Strategic & Systemic approach to address Security & Privacy in Digital Twin and Metaverse

ITU Workshop on the “Security and Privacy for Digital Twin and Metaverse ”

N. KISHOR NARANG

CONTEXT…

Disruption is everywhere and the future is uncertain — no one knows what the world will look like even a decade from now. As we head into future, we are surrounded by disruptive innovation

As we look to the years & decades ahead, tech-disruption will be driven as much by the methods and systems as it is by the devices, we associate with tech disruption.

The pace of innovation is incredibly fast, with new things getting discovered daily. The future trends in technology are very diverse, very intertwined, and very promising…

There are several developments that have and will continue to shape business strategies. From **Automation** to **Sustainability**, organizations are adapting to a whole new wave of consumer preferences.

narnix

The Digital Transformation

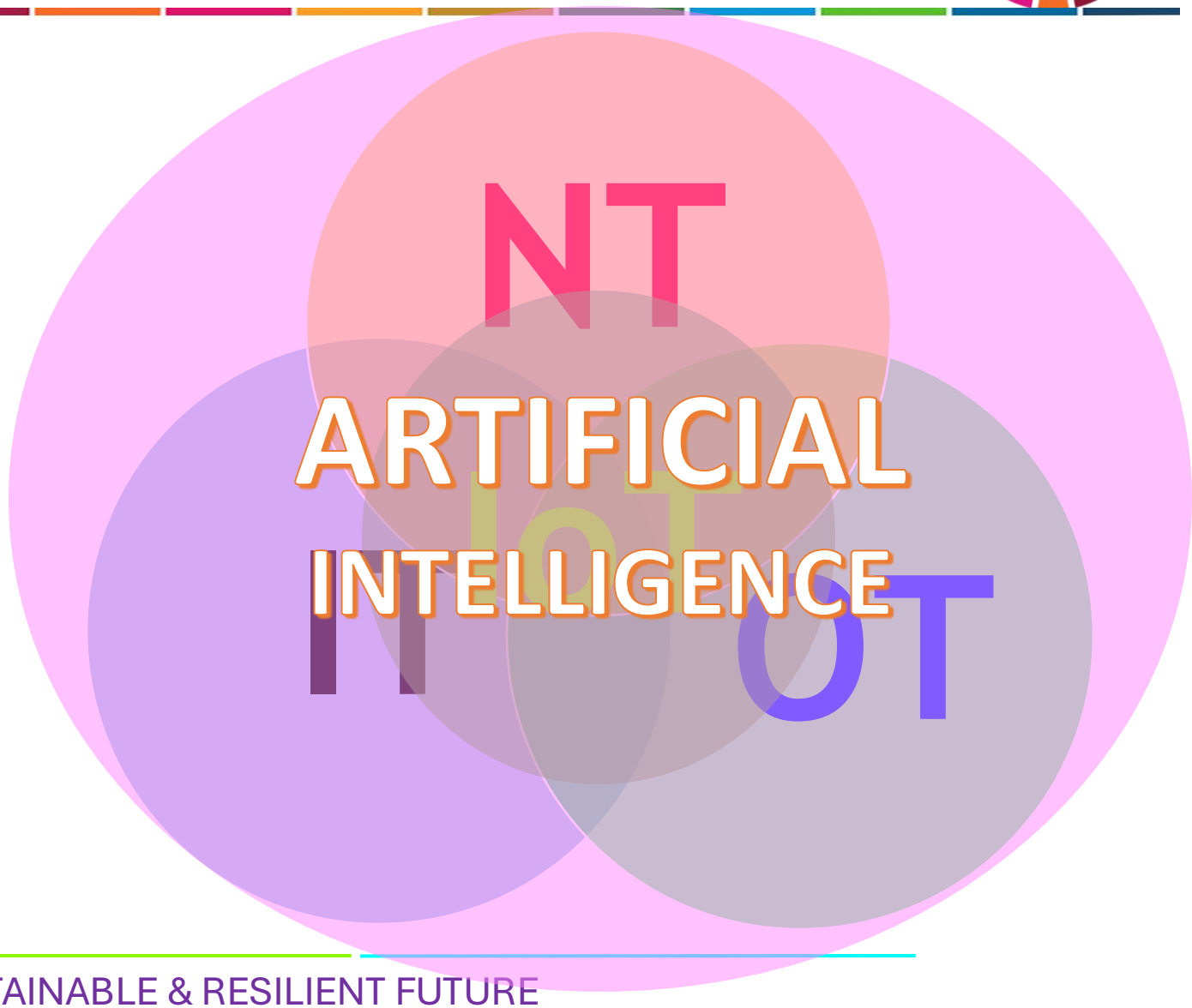
The society, the business, the infrastructure, the services and all other aspects of the civilization on the planet Earth are going through a paradigm shift in the wake of technological advancements, especially in the field of ICT

All the ecosystems, be it Smart Cities, Smart Grid, Smart Buildings or Smart Factories now find themselves making three classes of transformations:

- Improvement of Infrastructure – to make it resilient & sustainable…
- Addition of the Digital Layer- which is the essence of the *smart paradigm*; and
- Business Process Transformation - necessary to capitalize on the investments in smart technology.

Digital Transformation Constituents

- Information Technologies
- Operational Technologies
- Network Technologies
- IoT Technologies
- Artificial Intelligence
- SUSTAINABILITY ???



narnix

The genesis of Digital Transformation

In digital transformation in any paradigm, domain or ecosystem

- ‘Sustainability is the *True* Destination’
- ‘Resilience is the *Core* Characteristic’
- ‘Smart is *merely* the Accelerator’

Standards are the Chromosomes of Digital Infrastructure

narnix

Digital Transformation

We are living in an ephemeral world

narnix

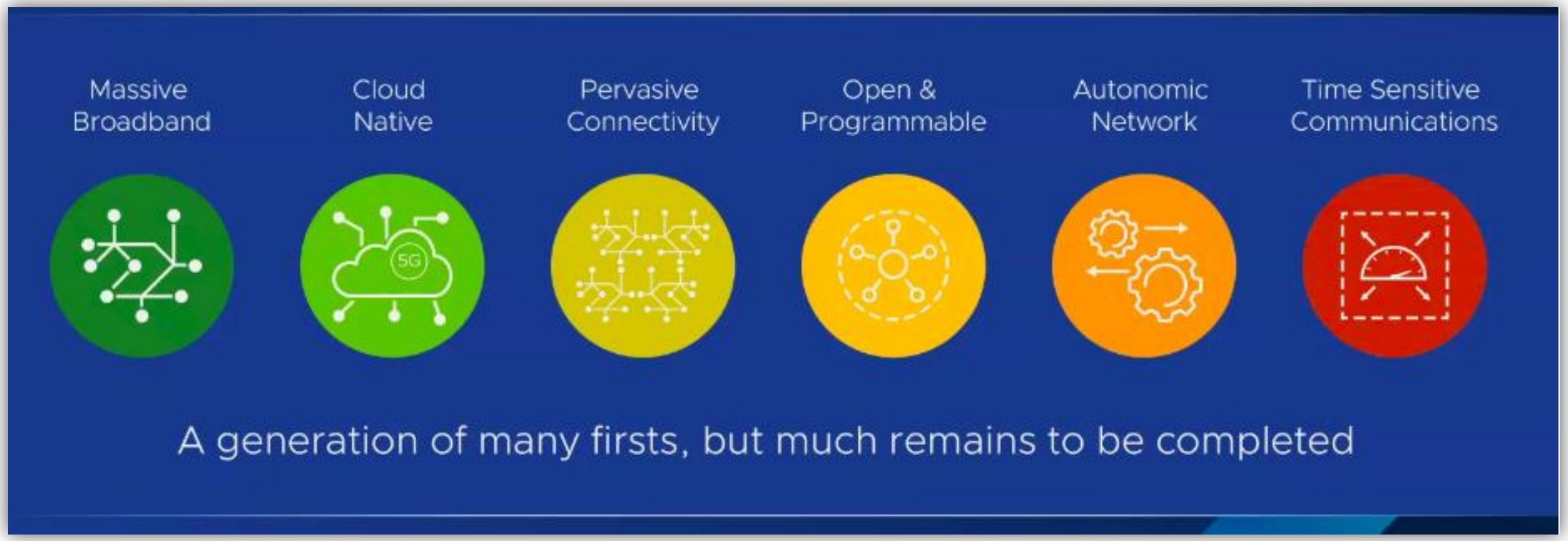
DESIGNING A SUSTAINABLE & RESILIENT FUTURE

Disruptive Technologies on the Radar

- Artificial Intelligence/ Machine Learning
- Blockchain
- Internet of Things/ Everything
- Big Data
- 5G/6G
- AR/VR/XR
- Web 3.0
- Robotics & Drones
- Data Centers
- Digital Twin
- Metaverse….

narnix

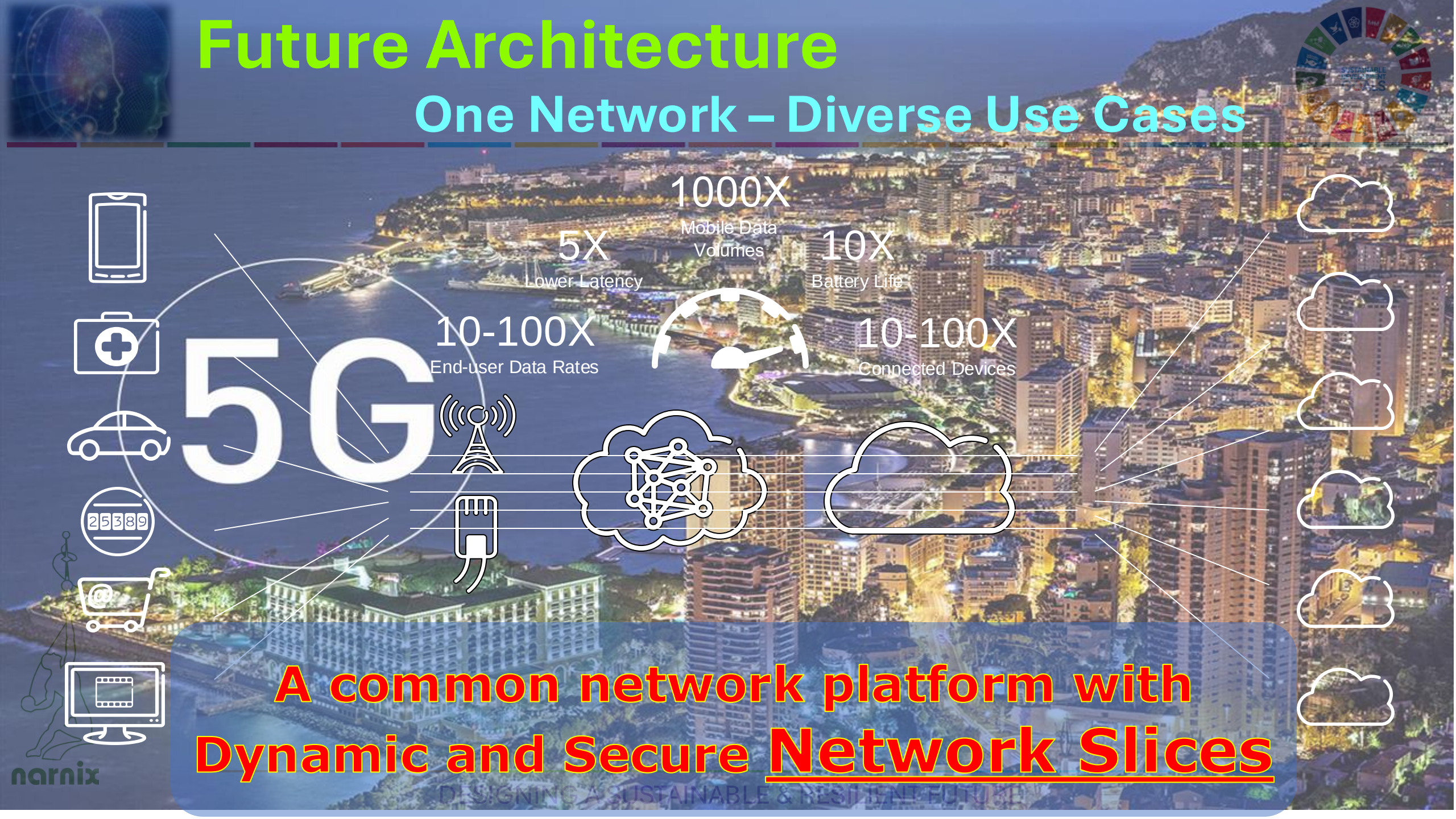
5G Foundation



narnix

Future Architecture

One Network – Diverse Use Cases



A common network platform with

Dynamic and Secure Network Slices

narnix

DESIGNING A SUSTAINABLE & RESILIENT FUTURE

5G – Only the Beginning…
The Carl Benz Automobile for the Internet

narnix

Projecting a Path- towards Universal Autonomy

narnix

Digital Twin

A digital twin is a virtual representation of a physical object, system, or process, continuously updated with real-time data to mirror its behaviour, characteristics, and performance.

Digital twins are used for simulation, integration, testing, monitoring, and maintenance of physical assets and processes.

They are created using real-time data, simulation, and modelling techniques to mimic the behaviour, characteristics, and performance of the physical entity.

Digital twins span the entire lifecycle of the physical object, from design and development to operation and maintenance.

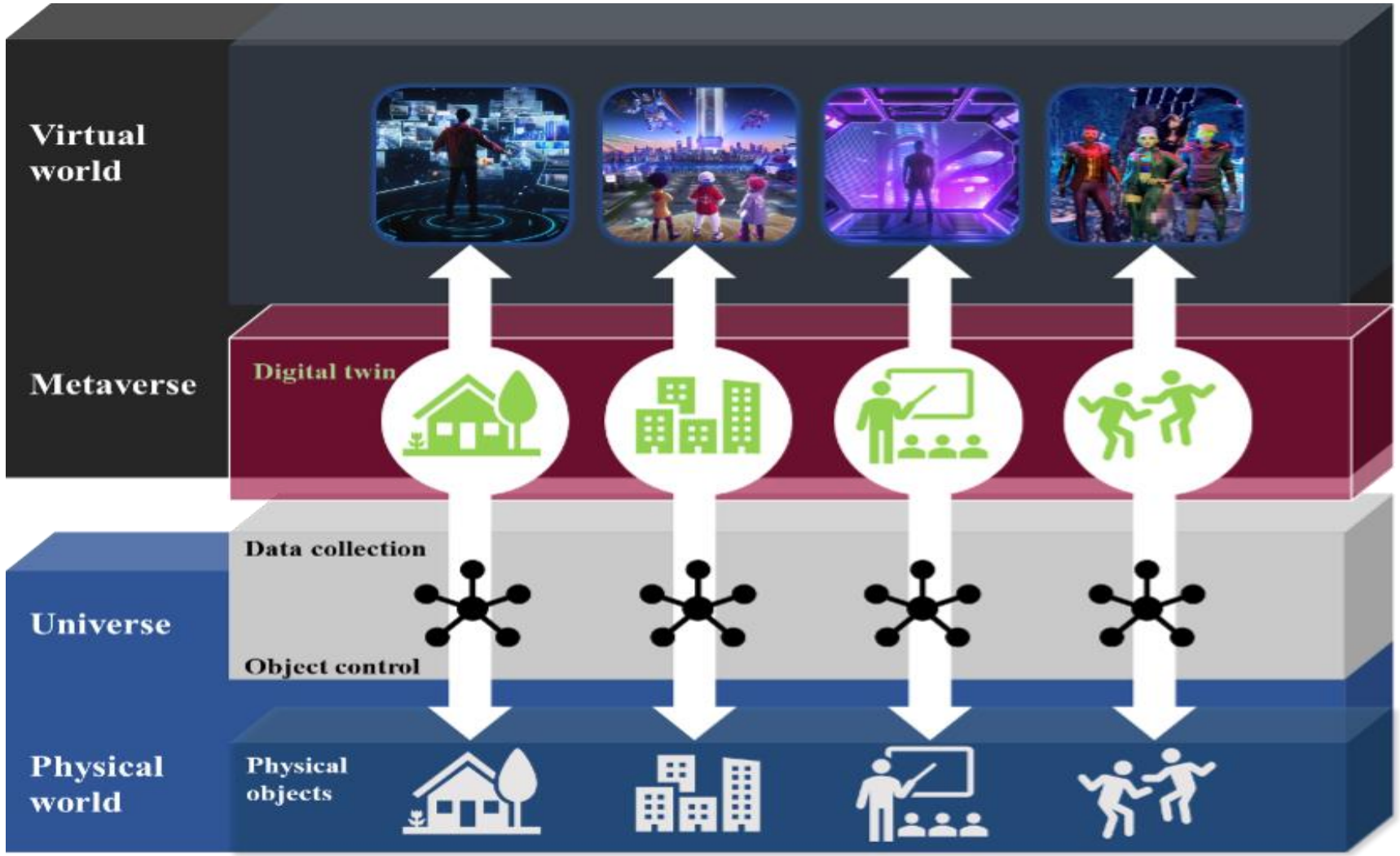
narnix

Metaverse...

- A metaverse is a network of 3D virtual worlds focused on social connection. In futurism and science fiction, it is often described as a hypothetical iteration of the Internet as a single, universal virtual world that is facilitated by the use of virtual and augmented reality headsets.
- The term "metaverse" has its origins in the 1992 science fiction novel Snow Crash as a portmanteau of "meta" and "universe." Various metaverses have been developed for popular use such as virtual world platforms like Second Life. Some metaverse iterations involve integration between virtual and physical spaces and virtual economies, often including a significant interest in advancing virtual reality technology.
- The term has seen considerable use as a buzzword for public relations purposes to exaggerate development progress for various related technologies and projects. Information privacy, user addiction, and user safety are some of the concerns within metaverses, stemming from challenges facing the social media and video game industries as a whole.

The metaverse can be defined as **a simulated digital environment** that uses augmented reality (AR), virtual reality (VR), and blockchain, along with concepts from social media, to create spaces for rich user interaction mimicking the real world.

Concept of the Metaverse based on Digital Twins



narnix

The Disruptive Technologies…

- Disruptive technology is the bearer of tremendous opportunity and equally, a harbinger of obsolescence.
- Technology's impact on society and business is substantial, if not underestimated.
- Though product cycle times are accelerating, the underlying technologies unfold over many years.
- Within each trend there are multiple enabling technologies, all at various stages of maturity and adoption.

The current wave of progress and enthusiasm for AI began around 2010, driven by three factors that built upon each other:

- The availability of *big data* from many sources;
- Dramatically *improved machine learning approaches and algorithms*; and
- The capabilities of *more powerful computers*.

narnix

Cyber Security Ecosystem

ARMS RACE!

Example

We managed WannaCry with damage
Total loss from attacks potentially at $T level soon!

Defense Landscape

- Defenders are disorganized
- Too much work at vision level
- Lacking execution
  - Stakeholders in 'babel tower'
  - Lack of technical consensus
  - Operational security is absent
  - Professionalization missing
  - Policy setting needs improvement
  - Certification push but not enough on labelling
  - Market dominancy questions
- Total revenue "only" at $133B

Attack Landscape

- Cybercriminals are organized
- Nation state cyberwarfare
- Increase in quantity and diversity
  - Ransomware
  - Target Attacks
  - DDoS
  - Espionage
  - Brain Attacks (phishing, fake news, disinformation)
- In military terms
  - **THEY HAVE THE INITIATIVE**

Explosion of the attack surface

- QUANTITATIVELY: Scale of a 5G infrastructure
- QUALTITATIVELY: Innovations change the architecture and increase the attack surface

But creates new conditions

Innovation

- FLOURISHING: Cloud, AI/ML, DLT, Quantum,
- BIGGER SOLUTIONS: 5G, IoT, ITS, Cyber currency,
- MARKETS/INDUSTRY: Digital Service Providers (ICT, OTT, Enterprises becoming Service Providers)

Both too slow and too fast (lack of ethics view) to adopt innovation

Gives conditions to …

Digitalization

- Transformative driving force
- Pre-requisite for our future societies

Very fast to adopt innovation against "us"; good intelligence of market and industry dynamics

GRAPHICS CREDIT: ARNAUD TEDDAI

narnix

Managing Risk is a Journey

Assets & Risks Discovery
What/Why need to be protected

Design

Organizational Roles & Responsibilities

Training

Awareness

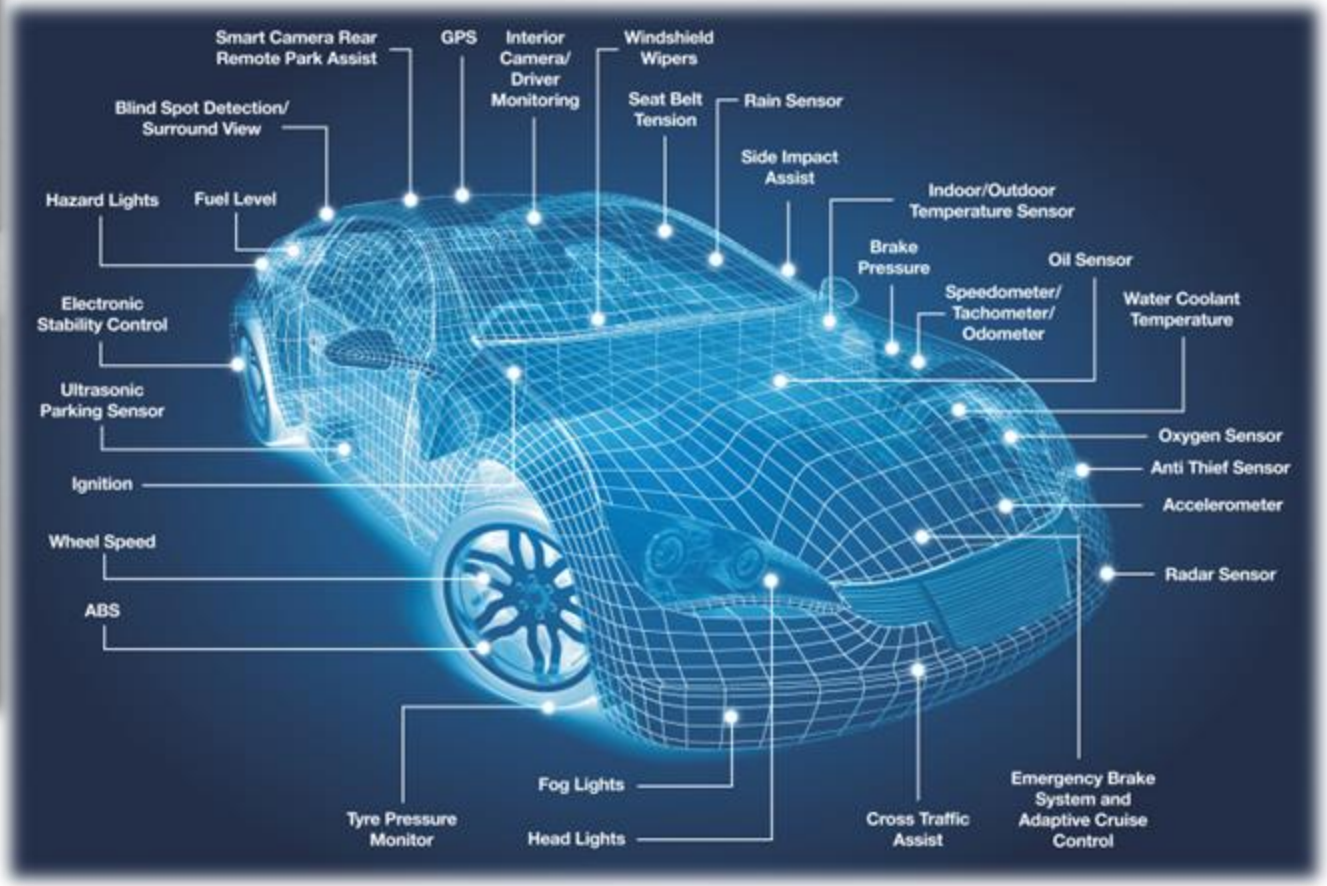
Patching and update management

narnix

A Strategic Approach is Required

Tactical Risk Management

Strategic Risk Management



narnix

Global Cyber Security Standardization

Direct impact to
- Regional/National strategy/priorities (E.g. EU CSA, NIS, GDPR, Data Spaces, AI, etc.)
- Certification/Labelling (e.g. ENISA)
- Regulation (e.g. Market Dominancy)
- Operation (e.g. Joint Cyber Unit, EU)

4 Stakeholders engaged in a huge battlefield

Administrations — Academia

Business — Civil Society

Stakeholders "Dark Matter"

Frames

Structures = Direct impact to
- Markets
- GDP
- Administrations

Security Standardization "Universe"

IEC ISO ITU

+ National Standard Bodies
Regional Standard Bodies, Industry Associations, etc.
NATO, MEF,

IETF
GSMA
3GPP

ETSI
OASIS
IEEE

BIS NIST

Coordination and collaboration exist but improvements are required

Security Standardization is increasingly fractalized

GRAPHICS CREDIT: ARNAUD TEDDAI

narnix

The Standardization Conundrum…

The beauty of Standards is that there are so many to choose from!

Andrew S. Tanenbaum, 1990

- In an ideal world, we would have exactly one standard for each task or interface.
- However, in reality, there are often overlapping or rivalling standards, driven by different vendor “camps”.
- In case of Cyber Security, Standards by different Global, regional & National SDOs.

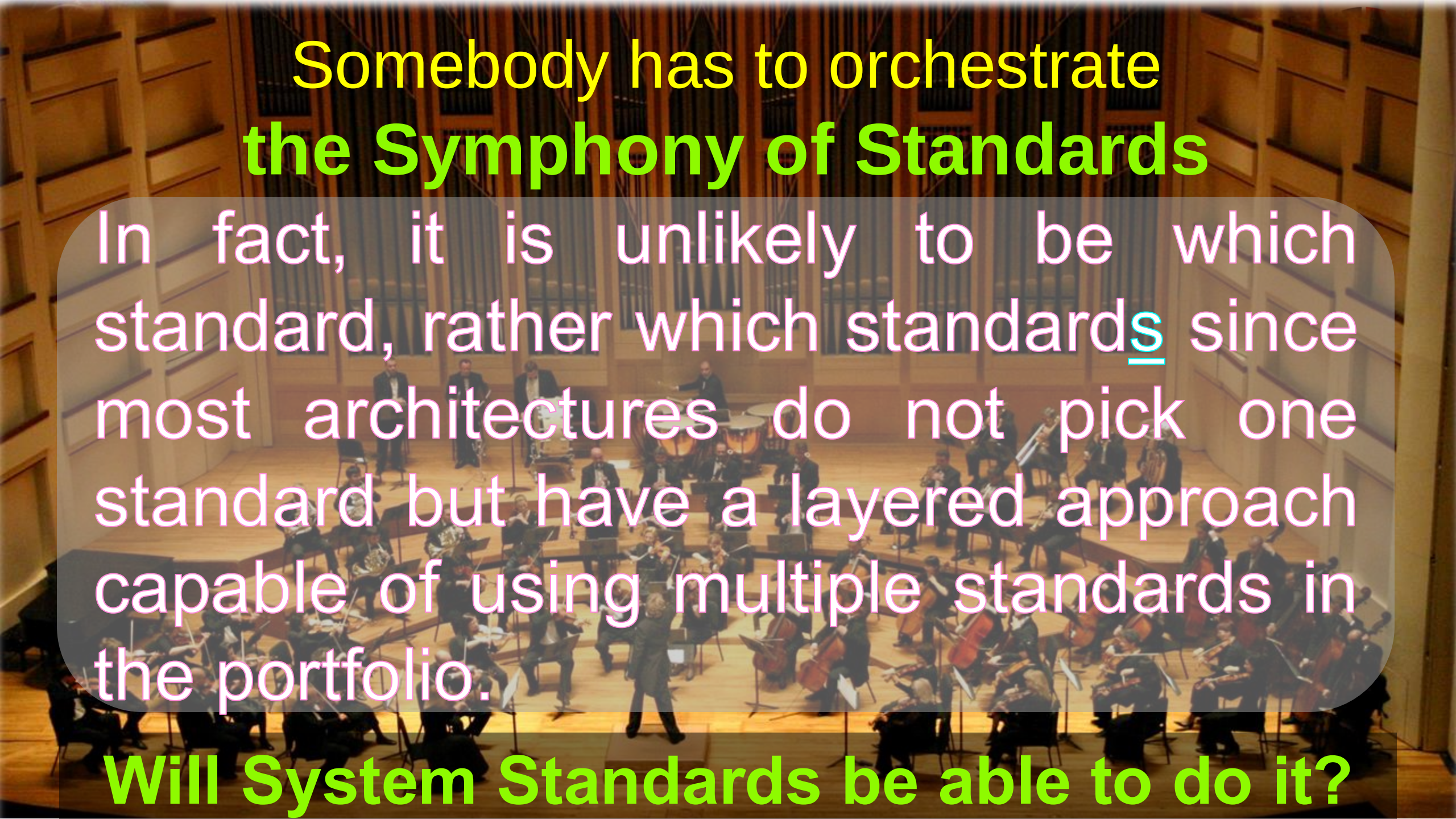
narnix

SYMPHONY or CACOPHONY ? ? ?

The Enraged Musician, William Hogarth, 1741

narnix

DESIGNING A SUSTAINABLE & RESILIENT FUTURE

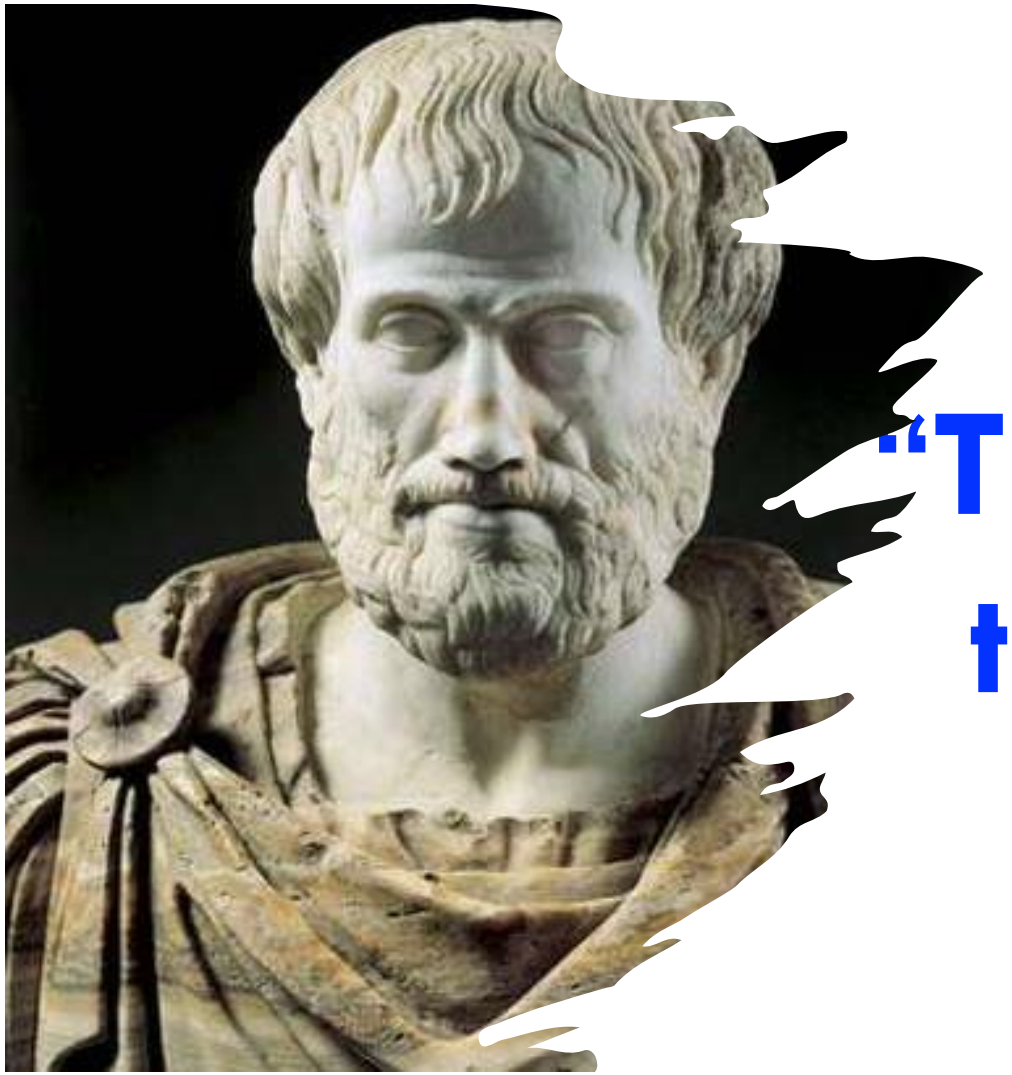


Somebody has to orchestrate **the Symphony of Standards**

In fact, it is unlikely to be which standard, rather which standards since most architectures do not pick one standard but have a layered approach capable of using multiple standards in the portfolio.

Will System Standards be able to do it?

Systems Approach: Holism



Aristotle (300 B.C.)

"The Whole is Greater than the Sum of its Parts"

narnix

Systems Approach imperatives

- The multiplicity of technologies and their convergence in many new and emerging markets, however, particularly those involving large-scale infrastructure demand a top-down approach to standardization starting at the system or system-architecture rather than at the product level.
- Therefore, the systemic approach in standardization work can define and strengthen the systems approach throughout the technical community to ensure that highly complex market sectors can be properly addressed and supported.
- It promotes an increased co-operation with many other standards-developing organizations and relevant non-standards bodies needed on an international level.
- Further, standardization needs to be inclusive, top down and bottom up; a new hybrid model with a comprehensive approach is needed.

narnix

What is a System?

- A purposeful collection of inter-related components working together towards some common objective.
- A system may include software, mechanical, electrical and electronic hardware and be operated by people.
- System components are dependent on other system components
- The properties and behaviour of system components are inextricably inter-mingled.

narnix

Complexity and Emergence

- **Complexity** is a measure of how difficult it is to understand how a system will behave or to predict the consequences of changing it.

- **Emergent properties,** which derive from the interrelation of the system parts and interaction with the environment, are among the key challenging aspects dealt within the Systems approach

narnix

Emergent Properties

- Properties of the system as a whole, rather than properties that can be derived from the properties of components of a system.

- Emergent properties are a consequence of the relationships between system components.

- They can therefore only be assessed and measured once the components have been integrated into a system.

narnix

Types of Emergent Properties

❖Functional Properties

These appear when all the parts of a system work together to achieve some objective. For example, a bicycle has the functional property of being a transportation device once it has been assembled from its components.

❖Non-functional Emergent Properties

Examples are reliability, performance, safety, and security. These relate to the behaviour of the system in its operational environment. They are often critical for computer-based systems as failure to achieve some minimal defined level in these properties may make the system unusable.

System and Systems Approach

- **System:** *A group of interacting, interrelated, or interdependent elements forming a purposeful 'WHOLE' of a complexity that requires specific structures and work methods in order to support applications and services relevant to the stakeholders.*

- **Systems Approach:** *A holistic, iterative, discovery process that helps first defining the right problem in complex situations and then in finding elegant, well-designed and working solutions. It incorporates not only engineering, but also logical human and social aspects.*

Systems Approach demystified…

- Identify and understand the relationships between the potential problems and opportunities in a real-world situation.
- Gain a thorough understanding of the problem and describe a selected problem or opportunity in the context of its wider system and its environment.
- Synthesize viable system solutions to a selected problem or opportunity situation.
- Analyze and trade off between alternative solutions for a given time/cost/quality version of the problem.
- Measure and provide evidence of correct implementation and integration.
- Deploy, sustain, and apply a solution to help solve the problem (or exploit the opportunity).
- All of the above, are considered within a life cycle framework which may need concurrent, recursive and iterative applications of some or all of the systems approach.

narnix

Shaping the Mess…

Goals

Needs

Stakeholders Requirements

Systems Requirements

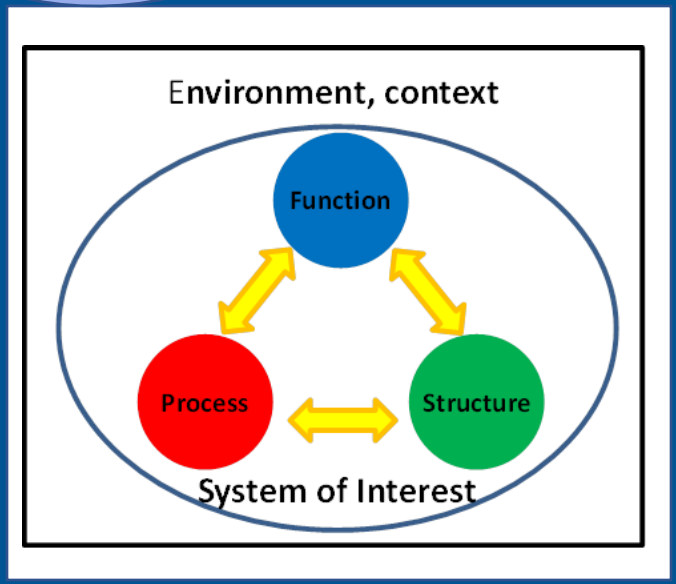
Systems Architecture

Technical Specifications

Values
Relevance
Priorities
…

From here…

…to here



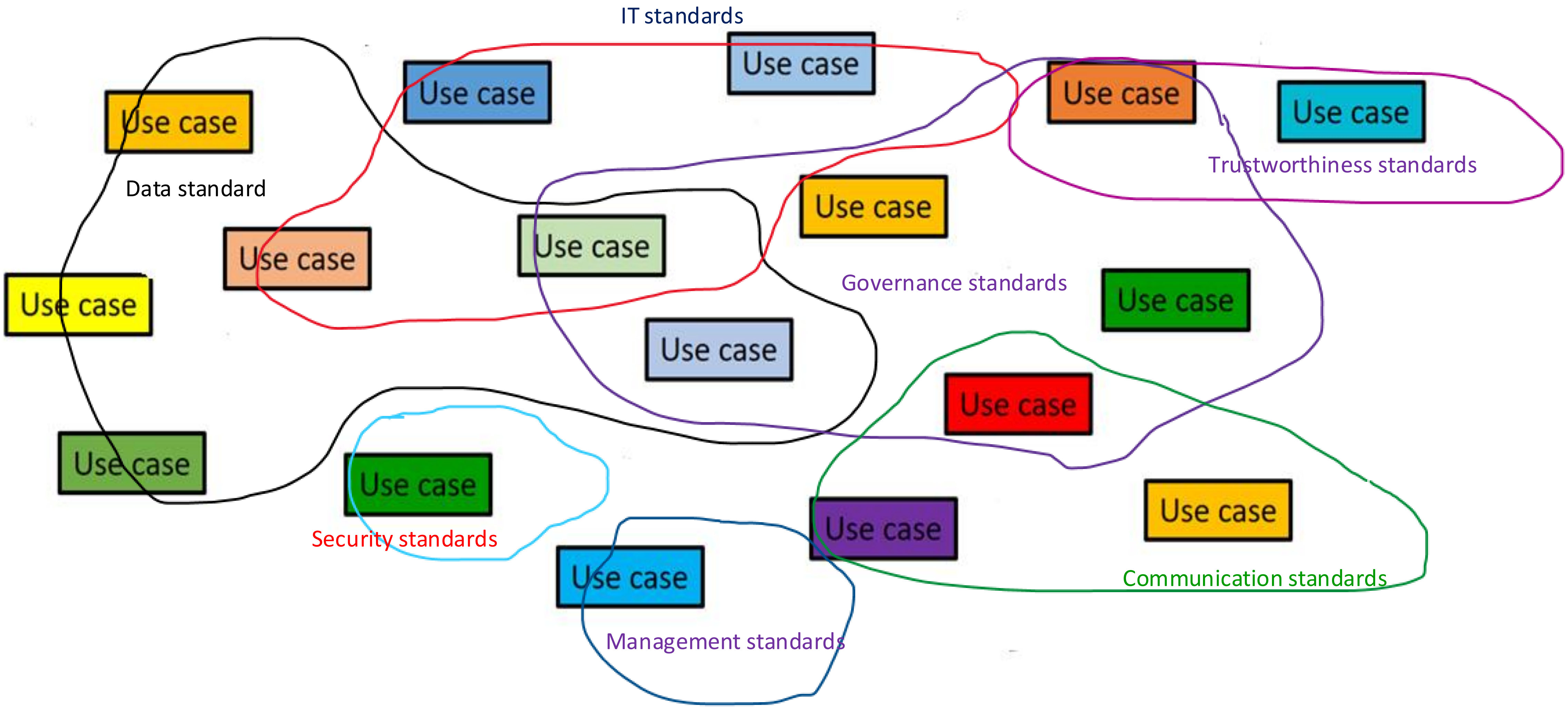
Resolution comes through an iterative process!

narnix

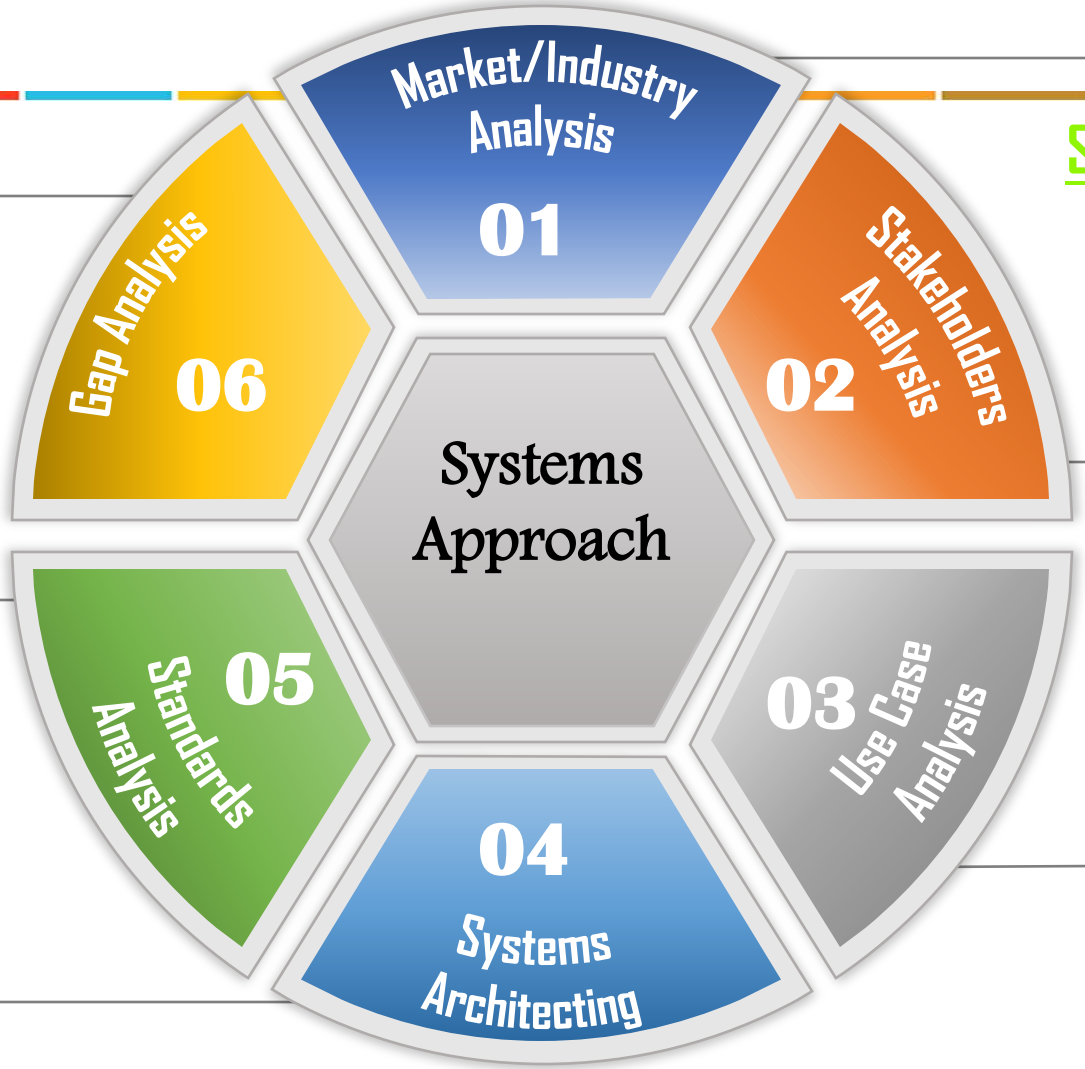
Collect the High-Level Use Cases

Use case
Use case
Use case
Use case
Use case
Use case
Use case
Use case
Use case
Use case
Use case
Use case
Use case
Use case
Use case

Scope out Family of Standards needed



SYSTEMS APPROACH PROCESS FLOW



Sys Market Analysis

Analyze and identify the the market/industry trends and needs?

Sys Stakeholders

Who are the key stakeholders of the system and what are their needs and objectives?

Sys Use Cases

What are the different use cases for the system and how do they interact with the system?

Sys Architecting

What is the reference architecture of the system and its boundaries?

Sys Standards

What are the existing standards and SDOs that pertain to this system?

Sys Gaps

What are the standards that are missing in the system?

narnix

Framework, Architecture, Design, Solution

framework

architecture

design

solution

- A *framework* sits at a broad, conceptual level and provides context for more detailed technical aspects.
- An *architecture* identifies a particular problem space and defines a technology-independent analysis of requirements
- The *design* maps architectural requirements into a particular family of solutions based upon standards and technical approaches.
- Finally, a *solution* manifests a design into a particular vendor technology, ensuring adherence to designs, models, and frameworks.

Four levels of abstraction in the Systems Approach

Reference Model

- abstract framework for understanding concepts and relationships between them in a particular problem space (or subject field)

Reference Architecture

- template for solution architectures which realizes a predefined set of requirements
  - Note: A reference architecture uses its subject field reference model (as the next higher level of abstraction) and provides a common (architectural) vision, a modularization and the logic behind the architectural decisions taken

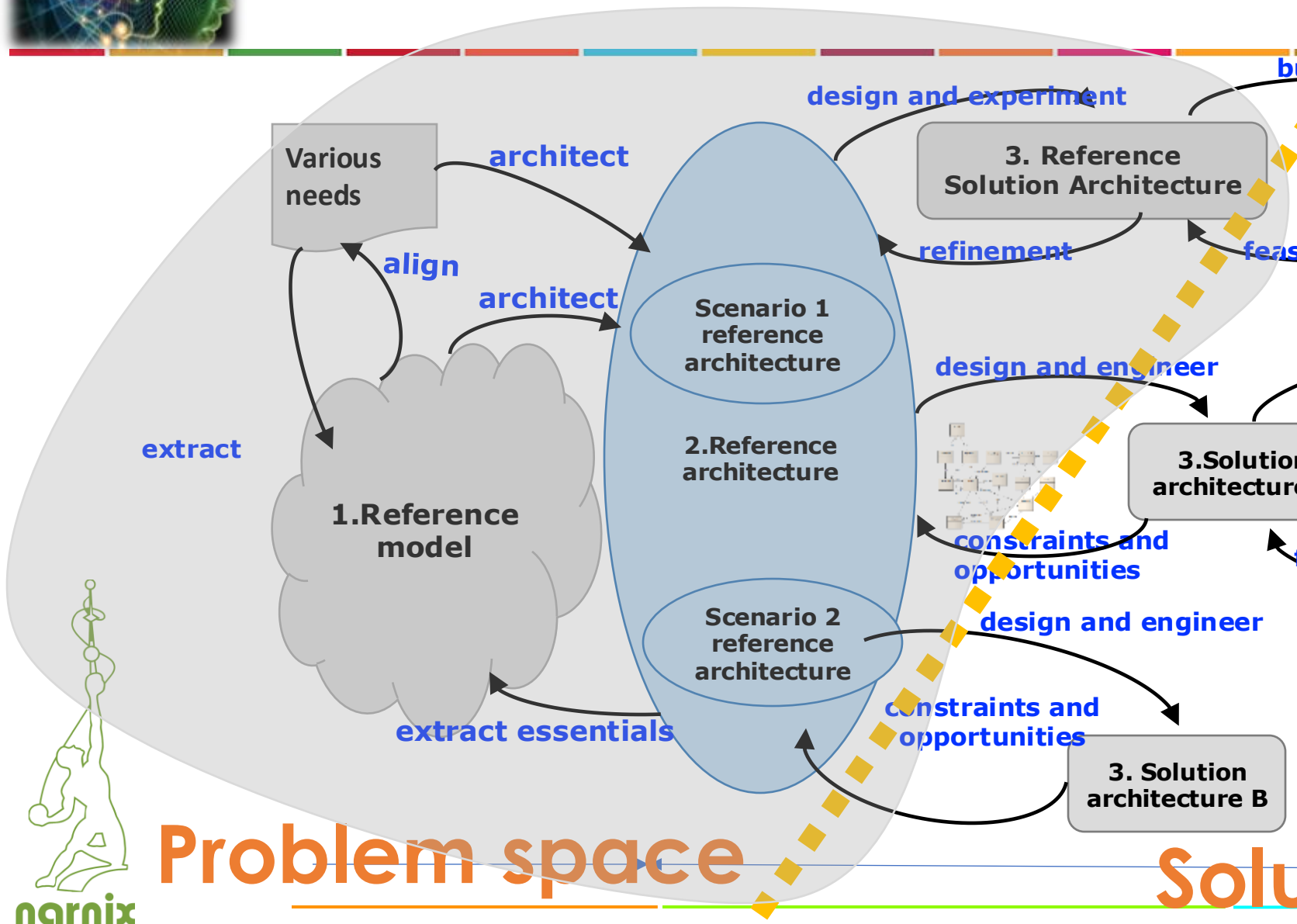
Solution Architecture

- architecture of the system-of-interest
  - Note: A solution architecture (also known as a blueprint) can be a tailored version of a particular reference architecture (which is the next higher level of abstraction)

Implementation - realisation of a system-of-interest

narnix

Levels of Architecting

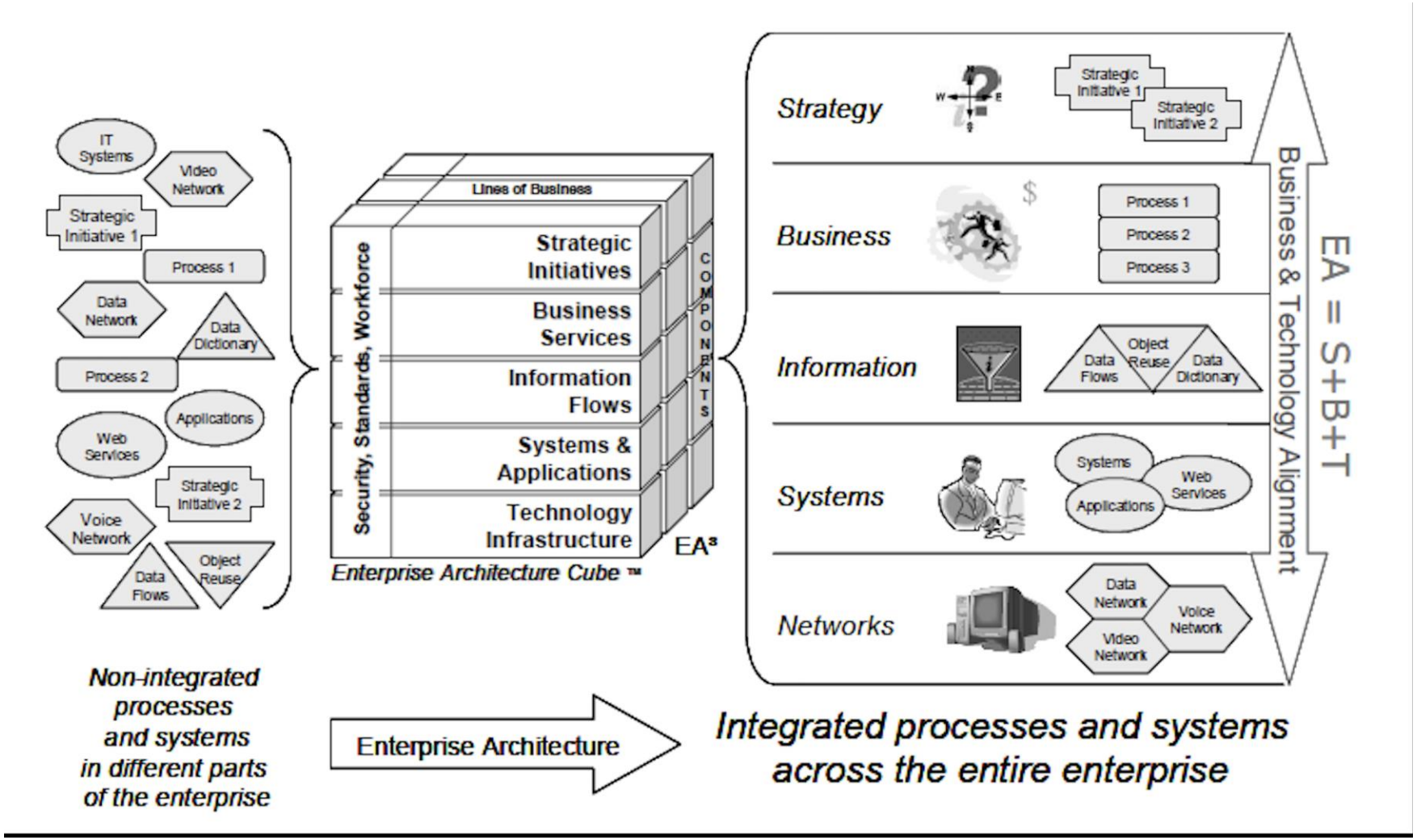


A few scenario reference architectures may be derived from the reference architecture
AAL: personal telehealth, home
Smart Cities: megalopolis, city, village, island

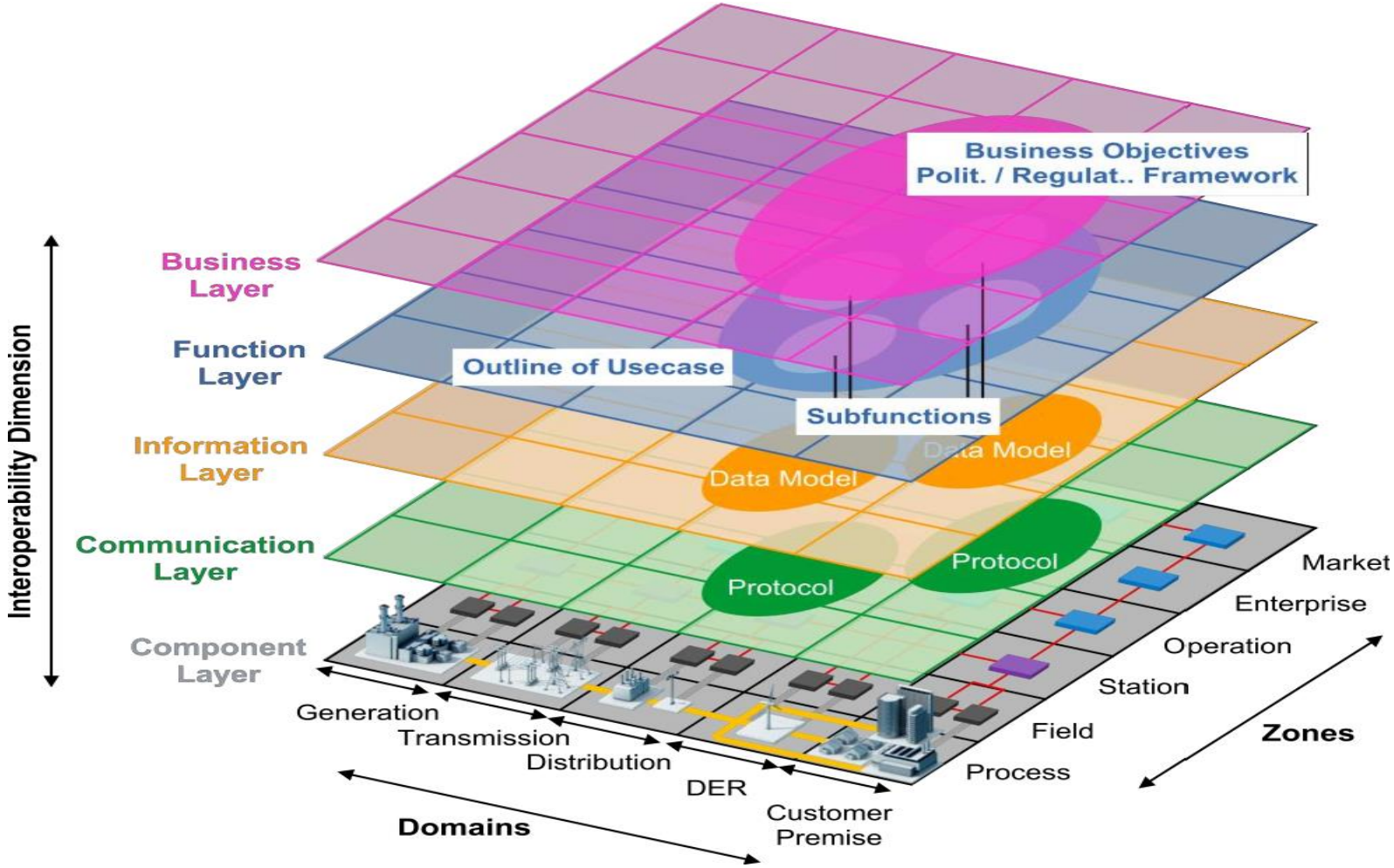
Problem space **Solution space**

narnix

Enterprise Architecture



Smart Grid Architecture Model（SGAM）



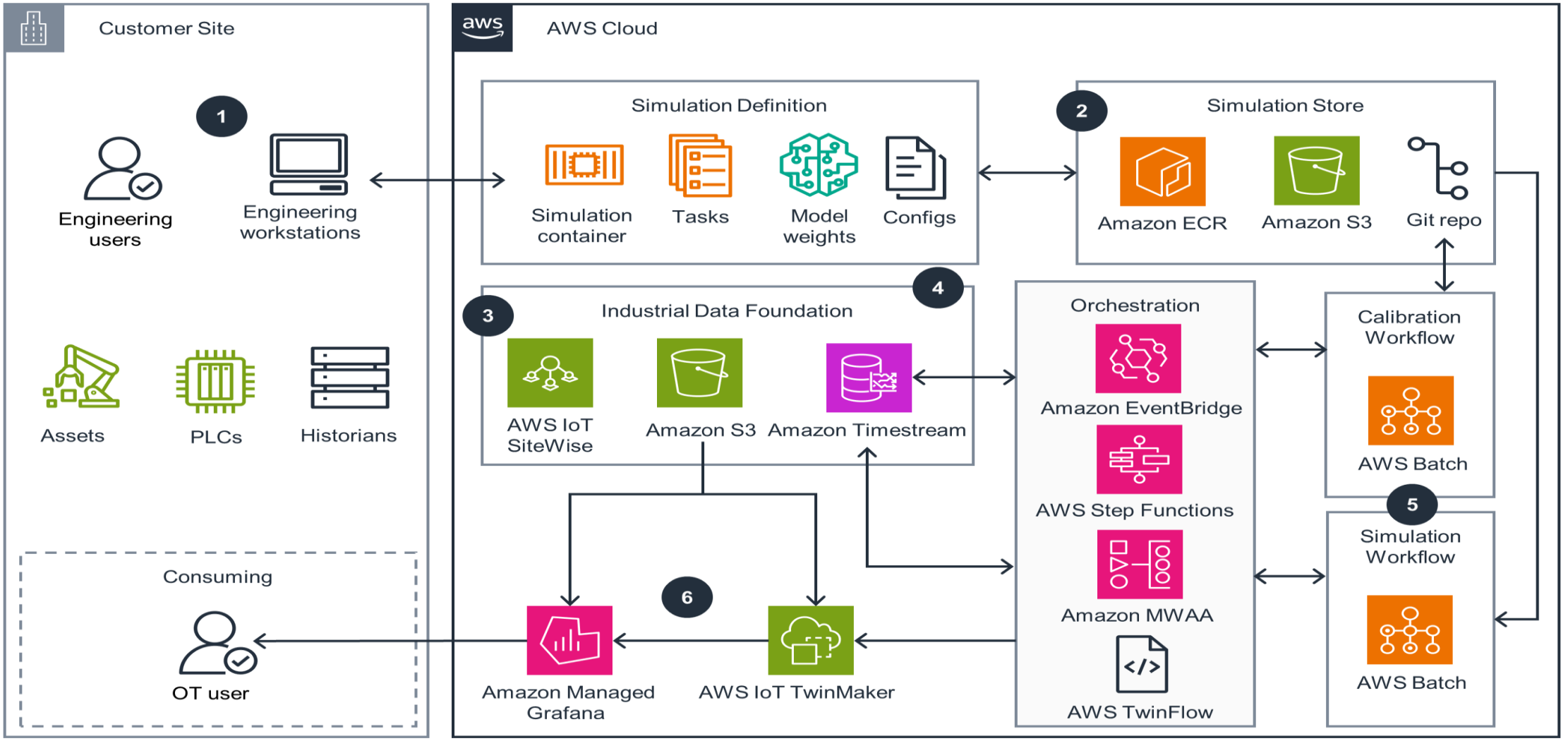
Reference）CEN-CENELEC-ETSI Smart Grid Coordination Group “SG-CG/M490/K_SGAM usage and examples, SGAM User Manual – Applying, testing & refining the Smart Grid Architecture Model (SGAM)”

Architectural approach…

- An Architectural Approach brings semblance in any chaotic ecosystem
- It helps diverse classes of stakeholders of the ecosystem to get comprehensive understanding about the inter-dependency and interplay among various heterogenous aspects of the Technology, the Domains, the Applications, the Use Cases and last but NOT the least the Standards…
- This understanding enables them to bring structured Interoperability in the relevant aspects of the systems, solutions and technologies.
- The architectural approach also opens the doors for structured innovation in any new domain, technology and/or application…

narnix

A typical Digital Twin Framework



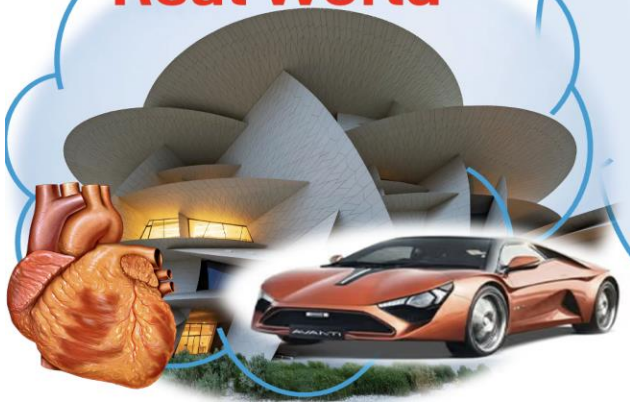
narnix

DESIGNING A SUSTAINABLE & RESILIENT FUTURE

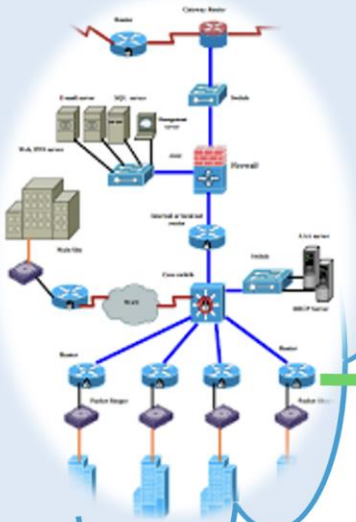
Metaverse Domains & Stakeholders…

End User

Real World



Network & Infrastructure Provider



Avatar Service Provider

Avatar Provider

Virtual Space Service Provider

Virtual Space Provider

Virtual Component Service Provider

Virtual Component Provider

narnix

Pattern “Reference Architecture”: a common need for a sustainable solution

Reference architecture helps to isolate unique & common parts of Metaverse

Big Picture View of Metaverse Reference Architecture

1 Individual

A A

Domain A Metaverse

B B

Domain B Metaverse

N N

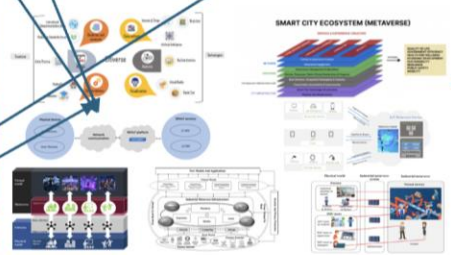
Domain N Metaverse

Common parts

Unique parts

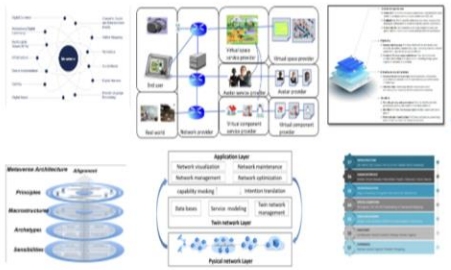
2 Siloed

with non-interoperable models and solutions



3 Architected

with common methodology



Metaverse Reference architecture (MV-RA) for individual Applications as systems

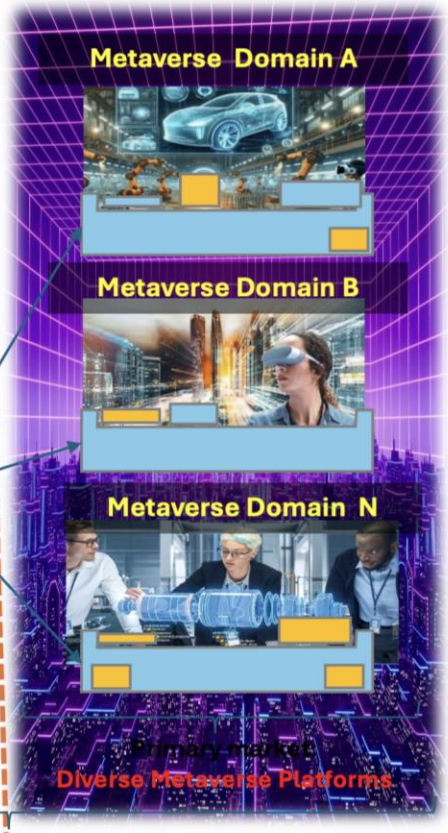
4 Collaborated

with common

- methodology
- architecture
- practices
- tools
- governance
- platforms
- solutions

Common platforms

5 Coordinated



Secondary market:
Common platform evolution and enrichment

narnix

Strategy Framework for Unified Digital Infrastructure

UNIFIED DIGITAL STRATEGY	GOVERNANCE & OPERATION	TRUSTWORTHINESS	SUSTAINABILITY
HARMONIZED STANDARDS	UNIFIED DIGITAL INFRASTRUCTURE	SAFETY	UNIFIED DIGITAL INFRASTRUCTURE
INTEROPERABILITY	HARMONIZED POLICIES & REGULATIONS	SECURITY	HARMONIZED POLICIES & REGULATIONS
CONTEXTUAL DATA MODELS	MEASURABLE INDICES & KPIs FRAMEWORKS	PRIVACY	CARBON FOOTPRINT OPTIMIZATION
SEAMLESS INTEGRATION	FRUGAL INNOVATION	RELIABILITY	FRUGAL INNOVATION
STAKEHOLDERS COLLABORATION	STAKEHOLDERS COLLABORATION	RESILIENCE	SUSTAINABLE DEVELOPMEMET GOALS

SCALABLE SECURE SUSTAINABLE & RESILIENT UNIFIED DIGITAL INFRASTRUCTURE

narnix

ITU-T FG-MV – Relevant Deliverables

FGMV-06	Guidelines for consideration of ethical issues in standards that build confidence and security in the metaverse	Technical Report
FGMV-10	Cyber risks, threats, and harms in the metaverse	Technical Report
FGMV-11	Embedding safety standards and the user control of Personally Identifiable Information (PII) in the development of the metaverse	Technical Report
FGMV-12	Children's age verification in the metaverse	Technical Report
FGMV-13	Responsible Use of AI for Child Protection in the metaverse	Technical Report
FGMV-23	Considering online and offline implications in efforts to build confidence and security in the metaverse	Technical Report
FGMV-24	A framework for confidence in the metaverse	Technical Report
FGMV-44	Security for things across metaverses in aspects of data processing and management	Technical Report
FGMV-45	Challenges to achieving trustworthy metaverse	Technical Report
FGMV-46	The essential components of trusted data use in building a trustworthy metaverse	Technical Report

narnix

Digital Trust…

Digital Trust (or trust in digital solutions) is a complex topic. When do users deem a digital product truly trustworthy?

What if a physical product component is added, as in smart, connected products?

While security is certainly a key enabler of Digital Trust, there are many other aspects that are important, including ethical considerations, data privacy, quality, and robustness (including reliability and resilience), and certification, compliance, testing as the proofed accordance with standards and rules.

narnix

Trustworthiness:

- A working definition of trustworthiness is the degree to which a user or other stakeholder has confidence that a product or system will behave as intended. This definition can be applied across the broad range of systems, technologies, and application domains.

- The paradigm has evolved thru many avatars beginning with Software Quality & Dependability, during its journey subsuming various concerns like reliability, availability, safety, security and many more to a single overarching conceptual framework, which is also considered, quite rightly as Dependability 4.0.

narnix

Trustworthiness paradigm…

- Characteristics of trustworthiness include - Reliability, Availability, Resilience, Security, Privacy, Safety, Accountability, Transparency, Integrity, Authenticity, Quality, Usability and Accuracy…

- Trustworthiness is an overarching paradigm with a multitude of nuances and distinct aspects such that it has different connotations for different sets of stakeholders, use cases and applications.

- What aspect or nuance of Trustworthiness may be highly critical in one use case may be absolutely trivial for some other use case depending on its context and/or domain

narnix

Cyber Immunity & Cyber Resilience…

- The **pandemic-induced digital transformation** has increased exposure to cyber threats as we cross the digital fault line due to remote working and escalated online presence. To counter this, **an intuitive and adaptive cyber posture** defined by zero latency networks and quantum leaps will be needed across industries. These developments, while great for humanity, will challenge privilege, privacy, and defend every citizen.
- **Cyber Immunity** at every layer will create networks that are inherently secure and self-learning. AI-induced digital intuition must be one of the pillars of any cyber-security strategy to allow intelligent adaption. The ability of AI systems to out-innovate malicious attacks by mimicking various aspects of human immunity will be the line of defence to attain **cyber resilience** based on both supervised and unsupervised machine learning.

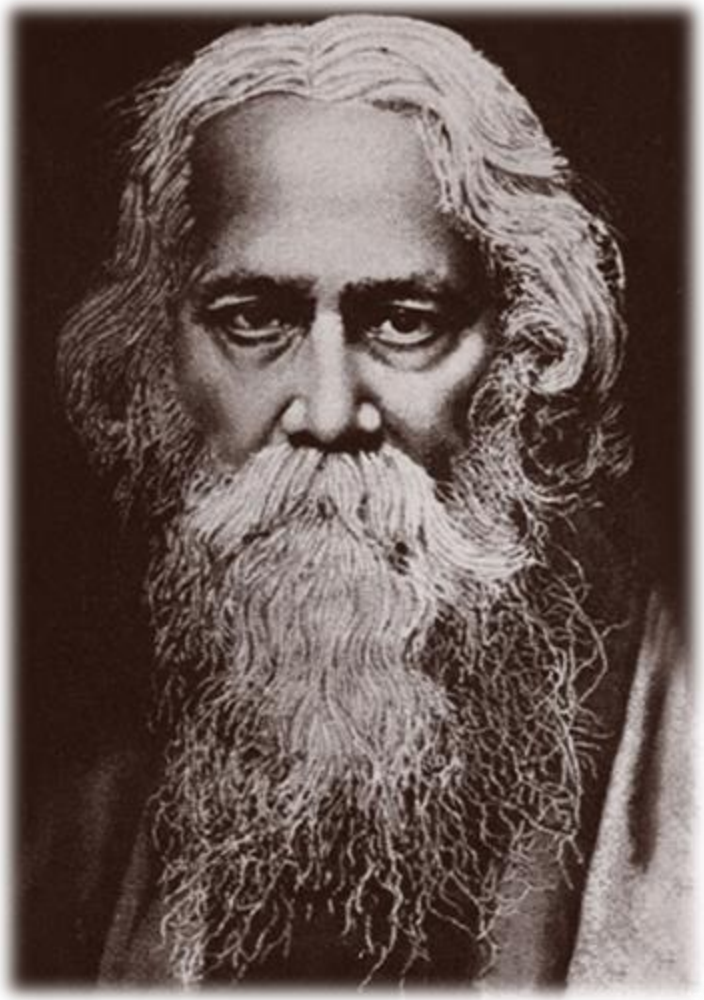
narnix

To sum up - The way forward…

To be able to address the Security & Privacy for Digital Twin & Metaverse, rather any Digital systems, we need to adopt a Top-Down approach:

- Starting with understanding the diverse use cases within the application domain or technology domain, enumerating & classifying the different stakeholders and their respective concerns.
- Extracting the Security & Privacy requirements out of use cases and stakeholders' concerns.
- Developing the Security & privacy Architecture and/or different architectural views based on each concern.
- Mapping the available Security & Privacy standards to the Architecture developed to identify the appropriate standards to address the respective concern.
- Undertake the standards Gap Analysis to develop the future standards development strategy and roadmap.
- However, it is recommended NOT to limit to the Security and Privacy concerns rather attempt to address comprehensive Trustworthiness in any Digital System, Solution, Service and/or Infrastructure…

Resilience....



Let us not pray to be sheltered from dangers but to be fearless when facing them

narnix

Thank you!

For a Sustainable & Resilient Future

narnix

narang n. kishor
+91 9810163990
kishor@narnix.com

About me… N. KISHOR NARANG

Technology Philanthropist, Ethicist, Innovation, Standardization & Sustainability Evangelist…

Technology Advisor, Mentor & Design Strategist & Architect in Electrical, Electronics & ICT; running an Independent Design House – NARNIX since 1981

- Over 47 years of professional experience in education, research, design and advisory .
- Over 36 years of hardcore Research and Design Development Experience in Solutions, Systems, Products - Hardware, Software & Firmware (Embedded Software) in fields of Industrial, Power, IT, Telecom, Medical, Automotive, Aerospace, Defense, Energy and Environment. Over 10 years of Strategic Advisory Experience to different segments of business & industry.
- Over 500 Research & Design Mentees in the Electronics & ICT Ecosystems.
- **Mentoring many Deep Tech & Disruptive Tech Startups.**
- Leading & contributing to multiple National & Global Standardization Initiatives at BIS, Niti Aayog, TSDSI, IEC, ISO, ITU, IEEE etc.…
- For the last 15 years, been deeply involved in standardization in the electrical, electronics, communications, information technology, digital infrastructure and cyber security domains with a focus on identifying gaps in standards to bring harmonization through system standards and standardized interfaces to ensure end-to-end Interoperability.
- **National Standards (INDIA) based on 10 years of Pre-Standardization Research Published Recently (December 2020) -**
  - Unified Digital Infrastructure ICT Reference Architecture – IS 18000:2020.
  - Unified Last Mile Communication Protocol Stack Reference Architecture – IS 18010:2020.

narnix

- **Founding Chairman of the Smart Infrastructure Sectional Committee LITD 28 in BIS** (20 + standards on Unified Digital Infrastructure already published).
- **Vice Chair-Strategy, and Project Leader of two international standards in IEC SyC Smart Cities** – SCRAM: Smart Cities Reference Architecture Methodology IEC 63188 (published in September 2022) and SCRA: Smart Cities Reference Architecture IEC 63205 being developed jointly with ISO TC 268 & ITU-T SG 20.
- **Member IEEE SA Standards Board**
- **Chair, IEEE SA Working Group P2784 – Smart Cities Technology Framework.**
- Vice Chair, IEEE SA Working Group P 2872 - Standard for Interoperable and Secure Wireless Local Area Network (WLAN) Infrastructure and Architecture
- Convenor, Communication Technologies Work Group in IEC SyC Communication Technologies & Architectures,
- Convenor, IEC SyC SET, ahG 1: Systems Architecture for Sustainable Electrified Transportation
- Convenor, IEC TC 13/JahG 17 – Identifying Synergy & Interplay between TC 13 & TC 69
- Member, IEC SMB/SG 12 -Digital Transformation and Systems Approach,
- Member, IEC SMB/SG 14– All Electrified & Connected Society
- Member, IEC SMB/ahG 96 - Governance of Artificial Intelligence
- Member, IEC MSB/SWG 14 - SMART Standards – A Market & Industry perspective.
- OCEANIS - Chair of Advancing Research Work Group & member Steering Committee.
- ITU-T SG 20, ITU-T SG 17 & ITU-R SG 5 - Proactive Contributor.
- ITU-T SG 17 – Editor – X.cs-ra – Cyber Security Reference Architecture; Co-editor, X.arch-design: Design principles and best practices for security architectures.
- Member UL STP 3600 - 'Measuring and Reporting Circular Economy Aspects of Products, Sites and Organizations'.
- ISO/IEC JTC1/WG11 - Co-Editor in Four Standards.
- **IEEE IoT Magazine** - Standards Column Editor.