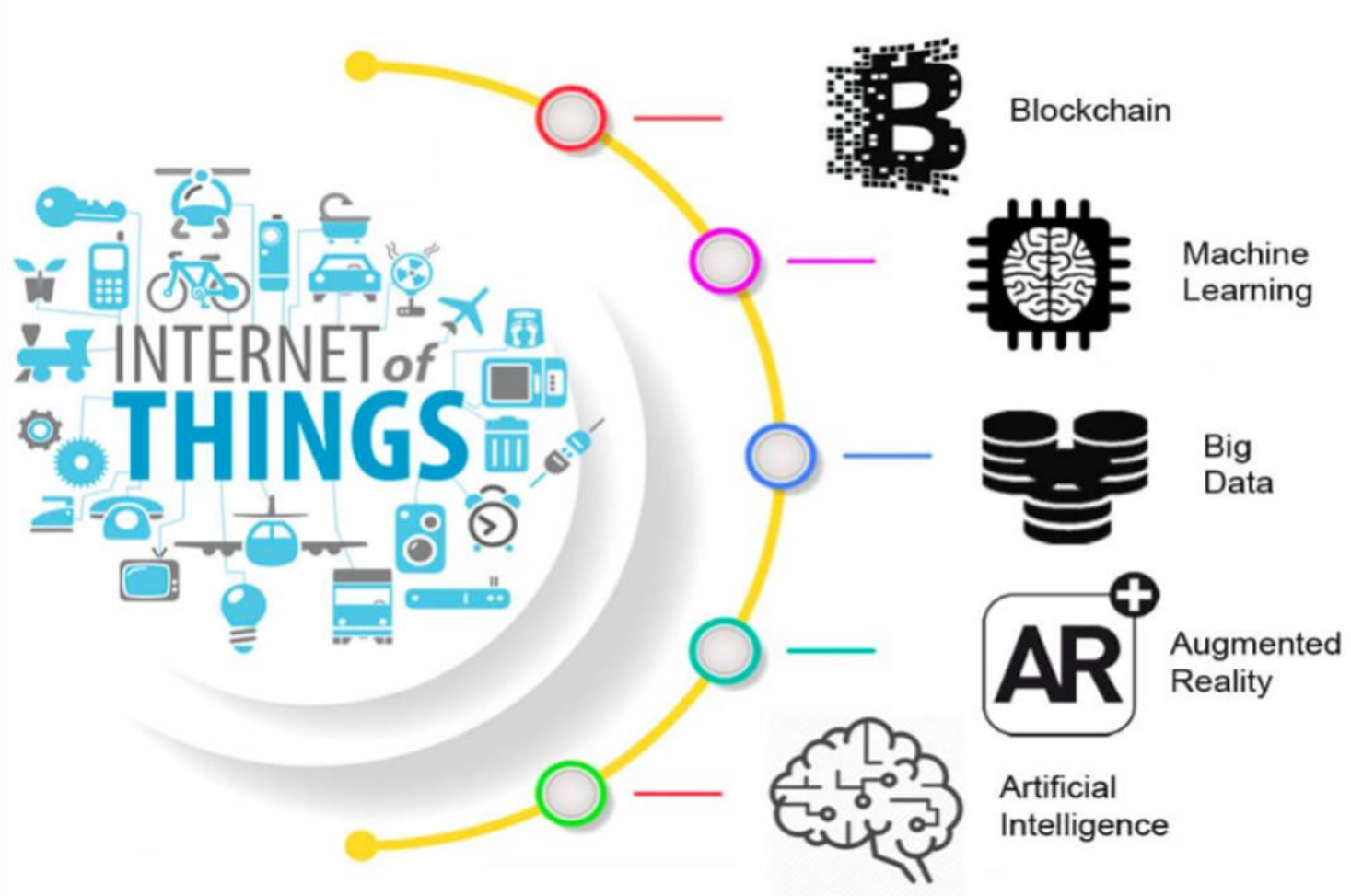
TIPPSS for the Next Generation of PKI and its Applications

Rajesh Murthy, GapAsk

Michael Shea, Aeolian Group

IEEE \UL 2933 Working Group

Advanced technologies enable digital transformation … and can increase RISK



Signals of a Risky Digital Future

- Since 2017, Pacemakers, insulin pumps, and implantable defibrillators found with critical vulnerabilities, sometimes allowing attackers to **change** device settings remotely.
- HVAC controllers in hospitals, infusion pumps, and medication dispensing systems **exploited** to disrupt patient care or access sensitive data.
- In 2024–25, over **162 unique vulnerabilities** have been cataloged in medical devices, including DICOM imaging systems, patient monitors, and information systems—many not patchable and widely exposed.
- Almost **22%** of healthcare organizations have had medical devices compromised, often leading to service downtime, manual backups, and patient transfers for safety.

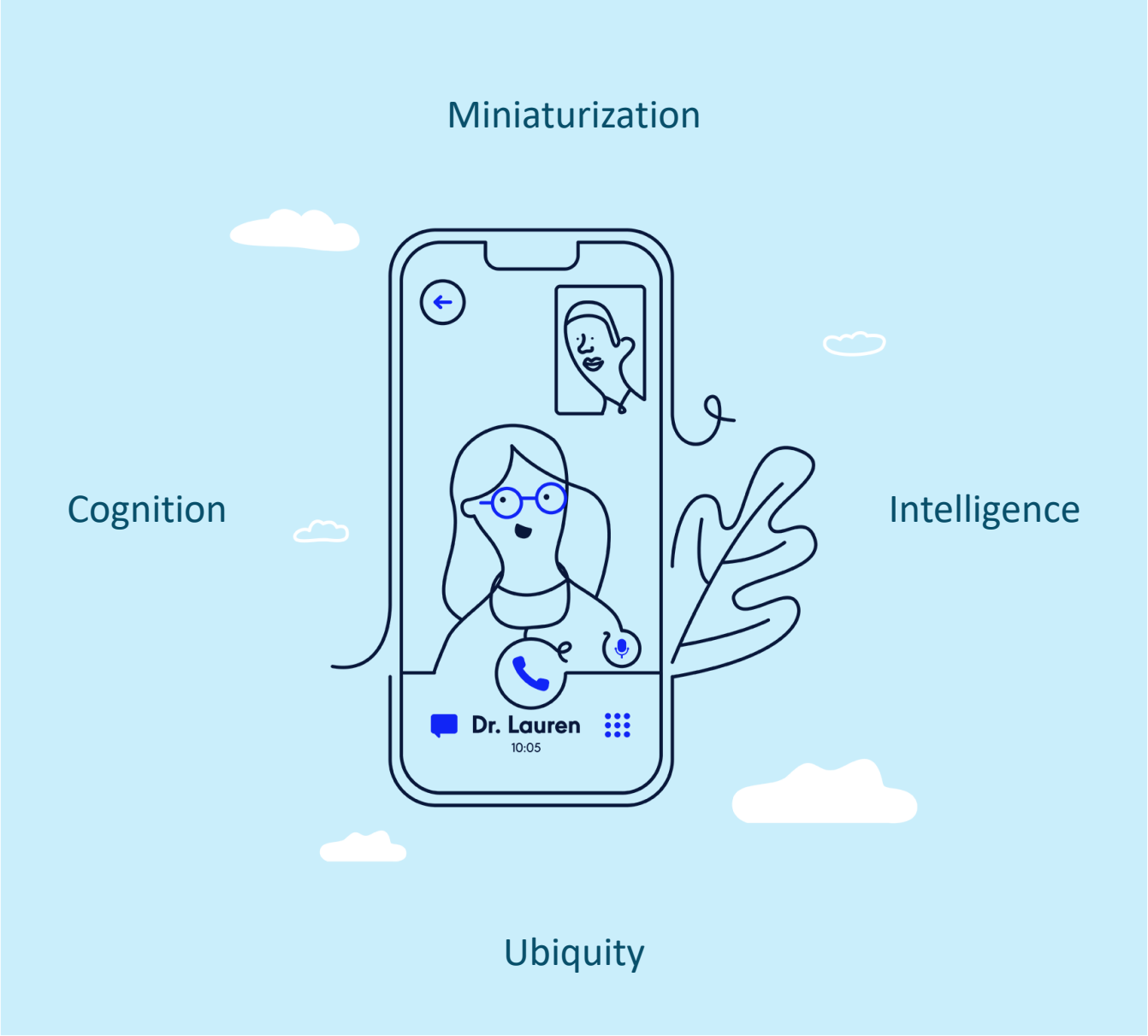
Countries Most Impacted

2025: Hitting Closer to Home

- Coinbase Breach (May 2025)
  - Improperly managed digital identities and privileged access granted to overseas contractors, affecting nearly 70,000 users
- SharePoint Zero-Day (July 2025):
  - A critical zero-day vulnerability (CVE-2025-53770) in Microsoft SharePoint Server was exploited in a large-scale campaign, with attackers bypassing key protection and trust controls

https://www.cisa.gov/known-exploited-vulnerabilities-catalog
https://www.mcafee.com/blogs/tips-tricks/how-to-protect-your-crypto-after-the-coinbase-breach/
https://canadiancybersecuritynetwork.com/hubfs/CS-Report-CCN-2025-All-v10.pdf

Rise of Digital Spaces



TIPPSS – Security from Human-Centric Lens

Trust

Ensuring reliable, authentic interactions between systems and stakeholders

Identity

Verified Authentication and Authorization across the ecosystem

Privacy

Securing sensitive data and respecting subject confidentiality

Protection

Safeguarding integrity of systems and data throughout its lifecycle

Safety

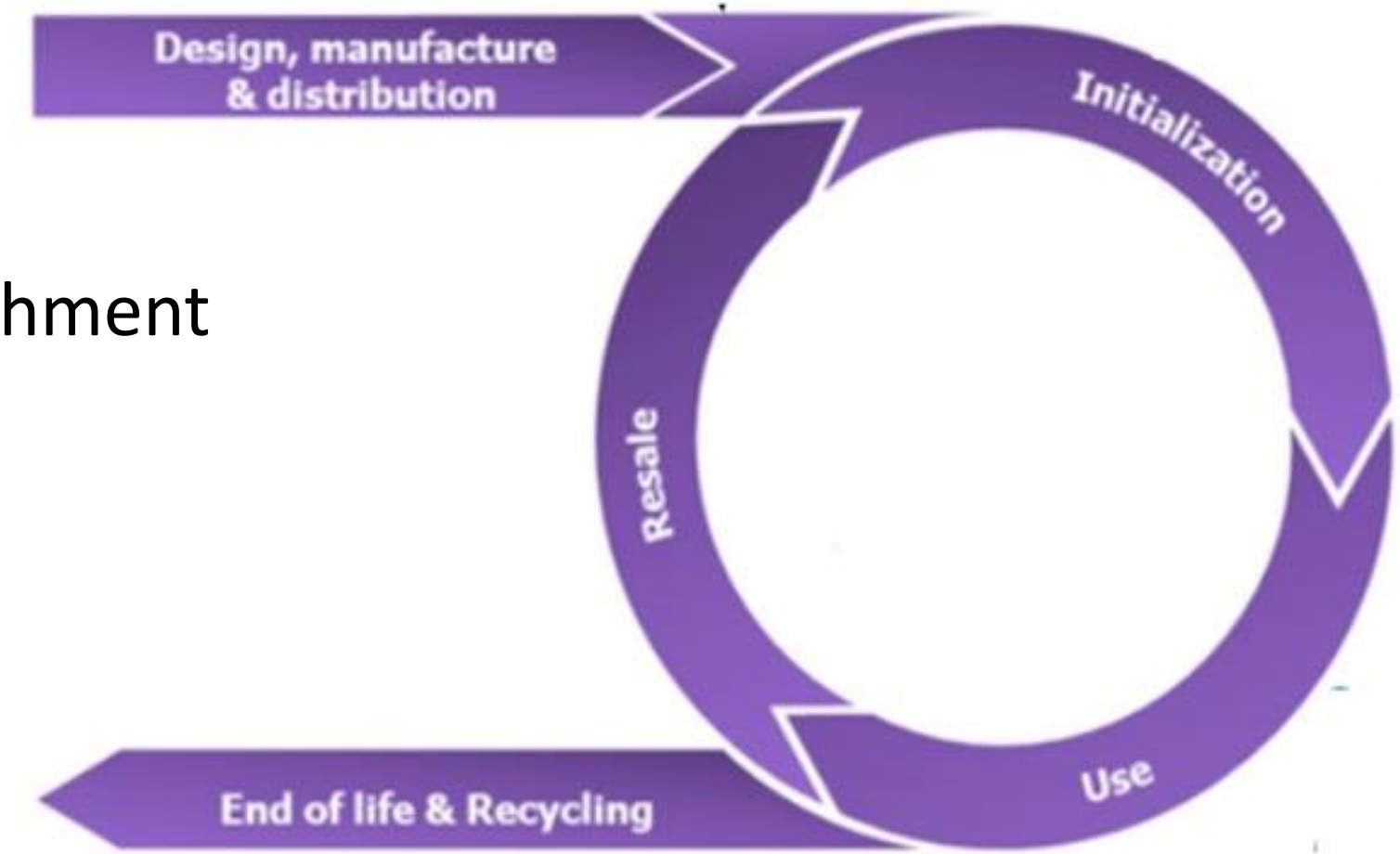
Preventing harm to people and property while maintaining operational validity

Security

Assuring robust technical controls against threats

Life Cycle (Simplified)

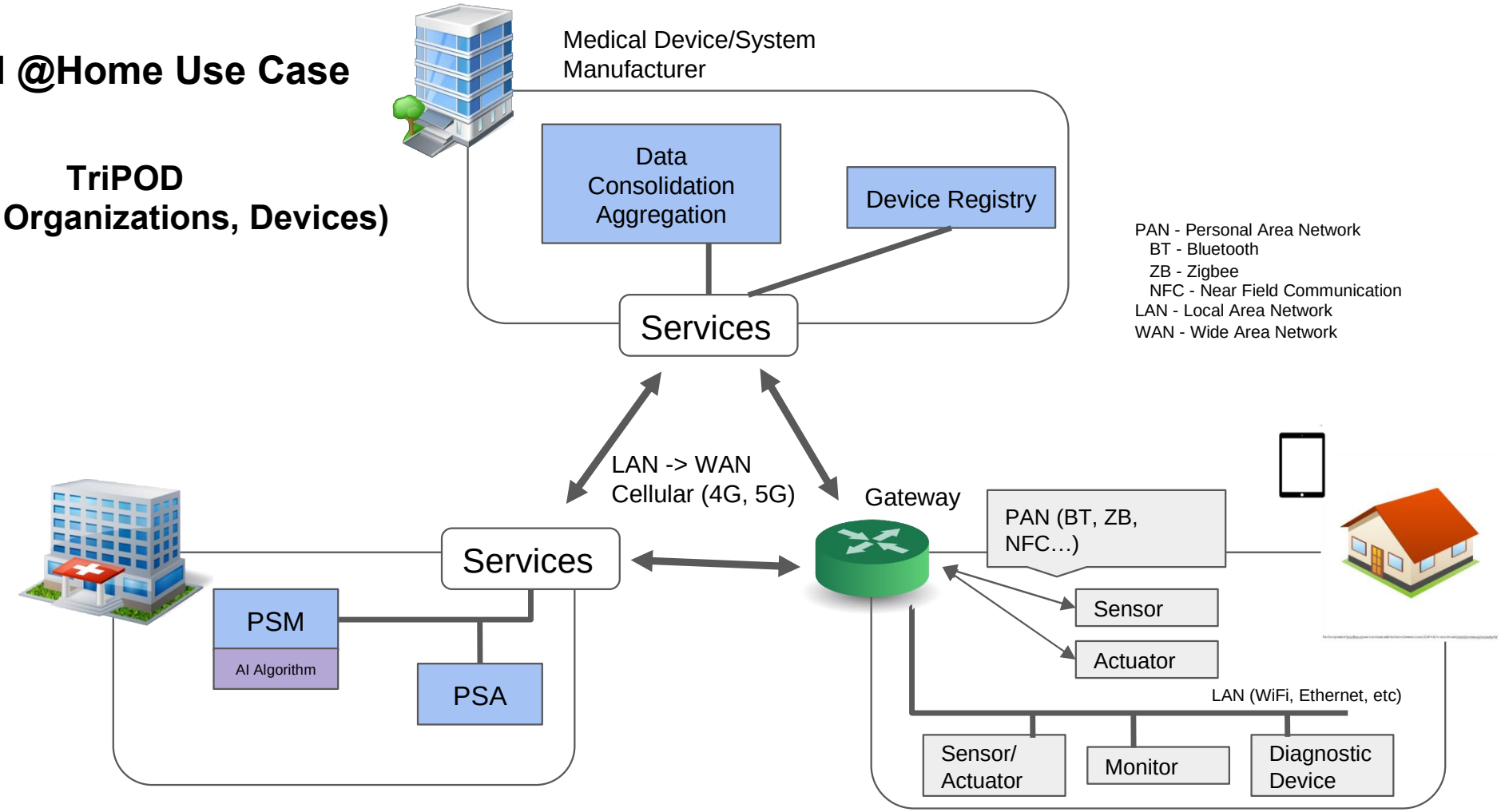
- Resale/Refurbishment
- Recycling
- End of Life



Sample content: IEEE 2933-2024 : Trust & identity interactions of people, organizations, and devices in the CIoT Hospital @Home use case

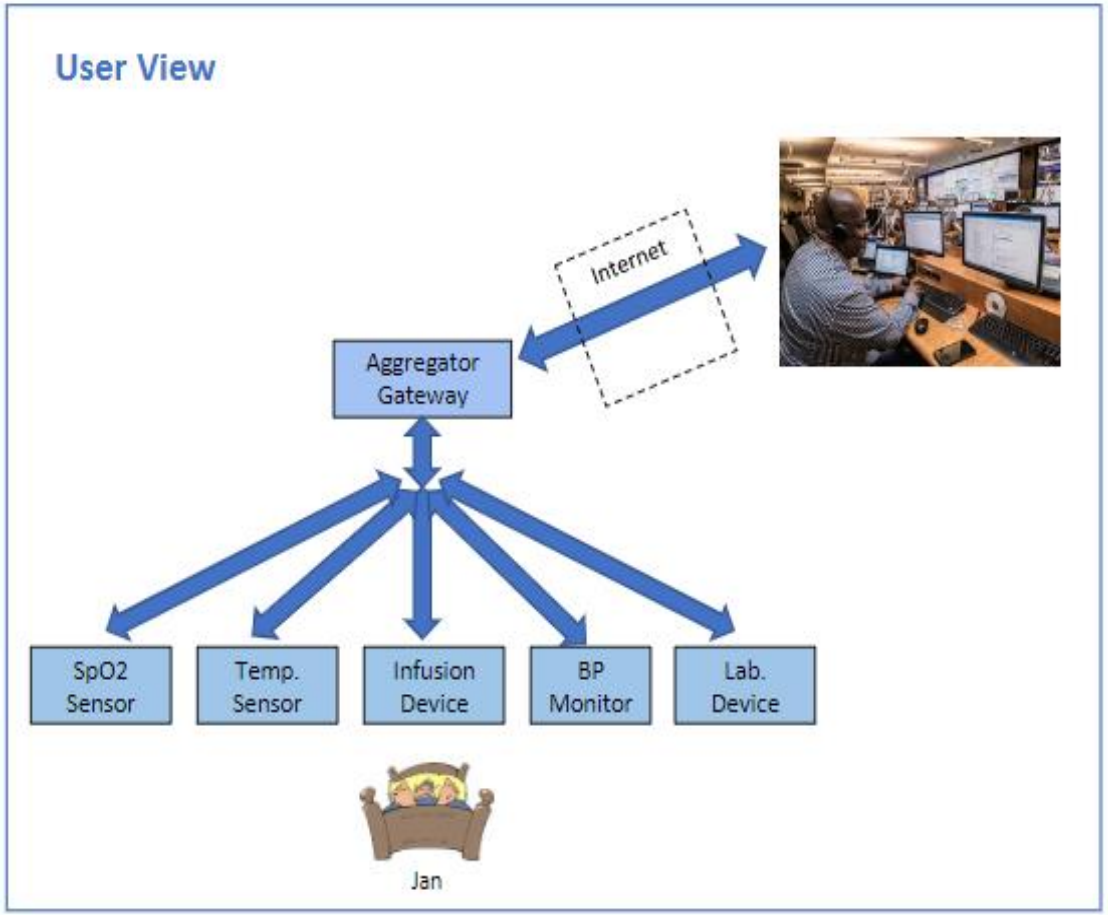
Hospital @Home Use Case

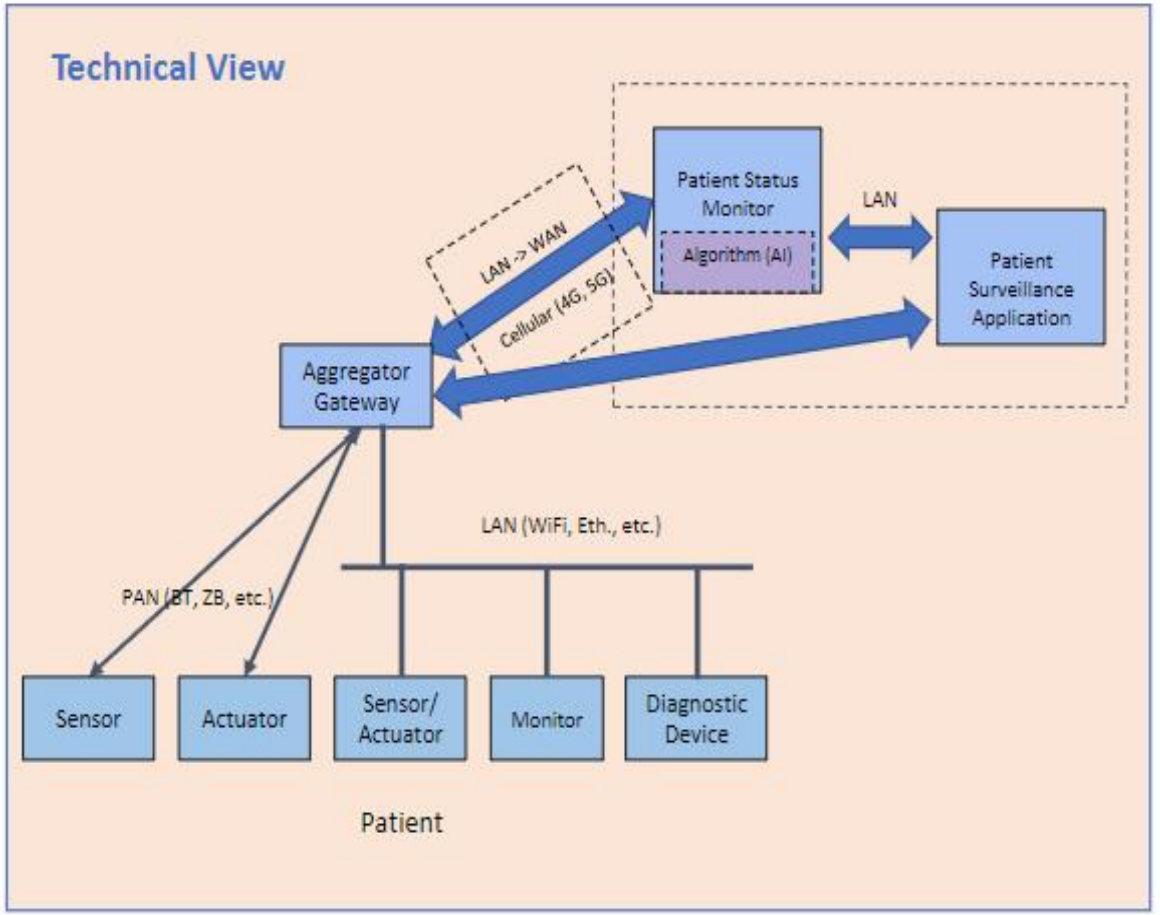
TriPOD
(People, Organizations, Devices)



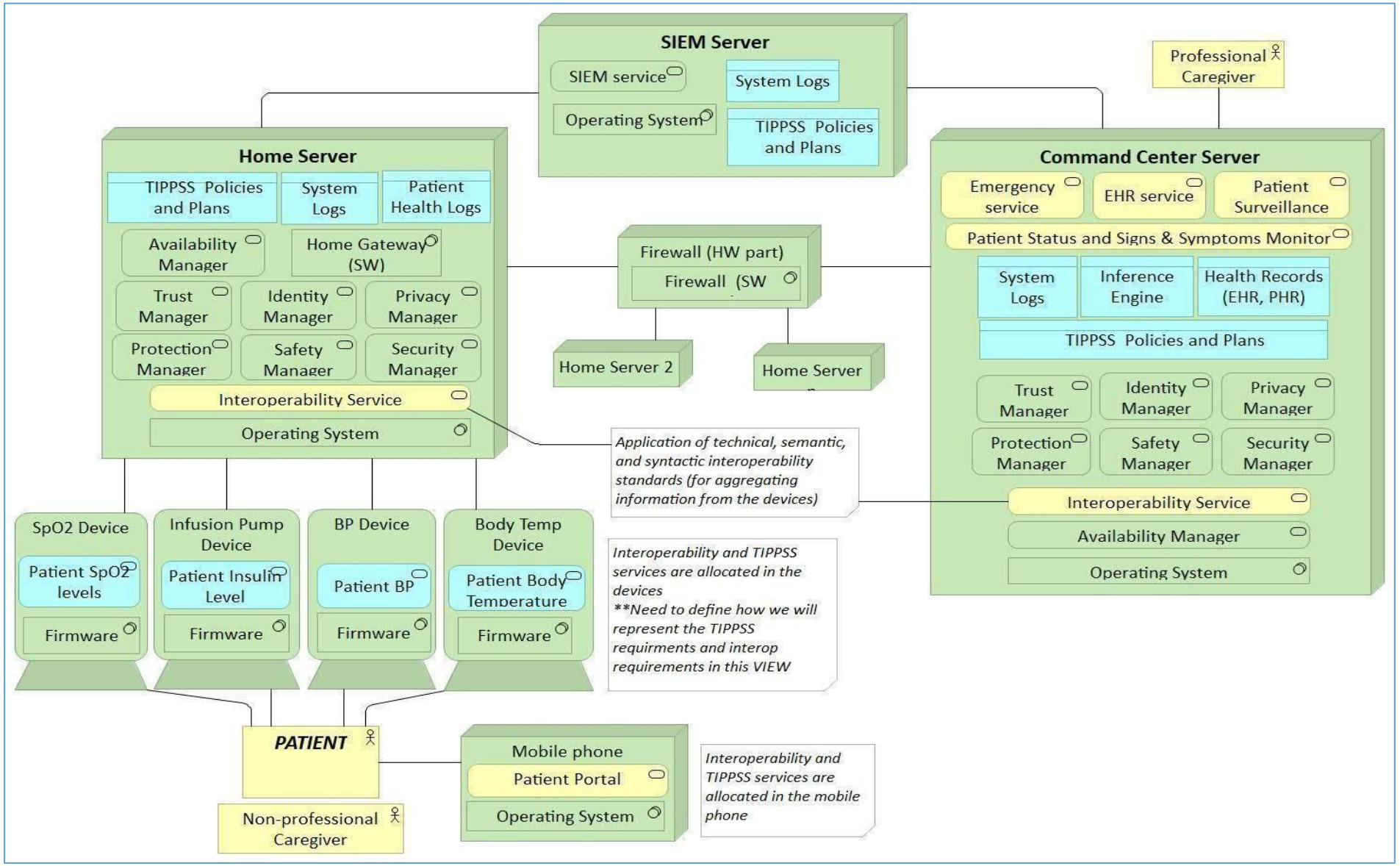
PSM - Patient Status Monitor
PSA - Patient Surveillance Application

Sample Use Case: Hospital @Home

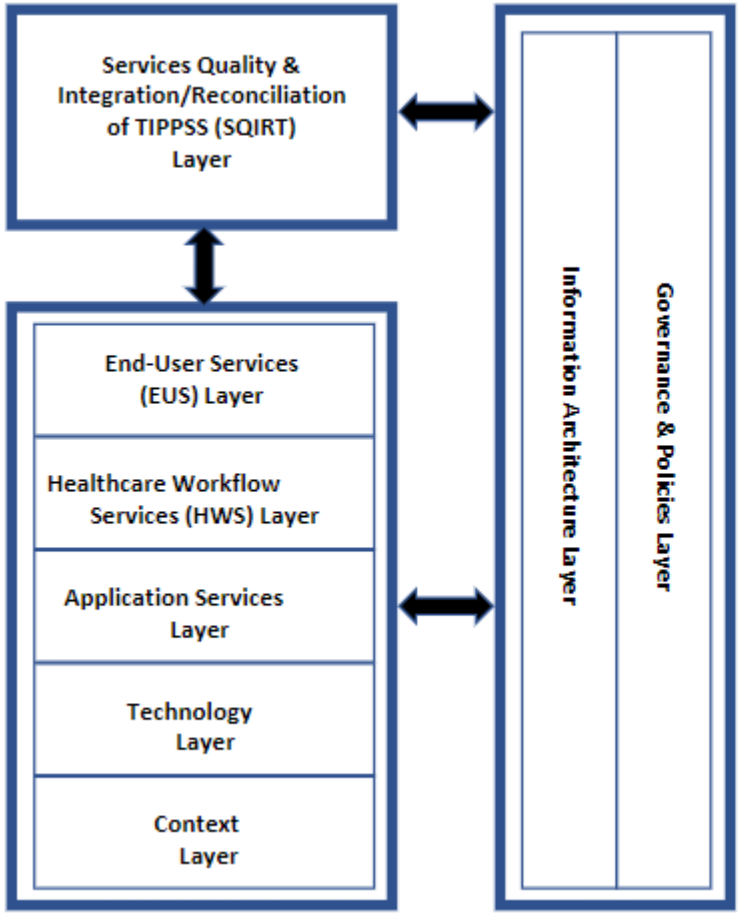




Deployment View of TIPPSS Architecture for Hospital @Home



IEEE/UL P2933 Clinical IoT Example Reference Architecture

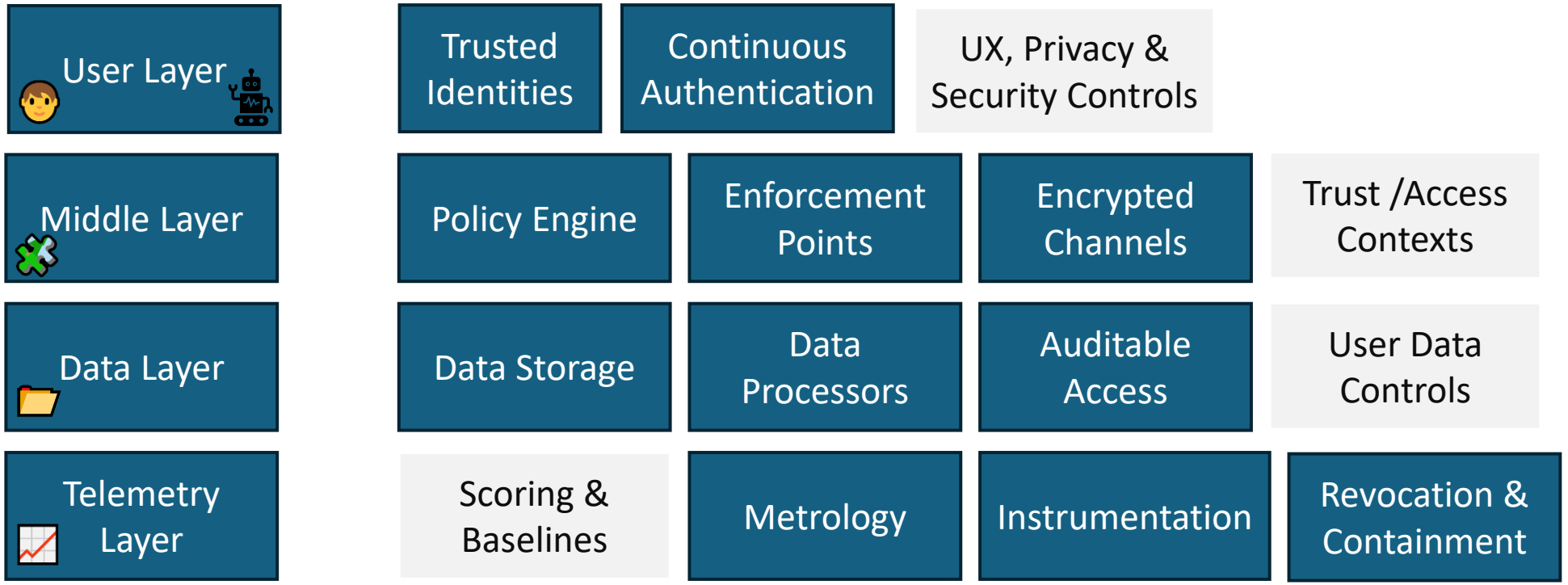


- Context – system environment
- Technology – the physical and virtual devices
- Application Services – supports the HWS and EUS
- HWS – captures and communicates patient information
- EUS – services to end-users
- SQIRT – routes the data and monitors quality
- IA – guides all data operations and interoperability
- Governance – includes standards, policies, guidelines, etc.

Digital Trust in TIPPSS Framework

TIPPSS Framework	Digital Trust Angle	Enabling PKI & Applications
Trust	Verifiable Sources, Integrity	Certificates, Registrars, Signing
Identity	Resource Access: Who /What /When /How	Digital Certs, IID, DID, FID
Privacy	User /Usage /Data Controls	Encryption, Consent
Protection	Robustness Against Misuse, Tampering	Signed Code, Revocation
Safety	UX, User Controls, Resilience	Not PKI Specific
Security	Technical Safeguards	PKI-Based Authentication, Cryptography

TIPPSS & PKI: An Hackathon Perspective



TIPPSS & PKI In Action: Domains

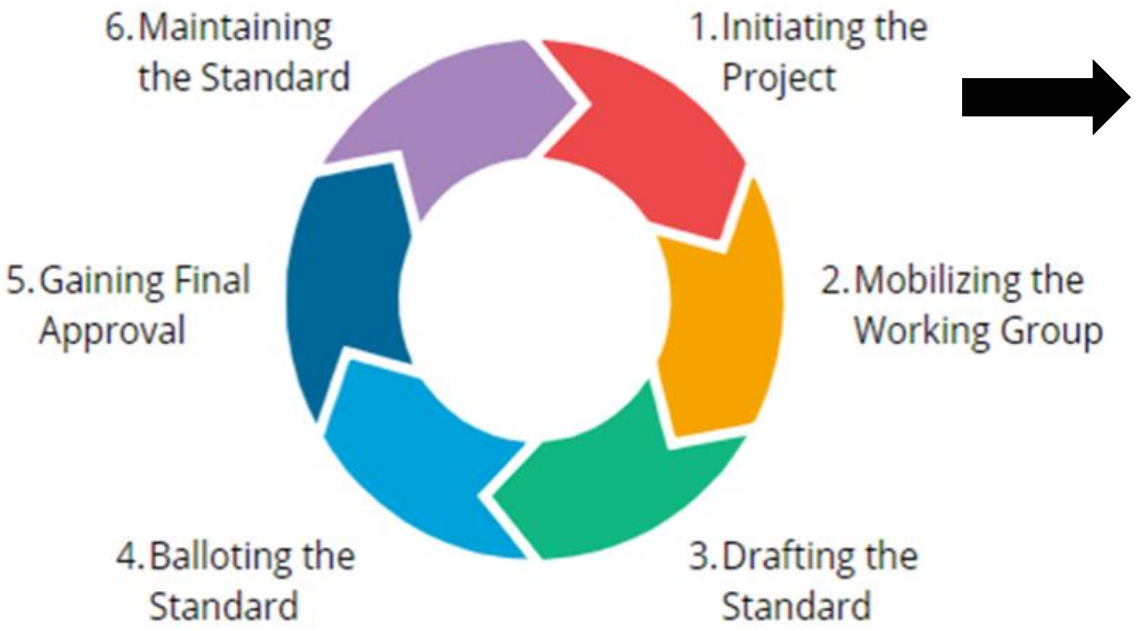
Cybersecurity
- Certificate Based User Authentication
- Signed Software and Container Images
- Integrity-protected Logs

IIoT /IoMT
- Device Onboarding with certificates
- Encrypted Telemetry
- Certificate Revocation in Mesh Networks

Automotive
- Secure OTA Updates (signed by PKI)
- Vehicle-to-Everything (V2X) Trust
- Driver Identity and Privacy Controls

Extending the IEEE 2933 TIPPSS Standard to all Cyber-physical Systems

IEEE 2933-2024 Approved June 2024



TIPPSS Roadmap Task Group Launched to create new standards opportunities:

- *Clinical IoT subdomain Study Groups being formed:*
  - *Remote Subject Monitoring with TIPPSS*
  - *AI-Based Coaching for Healthcare with TIPPSS*
- *Plans to extend TIPPSS to more industry domains:*
  - *Distributed Energy Resources / Smart Grid*
  - *Precision Agriculture*
  - *Connected Vehicles*
  - *Smart Cities…*

View IEEE TIPPSS webinars and register for new ones here: *https://engagestandards.ieee.org/gchc-virtual-workshops-register.html*

Join the TIPPSS Roadmap Task Group – email florence.hudson@columbia.edu

TIPPSS Resources

- IEEE/UL 2933-2024: IEEE/UL Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS--Trust, Identity, Privacy, Protection, Safety, and Security

  https://standards.ieee.org/ieee/2933/7592/

- Trust, Identity, Privacy, Protection, Safety, and Security (TIPPSS)

  https://nebigdatahub.org/tippss/

Thank you!

Michael Shea (michael.shea@thedinglegroup.com)

Rajesh Murthy (rkrish@ieee.org)