Smart Sustainable Cities ICT Infrastructure

Smart Sustainable Cities
Training Programme
Module 2
SSC-2

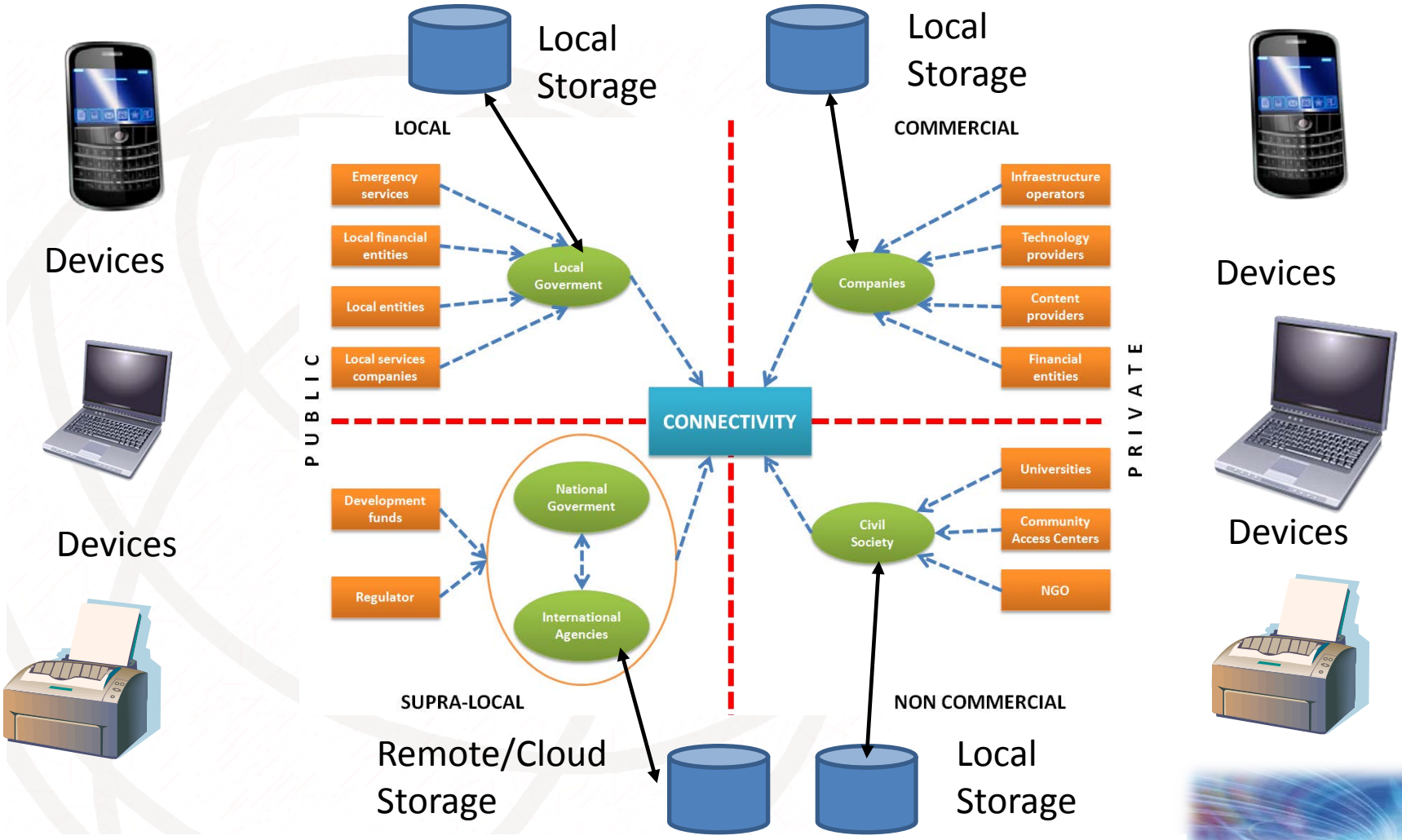
Contents

- Overview of SSC Infrastructure
- Cyber-Security, Data Protection and Cyber-Resilience
- Smart Buildings for SSCs
- Smart water management for SSCs
- EMF Considerations in SSCs
- ICTs for Climate Change Adaptation in Cities
- Integrated management for SSCs
- Anonymisation Infrastructure and Open Data

Aim of this Module

- The aim of this presentation is to provide a technical overview on infrastructure related to
  - information and communications technology (ICT) and
  - smart sustainable cities (SSC)

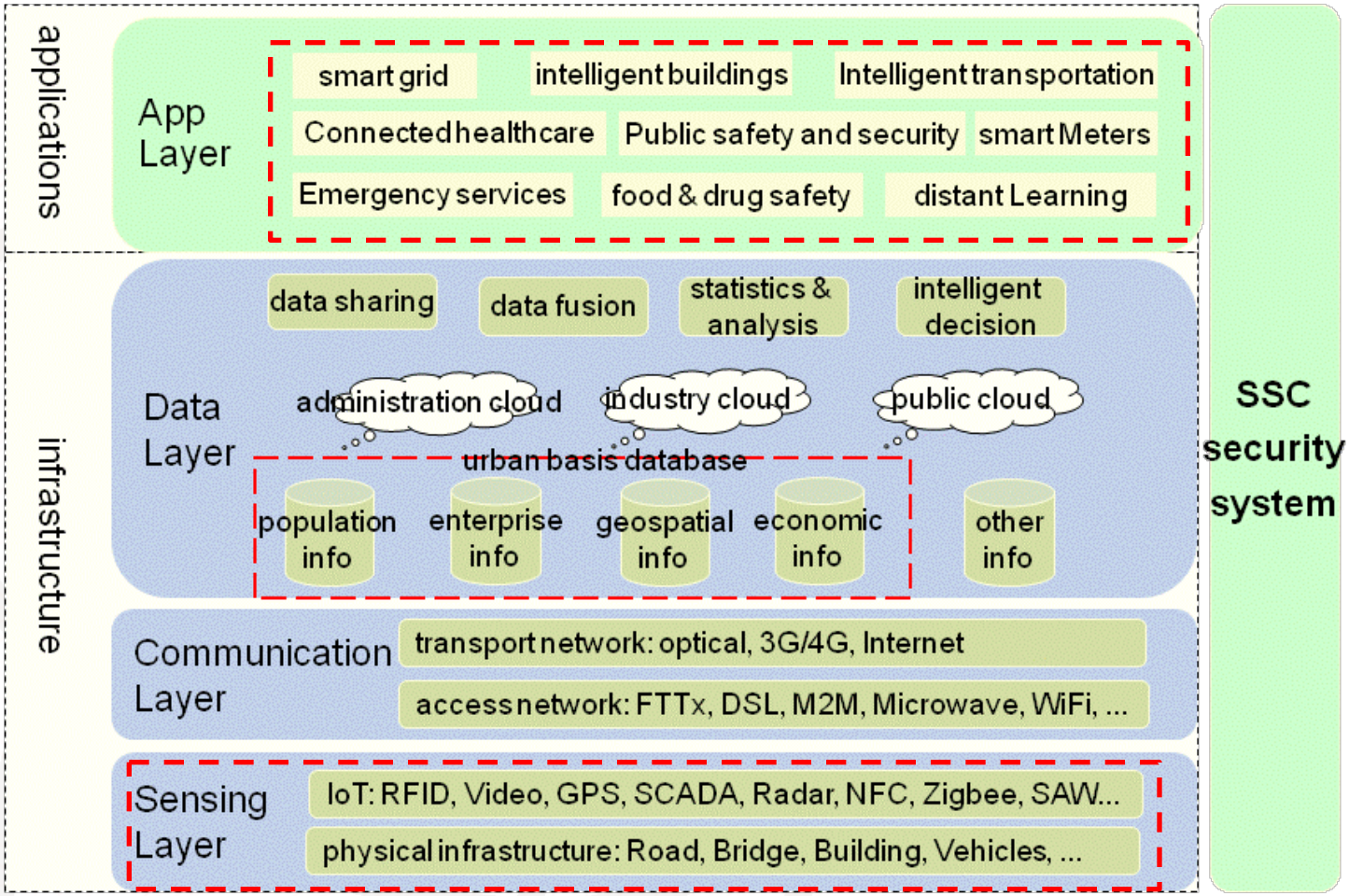
ICT Infrastructure Landscape for SSCs



Sources: Adapted from FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Page 11 and Ministry of Transportation and Communications of Peru

Layered Architecture

Note the presence of a Sensing Layer



This diagram introduces the concept of layers within the networks serving a Smart City or Community. Note: red lines indicate new features

Sources: FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Page 12 and document FG-SSC-0112, proposed by Fiber Home Technologies Group and Telecom Italia

Sensing layer and Internet of Things (IoT)

Physical Object
+
Controller, Sensor, and Actuators
+
Internet
=
Internet of Things

An equation for the Internet of Things

- IoT predictions show that we will have 16 billion connected devices by the year 2020, which will average out to six devices per person on earth and to many more per person in digital societies.
- Existing sensors may not have direct internet access. IoT devices are able to connect to the internet directly
- Smart phones and machine to machine (M2M) (or thing to thing -ToT) communications devices will be the main springboards for IoT development.

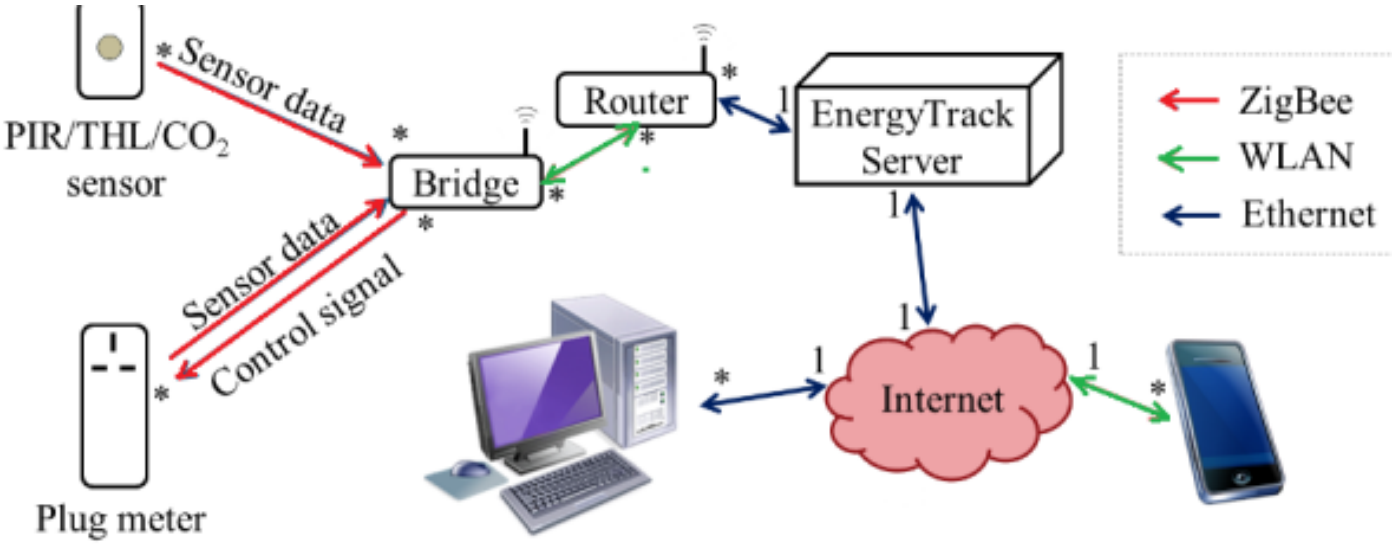
Source: FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Page 57 and "Designing the Internet of Things". By Adrian MCEwen, Hakim Cassimaly

Sensor Networks and Internet of Things (IoT)#2

- The sensing layer collects the data input from the system environment in order to capture and respond to various environment stimulations
  - The data are collected by sensors such as
    - thermometers, stress gauges, cameras, etc.
  - The data are transported via cables in conduits, manholes, common ducts, IT poles, etc.
  - This type of infrastructure is also used for services such as telecommunications, cable TV and electricity supply

Source: FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Page 12

Sensor Network

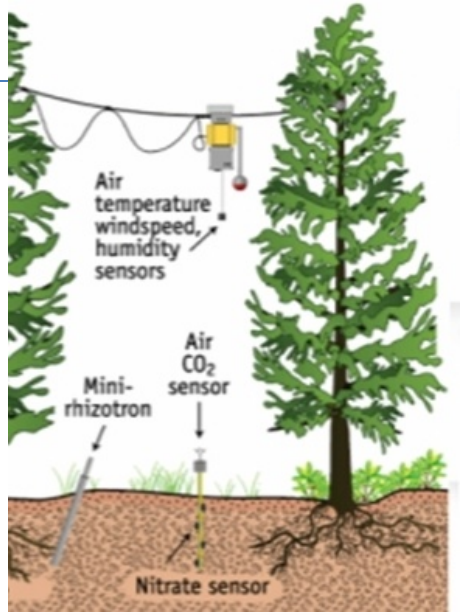


- Sensors don't need high bandwidth but they do need low latency (delay) and very low energy consumption for long battery lives
  - Standards such as Bluetooth and WLAN are not suited for low power applications, because of power-hungry RF-ICs and protocols.
- ZigBee is a new global standard for wireless connectivity, focusing on standardizing and enabling interoperability of products
  - ZigBee (IEEE 802.15.4) got its name from the way bees 'zig' and 'zag' while tracking between flowers and relaying information to other bees about where to find resources.

Sources: FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Page 51

Sensor Network Examples

- environmental data collection
  - collect sensor readings from hundreds of points over a period of time in order to detect trends and interdependencies
- security monitoring
  - security networks do not need to collect data continuously
  - sensors only have to transmit a data report when there is a security violation
- sensor node tracking
  - tracking of a tagged object, such as vehicle with an RFID tag through a region of space monitored by a sensor network



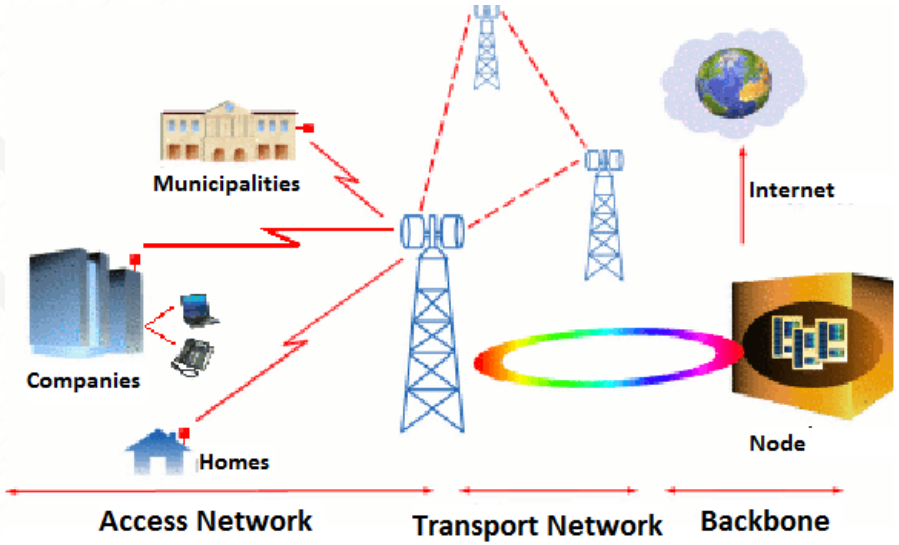
video camera sensor

On screen RFID

Sources: FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Pages 45-46

Communication Layer#1

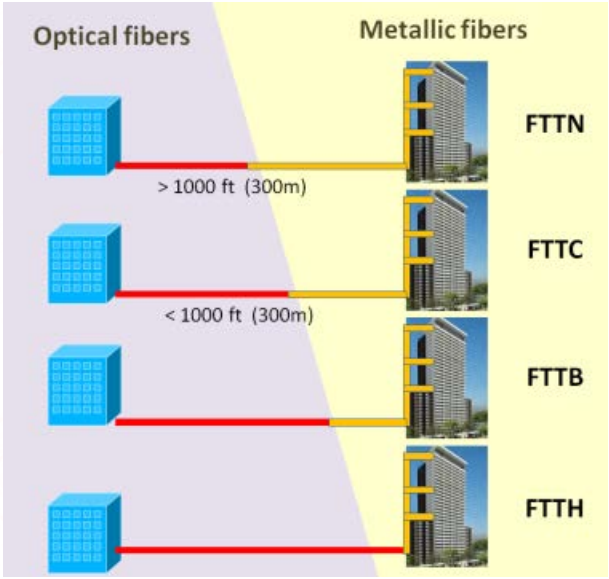
- This is the information superhighway in smart city
- The communication network of a future city consists of large-capacity, high-bandwidth, highly reliable optical networks, which would provide
  - city-wide coverage for the wireless broadband network
  - internet access to other cities and international internet transmission
- The legacy access network is gradually being upgraded from metallic twisted pair to optical fibre
  - Optical fibre offers increased capacity and more energy-efficient transmission
- Apart from telecommunications other networks exist in cities such as those providing closed circuit TV for traffic management or security surveillance



Sources: FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Page 13 and 26

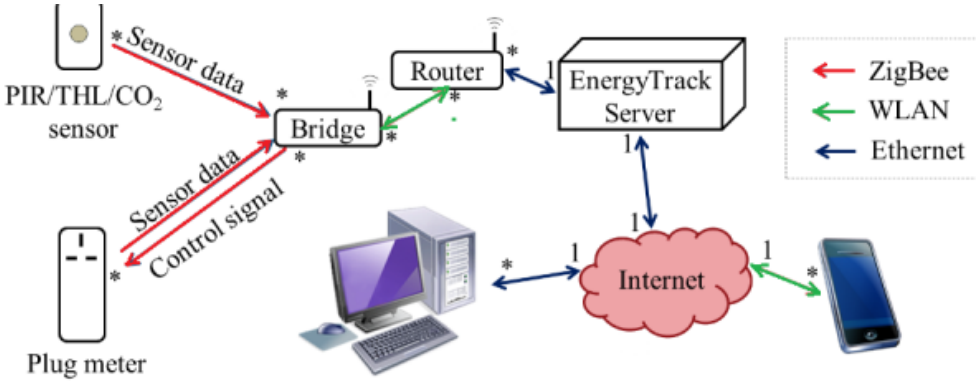
Communication Layer#2

- FTTx Access Networks
- Fibre to the X (FTTX) is a generic term for any broadband network architecture using optical fibre to provide all or part of the local loop used for last mile telecommunications
- The term is a generalization for several configurations of fibre deployment, ranging from
  - FTTN (fibre to the neighbourhood)
  - FTTC (fibre to the cabinet)
  - FTTB (fibre to the building)
  - FTTH (fibre to the home)
  - FTTD (fibre to the desktop)
- The nearer the fibre is to the end user the faster the end to end transmission can be



Sources: FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Page 32 and 33

Data Layer



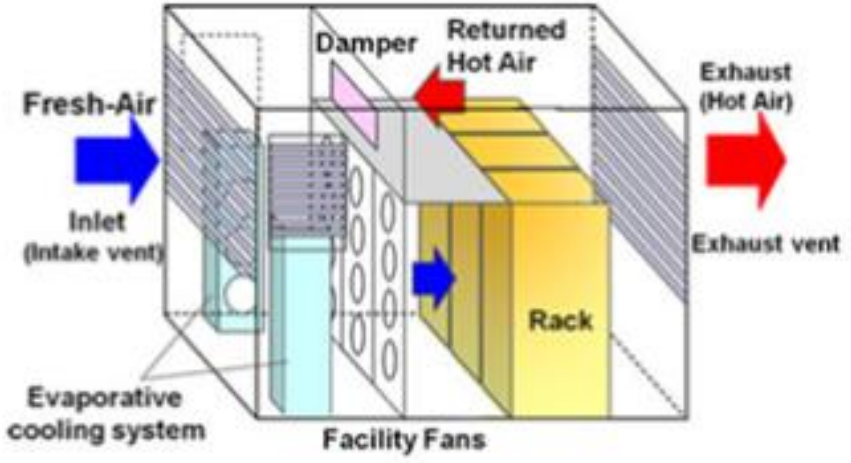
- The data layer transports between industries, departments and enterprises, as well as municipalities, etc.
  - It also transports data to centralised servers in data centres
  - Servers are computers connected to many users
  - Internet Protocol (IP) is an example format in which data is 'packaged' for transmission and acknowledgement
  - This protocol is transmitted over the physical layer which includes ZigBee (wireless), WLAN (wireless) and Ethernet (multiple twisted pairs)
  - Ethernet is the dominant data-link protocol for today's networks, supporting a multitude of communication applications. Also, Ethernet is one of the key protocols used to interconnect routers and to carry applications in high-speed optical networks to backhaul access traffic.

Sources: FG-SSC "Technical Report on Smart Sustainable Cities Infrastructure" Pages 14 and 51

Data Centre Energy Efficiency

- ITU-T Recommendation L-1300 “Best practices for green data centres”
  - Recommends features to improve the energy efficiency of a data centre or telecommunications building
  - It may be used as a basis for a checklist for an energy efficiency audit of an ICT building
- The use of external ambient air (e.g. at night or when appropriate) reduces the amount of electricity used by the air conditioning

Example: Prototype container-type data centre and schematic of the container’s contents (Fujitsu)



Source: FG-SSC “Technical Report on Smart Sustainable Cities Infrastructure” Pages 24 and 25
See also ITU-T Recommendation L-1300 “Best practices for green data centres”

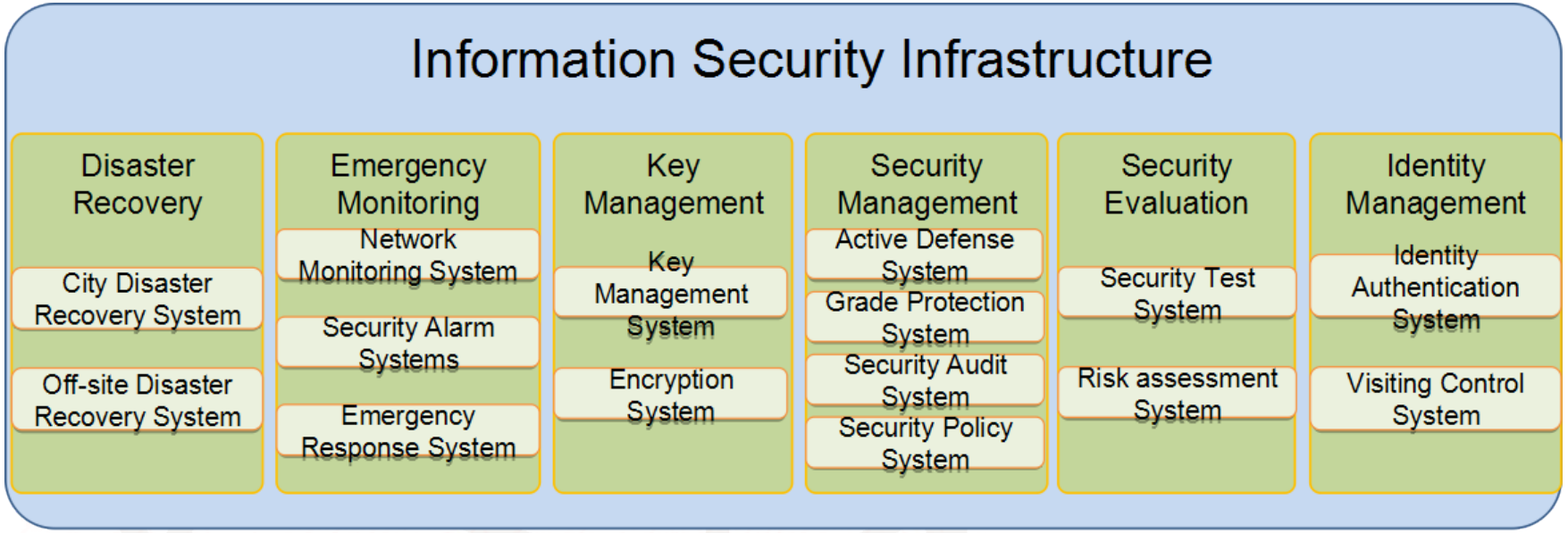
Next:
Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities

Introduction to Cyber Security

- In a SSC communications need to be
  - secure, reliable and resilient
- However
  - Hyper Complexity + Hyper Connectivity + Hyper Data Volumes = Hyper Vulnerability
- Vulnerabilities include
  - malicious violations
    - Hackers' motivations include financial gain, industrial espionage, cyber-sabotage, cyber-warfare, political activism
  - unintentional damage and
  - natural disasters

Source; FG-SSC "Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities", page ii

Information Security: Infrastructure of a SSC



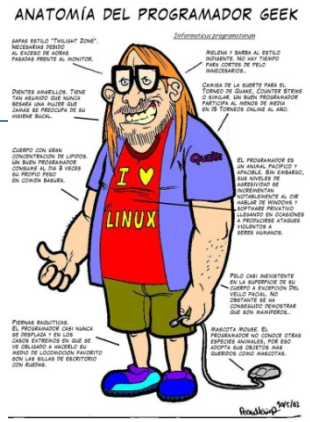
- The information security infrastructure of a SSC constitutes the technical foundation of the entire system, and as such, it provides a large number of security functions:
  - disaster recovery
  - emergency monitoring
  - key management
  - security management
  - security evaluation and
  - identity management

Source; FG-SSC "Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities", page 16

Recommendations to Ensure SSC Service Continuity#1

- Protecting information proactively
  - Securing endpoints, messaging and web environments, defending critical internal servers and implementing the backup and recovery of data, should be among the key priorities of SSC strategists. Organisations also need visibility and security intelligence to respond to threats rapidly.
- Authenticating users
  - Strong authentication enables organisations to protect public assets by verifying the true identity of a smart device, system or application. This prevents individuals from accidentally disclosing credentials to an attack site, and from attaching unauthorised devices to the infrastructure.
- Leveraging threat intelligence
  - In order to understand the major attack trends, CIOs (Chief Information Officers) can use an established observatory, like the Symantec Global Intelligence Network, to advise of trends on malware, security threats and vulnerabilities, from security research centres around the world.
- Balancing traditional versus cloud delivery
  - Within a SSC, online services may be delivered by a traditional client-server approach, but also through a cloud-computing model to leverage 'as-a-service' third party efficiencies
  - Service Level Agreements (SLAs) are needed in order to guarantee the provision of essential services to citizens

Source; FG-SSC "Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities", pages 15-18



Recommendations to Ensure SSC Service Continuity#2

- Managing security services and Computer Emergency Response Teams (CERT)
  - SSC should also consider outsourcing security services to providers who can leverage extensive, global expertise in the field of cyber security to minimise security-related disruptions and data loss. The ICT leadership can then focus on the functional duties of running the city.
  - SSC should also rely on their national Computer Emergency Response Teams (CERT) to align with national coordination on cyber incidents and security, and thus benefit from the international visibility this provides.
- Protecting the infrastructure
  - Securing endpoints, messaging and web environments, defending critical internal servers and implementing the backup and recovery of data, should be among the key priorities of SSC strategists. Organisations also need visibility and security intelligence to respond to threats rapidly.

Source; FG-SSC “Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities”, pages 15-18

Recommendations to Ensure SSC Service Continuity #3

- 24x7 availability of the critical infrastructure
  - Ensuring resilience in case of an incident can be achieved through the adoption of solid backup and recovery software processes and the use of resilient infrastructure which offers protection by having more than one transmission path available.
- Developing an information management strategy
  - This should include an information retention plan and policies.
  - Organisations need to refrain from using backup for archiving and legal retention, and should instead implement **deduplication** mechanisms to free up resources, adopt a full-featured archive and eDiscovery system, and deploy data loss prevention technologies.

Source; FG-SSC "Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities", pages 15-18

Recommendations to Ensure SSC Service Continuity#4

- Access control at the boundary of network
  - Access control at the boundary can isolate external attacks away from internal networks
  - A firewall is required to filter packets and application gateway. Since only selected protocols can pass through the firewall, the network environment is more secure
  - All security measures (such as passwords, encryption, authentication, and auditing, among others) can be configured on the firewall
  - A firewall can provide statistical data of network usage. When suspicious actions occur, the firewall can generate the appropriate alarm, and provide detailed information about the incident for threat analysis purposes.
- Protecting intrusion dynamically
  - Intrusion detection is another important dynamic security technology, which can collect and analyse information from a number of key points of the computer network and system, and detect any suspicious behaviour. There are three types of Intrusion Detection Systems (IDS):
    - Network-based IDS
    - Host-based IDS
    - Integrated IDS

Source; FG-SSC “Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities”, pages 15-18

Recommendations to Ensure SSC Service Continuity#5

- Preventing distributed denial-of-service (DDOS) attacks
  - For example , saturating the target machine with external communications requests
  - Measures Include: Specialist network equipment to guarantee sufficient network bandwidth, upgrading the host server hardware, using static web pages whenever possible, enhancing the operating system TCP / IP stack, and installing a specialized anti-DDOS firewall
- Network security audit
  - A mechanism to ensure the smooth running of the security systems and to record and clear incidents

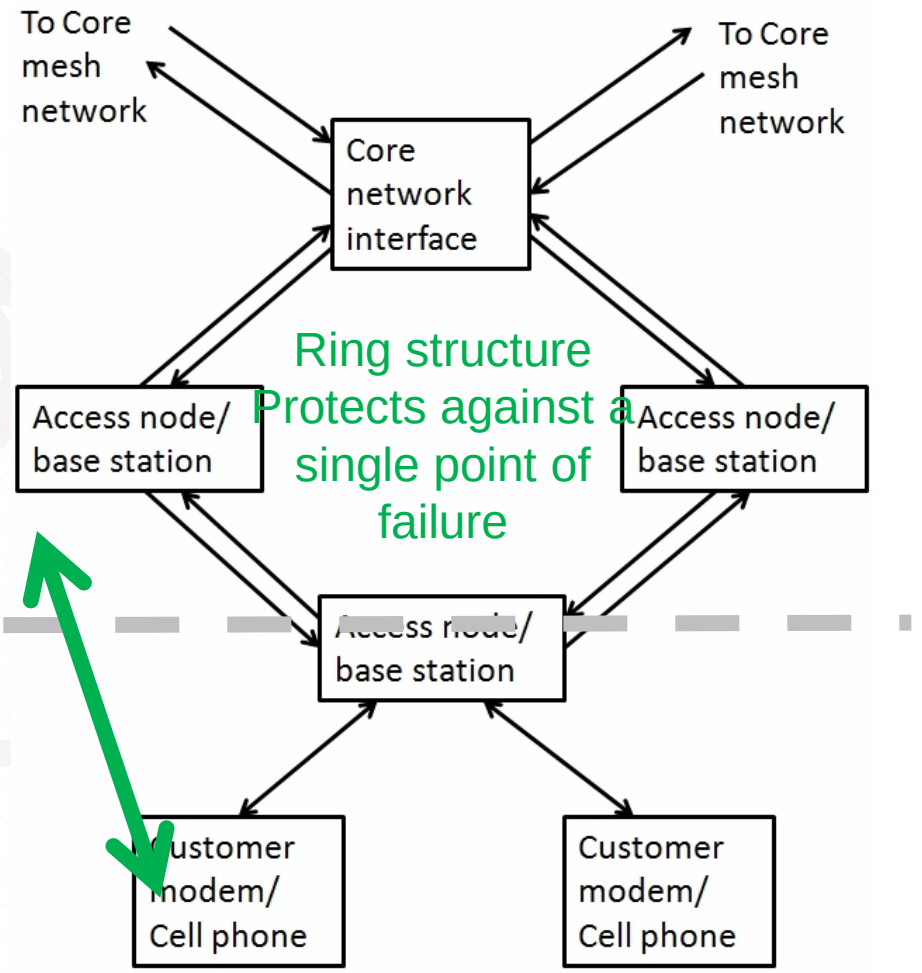
Source; FG-SSC “Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities”, pages 15-18

Example: Ensuring Service Continuity

Ring networks may be 'folded' automatically at any node in event of a link or device failure

Additional paths may be added to customer end to give added protection

e.g. fibre and/or wireless



Source: ITU-T "Resilient pathways: the adaptation of the ICT sector to climate change, page 27
http://www.itu.int/en/ITU-T/climatechange/Documents/Publications/Resilient_Pathways-E.PDF

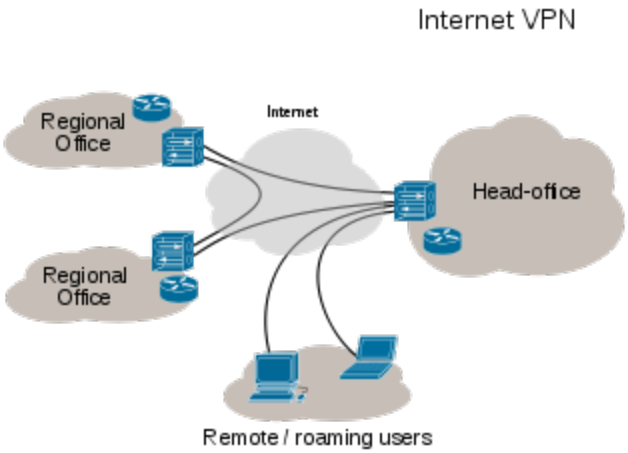
Child online protection in SSC

- Children are among the most vulnerable users of online services, as identified by the ITU-T Joint Coordination Activity on Child Online Protection (ITU-T JCA-COP)
  - http://www.itu.int/en/ITU-T/jca/COP/Pages/default.aspx.
  - "Child online protection covers a number of issues, and is being addressed at national, regional and international levels, across a myriad of environments, including social and legal. At the international level, and within the ITU, the Council Working Group on Child Online Protection has received much information on national activities, and has developed guidelines and identified many technical activities that are contributing to the safety of children on line at a global level."

Source; FG-SSC "Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities", pages 17-18

Protective Measures Example - WiFi hotspots

- Ensure that nobody is able to read your screen
  - A privacy screen can be used for extra security.
- The network configuration should be changed to manually select each wireless network
  - This reduces the risk of connecting to unknown WiFi hotspots
- Security software should be kept current and active
- File sharing should be turned-off while at a hotspot
- When using instant messaging or email, nothing should be sent that one wouldn't want made public.
  - Internet banking, stock trading or other sensitive online financial transactions should be avoided while using a public hotspot.
- A Virtual Private Network (VPN) encrypts data, username and password, allowing secure communications wherever you connect to the Internet.



Source; FG-SSC "Technical Report on Cyber-Security, Data Protection and Cyber-Resilience in Smart Sustainable Cities", page 16

Next:
Smart Sustainable Buildings

Smart Sustainable Building - Aims

- Objective
  - to create a building and its infrastructure which provides the owner, operator and occupant with an environment which is flexible, effective, comfortable and secure
- User experience
  - Can be enhanced using ICT in the building systems, to facilitate control and integration of utilities and services
    - The 'three utilities' are electrical, mechanical and plumbing
    - The 'fourth utility', the communications which enable buildings to be smart, is **traditionally ignored**!
    - Communications are needed for access control, elevators, HVAC, lighting systems, modern signage with VDUs, building condition monitoring, audio paging, fire alarm systems, telephone systems and surveillance systems

Source: Technical Report on Smart Buildings for Smart Sustainable Cities, Page 4-7

Examples of Best Practices and Standards

- Example of Best Practices
  - The Technology Roadmap for Intelligent Buildings*
    - The focus is on commercial, institutional and high-rise residential buildings, both new-build and retrofits
    - Issued by the Continental Automated Building Association (Canada)
- Examples of Standards
  - The LEED rating system for the design, construction, operation and maintenance of green buildings, homes and neighbourhoods **
    - LEED (Leadership in Energy and Environmental Design-USA)
    - Buildings can qualify for four levels of certification:
      - Certified: 40–49 points
      - Silver: 50–59 points
      - Gold: 60–79 points
      - Platinum: 80 points and above
  - ITU-T Recommendation L-1300 “Best practices for green data centres”
    - Provides a list of features which should be adopted to improve the energy efficiency of a data centre or telecommunications building
    - It may be used as a basis for a checklist for an energy efficiency audit of an ICT building

Source: ‘Technical Report on Smart Buildings for Smart Sustainable Cities’, Pages 8,15-16
* ‘Technology Roadmap’ http://www.caba.org/trm
**http://www.usgbc.org/Docs/Archive/General/Docs5546.pdf
*** http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12204

Smart Sustainable Buildings
The Hotel

- This is fertile ground for increasing the benefits of automation through integration of its operational systems
- A key requirement is
  - ability to adapt to the current occupancy rate
    - This can be improved by the use of ICT
    - The ability to “shut down a room” or to “open up a room” in response to an arriving or departing guest can provide a significant impact on the bottom line
- Key features are
  - To clean only rooms which have been used
  - To heat and light only rooms which are occupied
  - To monitor members of staff as part of the overall building effectiveness
  - To provide suitable “intelligent” links between the television and the hotel’s billing system.
    - E.g. A keyboard in each room and one of the TV channels set aside to provide a screen and communication system so that guests can check out, settle accounts and order special services as they may wish.

Source: ‘Technical Report on Smart Buildings for Smart Sustainable Cities’, Pages 12-13

Smart Sustainable Buildings - Example
T-30A Prefabricated 30 Storey Hotel #1

BROAD SUSTAINABLE BUILDING
远大可建科技有限公司
BROAD Low Carbon Community, Xiangyin County, China Zip 414600
Tel: 86-731-84086266 Email: bsbs@broad.net www.broad.com

You Tube Video* shows the “BROAD” 700 bed hotel being constructed in only 15 days

BSB Technological Features **

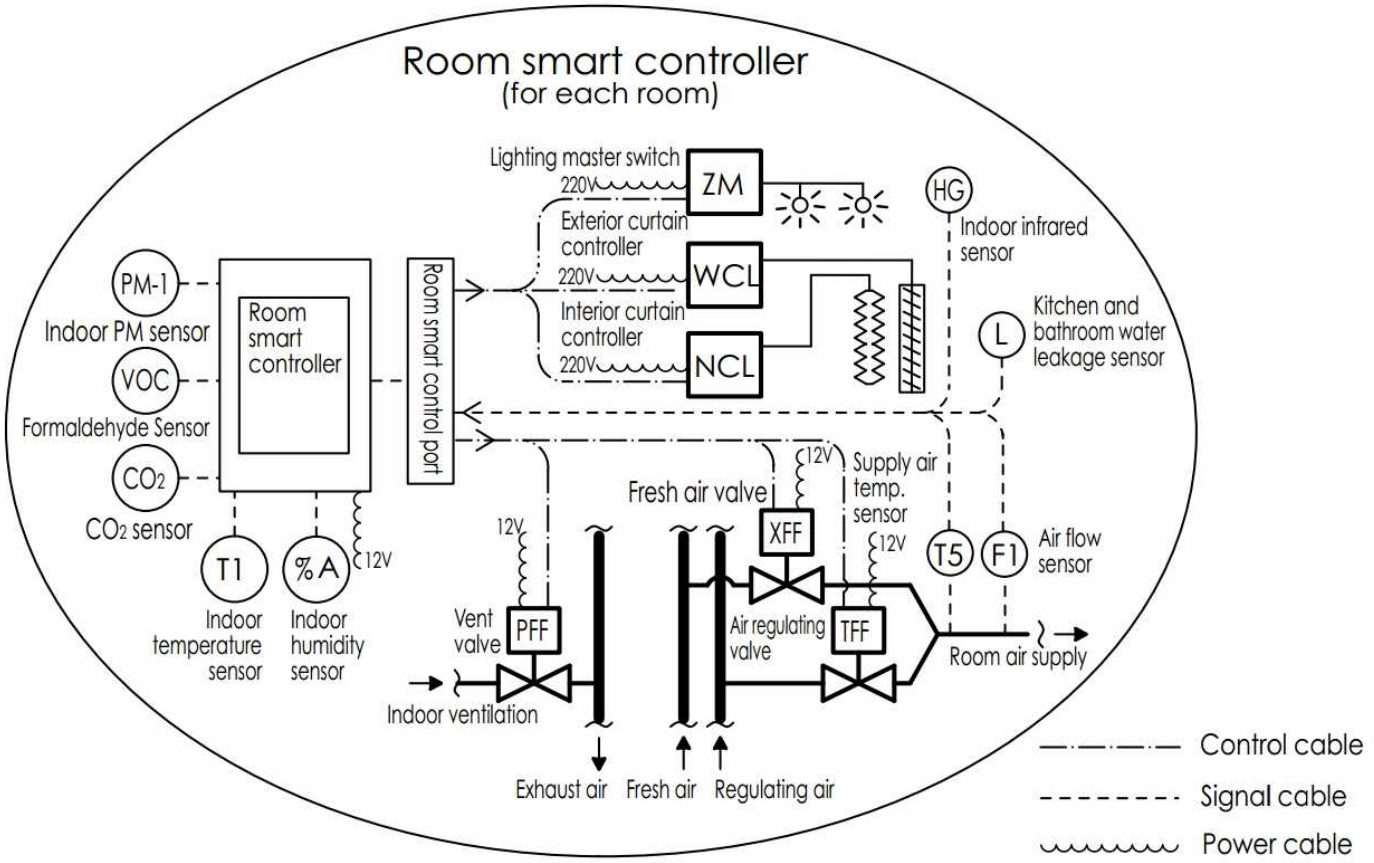
Sustainability

“BSB” is the abbreviation for BROAD sustainable building (factory-made). Its sustainability is derived from 8 aspects: earthquake resistance, energy conservation, air purification, durability, material saving, recyclable construction materials, construction materials free of formaldehyde, lead, radiation, asbestos and no construction sewage, dust or wastes. BSB has accomplished the extremity of these 8 aspects that today’s human technologies can ever imagine.

Sources: *https://www.youtube.com/watch?v=Hdpf-MQM9vY
**http://en.broad.com/uploads/pdf/tsjd.pdf

Smart Sustainable Buildings - Example:ICT

T-30A Prefabricated 30 Storey Hotel #2



The room controllers, together with energy and outdoor sensor inputs, are connected to a master computer, which also controls the centralised heating and cooling equipment.

Source: http://en.broad.com/uploads/pdf/tsjd.pdf

Smart Sustainable Buildings - Example: ICT

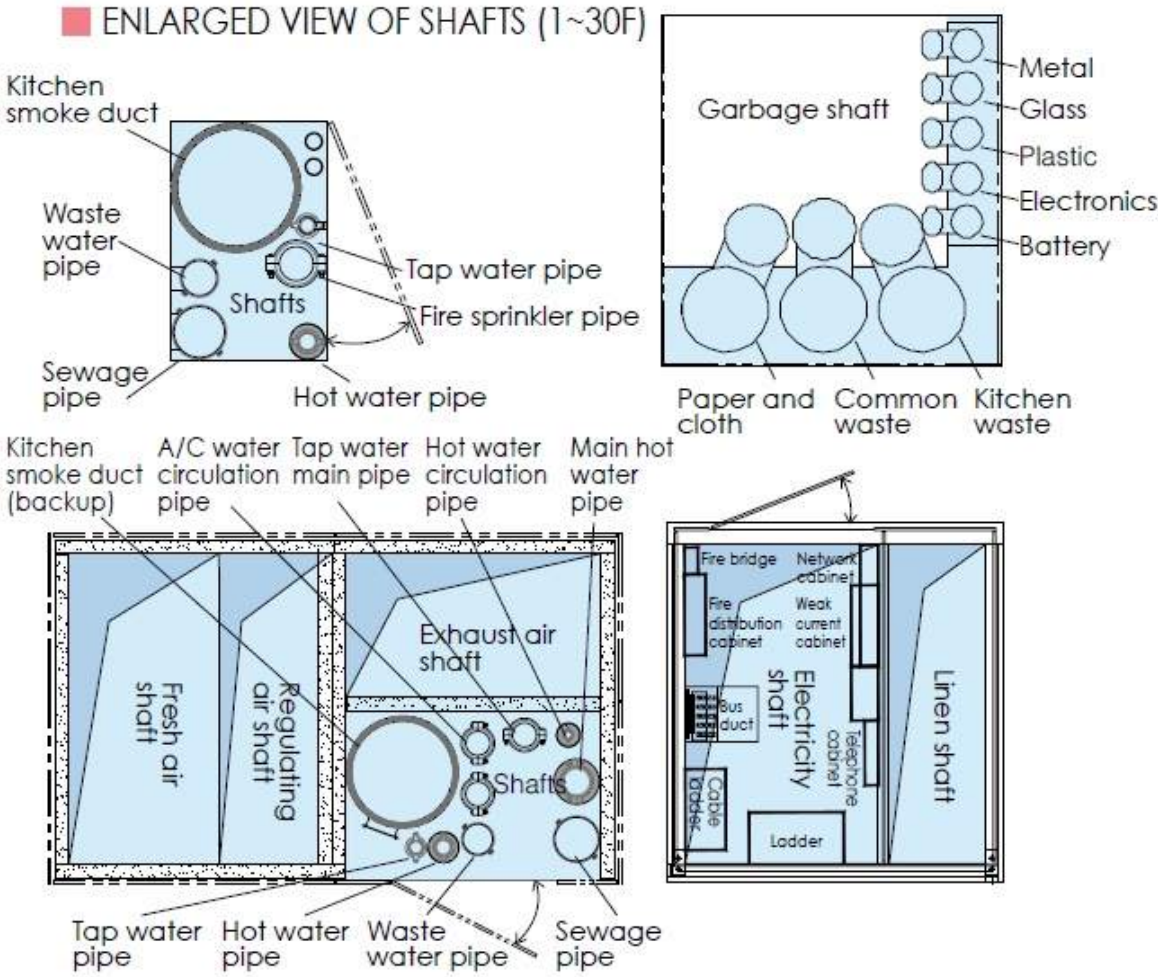
T-30A Prefabricated 30 Storey Hotel #3

The main service shafts are illustrated in the Technical Briefing

A wide range of environmental and user services can be seen.

This is “Vertical Infrastructure”

In a smart city how many services need to be carried by the “horizontal infrastructure”?



 – Source: http://en.broad.com/uploads/pdf/tsjd.pdf

Next:
Smart Water Management

Smart Water Management

- Three key water risks
  - shortage (including droughts)
  - inadequate quality
  - exceeding the capacity of the surface and groundwater drainage systems

Source: FG-SSC “Smart Water Management in Cities”, Page 3

SSC Water Services

- Raw water service
  - Diversion of raw water is necessary to facilitate treatment and distribution to a city's population. In some cities, retail water price includes water diversion project costs
- Water supply services
  - Provision of safe treated water to various sectors within the urban environment, including the residential, commercial, and industrial sectors
- Drainage services
  - Provision of urban drainage through pipe networks is important to safeguard public health and prevent flooding
- Wastewater treatment services
  - Provision of wastewater treatment for commercial/marketed services is necessary to ensure environmental protection.
- Reclaimed water service
  - Usually offered by the vast majority of sewage treatment companies as a value-added business to industrial customers/users such as power plants
- Other water supply services
  - The seawater desalination market is in transition from Engineering, Procurement and Construction (EPC) equipment provision to integral investment and operational service.

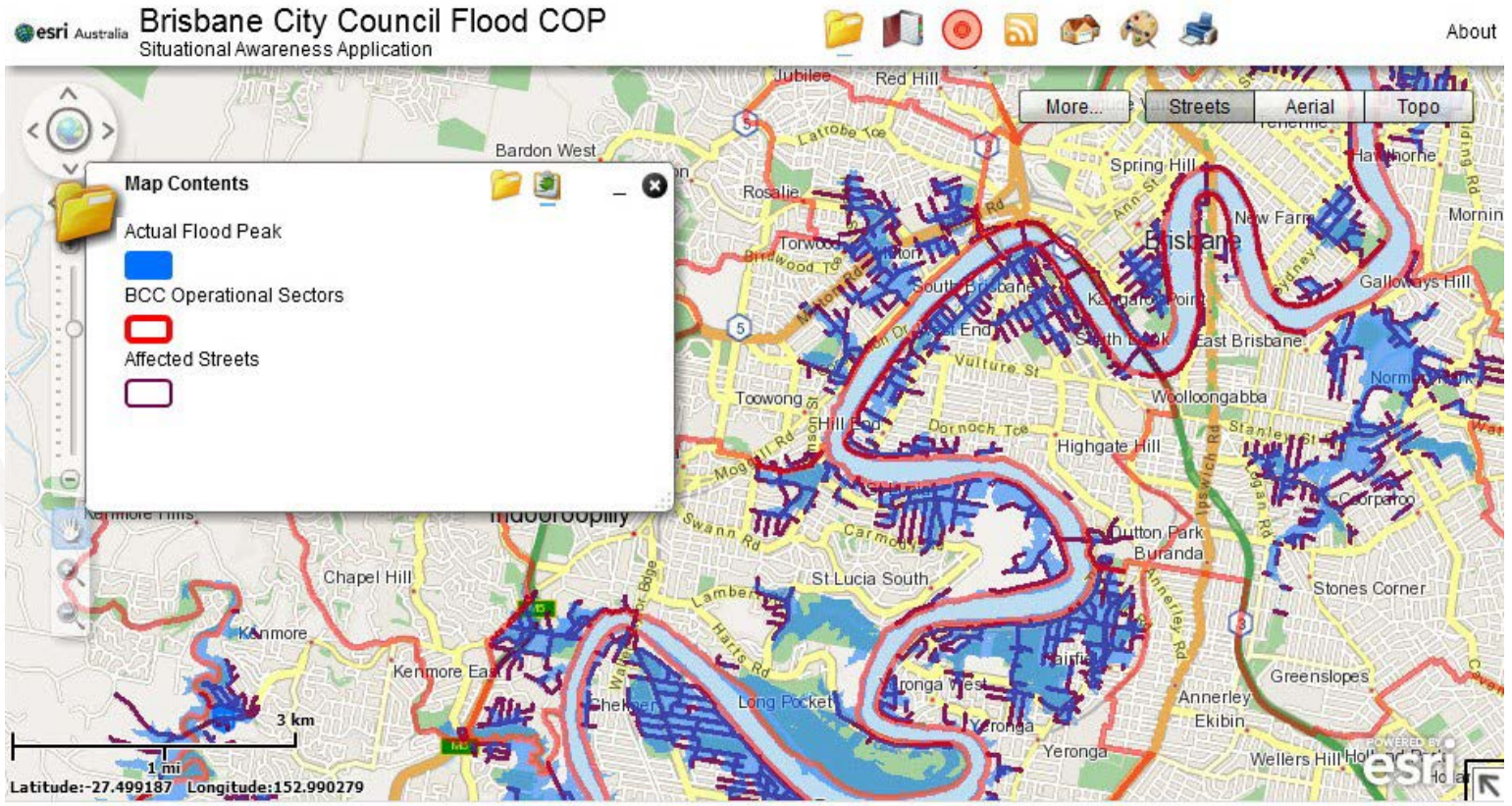
Source: FG-SSC “Smart Water Management in Cities”, Page 12

Smart Water Management (SMW) Tools

- SWM tools can be categorized in the six main areas
  - Data acquisition and Integration (e.g. sensor networks, smart pipes, smart meters).
  - Data Dissemination (e.g. radio transmitters, WIFI, Internet).
  - Modelling and Analytics (e.g. Graphical Information Systems).
  - Data processing and Storage (e.g. Cloud computing)
  - Management and Control (e.g. SCADA, Supervisory Control and Data Management)
  - Visualization and Decision Support (e.g. Web-based communication and Information systems tools)

Source: FG-SSC “Smart Water Management in Cities”, Page 20

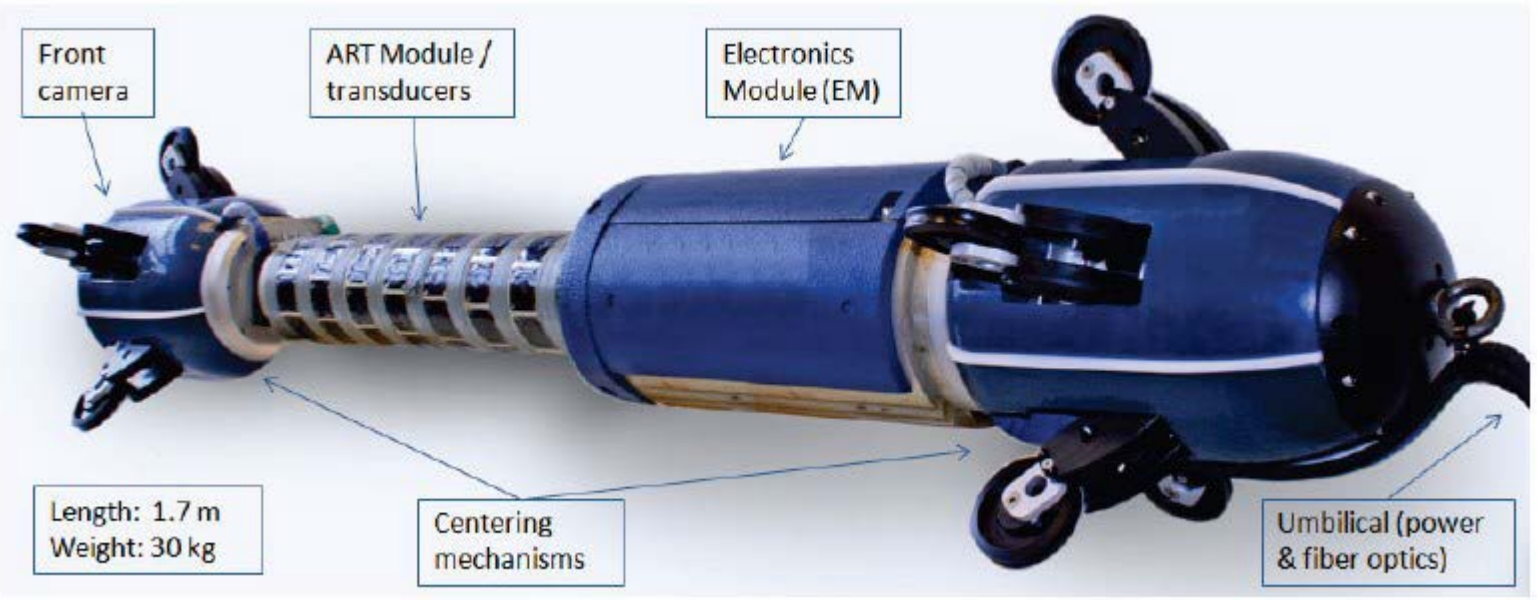
Smart Water Management Example



- This example provides citizens with an indication of flood risk
  - locations for remedial work or new building avoidance can identified

Sources: FG-SSC "Smart Water Management in Cities", Page 20 and
http://www.sweetmaps.com/blog/wp-content/uploads/2011/01/BCC_esri_flood_map.jpg

Example: Pipe Scanners



- 30% water worldwide is estimated to be lost though leaky pipes and theft
- This device uses acoustic resonance technology (ART) and cameras to detect leaks

Sources: FG-SSC "Smart Water Management in Cities", Pages 12, 31 and http://www.trust-i.net/downloads/index.php?iddesc=65

ITU-T Focus Group on Smart Water Management

- For more information read
  - reports being written by the Focus Group on Smart Water Management (FG-SWM)
    - This was established by the ITU-T TSAG meeting in Geneva, 4-7 June 2013
  - See
    - http://www.itu.int/en/ITU-T/focusgroups/swm/Pages/default.aspx

Source: FG-SSC "Smart Water Management in Cities", Page 1

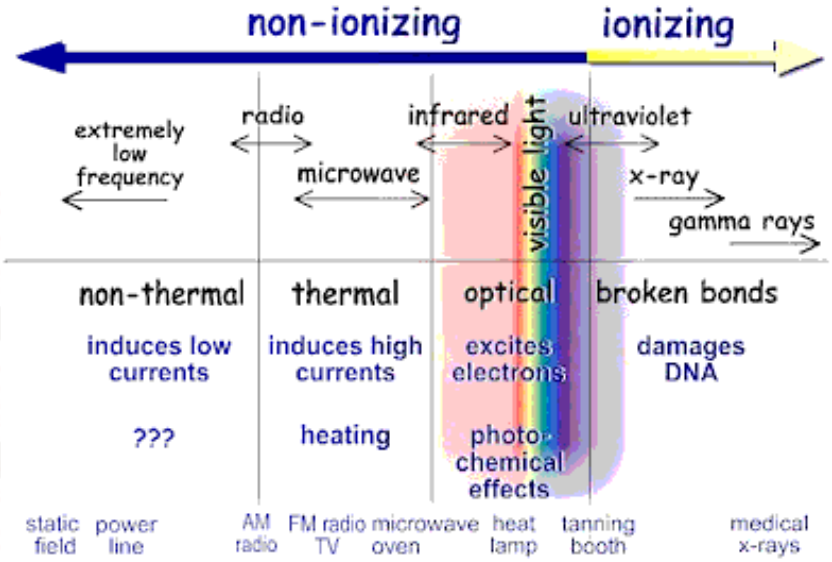
Next:
Electromagnetic Field (EMF) Considerations for SSCs

ICTs and EMF

- Scope
  - Electromagnetic fields (EMF) should be taken into account to ensure that the networks and connected devices operate safely and efficiently. These include
    - Mobile and in-building communication networks
    - Wireless networks for community services including
      - smart metering
      - remote health care and medical monitoring
      - smart cars
      - mobile education
      - smart homes and buildings

Source: FG SSC Report "EMF Considerations in Smart Sustainable Cities" page 1

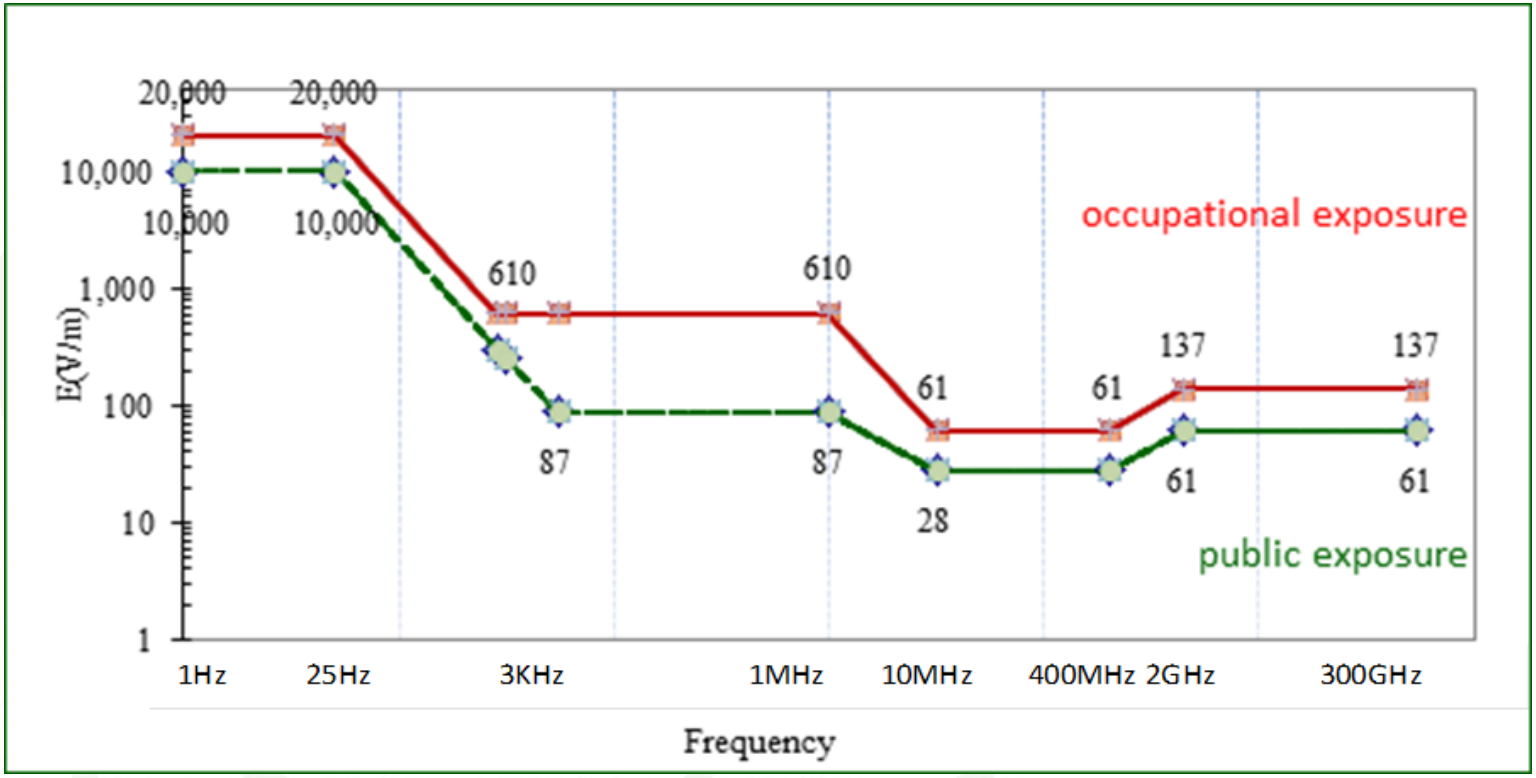
EMF and Health



- Extensive research has been carried out into EMF and health
  - The World Health Organization (WHO) encourages the adoption of exposure limits that provide similar levels of health protection for all people.
  - The International Commission on Non-Ionising Radiation Protection (ICNIRP) guidelines form the basis of WHO and ITU Recommendations to governments and have been widely adopted around the world.
  - The ICNIRP EMF Guidelines cover the frequency range 0-300 GHz which includes the frequency of all wireless ICT systems and devices.

Sources: FG SSC Report "EMF Considerations in Smart Sustainable Cities" page 27
http://en.wikipedia.org/wiki/Non-ionizing_radiation#mediaviewer/File:EM-spectrum.png

EMF Exposure Limits



- ICNIRP define the exposure thresholds. An example is shown above*
- The basic power restriction is expressed in Watt/kg. These are the fundamental limits while the reference levels are expressed in V/m, A/m or W/m2

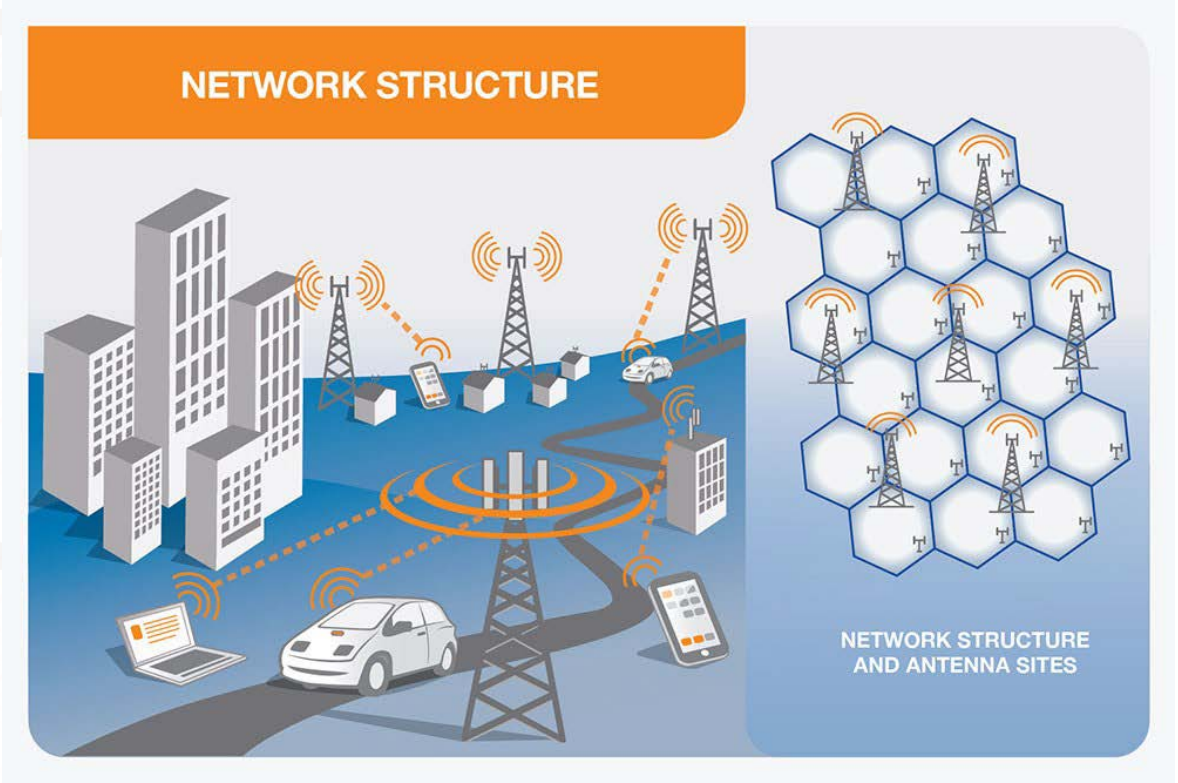
Sources: FG SSC Report "EMF Considerations in Smart Sustainable Cities" pages 19 and 20
*http://www.sviva.gov.il/subjectsEnv/Radiation/Radiation/non-ionising/Documents/RFCellularexposure.pdf

Community Information Consultation and Engagement

- In order to minimise risk to the implementation of wireless projects within a community the following steps should be considered
  - Build a working relationship with local stakeholders as a trustworthy and reliable party.
  - Ensure transparent information management in order to address concerns, reduce public scepticism and make the issues more understandable to the broader public.
  - Provide stakeholders with trusted sources of information, and/or foster a dialogue between the parties involved.
  - Emphasise the community benefits associated with improved mobile communications (or other radio communications projects)
  - Find ways of providing people with a sense of involvement in the project, in order to reduce their perception of being powerless

Source: FG SSC Report “EMF Considerations in Smart Sustainable Cities” page 37

Wireless ICT Network Infrastructure

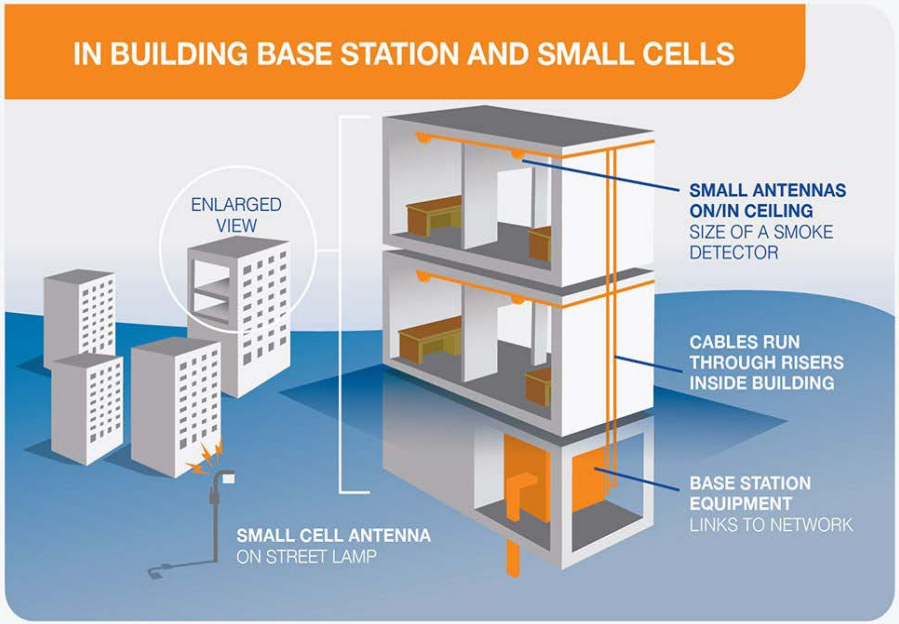


- Wireless infrastructure includes
  - devices, antennas, base stations and a backhaul network (e.g. access to telephony and global internet services)

Source: FG SSC Report “EMF Considerations in Smart Sustainable Cities” page 31

Wireless ICT Network
Achieving 'Full Coverage'

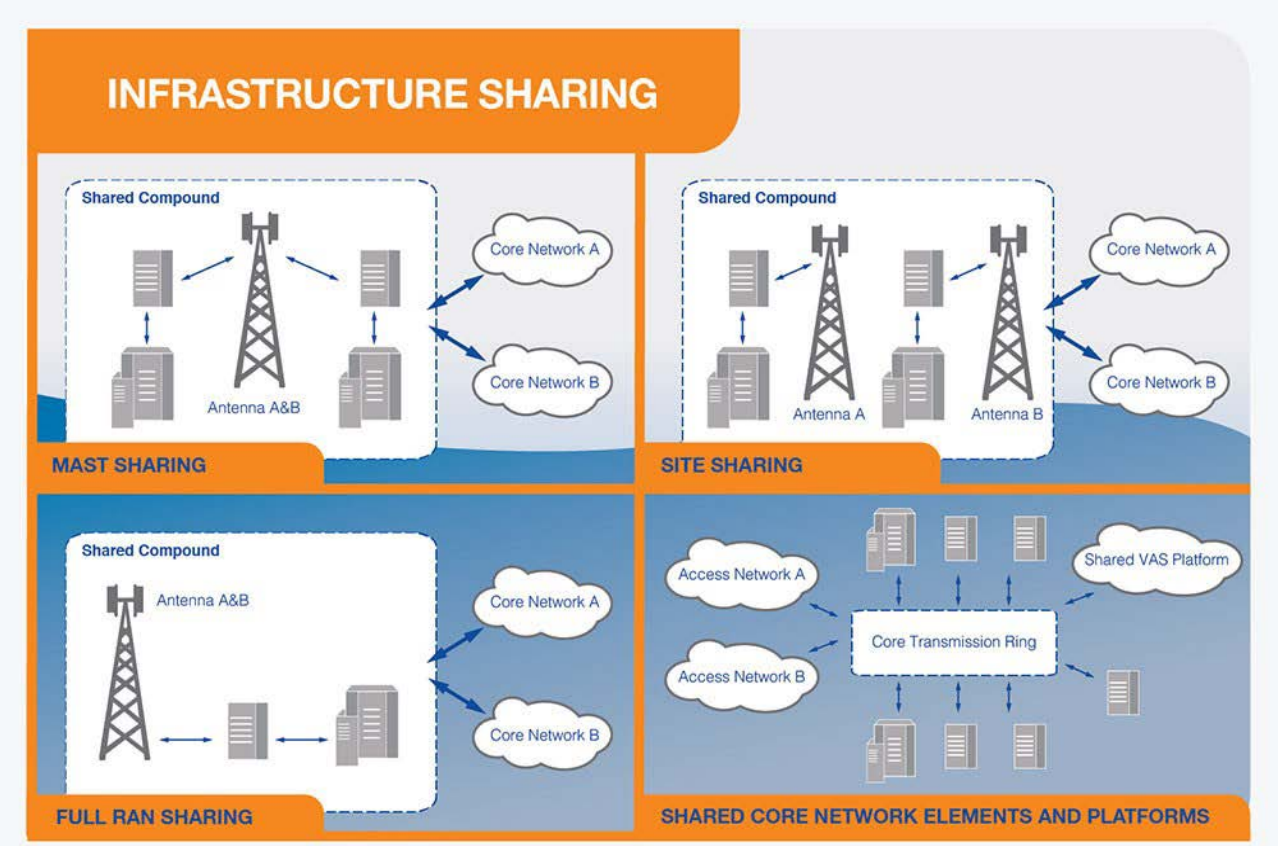
- Macro Base Station (Wide Area Network)
  - A Macro base station utilises antennas mounted on a tower, pole or building rooftop and typically covers a larger geographic area
- Small cells (e.g. street in radio shadow of a hill or tower block)
  - Small cells are low power base stations or antenna systems installed close to mobile terminal users to improve capacity on a small geographic area
  - Small cells are sometimes also referred to as micro, pico or feta cells.
- In-building base station sites
  - office buildings
  - shopping centres
  - apartments
  - underground railway systems
    - These systems are sometimes referred to as Distributed Antenna Systems (DAS) or small cell In-Building Coverage (IBC) and operate in a similar way to macro base stations but at much lower power levels.



Source: FG SSC Report "EMF Considerations in Smart Sustainable Cities" page 33

Infrastructure Sharing - wireless

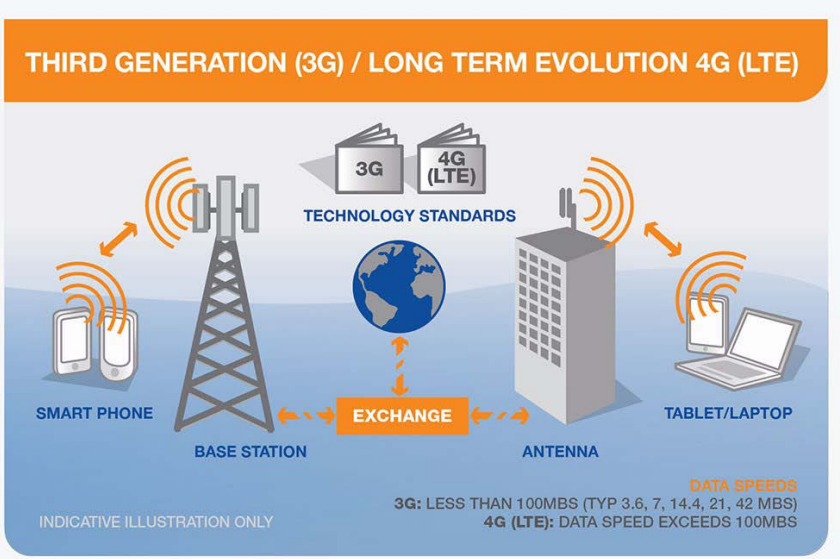
- May be between mobile operators and/or emergency services
  - Shares costs by leveraging existing technology to obtain a sensor layer network
  - demands more agreement between operators

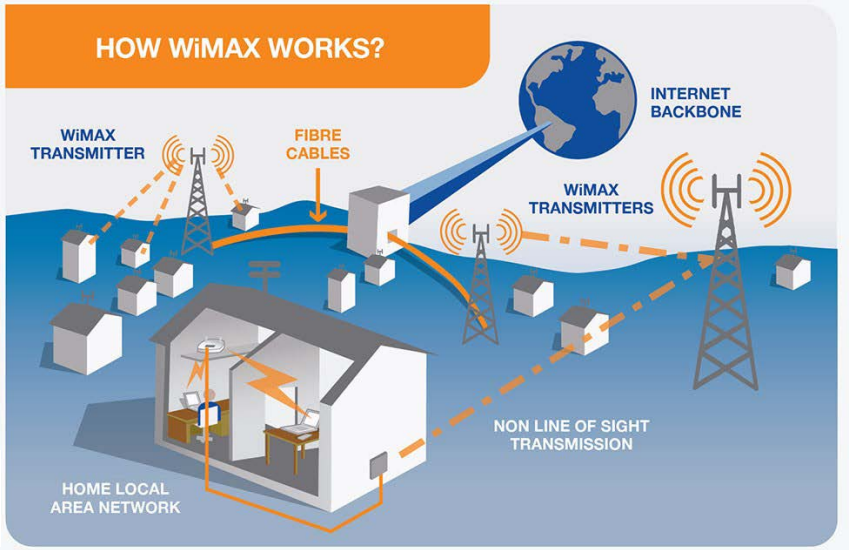


Source: FG SSC Report "EMF Considerations in Smart Sustainable Cities" page 34

Wireless Technologies #1

- Cellular Mobile technologies (for voice and internet access)
  - 4G LTE (Long Term Evolution) is the latest major enhancement to mobile radio communications networks
  - LTE is a standard that is part of the evolution of 3G, which incorporates significantly increased data rates to enhance the mobile broadband experience.
  - It should be noted that this improved level of service **can be** achieved without increasing the output power of the transmitters
- WiMax
  - The Worldwide Interoperability for Microwave Access (WiMAX) provides an alternative Internet wireless access technology to broadband cables and digital subscriber lines (or DSL)
  - Is aimed at providing wireless data over long distances in a variety of ways.
  - Uses (IEEE) 802.16 standards.

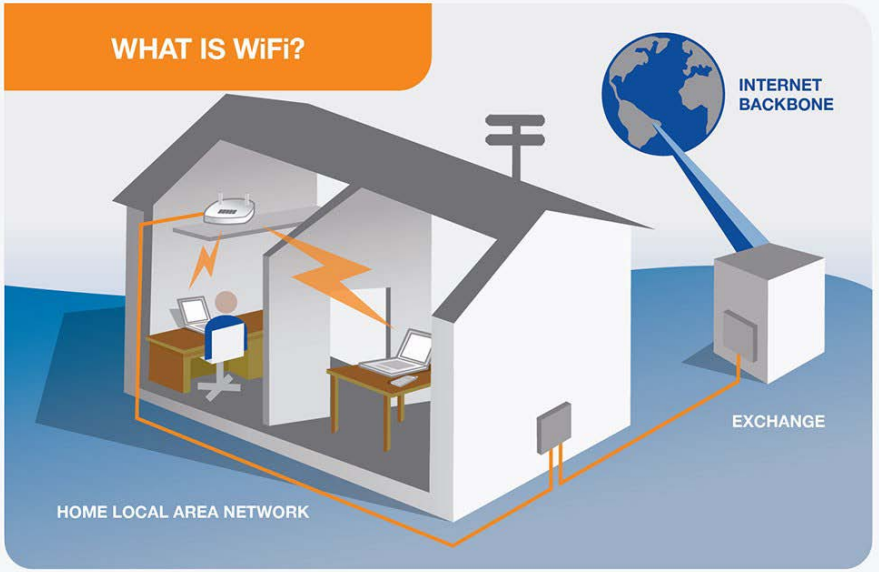


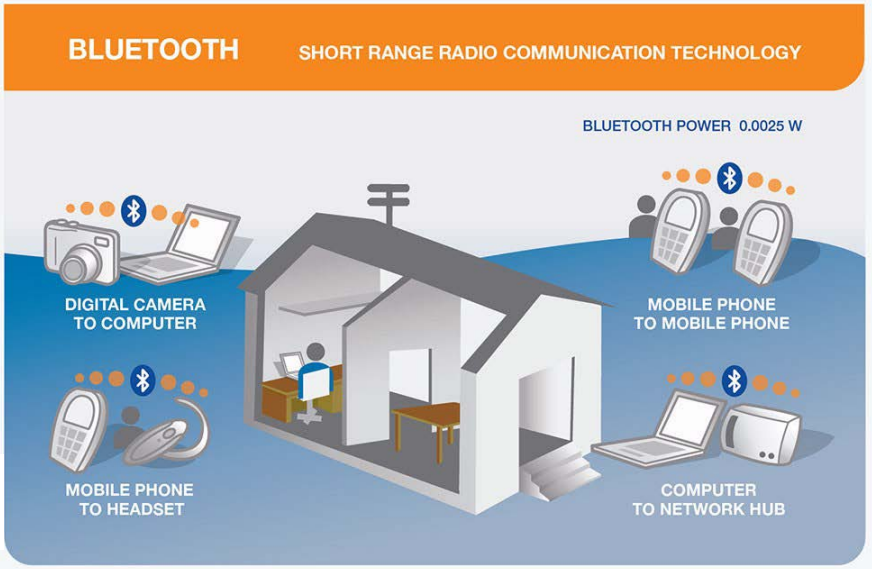


Source: FG SSC Report "EMF Considerations in Smart Sustainable Cities" pages 37-38

Wireless Technologies #2

- Wi-Fi
  - Wi-Fi is the term used to describe high speed wireless network connections over short distances between mobile computing devices (such as laptops) and the Internet
  - These are sometimes termed wireless local area networks (WLAN's) which are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards.
- Bluetooth
  - Bluetooth wireless technology is a short-range radio technology that uses radio frequency fields to transmit signals over short distances between telephones, computers and other devices
  - The technology offers simplified communication and synchronization between devices without the need for cables
- Zigbee (see slide 11)
  - Low power short range radio for sensor networks

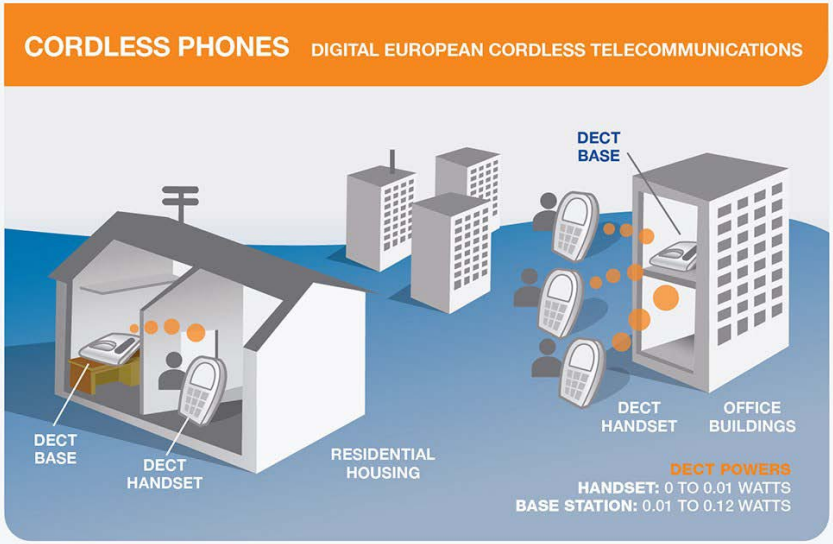




Source: FG SSC Report "EMF Considerations in Smart Sustainable Cities" pages 39 and 40

Wireless Technologies #3

- DECT
  - stands for Digital Enhanced Cordless Telecommunication
  - DECT is a common standard for digital cordless telephones and consists of a radio technology suited for voice, data and networking applications in residential, corporate and public environments
  - Many cordless phones used in residential properties use DECT technology.



Source: FG SSC Report "EMF Considerations in Smart Sustainable Cities" page 41

Example: Off-Grid Base Station and a Green Energy Solution

35,000 Green Sites and Counting

Indus Green Site

A PIONEERING DIESEL-FREE INITIATIVE IN THE TELECOM INDUSTRY

Indus has created 35,000 Green Sites where Zero diesel is used

"Launched in Aug 2011, the Indus Towers Green Sites Project flagged off with 6 major cities - Mumbai, Kolkata, Ahmedabad, Chandigarh, Palanpur & Gandhinagar – being declared Green. Green Cities were those cities with telecom sites within the limits of the Municipal Corporation, where no diesel would be consumed for cell site operations".

Source: http://www.industowers.com/green-sites.php

ITU ACADEMY

EMF Checklist

The 'Smart Sustainable City EMF Checklist' is designed to provide an easy to use reference for city officials and planners in order to ensure that smart city ICT designs using wireless systems operate efficiently and in compliance with EMF exposure standards.

Note that this is an example to illustrate the scope of a checklist covering safety and planning and needs to operate with national regulatory requirements

Source: FG SSC Report "EMF Considerations in Smart Sustainable Cities" page 54 Annex 1

#	Smart Sustainable City - EMF Checklist	check
1	**EMF Compliance Framework**	
	Ensure that an EMF compliance framework is established to protect the general public and workers from the adverse effects of EMF	Y/N?
2	**ICT devices meet ICNIRP RF EMF exposure guidelines**	
	Ensure that devices are assessed for compliance with the public exposure guidelines	
3	**Wireless networks meet ICNIRP RF EMF exposure guidelines**	
	Ensure that the network sites are assessed for compliance to the ICNIRP guidelines, and that access controls and safety procedures are in place for working at antenna sites	
4	**Document RF EMF Compliance**	
	Ensure that the EMF compliance for ICT devices and networks is documented	
5	**Base station antennas are selected to suit the ICT network requirements**	
	Ensure that the appropriate base station antennas are used to improve ICT efficiency, provide services and integrate with the environment	
6	**Wireless network antennas are located in close proximity to the ICT devices**	
	Ensure that network and base station antennas are located where the ICT devices are being used	
7	**Planning legislation incorporates ICT networks and antenna requirements -**	
	Ensure more efficient deployment of ICT systems through a consistent approach to planning approval	
8	**EMF ICT compliance information is available**	
	Ensure that EMF compliance information is available to the public and other interested stakeholders	
9	**General EMF Information is available to the community**	
	Ensure that the references for EMF information are the WHO and ITU resources	
10	**Existence of Wireless Network Information Program**	
	Ensure availability of information about the operation of wireless networks based on credible sources and using appropriate communication channels addressing compliance, health concerns and siting	

Next:
ICTs for Climate Change Adaptation in Cities

Climate Change risks, vulnerabilities and impacts in cities

- A City's sectors are interconnected
  - a failure in one sector because of an extreme event could have a 'domino effect' on other sectors and cause economic loss

- Climatic changes such as variation in rainfall or temperature patterns and sea level rise are having an impact on development dimensions such as
  - agricultural production and the food supply chain
  - water supply
  - health issues and disease proliferation

Source: FG-SSC "Technical Report on ICTs for Climate Change Adaptation in Cities", page 10

Example: Climate Change Adaptation Plans

- It is a United Nations Framework Convention on Climate Change (UNFCCC) requirement for countries to have a National Climate Change Adaptation Plan
- In developing its climate change strategy, the Durban Municipality in South Africa identified a set of ten interrelated climate change response themes:
  - water, sea level rise
  - biodiversity
  - food security
  - health
  - energy
  - waste and pollution
  - transport
  - economic development
  - knowledge generation and understanding
- Note that Climate Change Adaptation strategy includes the same sectors as the smart sustainable cities-but takes a long term view to 2100
- The response includes the development of an implementation framework, and a monitoring and evaluation system

Source: FG-SSC "Technical Report on ICTs for Climate Change Adaptation in Cities", page 15

Example: Use of ICTs for Disaster Early Warning

- Disaster Early Warning Network (DEWN), Sri Lanka
  - A public/private partnership delivered it
  - Multiple technologies were adopted
    - cellphones and alarm devices
    - cell broadcast (CB) and short message service (SMS) were specially developed for this initiative
  - The Disaster Management Centre (DMC)
    - receives early warning information from recognised technical agencies
      - floods, landslides, earthquakes and tsunamis
    - verifies the emergency situation and then issues alerts. Emergency personnel first followed by public alerts
  - It generates mass, personneldirected or locationbased alerts
    - DEWN2 is being developed for smart-phones

Source: FG-SSC "Technical Report on ICTs for Climate Change Adaptation in Cities", page 21

Next:
Integrated Management for SSCs

Objectives

- To integrate and process peoples' needs
  - Using Software Objects
  - Via Software Events
- To serve the Environment

Current Management Situation

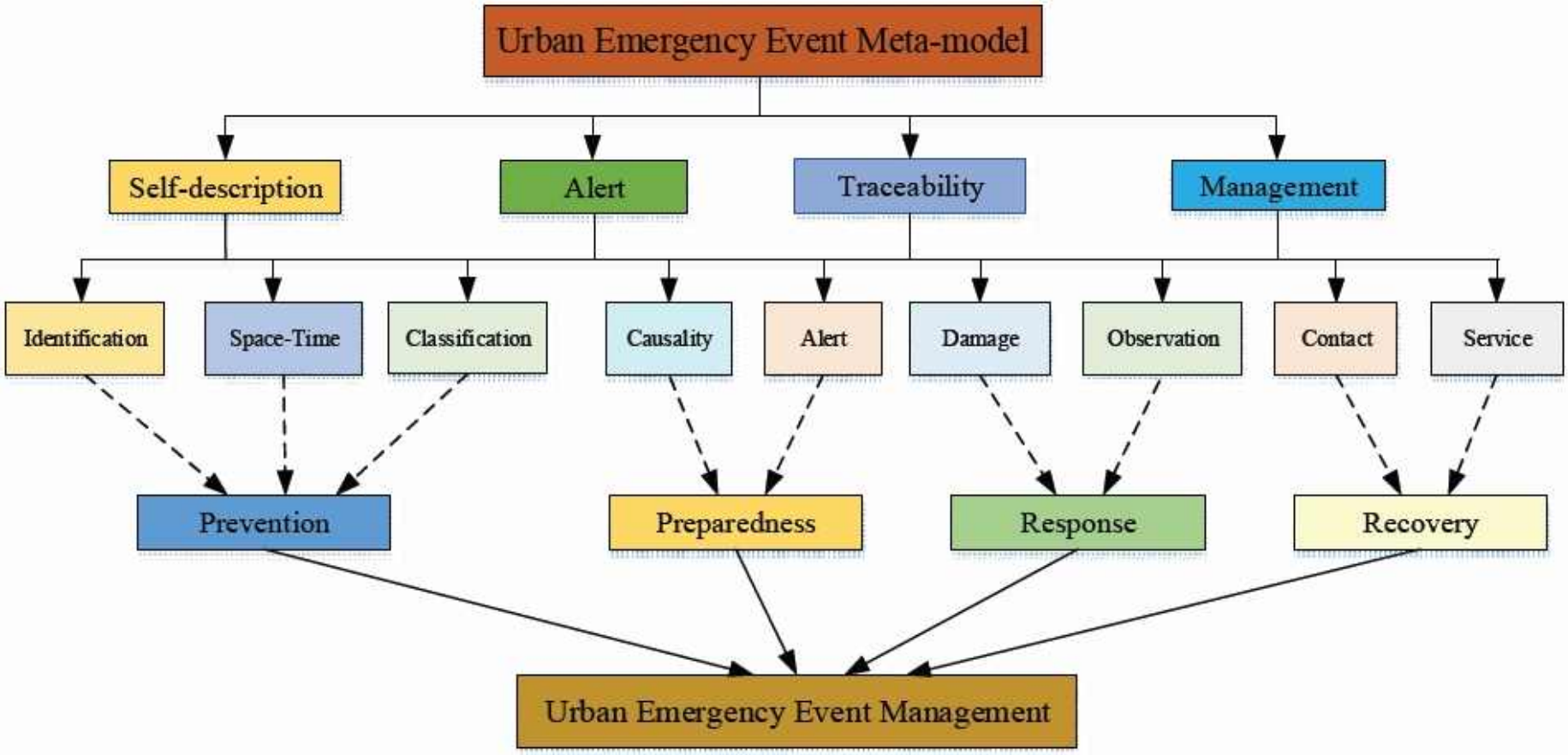
- Diverse requirements and information sources
- A passive information service (i.e. requiring human interactions)

- There is a need for unified service interfaces to enable active (automated) decision making and alerts
  - A standard set of interfaces, metadata (data about data) and processing steps are needed which can be applied to all ICT environments

Source: FG-SSC 'Technical report on Integrated Management for Smart Sustainable Cities", page 8

Example of Event Meta-model

- A flow diagram showing an automated event- management system is shown below



Source: FG-SSC 'Technical report on Integrated Management for Smart Sustainable Cities", page 21

Management Summary

- A standard set of interfaces, metadata and processing steps are needed which can be applied to all city ICT environments

Source: FG-SSC 'Technical report on Integrated Management for Smart Sustainable Cities", page 36

Next:
Anonymization Infrastructure and Open Data

Open Data

- Definition
  - Open data is the idea that certain data should be freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control

Source: http://en.wikipedia.org/wiki/Open_data

Data "Anonymization"

- Definition
  - Data anonymization is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous

Source http://en.wikipedia.org/wiki/Data_anonymization

Open Data Types

- Open Scientific Data (OSD)
  - In 2004, the Science Ministers of all nations of the OECD signed a declaration which essentially states that all publicly funded archive data should be made publicly available
- Open Government Data (OGD)
  - Open government data (OGD) is an important part of open data which can be traced back to the 2003 Public Sector Information Directive by The European Commission
- Open Industrial, Open Personal and Open Enterprise Data
  - are topics under study

Source: FG-SSC report "Technical Report on Anonymization Infrastructure and Open Data in Smart Sustainable Cities", Page 6

Motivation for Open Data in a SSC

- Governments may choose to publish open data to maximize public reuse
  - To strengthen transparency
  - To promote efficiency and effectiveness in administration
  - To release potential to create economic opportunity
  - To improve citizens' quality of life

Source: FG-SSC report "Technical Report on Anonymization Infrastructure and Open Data in Smart Sustainable Cities", Page 6

The Technology of Open Data #1

Metadata

Name:	**Introduction to Connexions**
ID:	m10884
Language:	English (en)
Summary:	An overview of Connexions, the Connexions home page, navigation tools, and accounts.
Subject:	Science and Technology
Keywords:	author, bug, connexions project, general information, home page, instructor, log in, report, student
License:	Creative Commons Attribution License CC-BY 1.0
Authors:	Mark Husband (mshusband@comcast.net)
Copyright Holders:	Mark Husband (mshusband@comcast.net), Connexions (cnx@cnx.org)
Maintainers:	Mark Husband (mshusband@comcast.net), Adan Galvan (agalvan@gmail.com), Kyle Barnhart (barnhart@rice.edu), Connexions (cnx@cnx.org)
Latest version:	2.26 (history)
First publication date:	Oct 7, 2002 12:00 am GMT-5
Last revision to module:	Aug 13, 2009 11:16 am GMT-5

- Metadata
  - Metadata is "data about data", which facilitates the understanding, usage and management of data, by humans and computers
  - Metadata summarizes basic information about data, which can facilitate finding and working with particular instances of data, but not the content of the message in the packet or container
  - (One example of Metadata is the size of the file in bytes)
- International standards
  - Are still at an early stage
  - ISO/IEC 11179-1:2004 only covers the definition of metadata and does not address the structuring of metadata storage or retrieval, nor administrative standardization

Source: FG-SSC report "Technical Report on Anonymization Infrastructure and Open Data in Smart Sustainable Cities", Page 20

The Technology of Open Data #2

- Linked Data
  - enables data from different sources to be connected and queried
  - public and private organizations as well as individuals contribute their data according to Semantic Web standards
  - developers can query Linked Data from multiple sources at once and combine it 'on the fly'
    - (Enables queries such as "Are there likely to be free seats on my train" to be performed as you travel)
- Data visualization
  - allows people understand data clearly using tables, maps, charts etc.

Source: FG-SSC report "Technical Report on Anonymization Infrastructure and Open Data in Smart Sustainable Cities", Page 22

The Technology of Open Data #3

- Social Networks
  - Allow people to create a personal profile
  - People are no longer anonymous and can access databases via service providers such as Facebook, Twitter, LinkedIn, Pinterest, GovLoop, MySpace, and Friendster
  - Subscribers may view the connections made by other people in the network
  - Governments have seen social networks and media-sharing as ways to disseminate the same information to different individuals and social groups
  - Government agencies are now using social networks approaches to promote access to and usage of open data
  - Cisco forecasts that by 2020, there would be 50 Billion 'things' connected to the Internet, including PCs, mobile, TVs, cars, vending-machines, cameras, alarm clocks, even cattle etc.
    - (New types of 'Social Network' are likely to apply to IoT)

Source: FG-SSC report "Technical Report on Anonymization Infrastructure and Open Data in Smart Sustainable Cities", Page 24

The Technology of Open Data #4

- Anonymization techniques
  - Replacement
    - Substitute identifying numbers
  - Suppression
    - Omit from the released data
  - Generalization
    - Replace birth date with something less specific, like year of birth
  - Perturbation
    - Make random changes to the data

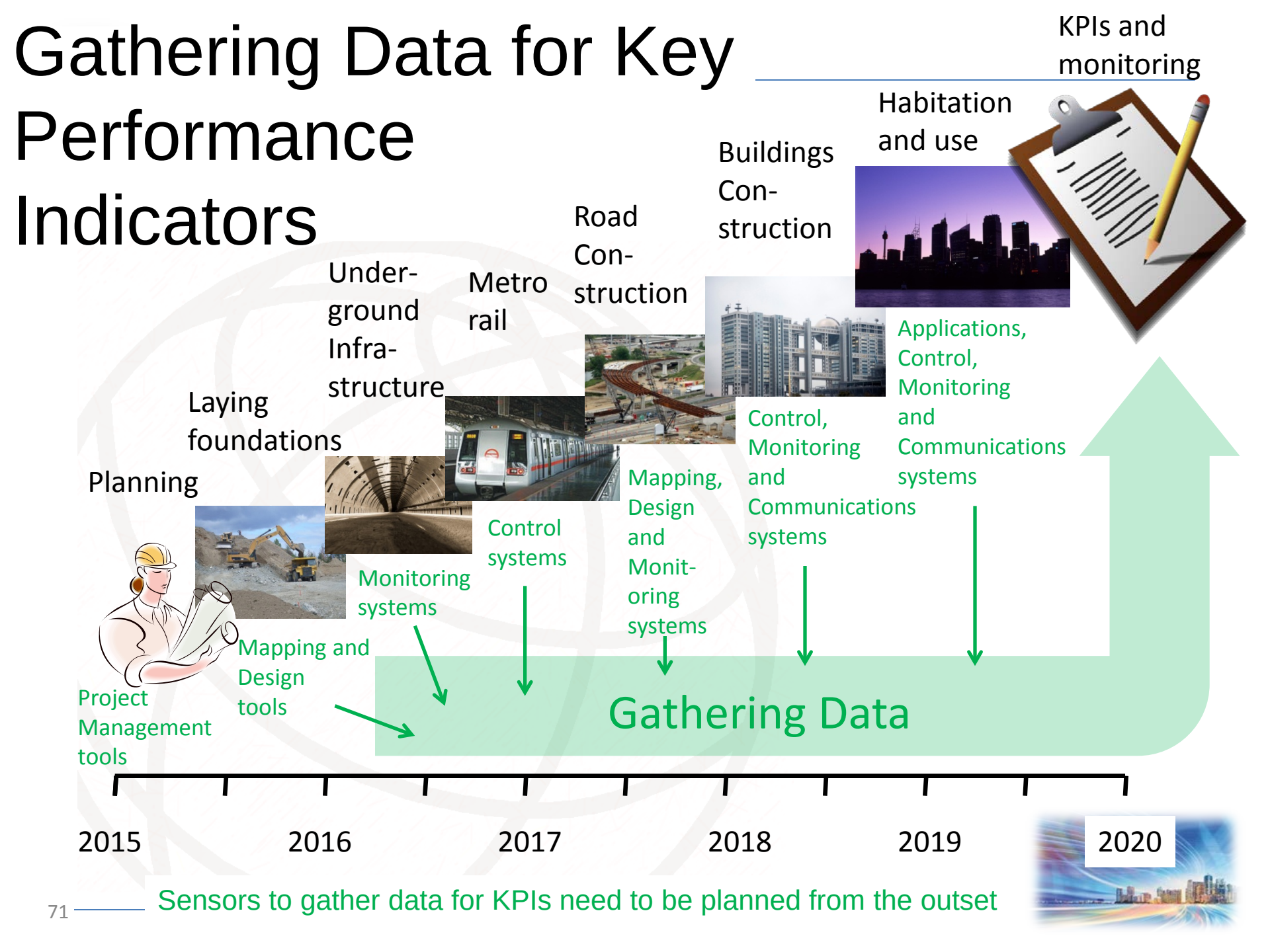
Source: FG-SSC report “Technical Report on Anonymization Infrastructure and Open Data in Smart Sustainable Cities”, Page 36

Open Data Quality Requirements

Data Quality	Characteristics	Example Metric
Accuracy	Is the data free from error?	Percent of values that are correct when compared to the actual value
Completeness	Is all the data present?	Percent of data fields having values entered into them
Consistency	Does all the data line up? Is it consistent?	Percent of matching values across tables/files/records.
Timeliness	Is the data up to date? When was it recorded?	Percent of data available within a specified threshold time frame
Uniqueness	Is the data duplicated?	Percent of records having a unique primary key
Validity	Is the data classified correctly?	Percent of data having values that fall within their respective domain of allowable values

Source: FG-SSC report "Technical Report on Anonymization Infrastructure and Open Data in Smart Sustainable Cities", Page 26

Gathering Data for Key Performance Indicators



Sensors to gather data for KPIs need to be planned from the outset

Conclusion

- For smart sustainable development a sensor network is needed in addition to traditional telecommunication networks
- Planning from the outset and infrastructure sharing are key to saving cost
  - Both physical and electronic
  - Existing communication networks should be exploited
    - both fixed and wireless
  - Sensors need adding at the ‘edge’ to gather data needed to monitor and manage essential services
    - Electricity, water, transport, etc.
    - In some cases a smart-phone may be used as both a sensor and an output device
    - In other cases a dedicated wired or wireless link will be needed to connect the sensors

davewfaulkner@gmail.com