
GSC
22
MONTREUX, SWITZERLAND
IEC
ISO

Smart Cities – Big Data

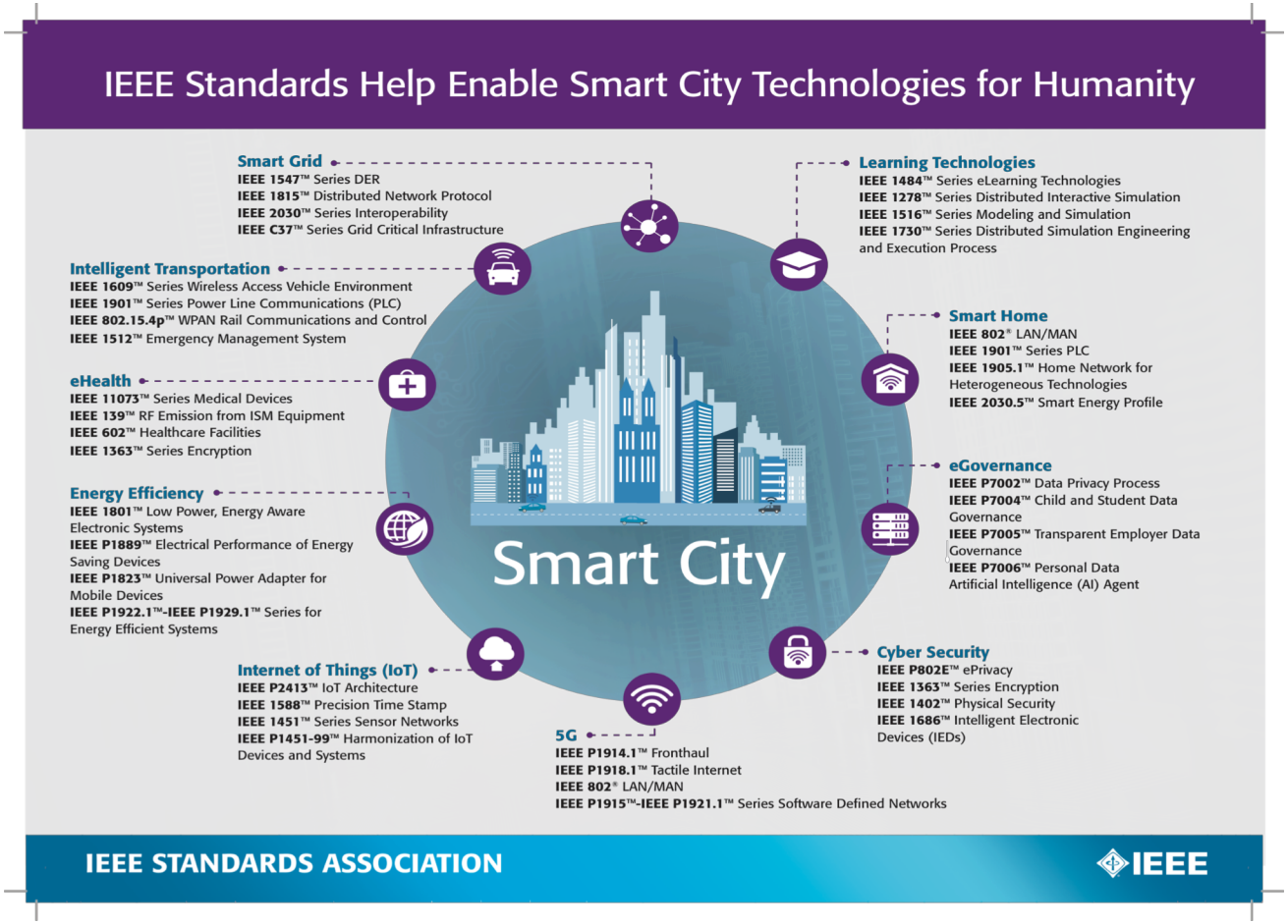
IEEE Initiatives enabling smart and secure data management

March 26-27, 2019, GSC22 – Montreaux, Switzerland

Overview

- IEEE Initiatives in Smart Cities
- Smart Cities Standards programs…and Digital Citizen
- IEEE Standards Association “Data Initiatives”
  - Big Data & Metadata Management
  - DIITA – Digital Inclusion, Identity, Trust & Agency
  - Children in Digital Environments
  - Security in an All-Connected environment

IEEE Standards Impact Smart City Technology



Digital Citizen, Internet of Things

Ubiquitous Connectivity

Mobile Communication Device
Wearable Electronics
Medical Devices

Integrated Horizontal and Vertical Technologies

IEEE-SA has a strong presence in the complete lifecycle of standards development – Industry Connections, Standards Development & Conformity Assessment

Vertical Focused Standards

- Smart Grid
- Transportation
- Digital Health
- Infrastructure Management
- Industrial Automation/Smart Factory
- Smart Homes

Horizontal Platforms

- IEEE 802 (wired/wireless) protocols
- **IEEE 5G** Standardisation
- IEEE IoT Standardisation
- Augmented Reality
- Cybersecurity
- Blockchain
- Ethics
- …

IEEE Standards on Smart Cities

Seamless Connectivity - New 802 Initiative: High Efficiency WLAN (HEW)

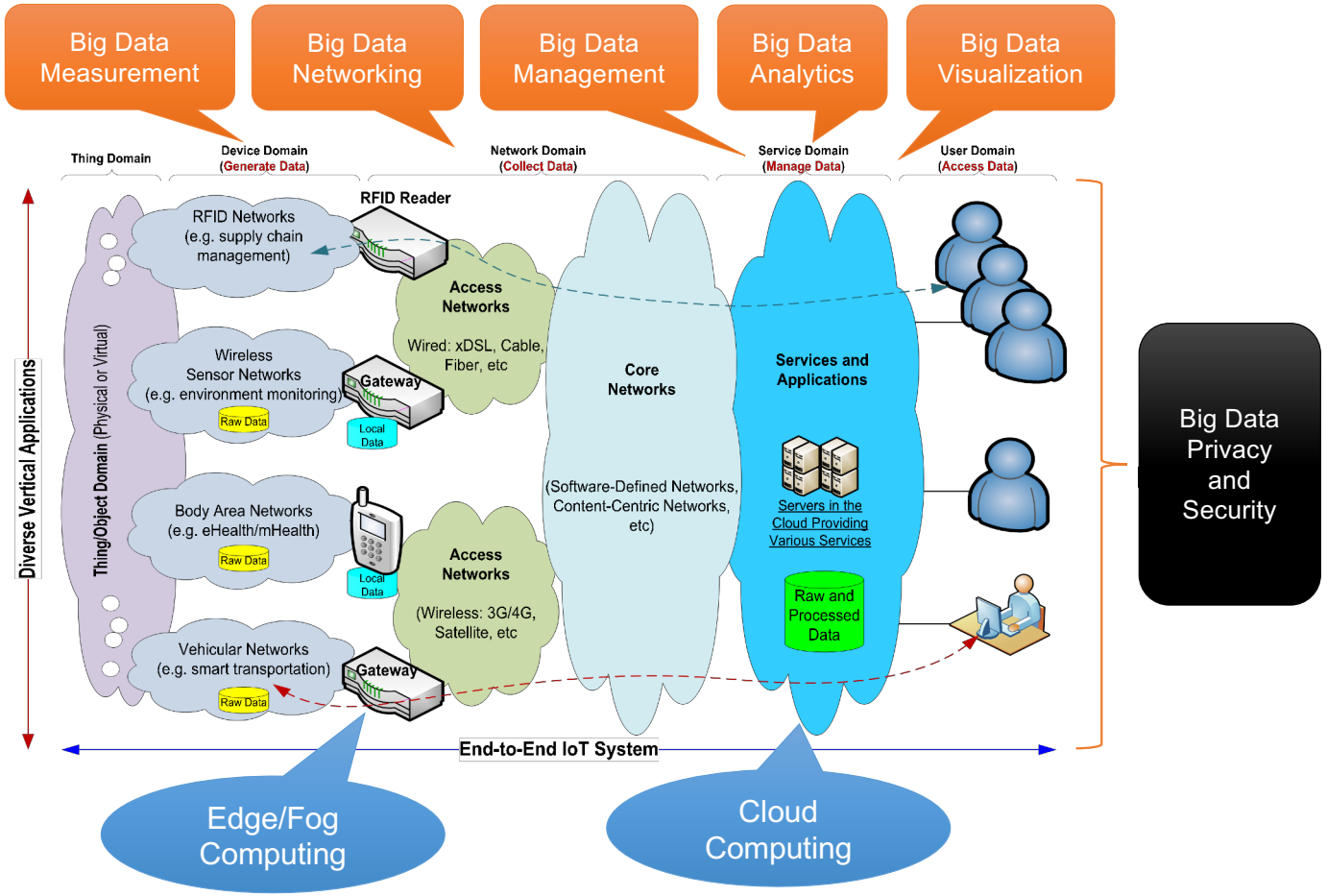
Point-of-Sight in Stadium

Location Services

Enhanced Video

Consumer Wearable

Background (End-to-End IoT & Big Data)



Big Data Governance & Metadata Management

- An IEEE-SA Industry Connections Activity created out of the IEEE Big Data Initiative; chaired by NIST
- **Goal:** Enable data integration/mashup among heterogeneous datasets from diversified domain repositories and make data discoverable, accessible, and usable through a machine readable and actionable standard data infrastructure
- **Deliverables**:
  1. Hackathons and workshops at related conferences to collect, analyze, and identify relevant use cases, requirements, and potential solutions.
  2. White paper(s) framing the problems and identifying the issues in more detail based on findings at the workshops & hackathons.
     - Big Data Governance and Metadata Management Standards Roadmap in progress
  3. Reference architecture(s) concepts and solutions from relevant best practices in big data metadata management to formulate data interoperable infrastructure to enable data integration/mashup between diversified domain repositories.
  4. Proposals for new IEEE standards activities (including recommended practices, guides) related to big data metadata management

Digital Inclusion, Identity, Trust, and Agency

Scope

Many areas of human activity in the 21st Century take place within cyberspace. Those excluded from cyberspace are thereby excluded from a key domain of human endeavor. Exclusion may arise from many causes, including affordability, availability, discrimination, and concern for safety. The scope of the “Digital Inclusion Identity, Trust, and Agency” (DIITA) Industry Connections Program considers causes of exclusion which can be addressed by advancing technology for humanity through standardization.

- Identity: We are known as we wish to be known
- Trust: We are safe in our on-line engagement
- Agency: We have control over our data and our activities

Initiative Goals

- Identifying barriers to digital inclusion and incubating activities to address those barriers.
- Engaging the broader community in the domains of digital identity, trust, and agency.
- Initiating families of standards, including data governance models and frameworks.
- Exploring the technical solutions for the concept of contextual sufficiency (the minimum data needed for a specific purpose) in relation to digital identity
- Developing a collaborative approach to standards design regarding health and other personalized data and its privacy implications across demographics.
- Partnering with other initiatives within IEEE with common areas of interest, focus and applications

Experts from around the world are driving specific work streams relating to these goals.

DIITA Workstreams

Current work streams:

- Internet Affordability & Accessibility
- Privacy by Design Whitepaper
- Dignity and Agency in Identity
- Privacy and Respect in Virtual and Social Gaming
- Governance in Identity

Work streams initiated under DIITA and transitioned

- Personalized Medicine & AI
- Portability of Readible Format of End-User Data
- Decentralized Identity for Health
- Certification of Ethical Framework for Agency on Blockchain

Children in Digital Environments: Universal Standards for Children

- 5Rights Foundation works towards a digital environment that meets and respects the rights of children & adolescence, and has identified standardization gaps
- The “Universal Standards for Children” standards family to be developed in IEEE to address these challenges:
  1. Kids-First Impact Assessment in Digital Environment
  2. Privacy Settings - Measurements
  3. I’m a Kid - Child Data Governance
- First standards project to be initiated in May 2019: **Universal Standards for Children - Kids-First Impact Assessment in Digital Environment**
- Outreach commenced to potential participants. Interdisciplinary stakeholders include, child development experts, online protection experts, lawyers, industry, technologists, NGOs, campaigners, academics, and policy makers

Soon, the Internet of Things Will Expand the Security Need to Almost Everything We Do

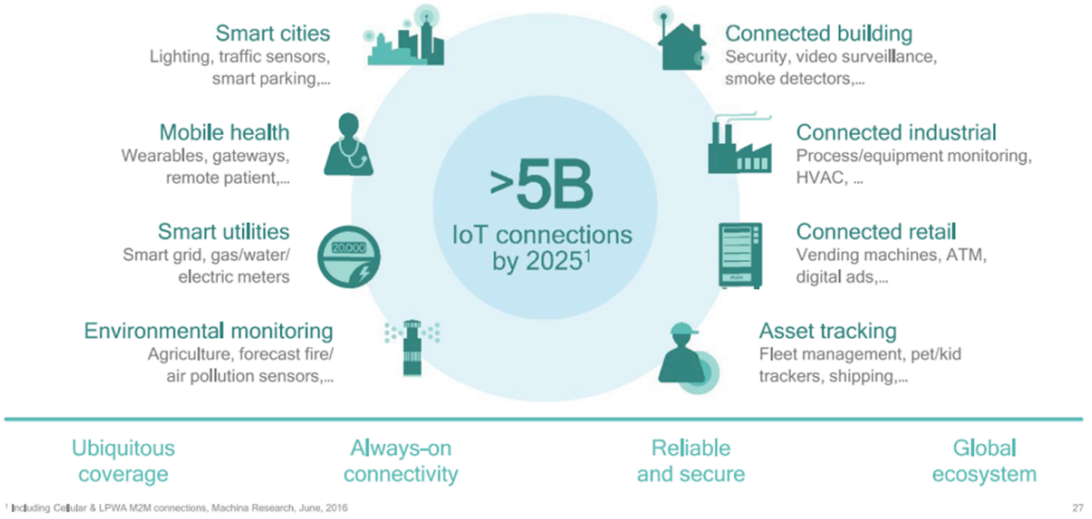
Beckstrom's* Laws of Cyber Security

1. Everything that is connected to the Internet can be hacked
2. Everything is being connected to the Internet
3. Everything else follows from the first two laws

*Rod Beckstrom, CEO and President of ICANN, former Director of the National Cyber Security Center

Source: "Secure Connections for Smart Cars," Kurt Sievers NXP March2014

Sensor & Wireless Technologies: “Always Connected” World

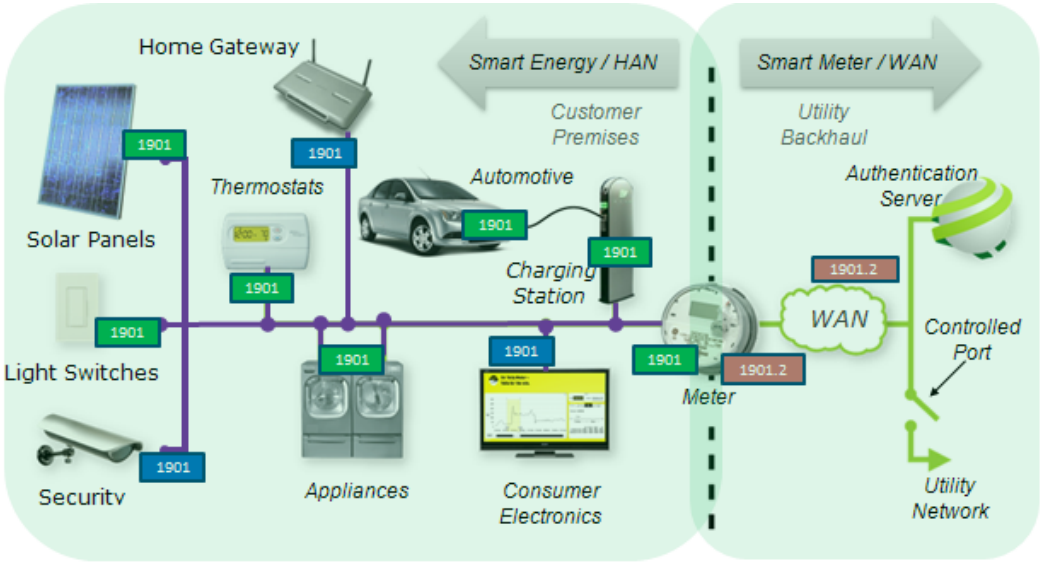


SECURITY – NEED FOR VERTICAL & HORIZONTAL STANDARDS!

Security in Healthcare & Wearables

- **ISO/IEEE 11073** series Health Informatics - Medical / Health Device Communication Standards
- **IEEE 2410-2015** - IEEE Standard for Biometric Open Protocol
- **IEEE 11073** PHD Cybersecurity (Pre-Standards Activity)

Security in Smart Grids



- **IEEE 1686** Standard for Substation IED Cybersecurity Capabilities
- **IEEE C37.240** Standard for Cyber Security Requirements for Substation Automation, Protection and Control Systems
- **IEEE 1711** Cryptographic Protocol for Cyber Security of Substation Serial Links
- **IEEE P1711.2** Standard for Secure SCADA Communications Protocol (SSCP_
- **IEEE 1402** Standard for Physical Security of Electric Power Substations
- **IEEE 2658** Guide for Cybersecurity Testing in Electric Power Systems

Find more smart grid standards and projects at http://smartgrid.ieee.org/standards

IEEE Security/IoT Standards Initiative Examples

- **IEEE P2721 Standard for Wireless Health Device Security Assurance**
  - Security assurance mandatory and optional requirements for wireless healthcare devices balancing needs for security and clinical application.
  - Assurance and certification against requirements
- **IEEE P7002 Data Privacy Process**
  - requirements for a systems/software engineering process for privacy oriented considerations regarding products, services, and systems utilizing employee, customer or other external user's personal data.
- **IEEE P2413 Standard for an Architectural Framework for the Internet of Things (IoT)**
  - Includes “quadruple trust” (protection, security, privacy, and safety) as a key component of IoT.
- **IEEE P2418.1 Standard for the Framework of Blockchain Use in Internet of Things (IoT)**
  - scalability, security and privacy challenges with regard to blockchain in IoT e.g. tokens, smart contracts, transactions.
- **IC17-013 11073 PHD Cybersecurity**
  - Build common ground about cybersecurity in the Personal Health Device community and create an "information security toolbox“
- **IEEE P802E**
  - Recommended Practice for Privacy Considerations for IEEE 802 Technologies
- **IEEE 1451**
  - Standard for a Smart Transducer Interface for Sensors, Actuators, Devices, and Systems - Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats
- **IEEE P1619**
  - Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices
- **IEEE P1912**
  - Standard for Privacy and Security Architecture for Consumer Wireless Devices
- **IEEE P2025.2**
  - Standard for Consumer Drones: Privacy and Security

Thank you

For more information, please contact:
Sri Chandrasekaran
sri.chandra@ieee.org

IEEE Standards Association
standards.ieee.org