
# Standardization Imperatives & Approach for a Trustworthy IoT Ecosystem

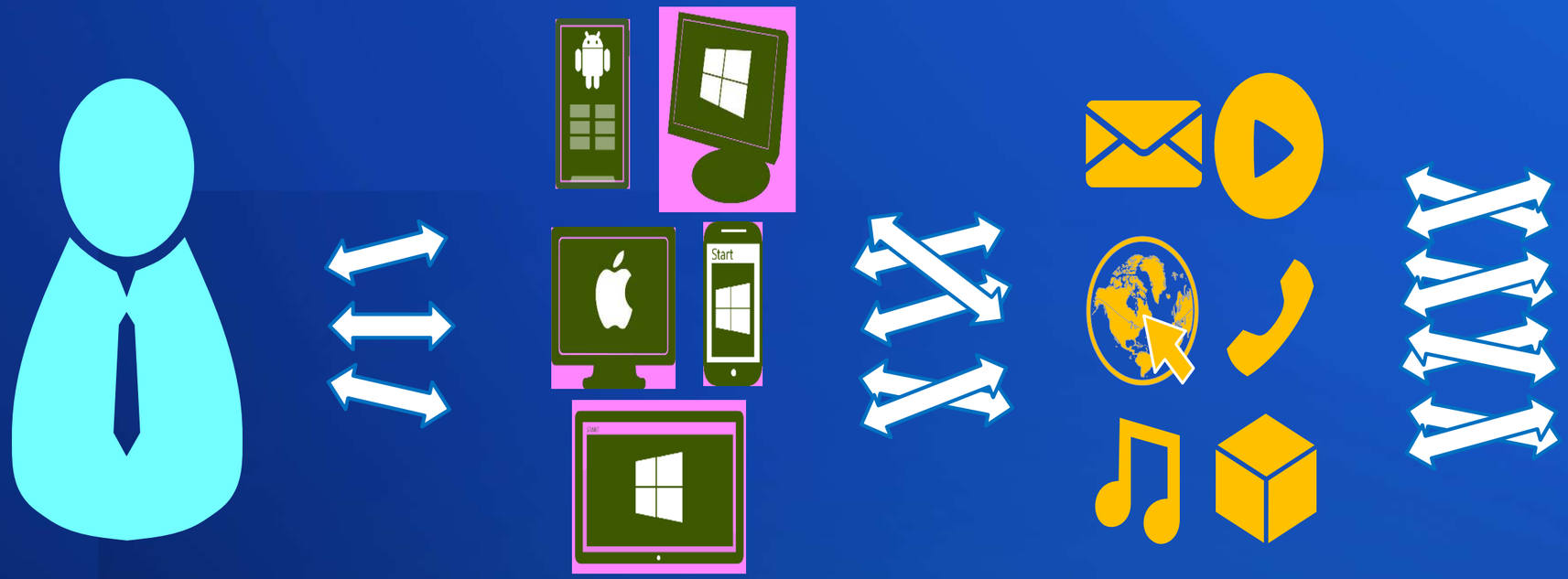
# Have we seen ALL that's in Cyber Security???

Those of us who have worked in cybersecurity for many years often start to think we've "seen it all".

## We haven't.

Recent years have ushered in a host of new adversaries, new attack methods and new challenges for those of us in the cybersecurity industry.

# Today’s challenges




## Users

Users expect to be able to **work in any location** and have access to all their work resources.

## Devices

The **explosion of devices** is eroding the standards-based approach to IT.

## Apps

Deploying and managing applications **across platforms** is difficult.

## Data

Users need to be productive while **maintaining compliance and reducing risk.**

# We: The Walking Host …

How many IP addresses are on a person?

- Smart watches
- Fitness Devices
- Medical devices
- Smartphones
- Tablets
- Smart glasses
- Headsets
- And more…

- Confidential information is passed between Smart Watches and Host Phones
- Medical and Health devices store and transmit personal data
- **Device firmware and application updates are not necessarily secure**

# India is among the top 10 countries facing cyber-attacks

Challenges that all economies are facing today in safeguarding the security and privacy of its ecosystem including citizen are - Transnational Nature of Cyber Crime, ‘Cultural’ Vulnerabilities, Internet Resilience and Threat Landscape.

It is evident that Cyber Security is a very complex paradigm, and with evolving new technologies, requirements and ever-increasing Attack Surface, the vulnerabilities are rising many folds with time. In such a dynamic scenario, how do we develop a Cyber Security Strategy to make our Critical Infrastructure comprehensively Safe, Secure, Resilient and Trustworthy?

narnix

# The Vision…

The vision is to ensure **a safe, secure, trusted, resilient** and **vibrant cyber space** for our **Nation's prosperity.**

AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE.

Secure Cyberspace Assurance –

Promise of a trustworthy Cyber-ecosystem

Internet Resilience of India - It is of utmost importance to ensure the security and resilience of the INTERNET within the country to enhance cyber security capabilities to better protect Indians and defend critical government and private sector systems.

# The Contrast…

It is easy to see why IT security and industrial control security are facing challenges when it comes to integration. These two Titans clash because at the lowest level the security considerations their entire design structures are based on, are at odds.

IT industry has been developed around the asynchronous behaviour of humans, while industrial controls require a synchronous component to communications.

Control systems primary concern for security is operational availability while providing highly accountable authentication of devices.

The primary concern for IT systems is to separate, secure and provide authenticated access for each user to their data.

# IoT Security…

designing a sustainable n resilient future

# 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.

# The genesis of Digital Transformation

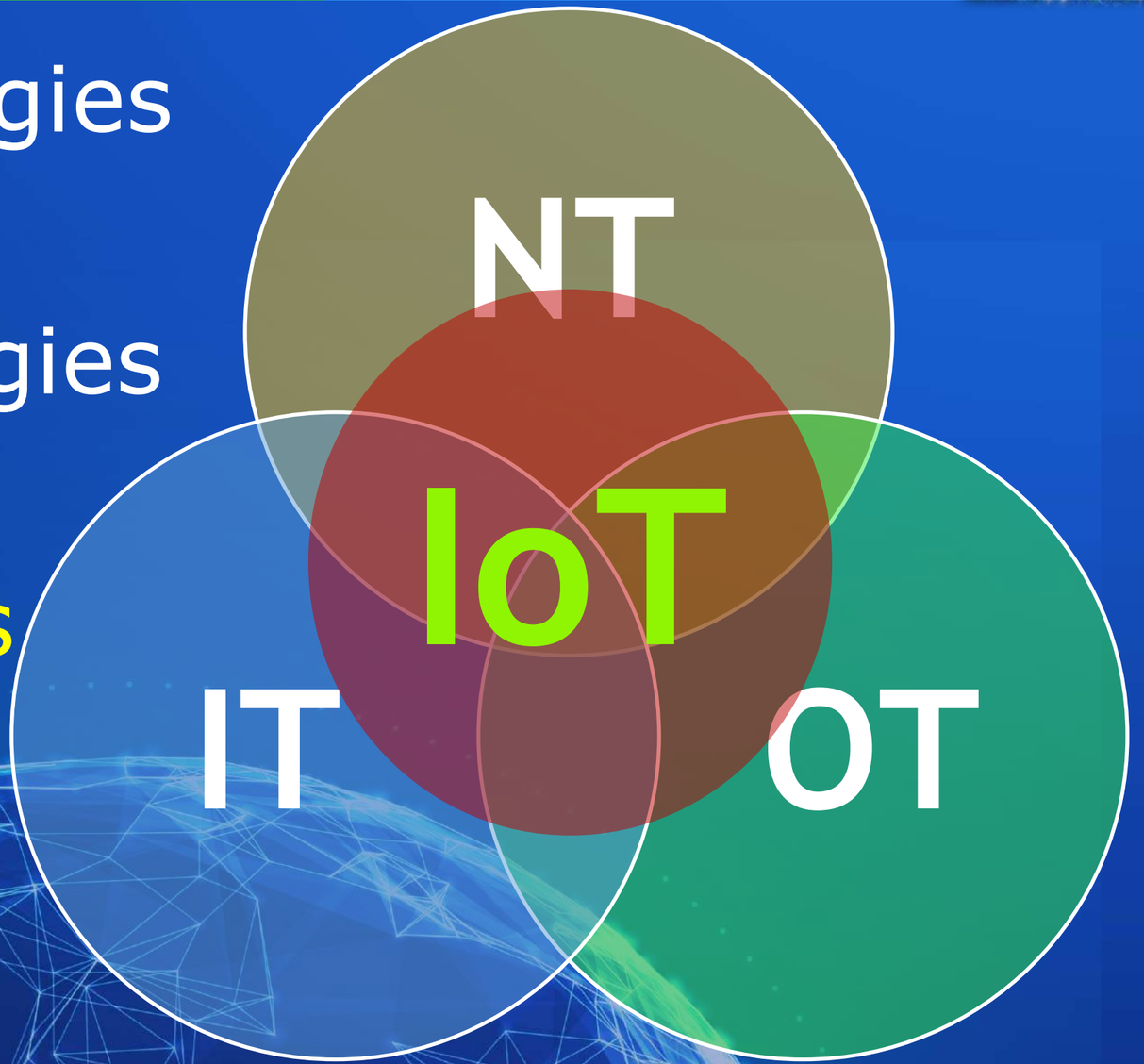
In digital transformation in any paradigm, domain or ecosystem --

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

## Standards are the Chromosomes of Digital Infrastructure

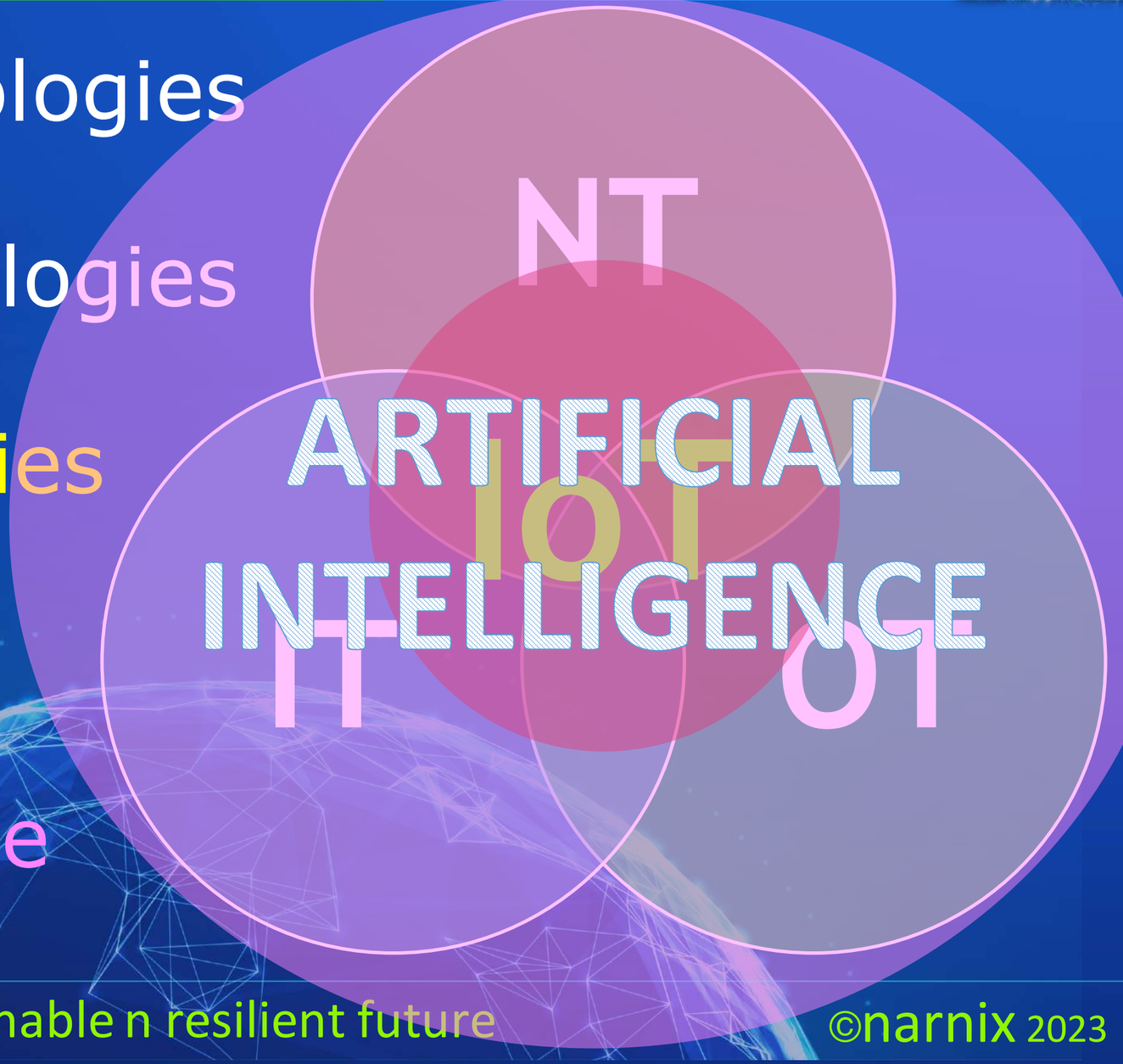
# Digital Transformation Constituents

- Information Technologies
- Operational Technologies
- Network Technologies
- IoT Technologies



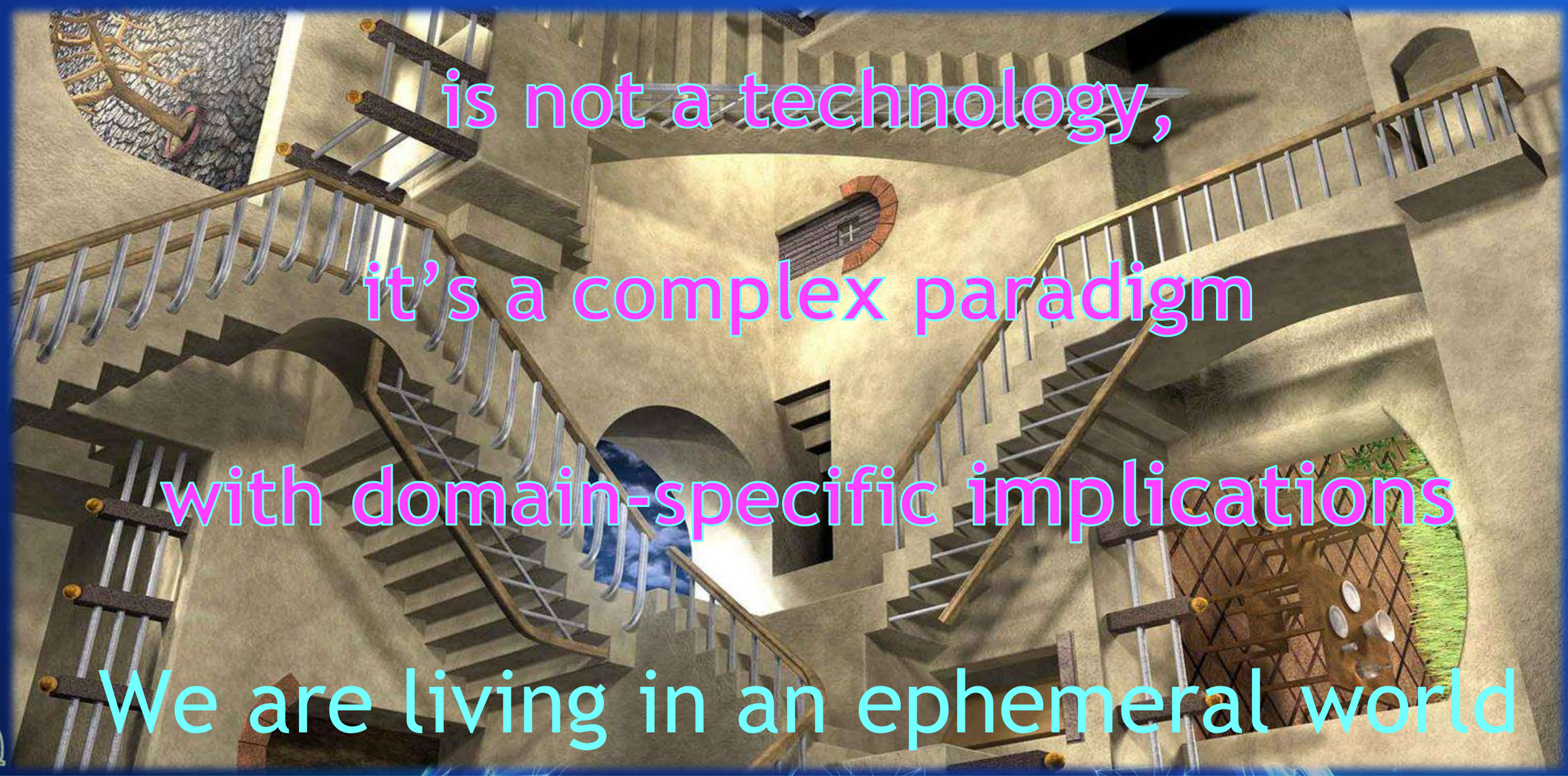
# Digital Transformation Constituents

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




narnix

# Digital Transformation

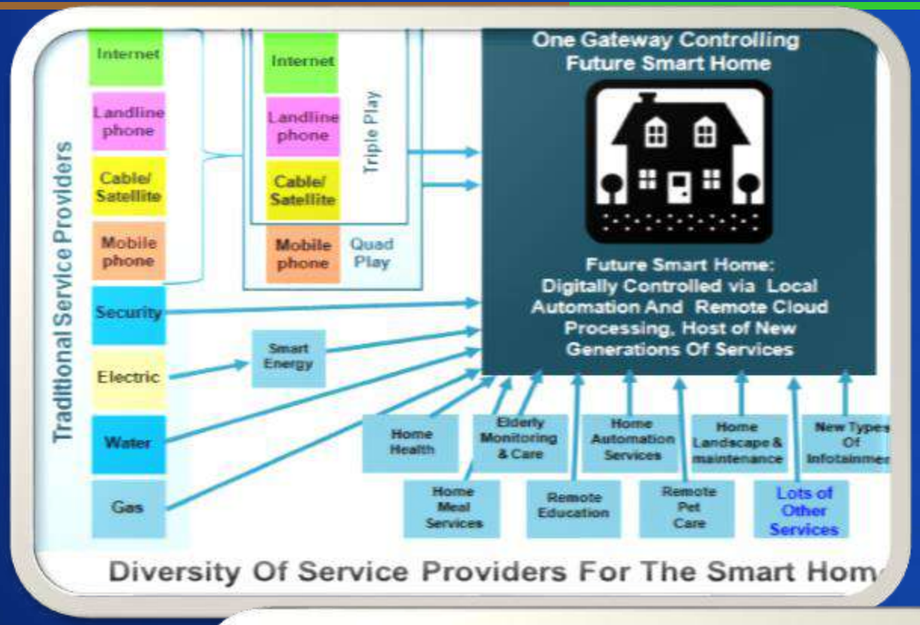


# IoT 2.0 – IoT Coming of Age…

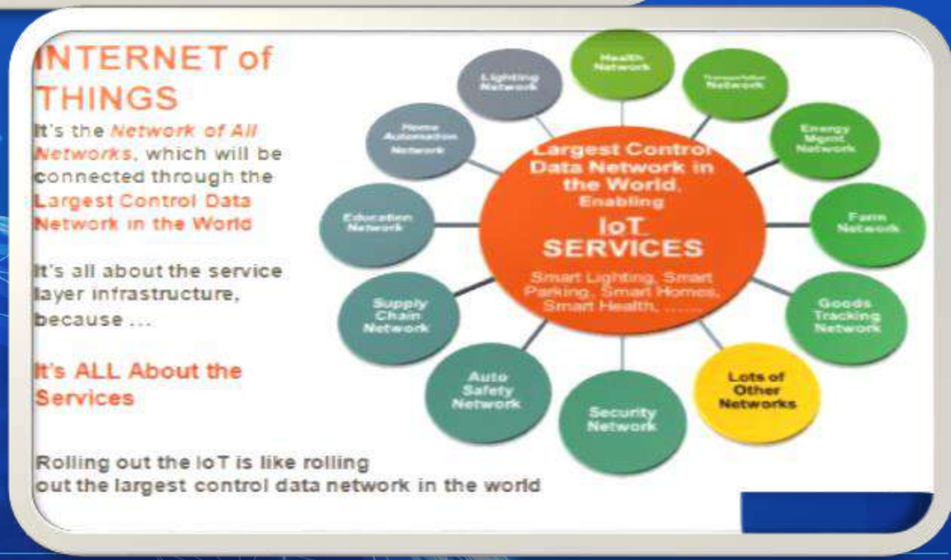
- "IoT", a concept that originally sounded like something out of sci-fi movie -- the "Internet of Things" -- is, in fact, a reality, and one that is bound to become even more widespread.

- From being considered as one of the most Disruptive Technologies in the early years of last decade to coming on the verge of becoming one of the most Profound Technologies by *weaving itself into the fabric of everyday life until it becomes indistinguishable from it…*

# Defining the IoT Systems:






narnix

designing a sustainable n resilient future

# Internet of Things…

Internet of Things is all about "heterogeneous" and "aware" devices interacting to simplify people's life in some way or the other.

# Key Components of IoT:

- Sensing Nodes,
- Local Embedded Processing Nodes,
- Connectivity Nodes,
- Software to automate tasks and enable new "Classes of Services"
- Remote Embedded Processing Nodes,
- and last but not the least "Full Security" across the "Signal Path".

narnix

# What's different about IoT?

Device Mgmt

Access Mgmt

Compute Mgmt

Protocol Mgmt

Data Mgmt

Connectivity Mgmt

**Peripheral Device**

**Edge Gateway**

**Field Area Gateway**

**Enterprise Gateway**

**Storage System**

**Data Processing System**

**Application**

**Workflow**

***Operational Technologies***

***Information Technologies***

**Event based actions on real time high velocity data**

**Query based action on non real time high volume data**

narnix

designing a sustainable n resilient future

# IoT Ecosystem & Value Chain…

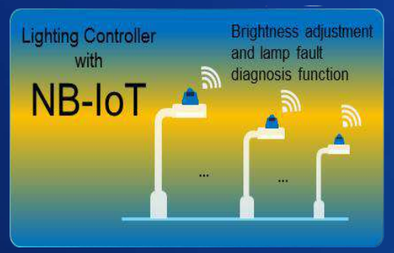
The IoT value chain is perhaps the most diverse and complicated value chain of any industry or consortium that exists in the world.

In fact, the gold rush to IoT is so pervasive that if you combine much of the value chain of most industry trade associations, standards bodies, the ecosystem partners of trade associations and standards bodies, and then add in the different technology providers feeding those industries, you get close to understanding the scope of the task.

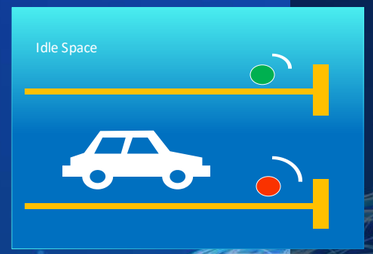
# IOT Use cases ready for Implementation

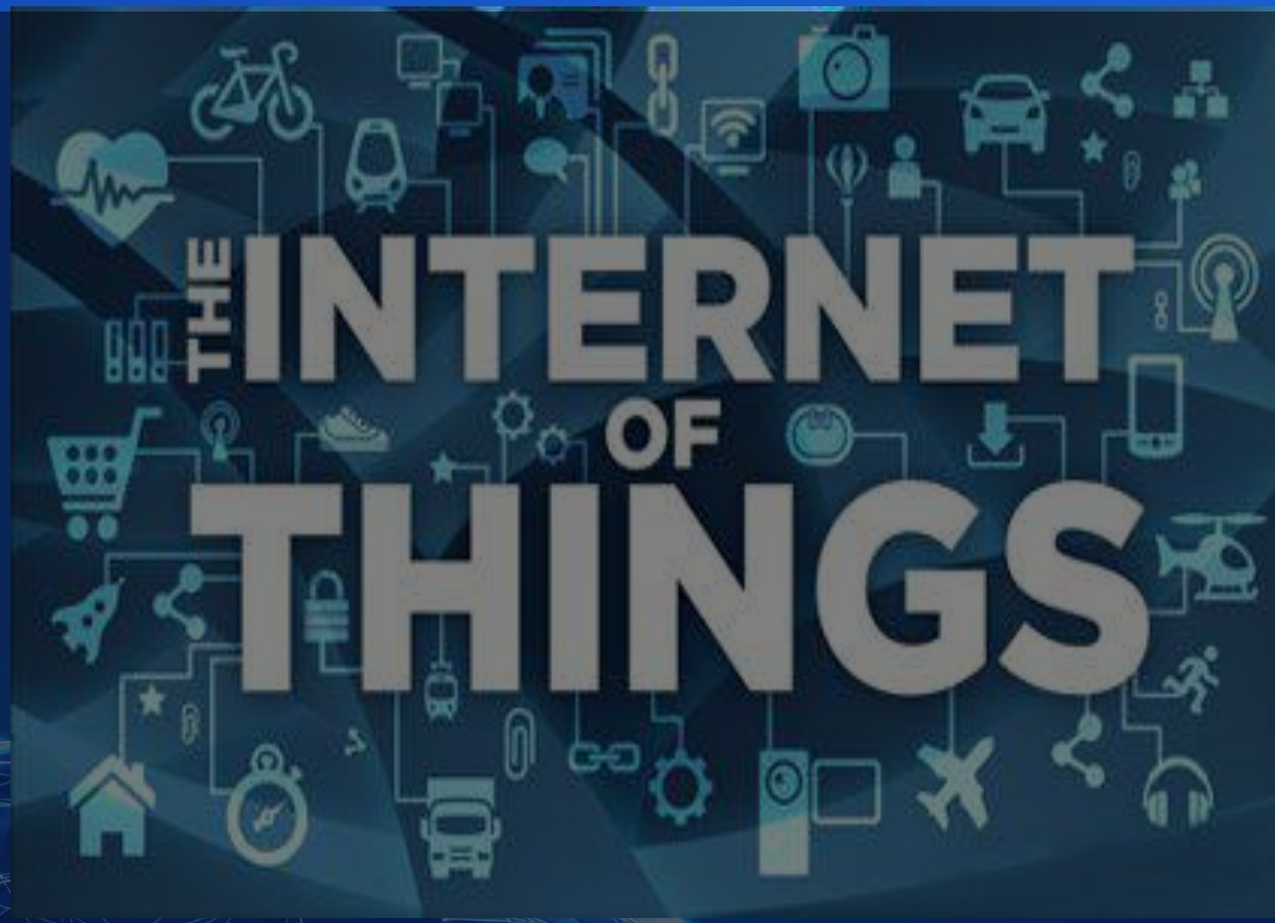
**Smart water meter**

**Smart street-light**




**Smart parking**




narnix

designing a sustainable n resilient future

# Features of a Smart City

- Citizen participation
- Identity and culture
- Economy and employment
- Health
- Education
- Mixed use
- Compactness
- Open spaces
- Housing and Inclusiveness
- Transportation & Mobility
- Walkable
- IT connctivity

**ICT and IoT Opportunities in all these areas!**

- Intelligent government services
- Energy supply
- Energy source
- Water supply
- Wastewater management
- Water quality
- Air quality
- Energy efficiency
- Underground electric wiring
- SanitatIon
- Waste management
- Safety

24 Features identified by MoHUA GoI

narnix

designing a sustainable n resilient future

# Smart Cities & Smart Infrastructure

## A sample Indian business case for next 5-10 years:

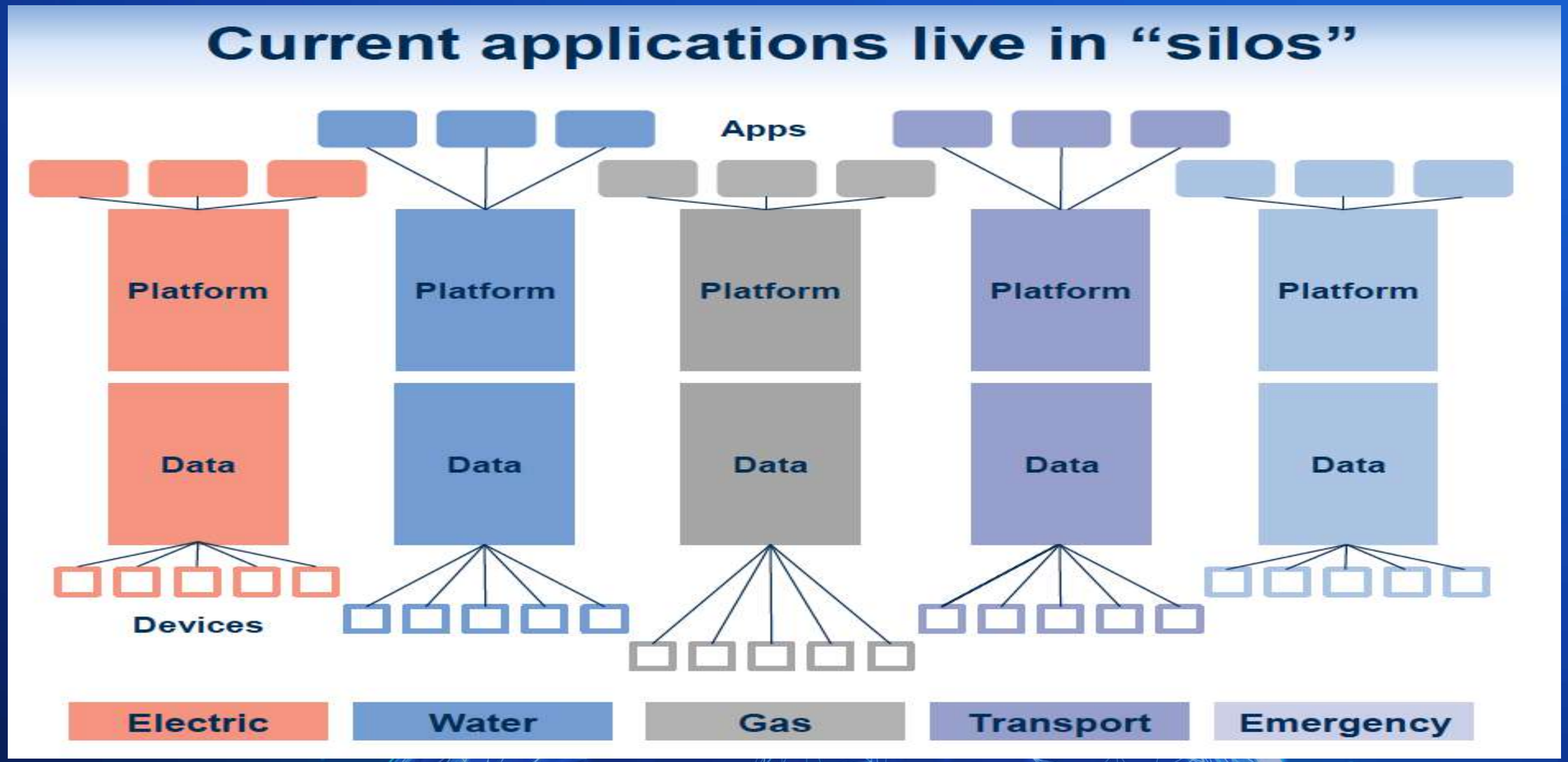
- 250 million Smart Electricity Meters are going to be procured & deployed under the NSGM (National Smart Grid Mission).
- All these **Smart Meters** are going to use **250 million Communication Modules** and minimum **0.5 million Gateways/DCUs** (Data Concentrator Units).
- **Smart Streetlights** are going to use more than **100 million Communication Modules** and at least **half a million of DCUs/Gateways**…
- **Smart Buildings** are going to deploy more than **50 million smart Sensors** and at **least 100K – 200K DCUs/gateways…**
- **Automobile**s shall be using at least **100-200 million** communication nodes for Vehicle O & M, V to V, V to I & other telematics applications…
- Similarly, various applications of the Smart Infrastructure paradigm like Smart Water, Smart Gas, Smart Traffic, Smart Environment, Smart sewage Disposal etc. are going to use a few billions of Smart Sensors with Communication Modules

To summarize, India ALONE, is going to need a minimum of 5 - 10 billion Communication modules to be integrated into the Smart Sensors and Controllers and 10– 50 million Gateways that shall be needed to operate and maintain the *Nation Wide Critical Infrastructure* that needs to be deployed to enable and empower the citizens to lead a sustainable, safe and secure life …

narnix

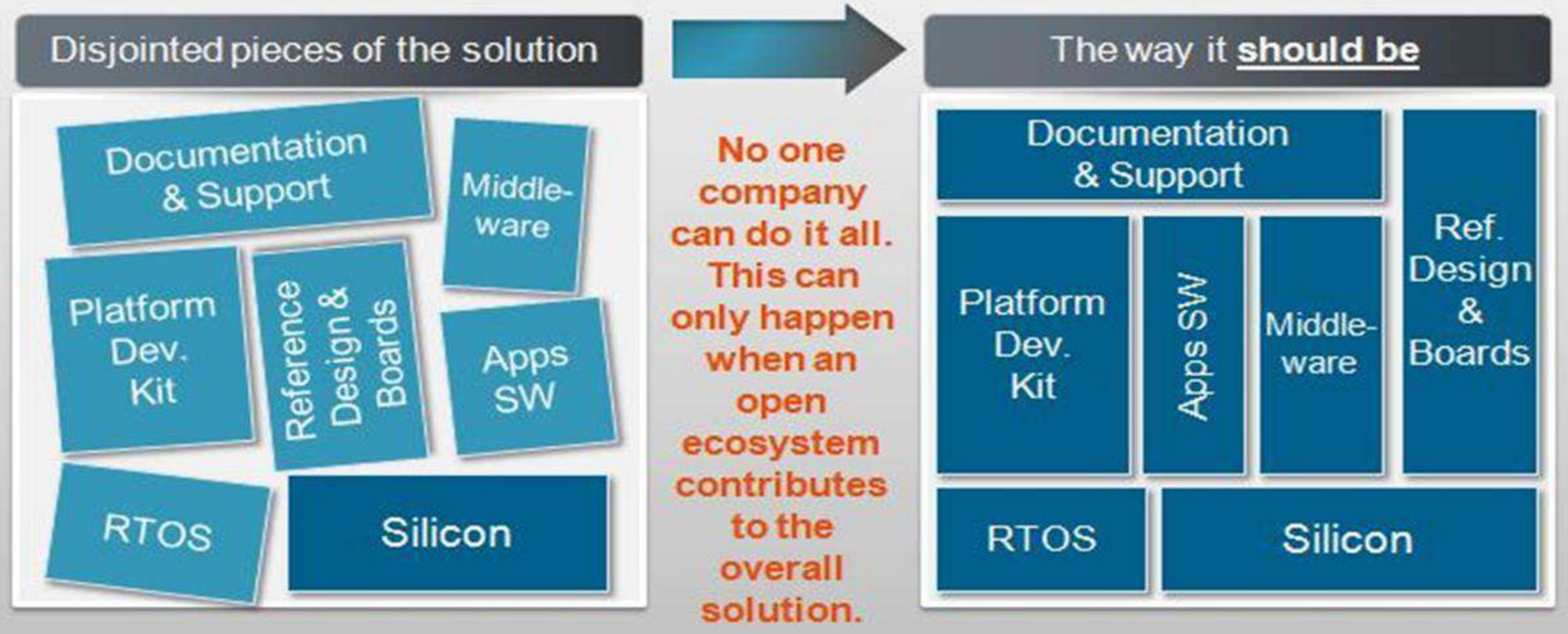
designing a sustainable n resilient future

# Current Applications live in silos



# Hurdles in fast growth of IoT:

*It is difficult for innovation to happen across disjointed platforms & technologies.*




***Creating the opportunity for ecosystem partners to work across common open platforms facilitates faster innovation.***

# Challenges in fast growth of IoT:

## The challenges that inhibit the IoT-related standards and hence a robust rollout of IoT services are:

- Security and privacy issues (Note that security and privacy measure are a lot of times at odds with each other)
- Endless IoT applications
- Endless potential types of edge node technologies, and the interface to the communication nodes (e.g. Sensors and use cases integration into Telco services)
- High fragmentation of today's IoT connectivity solutions
- Lots of legacy systems that will now be a part of IPv6 network, with no (or minimal) existing "co-existence" and interoperability plans

# Challenges in fast growth of IoT:

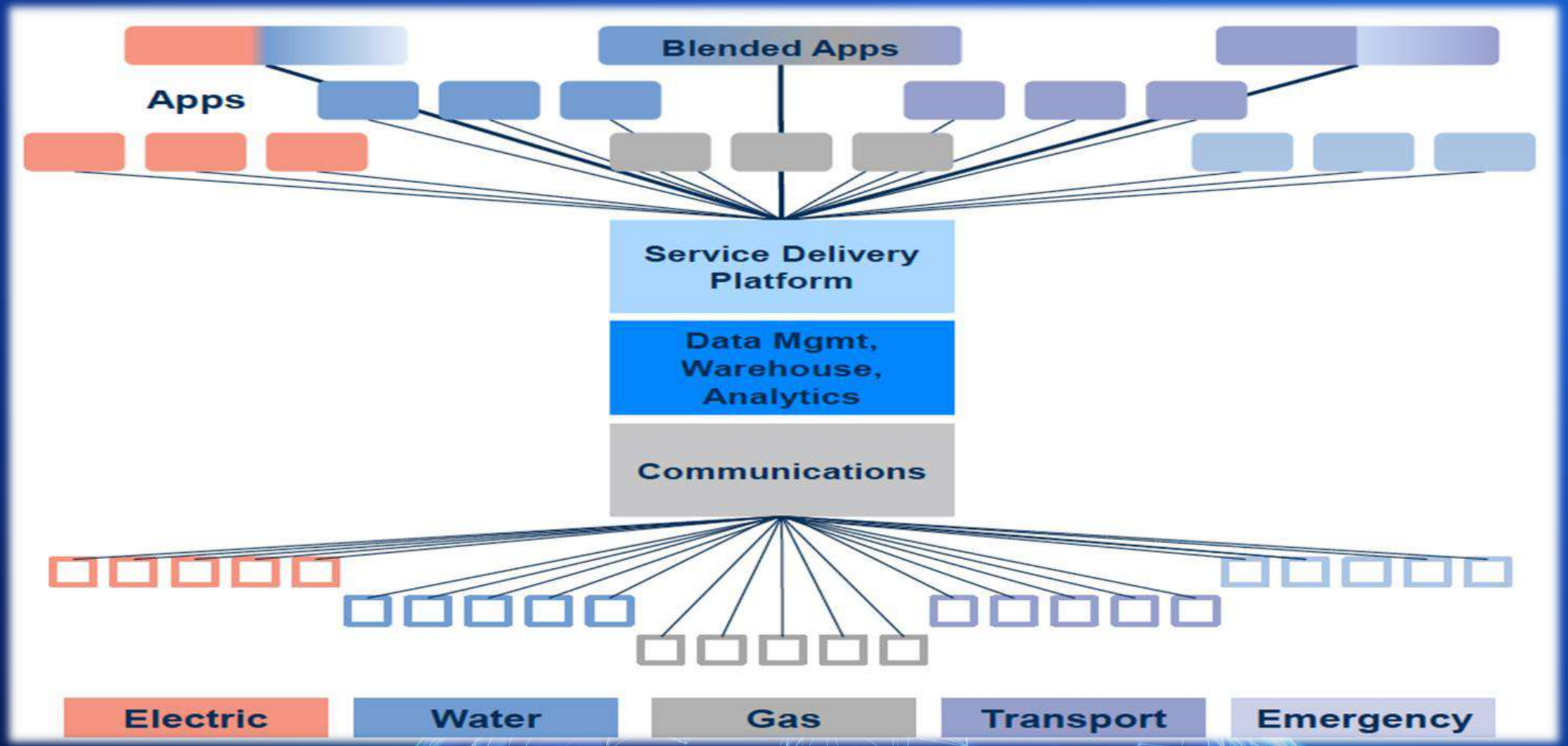
- Partnerships, between heterogeneous and diverse industries, and defining the associated business models involving multiple stakeholders and service providers of some of those legacy systems in number
- Management and provisioning of the various networked devices, applications, and services, and the network capacity planning that comes with it
- Regulatory issues that will hinder deployments on a worldwide basis
- Special needs of “industrial grade” product rollouts, with long lasting requirements in the field, that require future proofing of any standard recommended
- Slow development of the IoT services market, partially due to lack of future proof standards etc.

# Challenges…

- In this absolutely heterogeneous scenario, coming up with common harmonized standards is a major hurdle.

- We need to see acceleration and a maturing of common standards, more cross-sector collaboration and creative approaches to business models….

# The way forward: Unified Architecture



# The Imperative

- Hence, in spite of so much hype and even genuine potential, the IoT paradigm has not proliferated in a true sense to its desired potential.

- Bringing the “Internet of Things” to life requires a comprehensive systems approach, inclusive of intelligent processing and sensing technology, connectivity, Cyber Security, software and services, along with a leading ecosystem of partners.

# Smart but NOT Secure ! ! !

**“A chain is only as strong as its weakest Link”**

- currently the weakest link in the IoT deployment Signal Chain is our smart End Nodes.
- A robust Communication & IT Infrastructure shall be no good if we continue to use the devices, which are not Equally Secure. So, the new imperative for the design Community is to Design “Smart & Secure” Phones, Sensors, Devices or Instrument.

# Smart but NOT Secure ! ! !

- Amidst all the hype and hope of the expected benefits from the Internet of Things (IoT), Security remains its biggest challenge to overcome.
- IoT is dependent on a wealth of data being collected from numerous devices connected across different interfaces and locations within the Enterprise, while carrying sensitive company or customer information.
- Any kind of security breach could compromise the organization's customers, workers or even the business itself.
- A smart network is required to maximize the much-expected value from IoT, to securely connect thousands of these "things" with the highest levels of security including encryption, authentication, traffic segmentation, intrusion detection and remediation.

# Smart but NOT Secure ! ! !

- A majority of devices in today's connected world are out there for very long time.
- They are running old operating systems which may be vulnerable due to its openness or maybe they never ever got patches.
- The big threat is not because we expect people hacking into it. But *do we know what we don't know*?
- Also, Security by Obscurity is NOT a sound security strategy…

# Security philosophy…

## Extrinsic Security

Add-on Security

**PC/Datacenter Era**

- Bolt-On Security
- Layers of Security added to PCs, Servers, Networks and Devices

## Intrinsic Security

Security-by-Design

**Internet of Things Era**

- Built-In Security
- Security built into the device at manufacturing time

# Integrating cybersecurity into product development

**Training**
- Threat Modeling
- Risk Management
- Secure coding
- Security testing
- Cryptography
- Emerging technologies

**Requirements**
- Product and architectural review
- Threat Modeling
- Prioritized cybersecurity requirements

**Implementation**
- Recommend external libraries
- Source code analysis
- Implementation reviews
- Supplier contracts

**Verification**
- Verifying cybersecurity requirements
- Penetration testing
- Fuzz testing
- Robustness testing
- Verifying external libraries
- Malware testing
- Documentation review

**Release**
- Vulnerability mitigation/patch/update strategy plan
- Final security review

**Response**
- Swift incident response

narnix

# IoT Paradigm & challenges ! ! !

- Global Neural Network of Networks…
- Homogeneous Network of Heterogeneous Devices…
- Industrial IoT v/s Consumer IoT…
- Services v/s Applications…
- Infrastructure v/s Enterprise v/s Homes
- ***End to end Security in the Signal Chain…***

narnix

# 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….


The Impossible War
HI
versus
AI
blockchain
hashgraph

# ARTIFICIAL INTELLIGENCE

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.*

# Let’s see where we are heading….

# 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

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

Gives conditions to …

## Digitalization

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

# Managing Risk is a Journey

Assets & Risks Discovery
What/Why need to be protected

Design

Organizational Roles & Responsibilities

Training

Awareness

Patching and update management

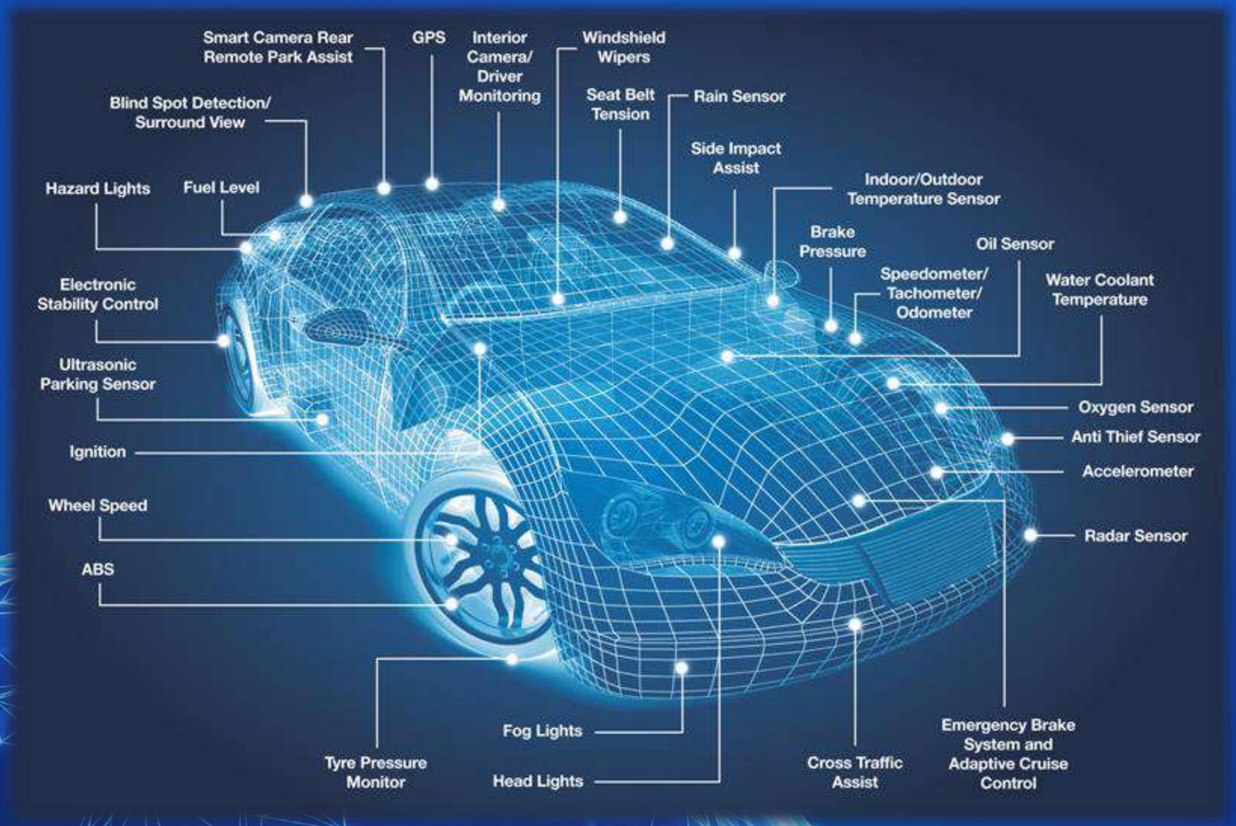

narnix

designing a sustainable n resilient future

# A Strategic Approach is Required

## Tactical Risk Management

## Strategic Risk Management



# An Important Metrics…

**BREAKOUT TIME:**

Security teams are encouraged to strive to meet the metrics of the 1-10-60 rule: detecting threats within the first minute, understanding threats within 10 minutes, and responding within 60 minutes. However, the average breakout time for all observed intrusions rose from an average of 4 hours 37 minutes in 2018 to 9 hours in 2019; 4 hours 37 minutes in 2020; and 1 hour 32 minutes in 2021.

**Adversary breakout time hits an all-time low of 79 minutes:**

The average time it takes an adversary to move laterally from initial compromise to other hosts in the victim environment fell from the previous all-time low of 84 minutes in 2022 to a record 79 minutes in 2023

# 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**

narnix

designing a sustainable n resilient future

# …The Standardization Conundrum

- "The irony is that Standards & even SDOs are not at the forefront of Solution designers, developers, providers, deployers or users' minds."
- There are misconceptions on what standards are for, and the case for use of standards has not been made. Most researchers, design engineers and even start-ups argue that standards block innovation.
- In fact, Standardization brings innovation and spreads knowledge. Standardization helps define the contours of structured innovation, first because it provides structured methods and reliable data that save time in the innovation process and, second, because it makes it easier to disseminate ground-breaking ideas and knowledge about leading edge techniques.
- Liberalization and Markets have a lot of great virtues, but they cannot create their own conditions of existences: they must be designed!

narnix

# 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.

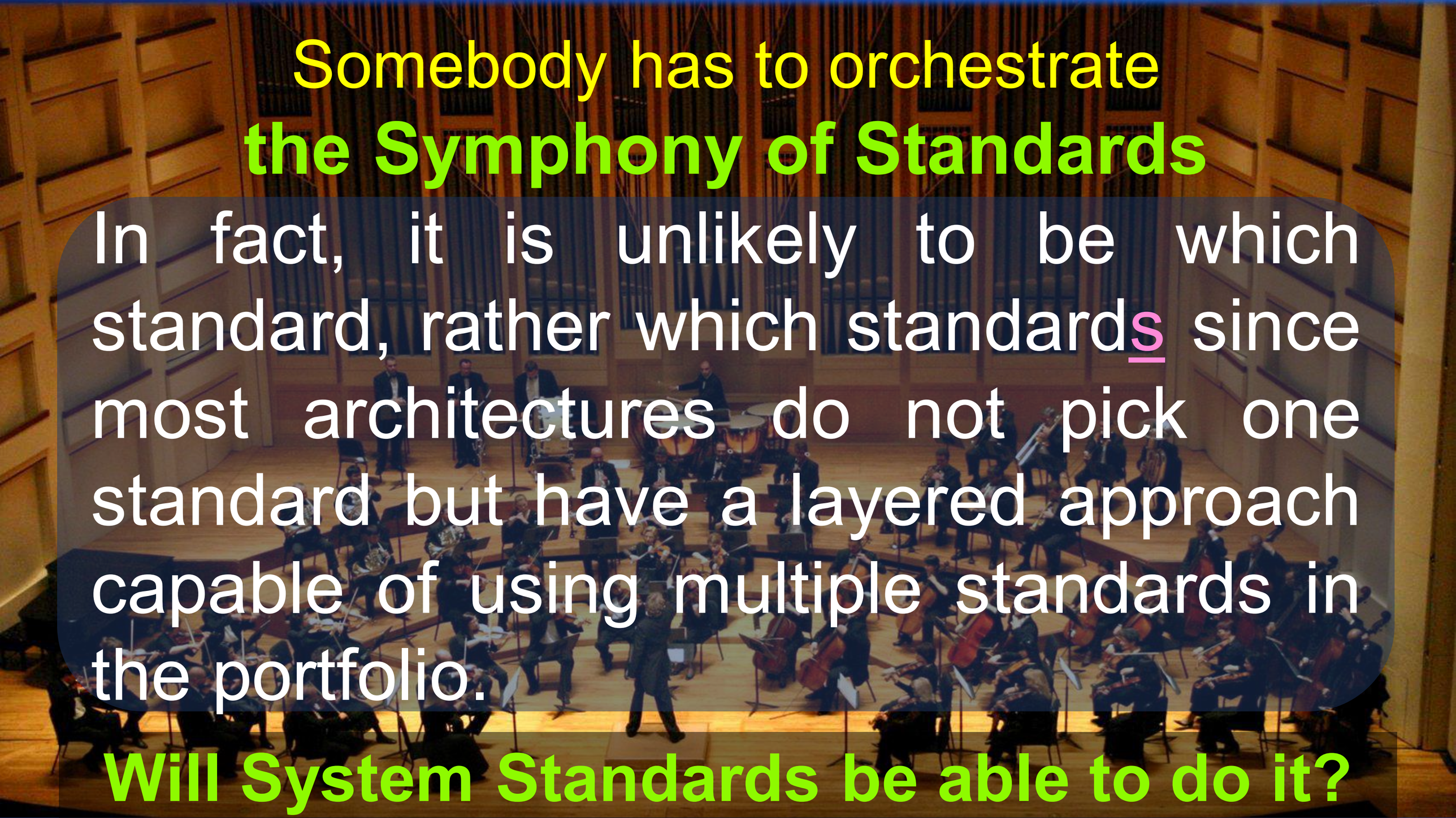
In reality, there are often overlapping or rivalling standards, driven by different vendor “camps”, in case of Cyber Security, Standards by different Global, regional & National SDOs.

# SYMPHONY or CACOPHONY ? ? ?

The Enraged Musician, William Hogarth, 1741

# Standardization Imperative

- Every SDO only talks about the concerns their respective standards shall address…
- No one has identified the Gaps in Cyber Security Standards at a comprehensive & granular level with a systems view…
- Need to build a comprehensive inventory of Security concerns in different aspects of Utilities/Critical Infrastructure followed by mapping them with corresponding technologies, processes, strategies and standards and developing corresponding Compliance Testing Framework & strategy.



# 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.

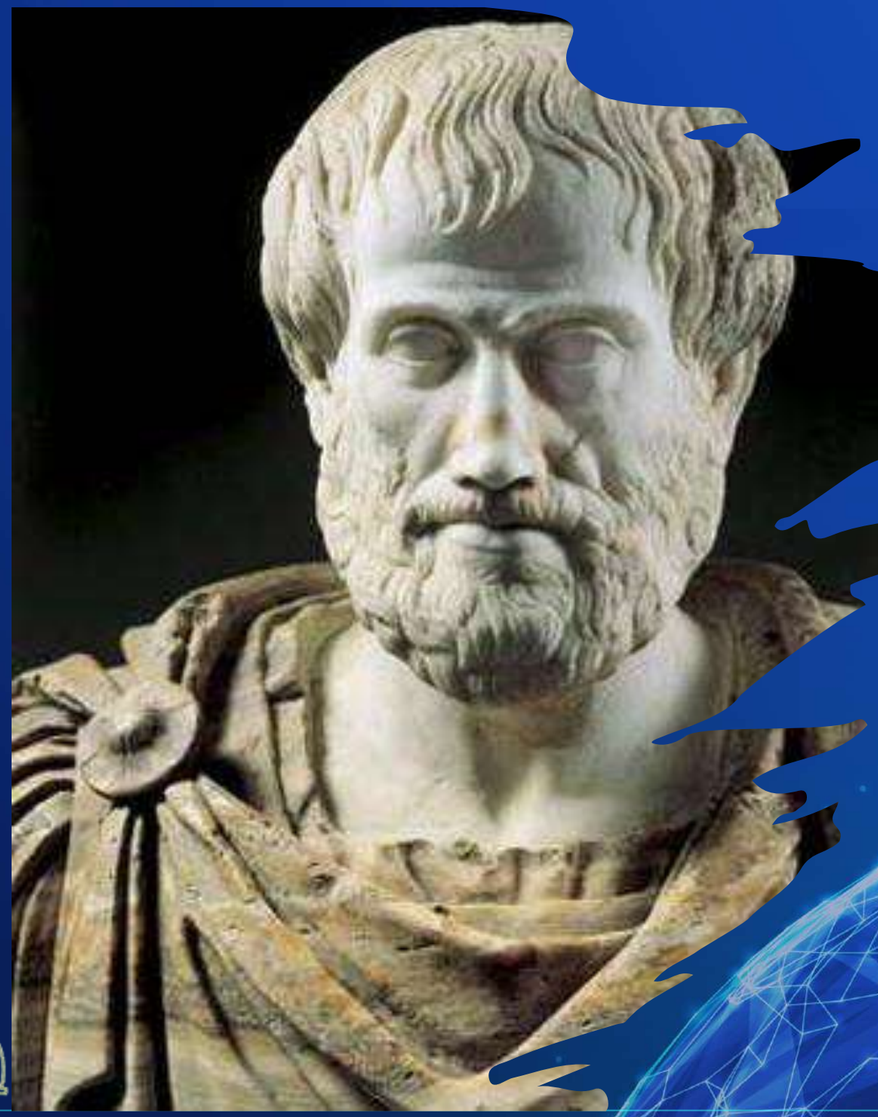
**Will System Standards be able to do it?**

# Crucial Imperatives…

Need to build a comprehensive inventory of Security & Trustworthiness concerns in different aspects of Utilities/Critical Infrastructure followed by mapping them with corresponding technologies, processes, strategies and standards and developing corresponding Compliance Testing Framework & strategy.

The only approach would be to adopt top-down approach to standardization starting at the system or system-architecture rather than at the product level. We need to Study & Analyze the diverse Use Cases, Applications and corresponding Stakeholders & their respective requirements to understand their respective Characteristics and concerns. Develop a Granular Architecture followed by developing a Cyber Security Architecture mapping all the security, privacy, safety, resilience characteristics with the Granular Critical Infrastructure Architecture.

# Systems Approach: Holism



**Aristotle (300 B.C.)**

**“The Whole is Greater than the Sum of its Parts”**

# 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.

# System and Systems Approach

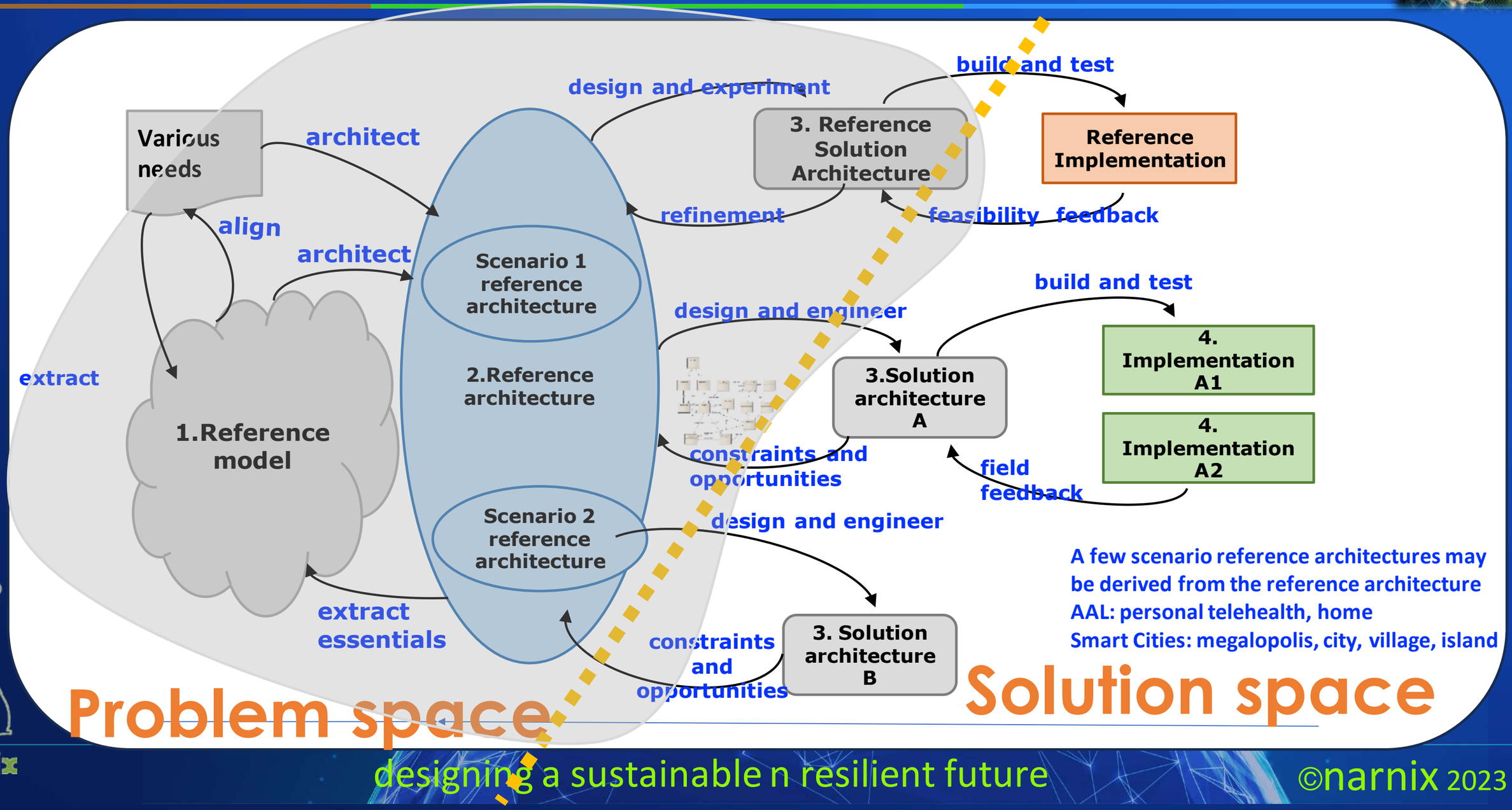
- System: *A group of interacting, interrelated, or interdependent elements forming a purposeful 'WHOLE' of a complexity that requires specific structures and work methods in order to support applications and services relevant to the stakeholders.*
- Systems Approach: *A holistic, iterative, discovery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

# Systems Approach Process Flow…

# Levels of Architecting



# National Priority…

Considering the current and future evolving Cyberthreat Landscape, it would be absolutely critical to have Two National Documents:

- A concise yet comprehensive **'National Cybersecurity Strategy'** that sets clear, top-down directions to enhance the cyber resilience for the ecosystem that includes government, public and private sectors, the citizenry, and also addresses international cyber issues.
- A separate **'National Cybersecurity Policy'** based on principles laid down in 'strategy'. It must be outcome-based, practical and globally relevant, as well as based on risk assessment and understanding of cyberthreats and vulnerabilities. The security framework must include the compulsory testing of cyber products, infrastructure skill capacity development, responsibilities of entities and individuals, and public-private partnerships.

An accountable integrated national cybersecurity apparatus to be structured/restructured and it must be provided clear mandates and be empowered adequately. It must be able to supervise and enforce policies across India, including policies regulated by independent regulators.

# Trustworthiness paradigm…

- Trustworthiness is an overarching paradigm with a multitude of nuances and distinct aspects that it has different connotations for different sets of stakeholders, use cases and applications.
- 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
- Characteristics of trustworthiness include - Reliability, Availability, Resilience, Security, Privacy, Safety, Accountability, Transparency, Integrity, Authenticity, Quality, Usability and Accuracy.

# Critical Infrastructure TRUSTWORTHINESS

## Reference Architecture

To explore the feasibility of developing a Granular TRUSTWORTHINESS Reference Architecture with multiple views and interdependence matrix of stakeholders, their respective concerns and technologies, standards (also Policies & Regulatory interventions) required to address them in a wholistic manner with the following granular actions:

- Mapping the already developed Standards on various aspects of the developed Reference Architecture.
- Identifying the GAPS in Standards and developing new Systems Standards and Products/Domain specific Standards.
- Developing a comprehensive Compliance Testing Framework and Ecosystem of Test Labs, supporting and enabling services.

narnix

# NATIONAL TRUST CENTRE

- As per recommendations of Telecom Regulatory Authority of India (TRAI) on "Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications" released on 5th September 2017 National Trust Centre (NTC) must be set up without any further delay.

- This NTC must be geared up to undertake the Security Testing and Evaluation comprehensively including but NOT limited to Devices, Systems, Networks, Application & System Softwares, Firmwares, Communication Stacks to ensure that the deployed Devices, systems and solutions are completely Trustworthy.

# National Charter of Trust:

- India needs its own National Charter of Trust to develop an ecosystem of Trustworthy vendors that all Utilities, service providers and other Critical National Infrastructure agencies can TRUST absolutely by establishing the best practices in the domain of cyber security that are globally harmonized in Standards, strategy, innovation, certification, transparency and all other core characteristics required to build a trustworthy ecosystem.

- Improving cyber safety and resilience requires all stakeholders to act together at scale and in a coordinated way, including governments, the engineering profession, operators of critical infrastructure and other systems, and developers of products and components. The evolving nature of the challenges will require continual responsiveness and agility by governments and other stakeholders.

# Security Perspective – As a NATION…

**Strategic Layer**

*Nuclear | Defense*
*Space | Energy*
*Critical manufacturing*

**Internal Security**

*Critical Facilities | Borders | Physical Infra | Law & Order*
*Crime Prevention*

**External Affairs**

*Policies | Doctrines*
*Missions | Diplomacy*
*Relations | Initiatives*

**Government Information**

*Strategic Plans | Policies | Ministerial Deliberations | Decisions*
*Geological Data | Tenders | Economic Data | Transaction Data*
*Public Sector IPR | Project Information | Social Security | Citizens Data*

**Financial Information**

*Financial Plans | Finance Architecture | Transaction Switches | Financial Transactions | Security Transactions | Trade Information | E -commerce | Payment Infrastructure | Account Info | Financial Performance | Financial & Social Funds | Business & Service Models |*

**Commercial Information**

*Research & Development | Products Ideas*
*Business Ideas | Intellectual Property |*
*Service Models | Business Alliances*

**Personal Information**

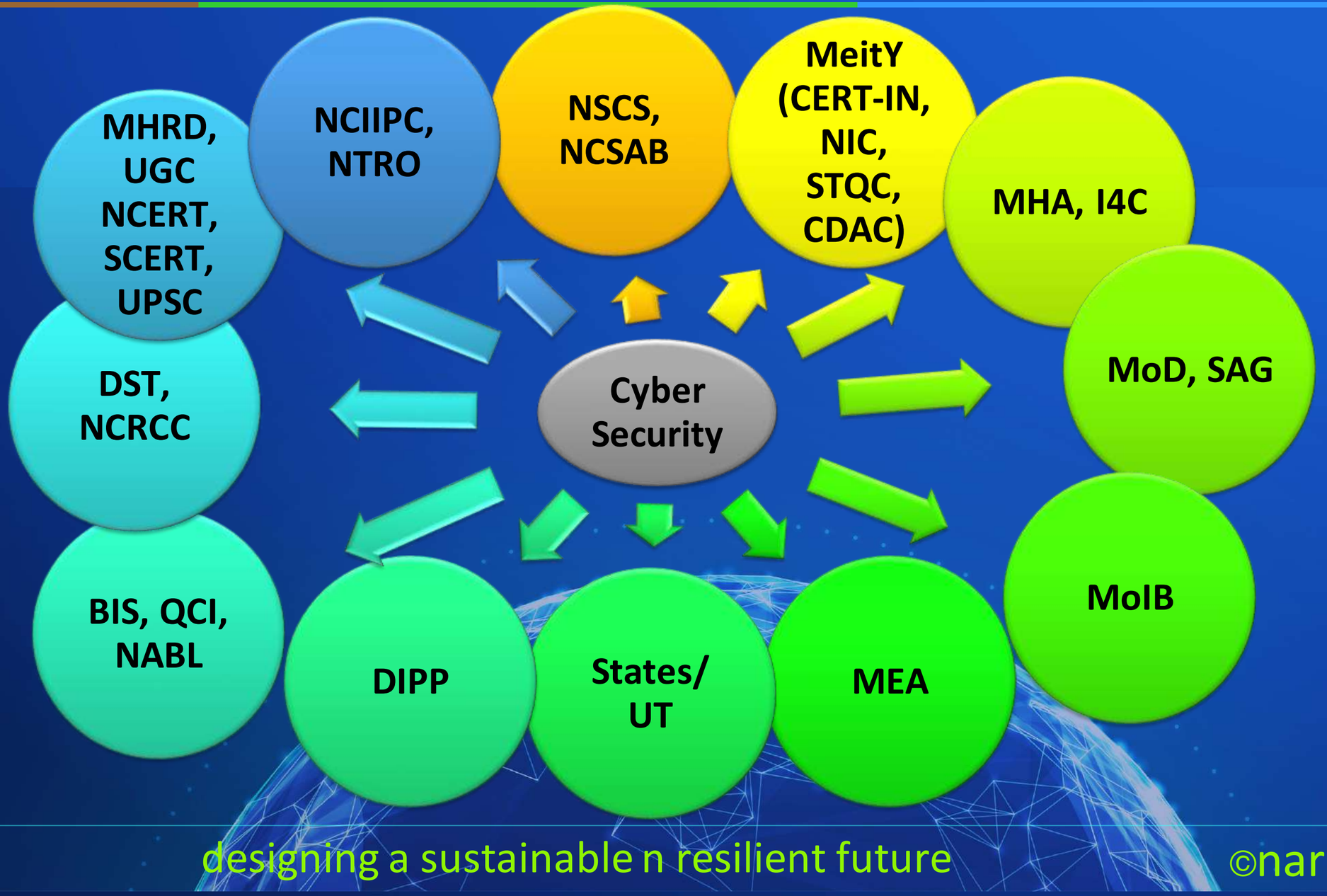
*Personal Identifiable Information*
*Financial Info | Health info | Transaction Info*
*Entitlements | Investments | Social Benefits*

narnix

# Cyber Security Paradigm


| National Security | Cyber Security | IT Asset Security | IPR Protection | Privacy |
|---|---|---|---|---|
| Strategic Deterrence | Health of Cyber Space | Security of IT Asset | Protect key Org Information | Limit Information Collection |
| Protection of Critical Assets | Critical Infrastructure Protection | Maintain Security Baseline | | Transparent Info Usage |
| Economic Stability | Cyber Threat Management | Manage Vulnerabilities | Secure Commercial Interests | Protect Information |
| Commercial Stability | Cyber Crime Prevention | Limit Exposures | | Protect Consumer rights |

# Cyber Security - Stakeholder Organisations



# Cyber Security - Responsibility Matrix

**National Security Issue – Detection and Prevention**

**National Security Issues – Crisis**

**National Security Issues – Investigation, Forensics Recovery & Restoration**

National Critical Information Infrastructure Protection Committee (NTRO) responsible under section 70 A of IT Act

- CERT-IN MeitY
- NTRO (National Technical Research Organization)
- DEFENCE
- REV INT (Revenue Intelligence)
- IB (Intelligence Bureau)
- RA&W (Research and Analysis Wing)
- POLICE
- CBI (Central Bureau of Investigation)
- DOT (Department of Telecommunication)
- NIC (National Informatics Center)

**NTRO Security Testing – Devil's Advocate**

**VA And PT by empanelled auditors of the systems, CERT-In and Auditing**

**STQC under MeitY tests the systems before implementation**

**Development of Information Systems R&D + Implementation Phase**

**NIC – Government Service Provider**

**Other Service Providers**

**SECURITY BREACH**

**CYBER INCIDNET**

**National Security Issues**

- IDS (Integrated Defense Services)
- NTRO

Intelligence Bureau

**Internal Security Issues**

- NIA (National Investigation Agency)
- Police Agencies

Crisis Management Plan of each Min

**Crime Related Issues**

- Customs Income Tax etc
- NCB (Narcotics control Board)
- DRI (Directorate of Revenue Intelligence)

**CYBER FORENSICS**

- Security Labs
- MHA CERT-In CBI
- LABS (Cyber Forensic Labs)

**TIMELINE**

**CERT – IN is responsible for Managing security breach under Section 70 B**

**Pre Cyber Incident Phase** → **On Cyber Incident Phase** → **Post Cyber Incident Phase**

narnix

designing a sustainable n resilient future

# 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.

narnix

# Cyber Immunity & Cyber Resilience

Cyber Immunity at every layer will create networks that are inherently secure and self-learning.

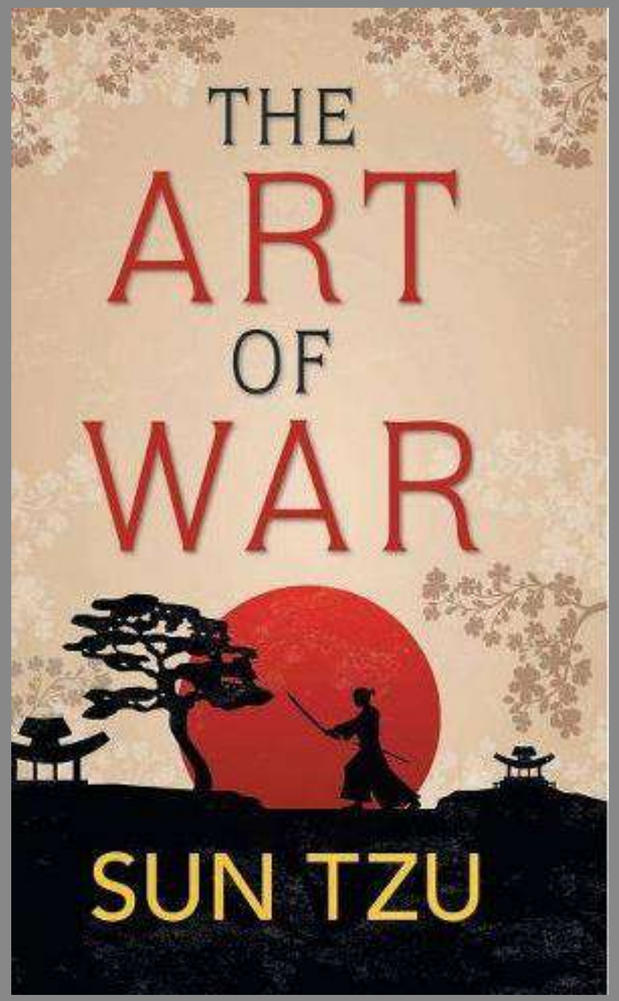
AI-induced digital intuition is one of the pillars of cyber-Security strategy that will allow intelligent adaption.

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.

# Cyber Immunity & Cyber Resilience

These systems will be designed to make the right decisions with the context-based data, pre-empt attacks based on initial indicators of compromise or attack, and take intuitive remediated measures, allowing any digital infrastructure and organization to be more Resilient.

# Cyber Security : Many Battles & A War




If you know the enemy and know yourself, you need not fear the result of a hundred battles.

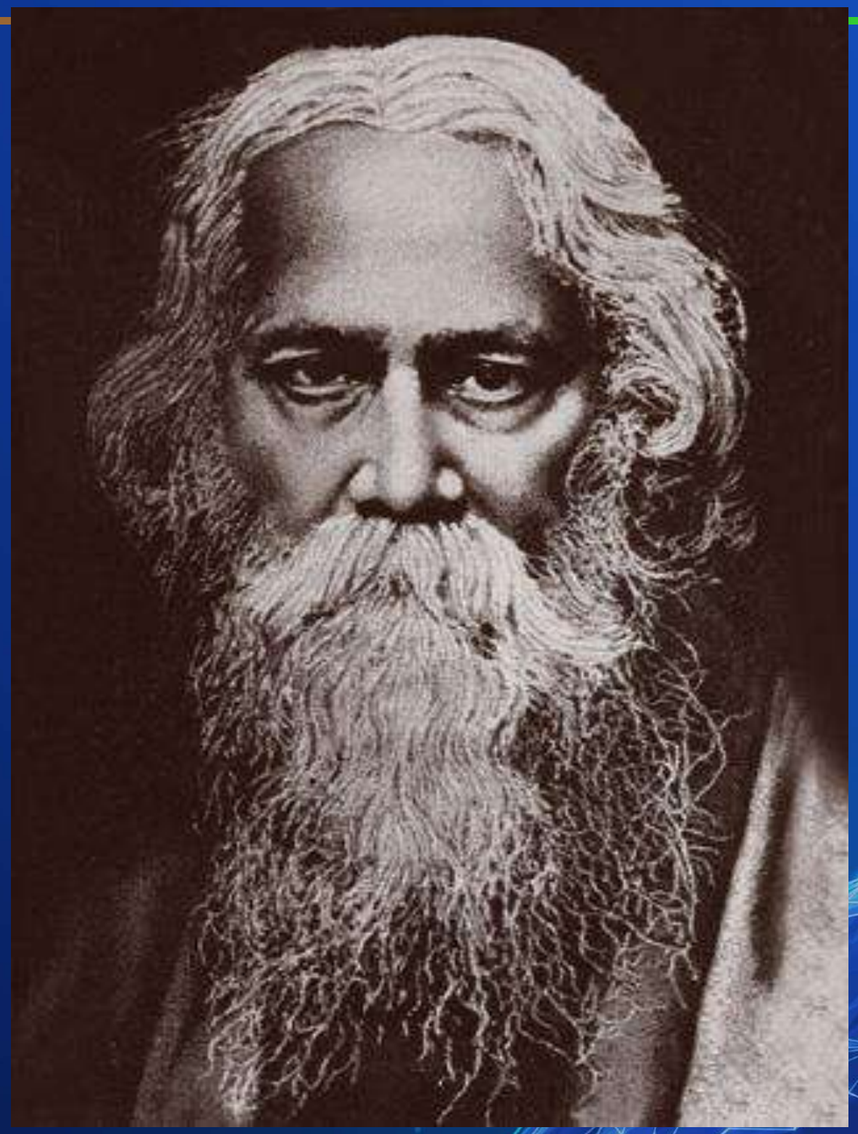
If you know yourself but not the enemy, for every victory gained, you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.”

Each of these 3 points of 5th Century B.C. book directly applies to the world of Cyber Security.

# In Conclusion…

# Resilience....



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

# Thank you!

## For a Sustainable & Resilient Future


narnix

designing a sustainable n resilient future

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

# About me…

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

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

- Over 45 years of professional experience in education, research, design and advisory .
- Over 35 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 Advisory Experience to different segments of business & industry.
- Over 250 Research & Design Mentees in the Electronics & ICT & STI 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 10 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.
- Standards based on 10 years of Pre-Standardization Research Published Recently (December 2020) –
  - Unified Digital Infrastructure ICT Reference Architecture – IS 18000
  - Unified Last Mile Communication Protocol Stack Reference Architecture – IS 18010.