The Regulatory Environment for Emerging Technologies in Fire Safety for USA and Europe

Lance Rütimann + Maria Marks
Siemens Smart Infrastructure

NFPA SUPDET®
SEPTEMBER 17–20, 2019
DENVER, CO

Introduction

Fire and Life Safety systems are growing up and leaving the house. They are reaching to the “clouds” to share information on their performance, availability, maintenance needs and more. In doing so they learn from other systems enabling actions such as automatic improvements. They will communicate to service organisations their needs for attention with details based on their analysis, providing recommendations on how to address it.

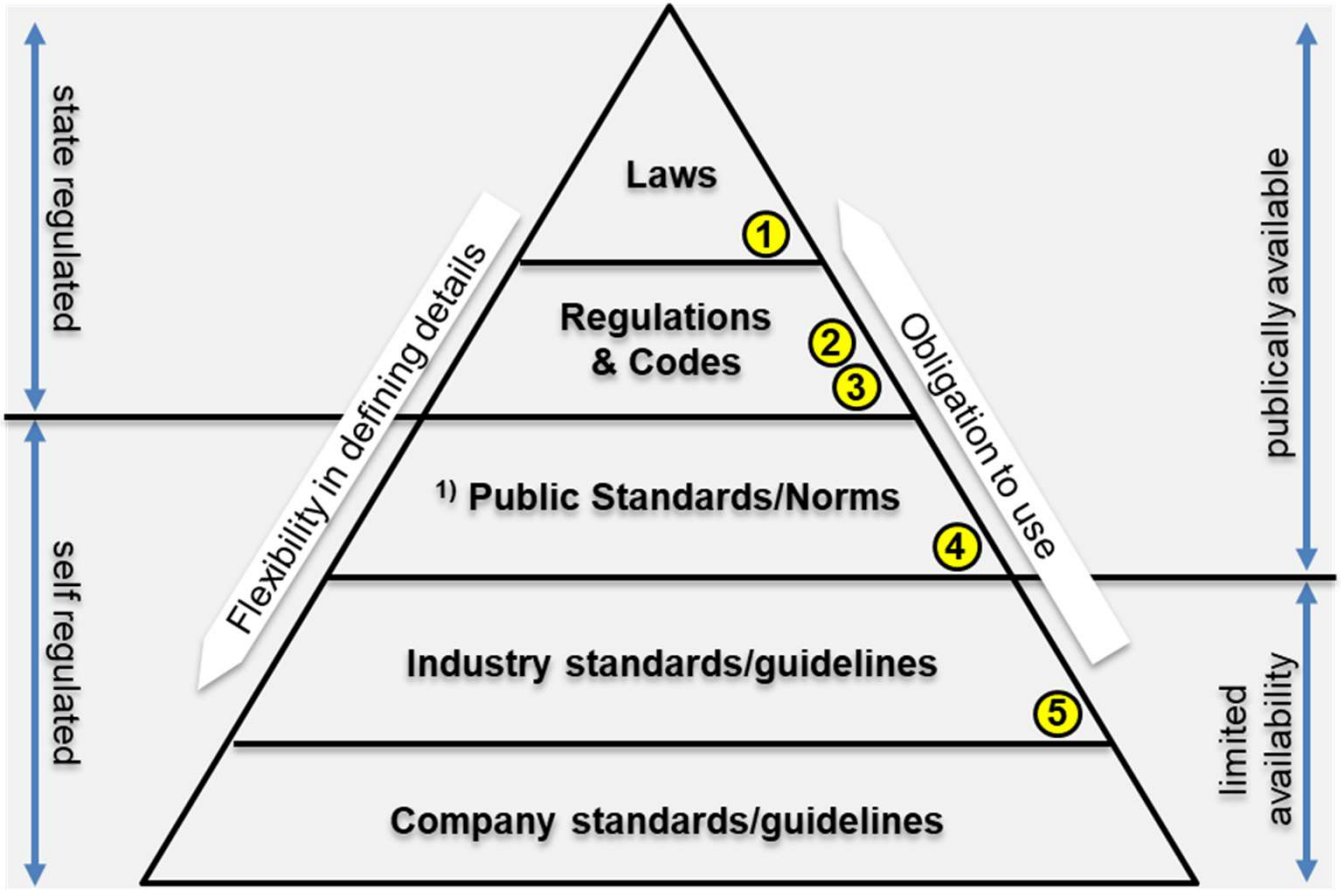
This description does not come as a surprise to anyone that has been following the developments in Information Communication Technology (ICT). What is important for this audience is that the things finding their way into existing building technologies will not stop at fire safety systems. As outlined in SUPDET presentations in the past few years, there are advantages for building owners and those responsible for the safe and secure operation of the buildings. We are on a path to self-sustaining buildings. On our way there, the framework to make this happen in a safe and secure manner must be developed.

Introduction

The fire safety industry has already stepped into the arena and invested heavily in understanding the emerging technologies. We are quite busy defining what terms such as cloud, edge, AI and others will/could mean for customers and suppliers, but also for standardisation and regulation. The latter is a challenge that has been accepted. But with respect to the regulatory and normative framework, where are we standing and what is the end in mind?

The objective of this presentation is to provide an overview of what is happening in the USA and Europe in the area of macro-environmental developments; in other words, standards, regulations, directives and similar. The audience can expect to take out of the discussion a better view of the defining framework, that will impact the design and application of emerging technologies. Further, this shall be an impulse to actively participate.

Terminology



Laws (Legislation) 1
- directive proposed by a legislative body
- internally generated within a government
- legally mandatory

Regulations 2
- legally mandatory requirement with details on enforcement of legislation
- may be internally or externally generated, especially pertaining to certain industry

Codes 3
- a type of legislation that purports to exhaustively cover a particular area of law
- can reference in part or whole to a standard
- usually legally mandatory

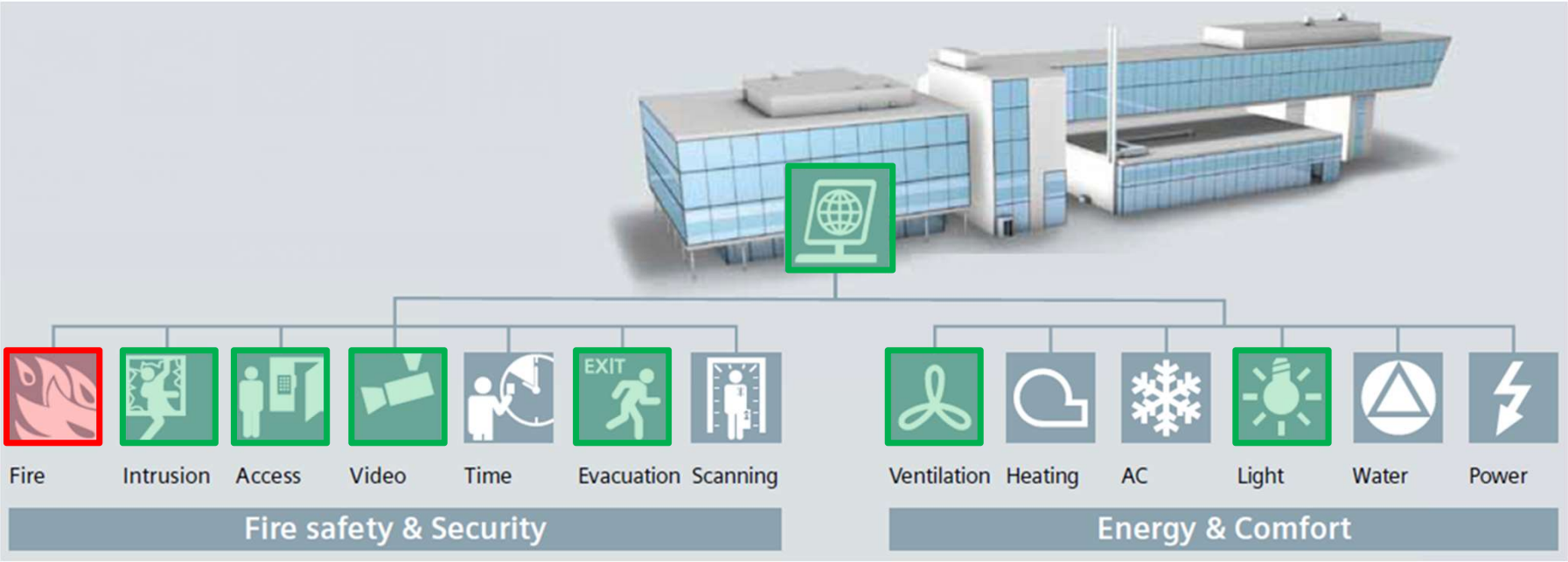
Public Standards/Norms 4
- defined set of definitions and requirements for products, systems, procedures, etc.
- created by recognised bodies such as ISO/IEC, CEN/CENELEC, UL/ULC or national organisations
- mostly voluntary

5

Industry standards/guidelines
- usually developed and published by industry associations
- can also be called Codes of Practice
- voluntary

What is the future of fire safety systems?

View a building as an accumulation of functions with processes enabling pre-defined activities to take place inside and around it.



What is the future of fire safety systems?

- New requirements on skill sets, tools, education
- Multi-disciplined teams with higher levels of collaboration
- Execute project phases in parallel vs. sequential

Analysis of current regulatory developments

1. The following slides address four aspects of emerging technologies in the following order:
   - Interoperability
   - Internet of Things (IoT)
   - Artificial Intelligence (AI)
   - Cybersecurity

2. For each technology, the following is addressed:
   - Definitions
   - Comparison USA and Europe
   - Status, Concerns, Industry Objectives

3. Summary conclusions for Regulatory Measures in respect to Emerging Technologies in Life Safety

Interoperability
Policy and Standards Development

Definition

ability of a system to work with or use the parts or equipment of another system

Source: https://www.merriam-webster.com/dictionary/interoperability

Overview USA

- Bicsi 007
- NFPA
- UL

Overview Europe

- EN54 Part 13
- national application guidelines

Interoperability
Basis for regulatory considerations

Status

- Standards in development or already published addressing either:
  - connecting different components together into one system
  - different systems work together as a whole

Concerns

- managing system performance, cybersecurity, exchange of data, glitches, software updates/upgrades
- avoidance of conflicting standards
- verify conformity with applicable standards
- design, install, commission, operate and maintain the system as a whole in a conform manner

Industry Objectives

- understand what interoperability is in terms of life safety and what it means for our industry
- guidelines on how to apply interoperability within our regulatory environment

Internet of Things (IoT)
Policy and Standards Development

Definition:
The networking capability that allows information to be sent to and received from objects and devices using the internet. *Source - www.merriam-webster.com/dictionary/Internet%20of%20Things*

Overview USA
- ANSI
- IEC - TC65
- IEEE
- NIST
- NEMA
- Oasis

Overview Europe
- IETF – IoT Directorate
- ISO/IEC JTC1
- IEC - TC65

Internet of Things
Basis for regulatory considerations

Status

- The Industry has started a discussion about how and where IoT can be used.
- Cyber security legislation is being enacted on a state by state basis (US) for any device that has the potential to connect to the IoT

Concerns

- Managing system performance, cybersecurity, exchange of data, glitches, connectivity
- Avoidance of conflicting standards
- Ability to design, install, commission and maintain the system as a whole with the expected results

Industry Objectives

- Understand how the Internet of Things impacts Life Safety and what it means for our industry.
- Guidelines for how to leverage the Internet of Things in our regulatory environment

Artificial Intelligence (AI)
Policy and Standards Development

Definition

The ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings. *source www.britannica.com/technology/artificial-intelligence*

Overview USA

- Company specific soft initiatives (e.g. Google, Microsoft, IBM)
- IEEE
- Partnership on AI
- TIA

Overview Europe

- ETSI
- European Commission
- House of Lords (UK) - Code of Conduct
- IEC - Seg10
- ITU

Artificial Intelligence (AI)
Basis for regulatory considerations

Status

- Activities and discussions on creating a basis for the ethical use of AI for the good of society and not against it
- Different countries and regions actively promoting themselves for development of AI

Concerns

- Managing system performance, cybersecurity, glitches, exchange of data
- Balance between technological advances and ethical & societal issues

Industry Objectives

- Guidelines for how to leverage Artificial Intelligence in the current/ future regulatory environment

Cybersecurity
Policy and Standards Development

Definition

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack. *source www.merriam-webster.com/dictionary/cybersecurity*

Overview USA

- ANSI
- Charter of Trust
- IEC – TC65
- NERC
- NIST
- UL

Overview Europe

- Charter of Trust
- ENISA
- ETSI
- ISO/IEC
- ITU

Cybersecurity
Basis for regulatory considerations

Status

- In the EU there is legislation for the protection of data (GDPR) and ENISA has been designated to achieve high common level of cybersecurity.
- In the US, states are adopting legislation to provide reasonable cybersecurity for devices capable of connection to the internet

Concerns

- Ongoing "maintenance" needed to update systems for cybersecurity concerns
- The impact of Cybersecurity on system stability & speed of response

Industry Objectives

- Understand how Cybersecurity impacts the life safety environment without impacting response time
- Guidelines for how to apply Cybersecurity protections in the current regulatory environment

Summary Conclusions for Regulatory Measures in respect to Emerging Technologies in Life Safety

We need to …

1. build up and maintain our knowledge on the regulatory developments of emerging technologies.
2. recognise which emerging technologies are affecting or potentially will affect life safety systems and solutions.
3. learn how to apply emerging technologies within our regulatory environment, without adding levels of complexity or decreasing the effectiveness of life safety systems.
4. keep an ongoing dialogue on what these emerging technologies mean for our industry and our clients.
5. ask the question whether our existing regulatory environment is fit for the digital future and look for acceptable and reasonable answers.