# Managing Security Concerns in Smart Sustainable Cities

**Ziqin Sang**

Vice-chairman of ITU-T Focus Group on Smart Sustainable Cities

Fiberhome Technologies Group, China

+86 27 87694040

zqsang@wri.com.cn

# cyber-security work

ITU-T FG-SSC:

■ technical report on Cyber-security, data protection and cyber-resilience in smart sustainable cities

ITU-T SG17

■ leading group, coordinates security-related work across all ITU-T Study Groups

# Challenges

▪SSC highly dependent on ICT, including IoT, RFID, M2M.

▪hyper-connectivity for smart and sustainable city components and services, introduces higher levels of complexity, higher volumes of data to the extent of Big Data, opens new doors for malicious cyber-attacks

▪relate to governance and policy-- need attention to ICT systems and critical infrastructure, and citizens of essential services, including smart grid, water management, healthcare, emergency services, public safety etc.

hyper-complexity + hyper-connectivity + hyper-volumes of data = Hyper-vunerability

# The SSC cyber-equation

- "Smart and Sustainable Cities" have ICT as key enabler
- This implies:
  - Highly complexity of the ICT systems
  - Highly interconnected components
  - High volume of data generated

$$\frac{\text{Hyper-connectivity} + \text{Hyper-complexity} + \text{Hyper-volume of data}}{} = \text{HIGH VULNERABILITY}$$

# A resilient Smart and Sustainable City...

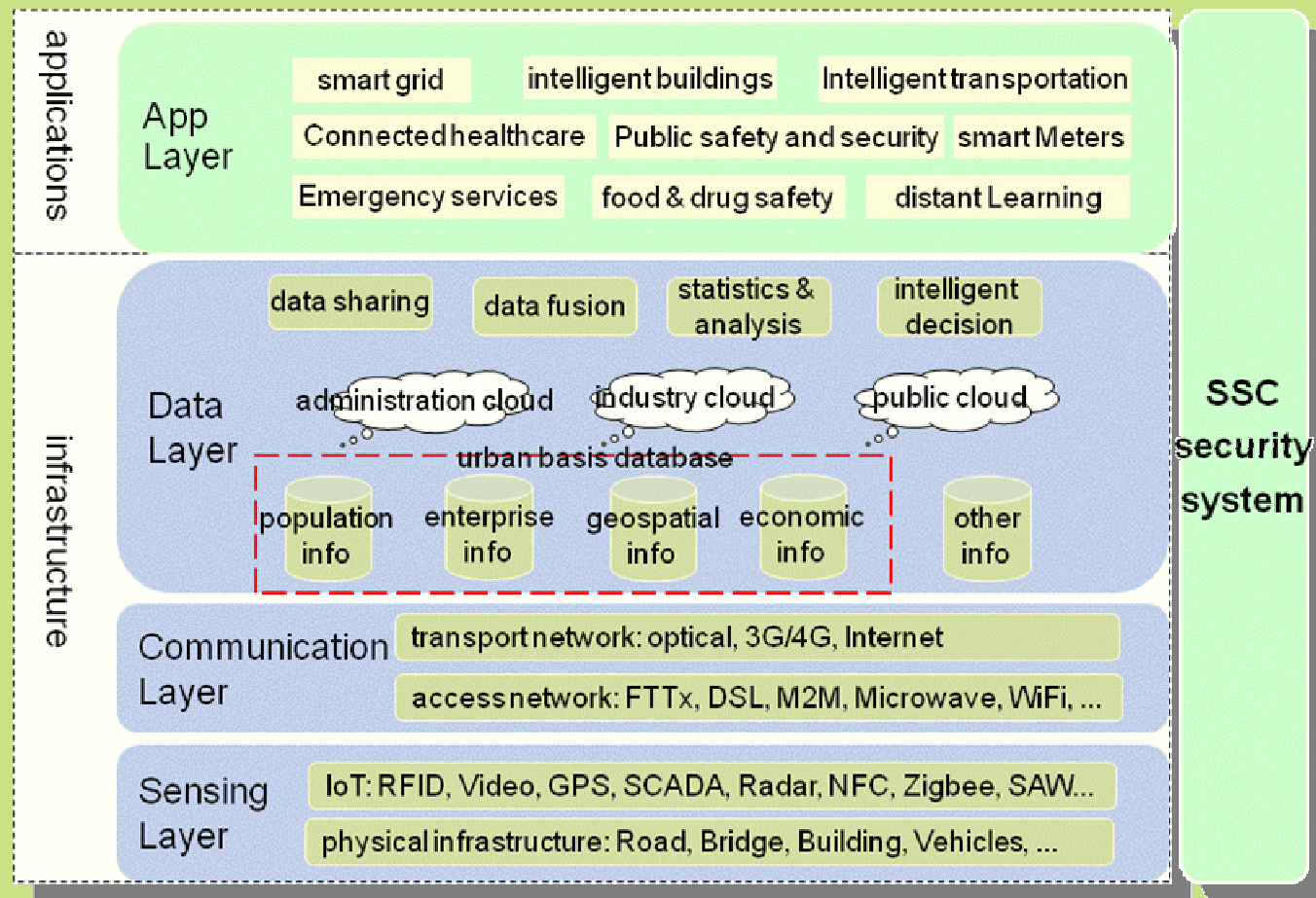…needs to be designed, from inception, with…

- Cyber security
- Privacy
- Integrity
- Compliance
- Reliability
- Resilience

…in mind.



HIGH VULNERABILITY

# Layered view, and architecture...

# Smart grids and energy efficiency

- Cities consume between 60 and 80% of world's energy
- Smart Grid, smart metering with IP address and sensors allow monitoring and adjust generation and delivery based on consumption models
- Reduce cost and environmental impact

# Intelligent transportation: keeping the city moving

- Real-time traffic flow information
- Telco, Global Positioning Systems (GPS)
- M2M communication, Wi-Fi and RFID technologies
- Data analytics and prediction techniques
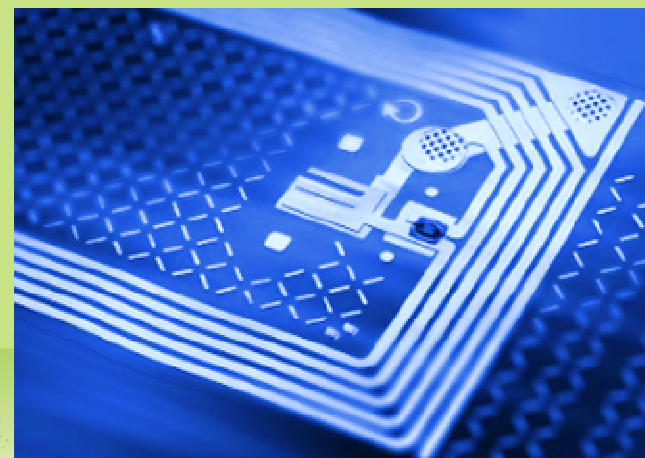
# Connected Healthcare



- Secure collaborative access for authorised medical services, to Electronic Patient Records, in a way, at any time, from anywhere, from any accredited device
- Telemedicine solutions for remote areas or in case of natural disaster
- Ageing population: assisted living and monitoring service for independence at home
- All require privacy, identification and cyber security

# Public safety and security

- Protecting against crime, natural disasters, accidents or terrorism.

- Tele-surveillance systems to help emergency services

- First respondents to benefit from secure connectivity
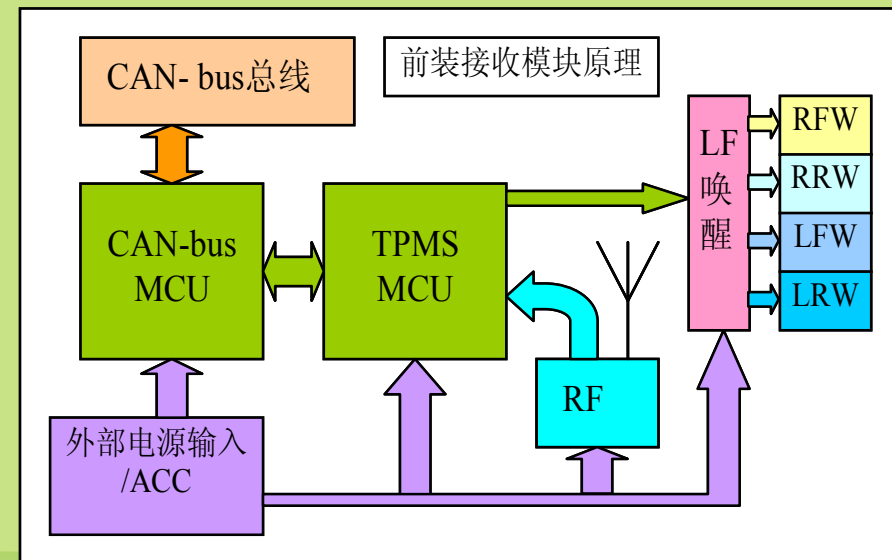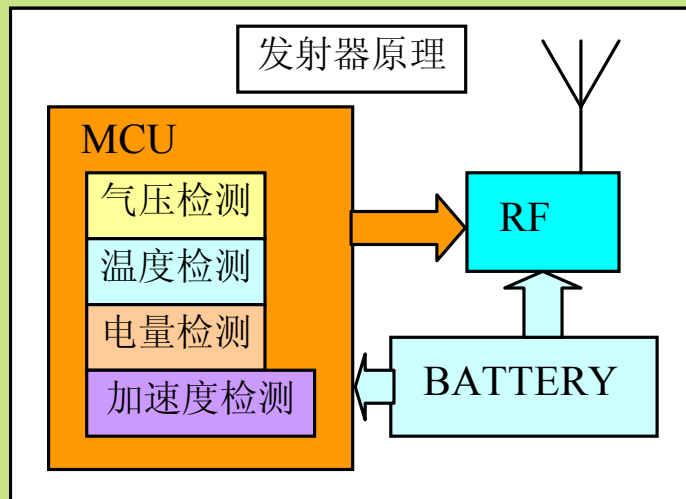
- Secure data access and sharing

# Wireless communications & hotspots



- Increasingly popular service, with increasing vulnerability

- Unsecure access to sensitive and personal data (online banking, social network, etc.)

- Younger population particularly exposed

- Cyber-crime increasingly active in these environments

# a case study: vulnerability of tire pressure detection system (TPDS)

- Transmitter collect data of tire pressure and temperature, then transport it to the receiver through the wireless communication

- receiver get the data, then determine whether it exceeds the normal value.
- When there is failure to make a sound and light alarm

发射器原理

MCU
气压检测
温度检测
电量检测
加速度检测

RF

BATTERY

CAN- bus总线

前装接收模块原理

CAN-bus MCU

TPMS MCU

LF 唤醒

RFW
RRW
LFW
LRW

外部电源输入/ACC

RF

# a case study: vulnerability of tire pressure detection system (TPDS)
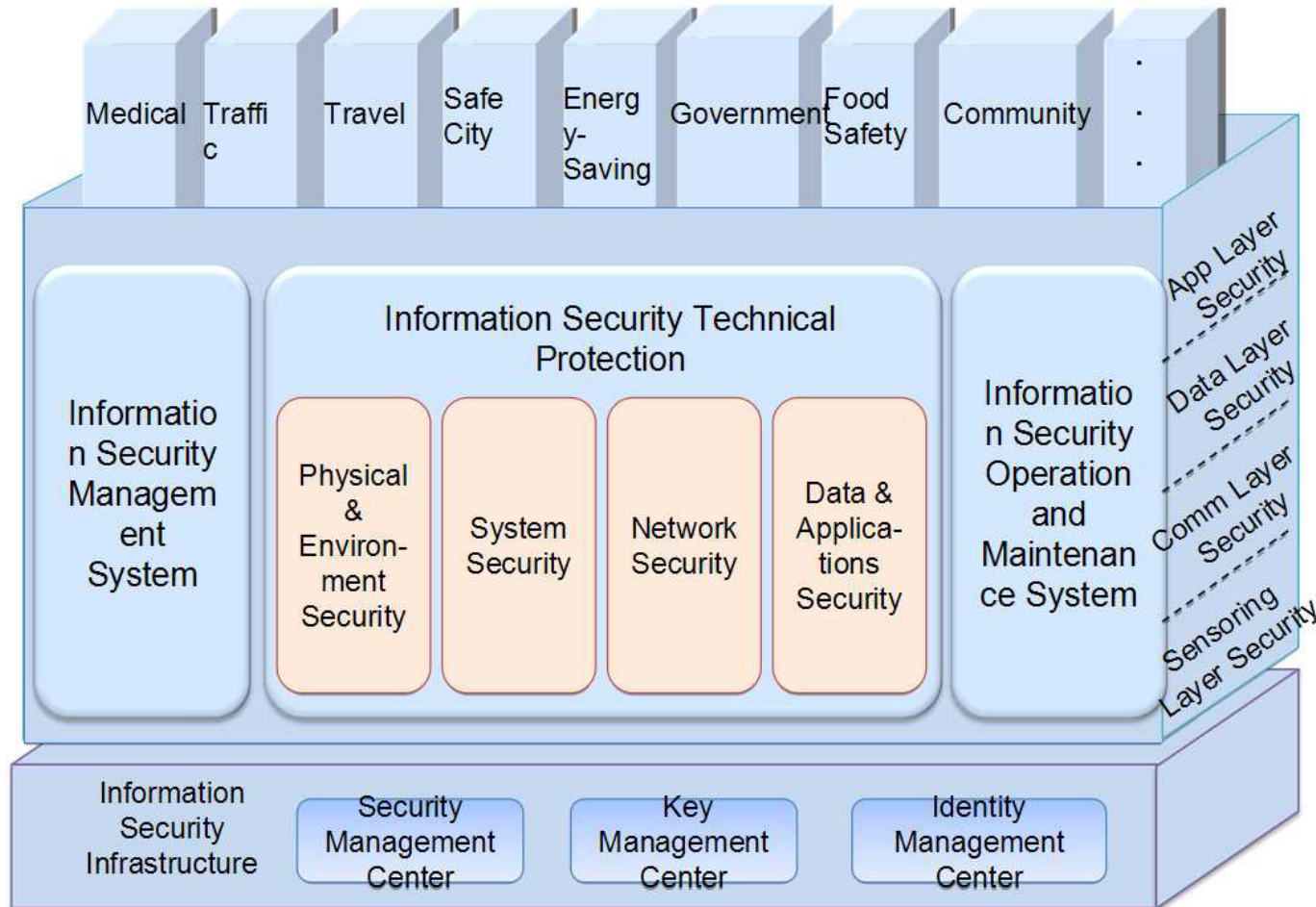
- Each sensor reports its unique identification number, each tire has a specific identification number

→

- ID can be decrypted at 40 meters. ie
- In the range of 40 meters any car can be tracked, each tire becomes automatic tracking devices

→

- intrude TPDS
- attack Car PC

now:
- track car
- record the conversation within the car
- start a locked car
- ……

# Security Architecture of a SSC



Application layer boxes: Medical, Traffic, Travel, Safe City, Energy-Saving, Government, Food Safety, Community

Information Security Management System

Information Security Technical Protection
- Physical & Environment Security
- System Security
- Network Security
- Data & Applications Security

Information Security Operation and Maintenance System

App Layer Security
Data Layer Security
Comm Layer Security
Sensoring Layer Security

Information Security Infrastructure
- Security Management Center
- Key Management Center
- Identity Management Center
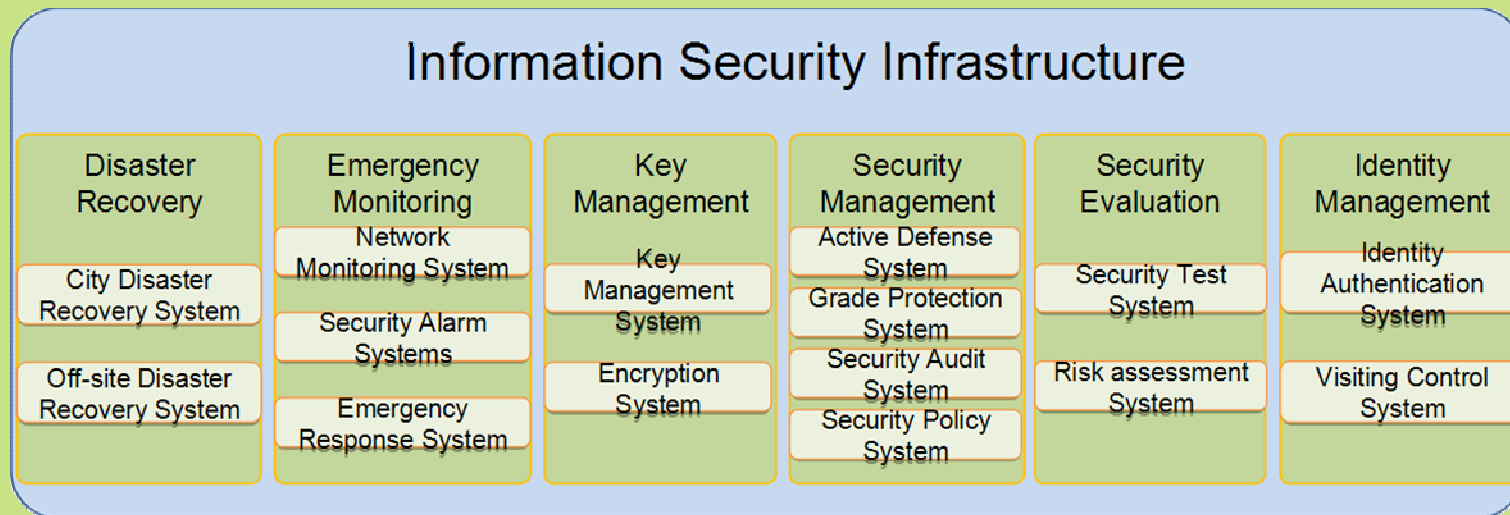
# Security Architecture of a SSC

- SSC Information Security Infrastructure
- SSC Information Security Technical Protection
- SSC Information Security Management System

## Information Security Infrastructure

| Disaster Recovery | Emergency Monitoring | Key Management | Security Management | Security Evaluation | Identity Management |
|---|---|---|---|---|---|
| City Disaster Recovery System | Network Monitoring System | Key Management System | Active Defense System | Security Test System | Identity Authentication System |
| Off-site Disaster Recovery System | Security Alarm Systems | Encryption System | Grade Protection System | Risk assessment System | Visiting Control System |
| | Emergency Response System | | Security Audit System | | |
| | | | Security Policy System | | |

# Ensuring continuity of critical services

- City governance to ensure that ICT strategies are strongly interwoven into the fabric of the wider city evolution strategy

- Technology to enable policy

- City CIOs increasingly part of strategic policy discussions

- Systems/IoT, need to be standardised, interoperable and open, but also secure

- Cyber-security and resilience to be embedded from inception

- Cyber-security + backup and recovery systems for mission-critical administration data (& Big Data)

# Recommendations (1)

- **Establish Governance -** Identify and organise key stakeholders
- **Governance, Risk and Compliance (GRC) -** Fulfil through policies and processes, enabled by *ad hoc* IT suites: stay compliant and mitigate risks
- **Service continuity** - Solutions and methodologies on Cyber-security, backup, data loss prevention, archiving and disaster recovery.
- **Protect information proactively**
  - Information-centric approach
  - Embed security within data
  - Utilise encryption
- **Authenticate users** with Strong Authentication
  - This also prevents from accidental disclosing of credentials and from attaching unauthorised devices to the infrastructure.

# Recommendations (2)

- **Threat intelligence** - In order to understand the major trends in terms of potential attackers, through analysing trends on malware, security threats, and vulnerabilities
- **Managed security services** - Outsourcing security services to providers. The ICT leadership can in that way focus on their functional duties of running the city systems
- Rely on their national Computer Emergency Response Teams (CERT), in order to be aligned with national coordination on cyber-incidents and security, and benefit from the international visibility this provides these entities provide.
- **Protect the infrastructure** by securing endpoints, messaging and web environments.
- **Ensure 24x7 availability of the critical infrastructure**
- **Develop an information management strategy**

# Links & Additional Information

- ITU-T and Climate Change
  [itu.int/ITU-T/climatechange](itu.int/ITU-T/climatechange)

- ITU Focus Group on Smart Sustainable Cities
  [itu.int/en/ITU-T/focusgroups/ssc/](itu.int/en/ITU-T/focusgroups/ssc/)

- ITU Symposia & Events on ICTs and Climate
  Change   [itu.int/ITU-T/worksem/climatechange](itu.int/ITU-T/worksem/climatechange)

## Thank YOU

**tsbfgssc@itu.int**