Cyber Immunity, Cyber Resilience & Trustworthiness Imperatives for Digitized Grid

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.

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?

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.

Power systems are among the most complex and critical infrastructures of a modern digital society, serving as the backbone for its economic activities and security. It is therefore in the interest of every country to secure their operation against cyber risks and threats.

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

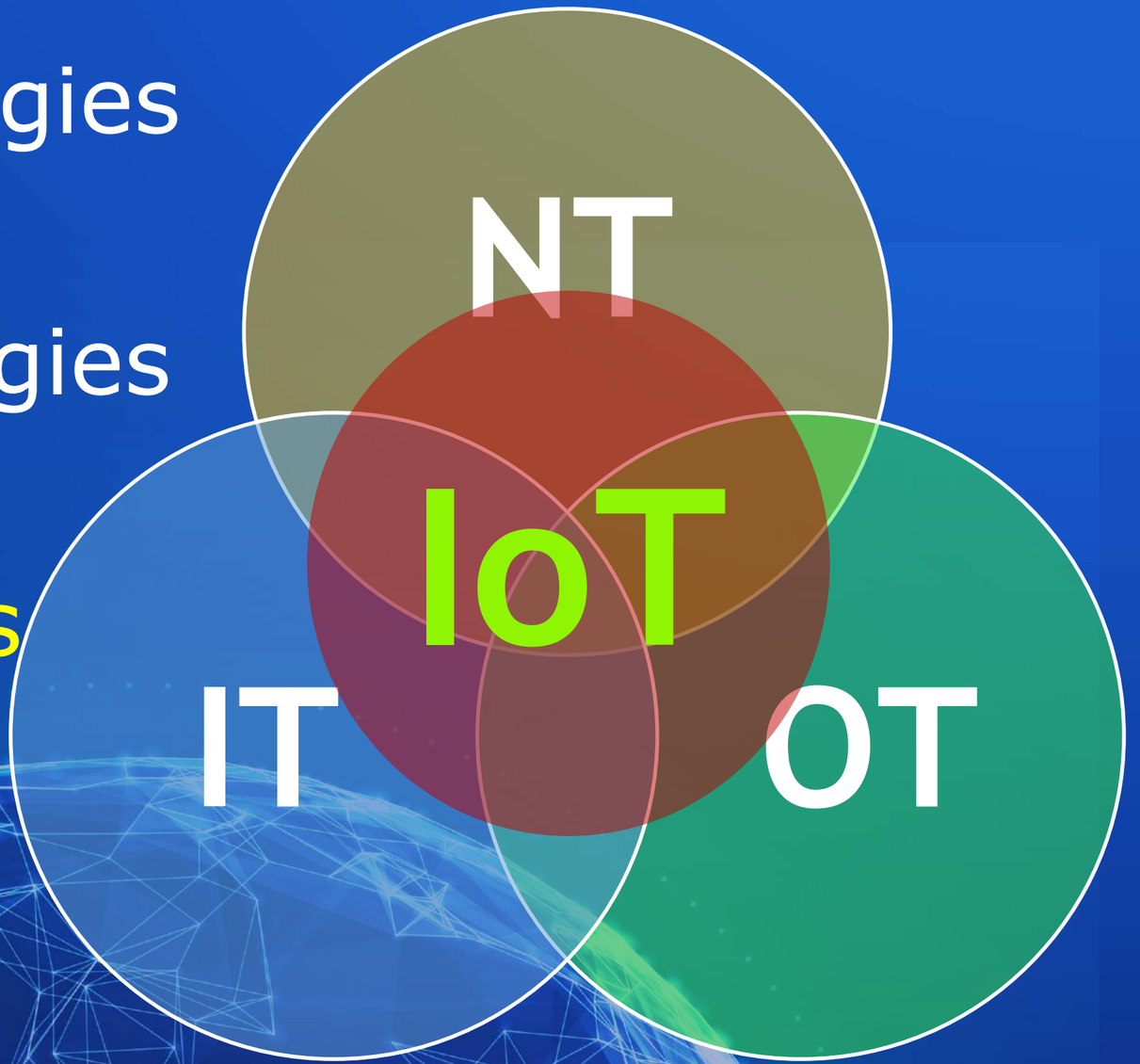
In digital transformation in any paradigm, domain or ecosystem --

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

Standards are the Chromosomes of Digital Infrastructure

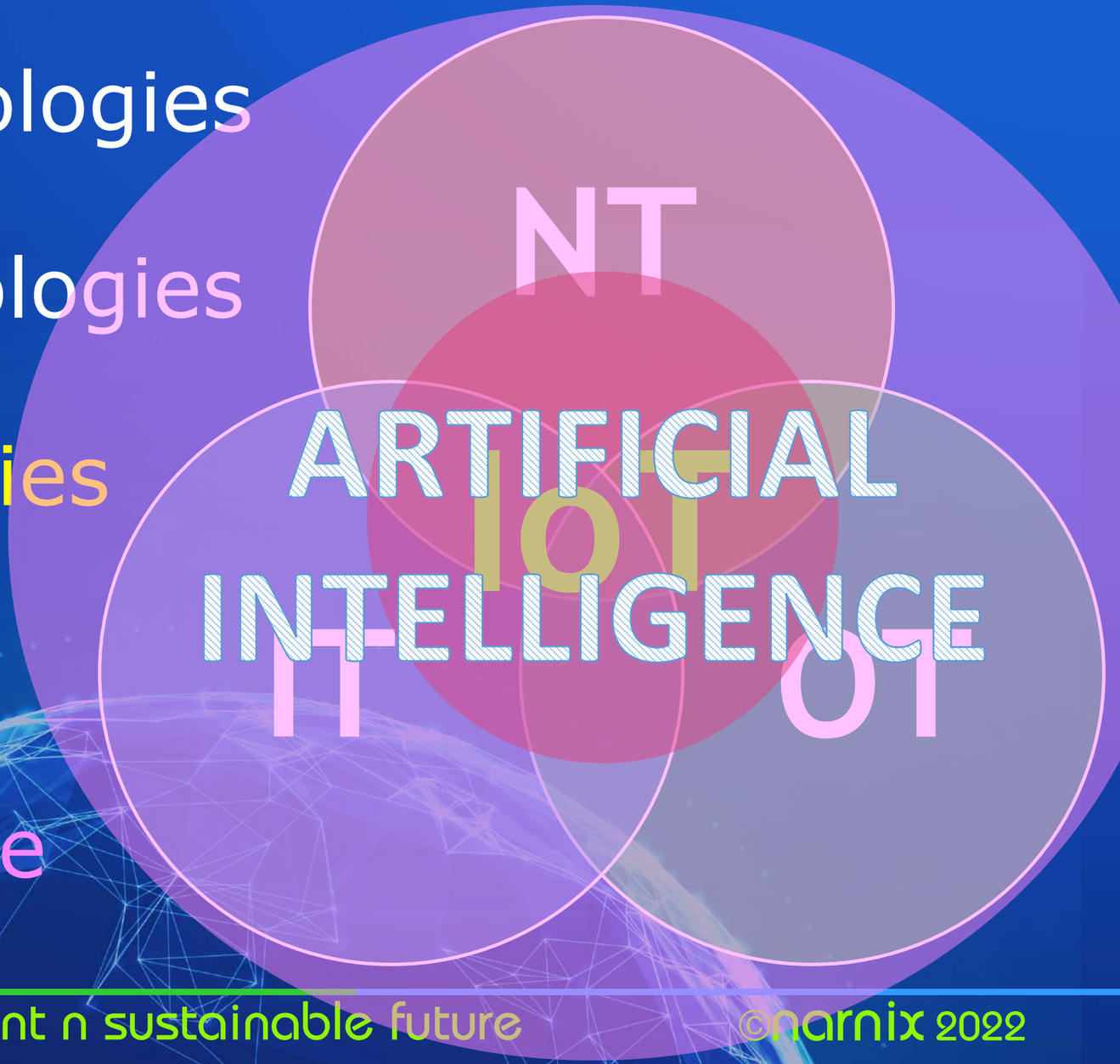
Digital Transformation Constituents

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



Digital Transformation Constituents

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



Digital Transformation

is NOT a technology

It's a

Complex Paradigm

with domain-specific implications

We are living in an ephemeral world

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

Business Impact of Tactical Approach

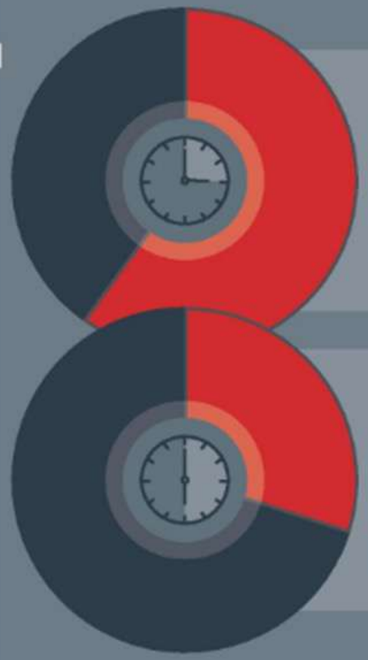
CYBER SKILLS SHORTAGE

Does your organisation have enough security personnel to keep you secure?

68%

NEED MORE STAFF

FALSE POSITIVES



60% SPEND 3+ HOURS DAILY

30% SPEND 6+ HOURS DAILY

UNUSED SECURITY SOLUTIONS

Have you purchased a security solution which was left unused?

39% WASTE THOUSANDS

ASSET MANAGEMENT

Are you fully aware of your organisation's web apps and endpoints?

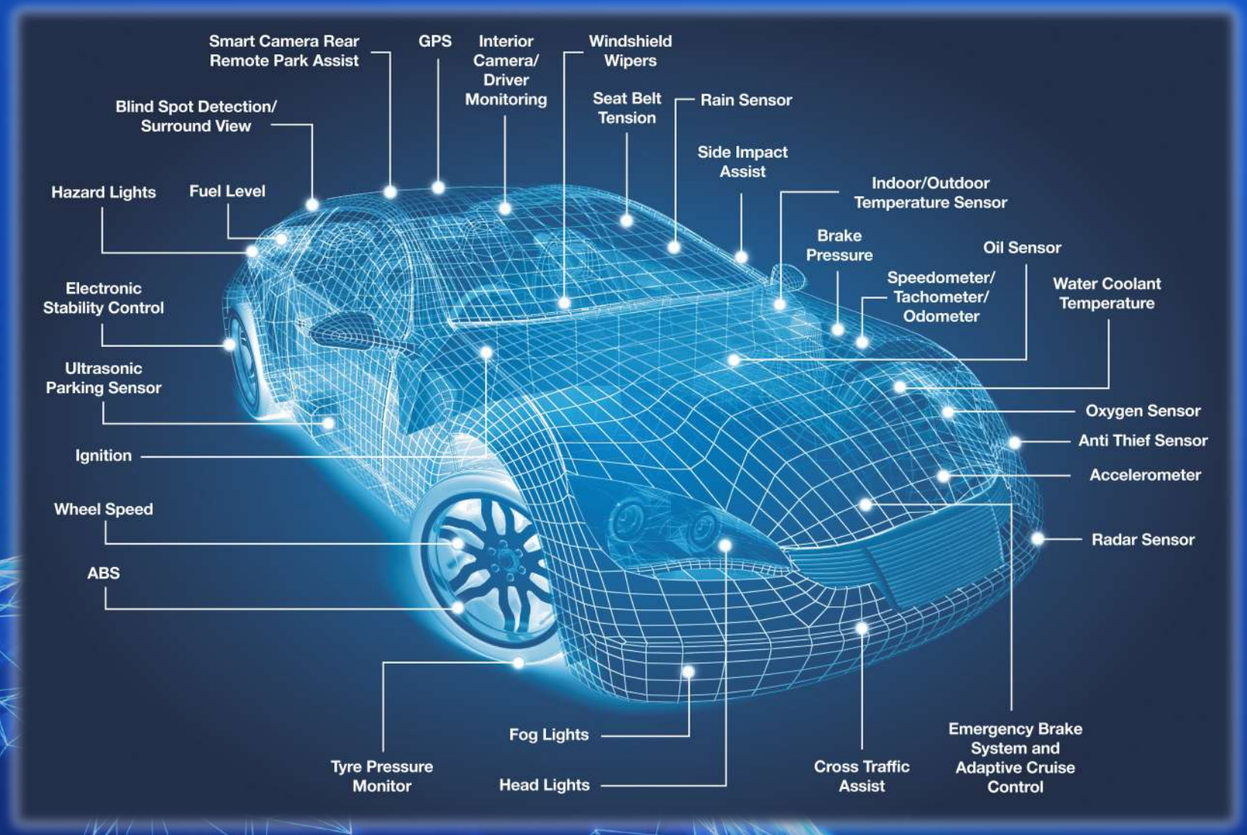
68% SAY THEIR VISIBILITY IS **'AVERAGE'**

Source: Edgescan Europe 2019 Security Survey Results

A Strategic Approach is Required

Tactical Risk Management

Strategic Risk Management



FIRST LINE OF DEFENSE IS THE EMPLOYEES THEMSELVES

Security Requirements for Utility Operation: Security Processes

Security Policy,
Security Assessment,
Security Deployment,
Security Training and
Security Audit (Monitoring).

7 Layers of Security

Information Security Policies. These policies are the foundation of the security and well-being of our resources:

- Physical Security;
- Secure Networks and Systems;
- Vulnerability Programs;
- Strong Access Control Measures;
- Protect and Backup Data;
- Monitor and Test Your Systems.

“IF YOU THINK TECHNOLOGY CAN SOLVE YOUR SECURITY PROBLEMS, THEN YOU DON'T UNDERSTAND THE PROBLEMS AND YOU DON'T UNDERSTAND THE TECHNOLOGY. ”

The Chain is as STRONG as the WEAKEST Link

"The current situation is very tricky. We do not have the facts to decide on actions. This paralysis puts our critical infrastructure at risk."

Experience confirms that when the entire organization shares a common way of thinking about vulnerabilities, security can be significantly enhanced.

"Step by step, we can make the cyber risk MIS our own. The whole process takes less than half a year, and yet the finished product really feels like something that was made for us, not like an off-the shelf solution."

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.

The speed of processing of AI systems is currently seen as providing protection for ICS and other networks that human operators may not be able to match, especially as cyber-attackers are employing increasingly sophisticated methodologies. AI can potentially respond to a cyberattack scenario far more quickly than a human decision maker.

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

Standardization Conundrum

- "Standards & even SDOs are not at the forefront of Critical Infrastructure Planners', Utilities' or Users' minds"
- There are misconceptions on what standards are for, and the case for use of standards has not been made.
- Liberalization and Markets have a lot of great virtues, but they cannot create their own conditions of existences: they must be designed!

SYMPHONY or CACOPHONY ? ? ?

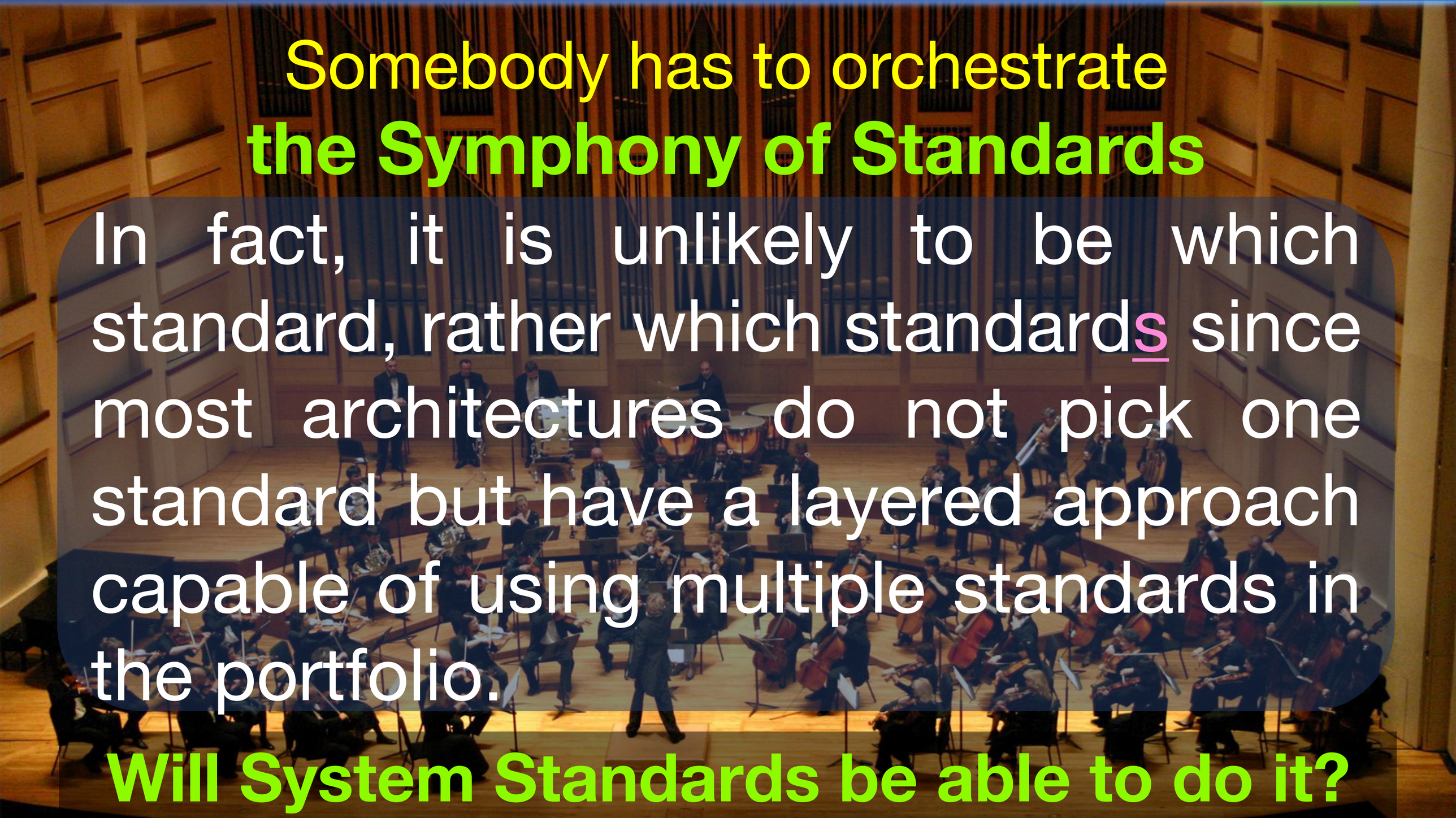
"The beauty of standards is that there are so many to choose from!"

Andrew S. Tanenbaum, 1990

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?

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.

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.

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.

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

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 Electricity Utilities 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 an absolutely 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.

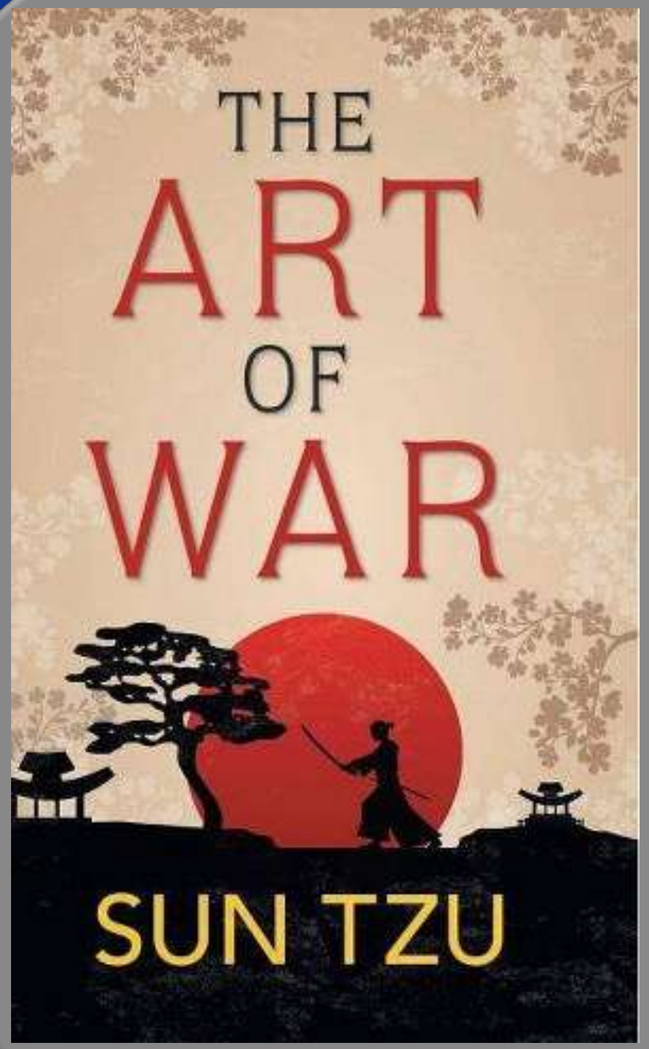
Cyber Immunity & Cyber Resilience

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 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.

These systems will be designed to make the right decisions with the context-based data, pre-empt attacks on the basis of 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.

Key Takeaways

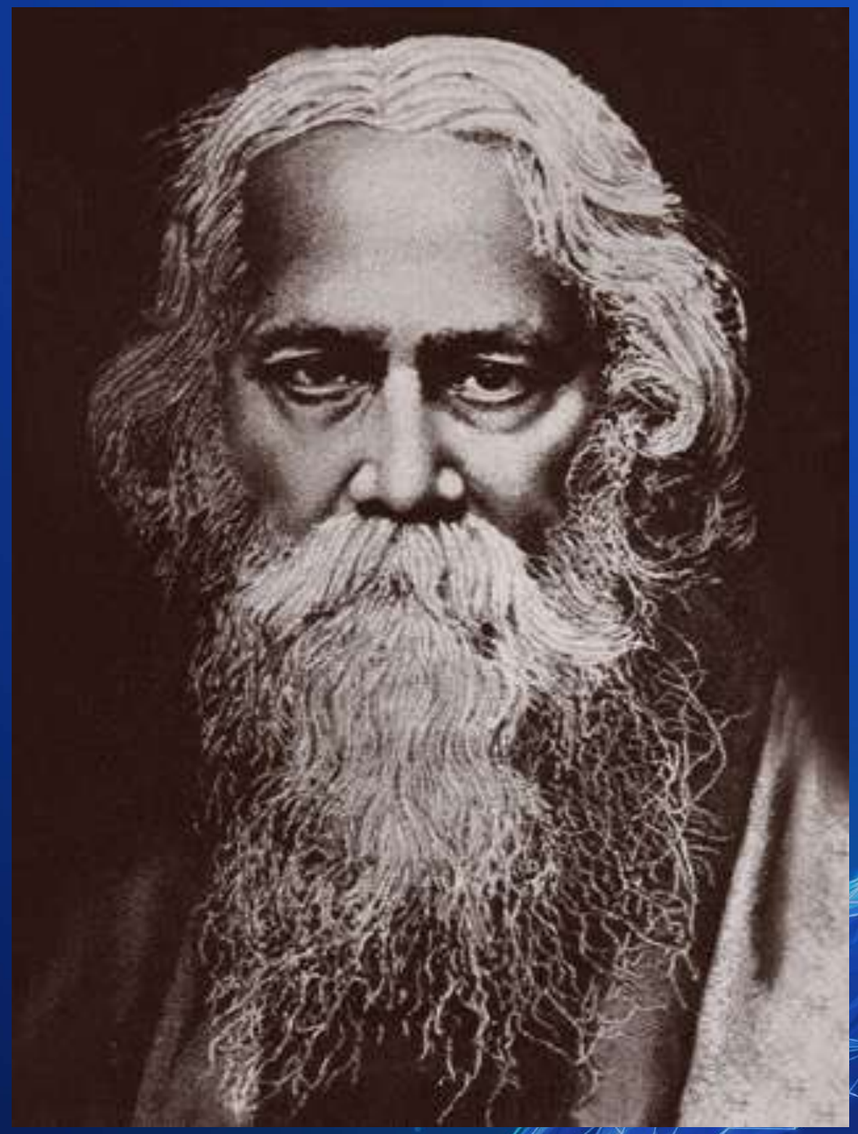
Need to develop a Comprehensive approach to

- Sustainability
- Security & Resilience
- Leveraging Disruptive Technologies
- Ethically Aligned Designs

And adopt Systems approach to Design complex Systems, Solutions & STANDARDS…

In Conclusion…

Resilience....



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

RACE TO ZERO

RACE TO RESILIENCE

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

Credentials…

narang n. kishor
Mentor &
Principal Design
Architect

Technology Philanthropist,

Innovation, Standardization & Sustainability Evangelist…

Technology Advisor, Mentor, Design Strategist &Architect in Electrical, Electronics & ICT…

- Over 40 years of professional experience in education, research, design and consulting .
- Over 30 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, Energy, Environment, Defense & Aerospace.
- Over 10 years of Consultancy & Advisory Experience to different segments of business & industry.
- Over 250 Research & Design Mentees in the Electronics, ICT & STI Ecosystems.
- Leading & contributing to multiple National & Global Standardization Initiatives at BIS, Niti Ayog, TSDSI, IEC, ISO, ITU, IEEE etc.…
- 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.

Credentials…

Pro-actively contributing in:

- Smart Cities Reference Architecture (IEC & ISO)
- Unified & Secure Digital Infrastructure R A (BIS)
- Unified & Secure Last Mile Communication Protocol Stack Reference Architecture (BIS)
- Trustworthiness Reference Architecture (ISO/IEC/JTC1).
- Smart Grid Reference Architecture & Cyber Security Reference Architecture for Smart Grid (IEEMA)
- IEEE Future Networks Initiative
- IEEE Smart Cities Initiative
- ITU-T Focus Group on Technologies for NETWORK 2030
- ITU-T Focus Group on Autonomous Networks
- IEEE 802.xx.x
- 5G Application Layer Standards