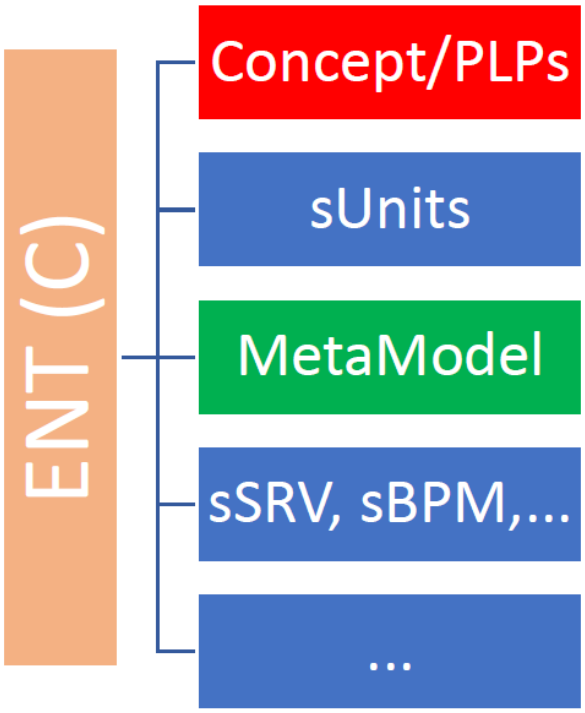

Figure 25: Viewpoint's "U" evolution roadmap.

The RDP is a part of a series of publications on *Projects*, Security strategies, *Concept*, *MetaModel*, TDM/EA, Polymathic models… The *Project* uses the HDT and Factors to support *Concept* activities, where the *Concept* focuses on managing PLPs and complex USP's outputs. The *Concept* synchronizes a structured relationship between: Security, PLPs, sRisks' management, sMDTCAS, TDM/EA, *Project* constraints, and HDT based *Intelligence*. *Project's* most important recommendation, is that the *Project* team must be skilled to manage *Concept* activities. The PoC's Table 5 result of (rounded) 8.40 that used Factors and CSFs' binding to a RDP

resources, the *Intelligence*, RQ, *Concept,* and sSRVs, shows that the *Concept* is very complex due to ICS' siloed nature and lack of Polymathic approach. The *Concept* uses an IHI process/methodology and framework; and this article's set of recommendations are:

- This article presents the IHI *Concept* which tries to avoid locked-in security strategies and ensures *Project's* success.
- This RDP uses a multi-dimensional *Concept*, because it has: 1) An adapted mixed-research approach; 2) Shows how to build an IHITF; and 3) A methodological approach based on EA and AI.
- The RLR proved the existence of an important knowledge gap.
- To use a MM, like the AHMM4AI, to support PLPs and HDT, to other *Intelligence's* operations.
- Cross-functional/Polymathic skills are needed for the *Concept* and such *Projects*.
- The *Concept* coordinates PLPs' integration to deliver knowledge blueprints, patterns, …
- To implement a PLPWT based teamwork.
- *Concept* is optimal because it promotes Polymathism, critical-thinking, and a unified security viewpoint.
- The sMDTCAS and *MetaModel* based *Concept* fits in the TDM.
- TDM's integration in the *Concept* enables the automation of all its refinement activities.
- *Concept* constraints are controlled and monitored by the ICS.
- *Entities'* sustainability is orthogonal to its *Concept* capacities.
- To avoid any form of security locked-in scenario the *Entity* must build its own *Concept*, ETP-HSC, and IHITF.
- The *Project* can R2C, which should be predicted by using the IHITF.
- The high demand for *Projects'* and the hyper evolution of sICS and related security technologies, can create major problems because of the differences in their evolutions.
- All author's works are based on *TRADf*, AHMM, TDM, and RDP; which are today mature and can be applied in various APDs and any type of *Project*.
- *Concept* like the USP, is a *Project's* critical phase.
- A *Project* must build a holistic TDM and sMDTCAS to support *Concept's* activities.
- The *Concept* unbundles the legacy BPMs to support sUnits, which can face problems in the alignment of various sSRVs.
- Each *Entity* constructs its own IHI *Concept*, *MetaModel*, and ETP-HSC.
- The *Concept* replaces legacy security environments using conversion concepts in order to ensure *Project's* success.
- The *Concept* interface *Entity's* TDM and delivers the pool of sSRVs based diagrams.
- The ADM based TDM, manages design, *Concept*, DevSecOps, and governance activities.
- TDM's and DevSecOps' integration with the *Concept*, enables the automation of all *Project's* security activities.
- *Entity's* sSRVs and sBPMs stability and coherence are crucial for its evolution.
- sSRVs can be (re)used in sBPMs; where a sUnit is a set of sBPMs and different sUnits can share sBPMs.
- sUnit's transformation needs an IHITF and sMDTCAS that transforms and secures an *Entity*.

- Avoid consulting firms and commercial products to build internal *Concept* mechanisms.
- *Concept* and ETP-HSC are very complex and will very probably face major complexities.
- Each *Entity(S)* constructs its own IHI security strategy.
- The *Concept* unbundles legacy system and security modules to support the *MetaModel*, which form new sUnits; and a maintainable *Entity(C)*.
- Viewpoint's "C" presents a structured evolution's roadmap for the *Concept*, as shown in Figure 25.
- *TRADf* was used to show to iimplement an IHITF and sMDTCAS.
- The IHITF manages all *Project* requirements.
- To use the TDM for defining *Project's target architecture*, which can support the *Concept*.
- The TDM EA serves as a methodology and tool to provide the link between the *Concept*, *Project*, and PLPs.
- The TDM manages the USP and relates it to *Concept* activities.
- Implement a TDM that manages the delivered pool of sCBBs and sSRVs.
- Implement a flexible and scalable sICS.
- Establish an optimal *MetaModel*.
- The NLP concept is mature to support the HDT.
- The *Concept* is complex, but is feasibility; and it interface the *MetaModel*.
- A *Project* uses NLP scripts to integrate *Intelligence*.
- A *Project* must apply *Concept* for the *Entity*'s security activities.
- The *Concept*'s complexity lies in sICS heterogeneous components.
- Use AR for PLPs.
- Collect ROXs to enhance LPs.
- The Project uses PLPWT to integrate *Concept*.
- *Intelligence* interfaces existing AI-domains like ML, DL, OR, LP,…
- Use the RWC based decision tables to filter and weight CSAs.
- Use the HDT to solve security problems and updates the related PLPs.
- *Intelligence* defines a strategy to persist the PLPs and how to use them for future problems.
- The *Concept* interfaces high-level methods like SWOT/STORM.
- Accumulated experiences and PLPs are fed in the *Entity's* storage.

References

[1] A. Trad. Enterprise Transformation Projects-The Role of Enterprise Architecture in Implementing a Holistic Security Concept (ETP-HSC). ISSN: 2795-4609 | ISSN: 2795-4560. Advanced Research on Information Systems Security, an International Journal (ARIS2) (2023) Volume 3, No 1, pp 04-35. International Journal. 2023.

[2] A. Trad. Enterprise Transformation Projects- The Polymathic Enterprise Architecture Based Generic Learning Processes (PEAbGLP). 2024. Submitted.

[3] A. Trad and D. Kalpića. Using Applied Mathematical Models for Business Transformation. IGI Complete Author Book. IGI Global. USA. 2019.

[4] A. Trad. Academic and Educational Transformation Projects-The Role Team-Based Learning in Polymathics (RTBLP). IGI Global. USA. 2023.

[5] A. Trad. Academic and Educational Transformation Projects-The Role Team-Based Learning in Polymathics For University Cycle (RTBLP4UC). IGI Global. USA. 2023.

[6] H. Pushpakumara, P. Jayaweera and W. Manjulan. Using the Open Group Architecture Framework (TOGAF) for Quality Assurance in Higher Education Teaching and Learning. January 2021 SSRN Electronic Journal. DOI: 10.2139/ssrn.3808691. 2021.

[7] A. Trad. The Business Transformation and Enterprise Architecture Framework-The Applied Holistic Mathematical Model's Persistence Concept (AHMMPC). WSEAS. 2019.
[8] A. Trad. A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-Intelligent aBB architecture. Centeris. Portugal. 2015.
[9] A. Trad. Organizational and Digital Transformation Projects-A Mathematical Model for Building Blocks based Organizational Unbundling Process. IGI-Global. USA. 2023.
[10] A. Trad and D. Kalpić. Business Transformation Projects based on a Holistic Enterprise Architecture Pattern (HEAP)-The Basics. IGI. USA. 2022.
[11] A. Trad and D. Kalpić. Business Transformation Projects based on a Holistic Enterprise Architecture Pattern (HEAP)-The Implementation. IGI. USA. 2022.
[12] A. Trad. Business Transformation Project's-The Impact of Rise of Over-the-Top (OTT). IGI-Global. USA. 2023.
[13] R. Blackburn and B. Rosen. Total quality and human resources management: lessons learned from Baldrige Award-winning companies. Academy of Management PerspectivesVol. 7, No. 3 Articles. Published Online:1 Aug 1993.
[14] J. Koenig, K. Rustan and M. Leino. *Programming Language Features for Refinement*. Stanford University. USA. 2016.
[15] A. Trad and D. Kalpić. An applied mathematical model for business transformation-The Holistic Critical Success Factors Management System (HCSFMS). Encyclopaedia of E-Commerce Development. Journal: Encyclopaedia of E-Commerce Development, Implementation, and Management. Hershey, PA: IGI-Global. 2018.
[16] S. Peterson. Why it Worked: Critical Success Factors of a Financial Reform Project in Africa. *Faculty Research Working Paper Series*. Harvard Kennedy School. 2011.
[17] B. Dick. *Action research: action and research*. Australia: Southern Cross. University Press. [21-27]. 2001.
[18] T. Ylimäki. Potential critical success factors for EA. *Journal of Enterprise Architecture*, Vol. 2, No. 4, pp. 29-40. 2006.
[19] H. Daellenbach, D. McNickle and Sh. Dye. Management Science. Decision-making through systems thinking. 2nd edition. Plagrave Macmillian. USA. 2012.
[20] A. Trad. Applied Holistic Mathematical Models for Dynamic Systems (AHMM4DS). International Journal of Cyber-Physical Systems (IJCPS). IGI-Global. USA. DOI: 10.4018/IJCPS.2021010101. 2021.
[21] A. Trad. Business Transformation Projects-The Role of a Transcendent Software Engineering Concept (RoTSEC). IGI Book Chapter. IGI Global. USA. 2022.
[22] A. Trad. Business Transformation Projects-The Role of Requirements Engineering (RoRE). *IGI Book Chapter*. IGI Global. USA. 2022.
[23] A. Trad. Business Transformation Projects based on a Holistic Enterprise Architecture Pattern (HEAP)-The Basic Construction. IGI Book Chapter. IGI Global. USA. 2023.
[24] A. Trad. Integrating Holistic Enterprise Architecture Pattern-A Proof of Concept. IGI Book Chapter. IGI Global. USA. 2023.
[25] A. Trad. A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-Intelligent atomic building block architecture. *Journal: Procedia Computer Science*, Volume 64, Pages 214-223. Elsevier. 2015.
[26] A. Trad. A Transformation Framework Proposal for Managers in Business Innovation and Business Transformation Projects-An Information System's Atomic Architecture Vision. *Journal: Procedia Computer Science*. Volume 64, Pages 204-213. Elsevier. 2015.
[27] A. Trad. Organizational and Digital Transformation Projects-A Mathematical Model for Building Blocks based Organizational Unbundling Process. IGI Global. USA. 2023.
[28] A. Trad. Organizational and Digital Transformation *Projects*-A Mathematical Model for Enterprise Organizational Models. IGI. USA. 2022.
[29] B. O'Riordan. INNOVATION-Why Transformations Fail And How They Can Succeed With People Power. Forbes. 2021.
[30] Standish. The Chaos Reports. http://www.standish.com, Standish. USA. 2011.
[31] The Open Group. Introduction to the Architecture Development Method (ADM). The Open Group. USA. 2011.
[32] Bizzdesign. Digital Transformation. Bizzdesign. 2022. Avalable https://bizzdesign.com/blog-category/digital-transformation/
[33] M. Möhring, B. Keller, R. Schmidt, L. Sandkuhl and A. Zimmermann. Digitalization and enterprise architecture management: a perspective on benefits and challenges. SN Bus Econ 2023. Avalable https://doi.org/10.1007/s43546-023-00426-3
[34] A. Liu. Rumbaugh, Booch and Jacobson Methodologies. Opengenus. 2022; Avalable https://iq.opengenus.org/rumbaugh-booch-and-jacobson-methodologies/
[35] Hosiaisluoma. Holistic Enterprise Development. 2022. Avalable https://www.hosiaisluoma.fi/blog/archimate-examples
[36] D. Greefhorst. Using the Open Group's Architecture Framework as a pragmatic approach to architecture. NIRIA. Jaarbeurs, Utrecht. KIVI NIRIA, afd. Informatica. Netherlands. 2009.
[37] The Open Group. Building Blocks. Introduction to Building Blocks. The Open Group. USA. 1999.
[38] The Open Group. Foundation Architecture: Technical Reference Model. The Open Group. USA. Avalable http://www.opengroup.org/public/arch/p3/trm/trm_dtail.htm. 2011
[39] The Open Group. The Open Group Cloud Ecosystem Reference Model – Using the Cloud Ecosystem Reference Model with the TOGAF Standard (Informative). The Open Group. Avalable http://www.opengroup.org/cloud/cloud_ecosystem_rm/p5.htm. 2011.
[40] F. Pavel. Grid Database—Management, OGSA and Integration. Academy of Economic Studies Romania, Bucharest, Database Systems Journal, Vol. II, No. 2/2011, Romania. 2011.
[41] RedHat. Decision Model and Notation (DMN). RedHat. 2022. Avalable https://access.redhat.com/documentation/en-us/red_hat_process_automation_manager/7.1/html/designing_a_decision_service_using_dmn_models/dmn-elements-example-con

[42] The Open Group. Sample catalogs, matrices and diagrams. The Open Group. USA. 2011. Avalable http://www.opengroup.org/bookstore/catalog/i093.htm
[43] K. Kuwashima. How to Use Models of Organizational Decision Making? Annals of Business Administrative Science 13 (2014) 215–230. 2014. Avalable www.gbrc.jp http://dx.doi.org/10.7880/abas.13.215. ISSN 1347-4456 Print ISSN 1347-4464. ©2014 Global Business Research Center.
[44] SABSA. *Sherwood Applied Business Security Architecture*. SABSA. 2020. Available https://sabsa.org/
[45] J. Kasarkod. Integration of SABSA Security Architecture Approaches with TOGAF ADM. InfoQ. Avalable https://www.infoq.com/news/2011/11/togaf-sabsa-integration/. 2011.
[46] V. Crittenden and E. Wilson. An Exploratory Study of Cross-Functional Education in the Undergraduate Marketing Curriculum. April Journal of Marketing Education 28(1):81-86. DOI: 10.1177/0273475305284643. 2006.
[47] T. Thune. Success Factors in Higher Education–Industry Collaboration: A case study of collaboration in the engineering field. Tertiary Education and Management volume 17, pages31–50. 2011.
[48] S. Heywood, R. Hillar and D. Turnbull. Insights into organization-How do I manage the complexity in my organization? Organization Practice. McKinsey & Company. 2010.
[49] Wikipedia. Polymath. Wikipedia. https://en.wikipedia.org/wiki/Polymath. 2021.
[50] Wikipedia. Complexity management. Wikipedia. 2023.
[51] M. Woudenberg and C.J. Unis. Systems Thinking-Skills and Insights to Resolve Wicked Problems. Systems Thinking. https://www.polymathicbeing.com/p/systems-thinking. 2023.
[52] G. Mobus and P. Fisher. Foraging Search at the Edge of Chaos. Lawrence Erlbaum & Associates, Mahwah, NJ. USA. 1999.
[53] K. Walch & R. Schmelzer. AI Today. AI and data Today. https://www.aidatatoday.com/
[54] A. Kapoor. Artificial intelligence and machine learning: 5 trends to watch out for in 2021. AI Zone. 2021 DZone. https://dzone.com/articles/artificial-intelligence-amp-machine-learning-5-dev. 2021.
[55] A. Trad and D. Kalpić. Transformation and Enterprise Architecture Projects-The Integration of Operational Research. The 3rd International Conference on Machine Learning and Intelligent Systems (MLIS 2021). 2021.
[56] J. Dornemann N. Rückert, K. Fischer and A. Taraz. Artificial intelligence and operations research in maritime logistics. Econstor. Leibniz Information Centre for Economics. Germany, 2020.
[57] F. Della Croce and V. T'kindt. A recovering beam search algorithm for the one-machine dynamic total completion time scheduling problem. J Oper Res Soc. 2002.
[58] BRM. Action Research. Business Research Methodology. BRM. 2022.
[59] A. Burns. CHAPTER ELEVEN-Action Research. UNSW Sydney. 2015.
[60] O'Leary. Action Research-Research Methodologies Guide. A collection of resources describing research. 2007.
[61] A. Trad. A Relational DataBase based Enterprise Transformation Projects. Journal: International Journal of Mathematics and Computers in Simulation. Volume 17, Pages. 1-11. NAUN. npublications.com. 2023.
[62] A. Trad and D. Kalpić. Business Transformation and Enterprise Architecture: The Holistic Project Asset Management Concept (HPAMC). Book: Handbook of Research on Strategic Fit and Design in Business Ecosystems. Pages: 194-230. IGI Global. USA. 2020.
[63] Javatpoint. Understanding SWOT Analysis. Javatpoint. https://www.javatpoint.com/swot. 2021.
[64] A. Trad and D. Kalpić. SWOT based Transformation's Organizational Risks' Management (STORM). E-leaders conference, Check Republic. www.g-casa.om. 2023
[65] S. Patni. Pro RESTful APIs Design, Build and Integrate with REST, JSON, XML and JAX-RS. 2017.
[66] D; Janzen and H. Saiedian. Test-driven development concepts, taxonomy, and future direction. Published in: Computer (Volume: 38, Issue: 9, Sept. 2005). IEEE. 2005.
[67] N. Koudelia. Acceptance test-driven development-Master Thesis. Uuniversity of Jyväskylä. Department of mathematical information technology. Jyväskylä. Finland. 2011.
[68] A. Trad. The business transformation enterprise architecture framework for innovation: The role of artificial intelligence in the global business education (RAIGBE). Journal: The Business & Management Review. Volume: 12, Issue 1, Pages: 82-97. Centre for Business & Economic Research. UK. cberuk.com. 2021.
[69] A. Trad and D. Kalpić. Business transformation project's architect's profile (BTPAP). The Business & Management Review. Volume 12, Issue 2, Pages 137-153. Centre for Business & Economic "Research. cberuk.com. 2021.
[70] P. Curtis and M. Carey. Committee of Sponsoring Organizations of the Treadway Commission-Risk Assessment in Practice. Deloitte & Touche LLP. 2012.
[71] A. Trad. The transformation framework The role security in the global education system. Journal: International Journal of Higher Education Management. Volume: 8, Issue 1. Centre for Business & Economic Research. UK. ijhem.com. 2021.
[72] A.Trad. Organizational Transformation Projects-The Role of Global Cyber Security and Crimes (EPSC). IGI Global. USA. 2023.
[73] Th. Neubauer, M. Klemen and S. Biffl. Secure business process management: A roadmap. Conference: Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on. DOI: 10.1109/ARES.2006.121. 2006.