Impact of Standards on Systems Engineering

Ken Zemrowski

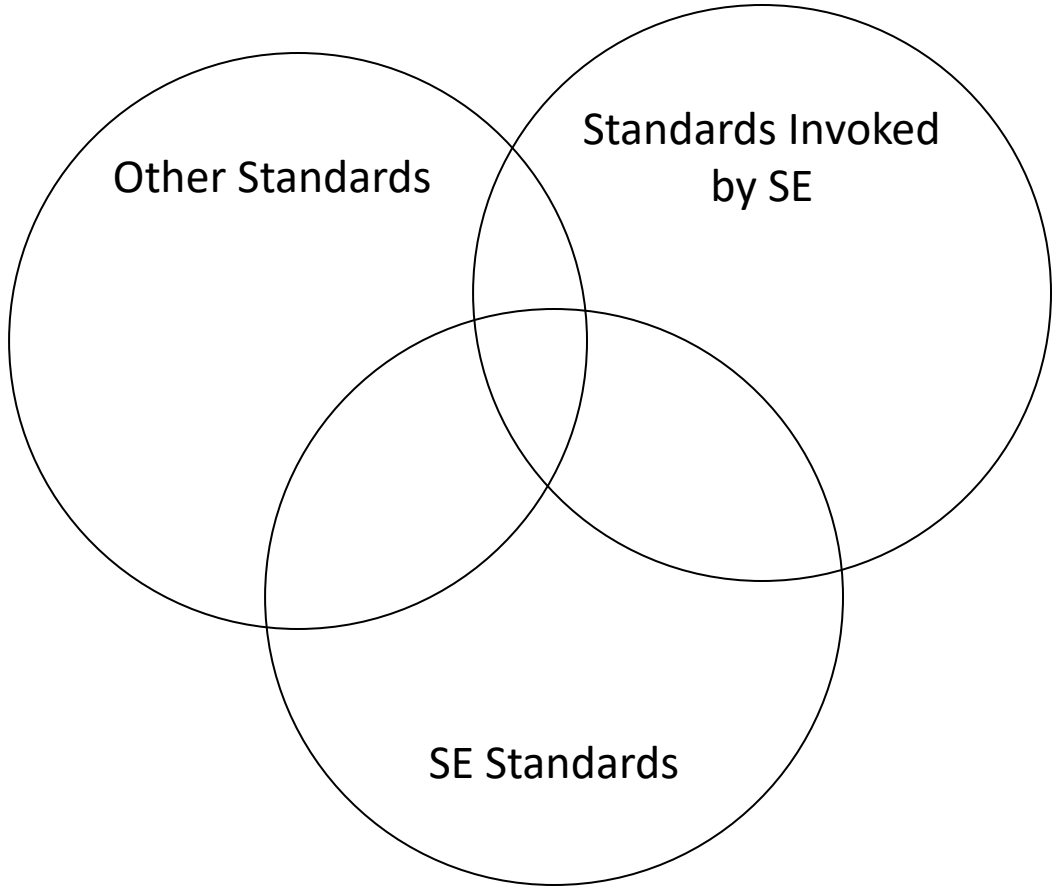
2016-11-16

INCOSE

Standards affect the practice of SE

- Standards such as ISO/IEC/IEEE 15288 establish a common base for SE, as well as a foundation for assessing competency.
- Other standards promote the usability of SE tools, from a knowledge perspective and tools being able to work together.
- Standards also affect the systems we engineer; standards can impose requirements but can also help systems work together, such as interface protocols.

The Roles of Standards in SE



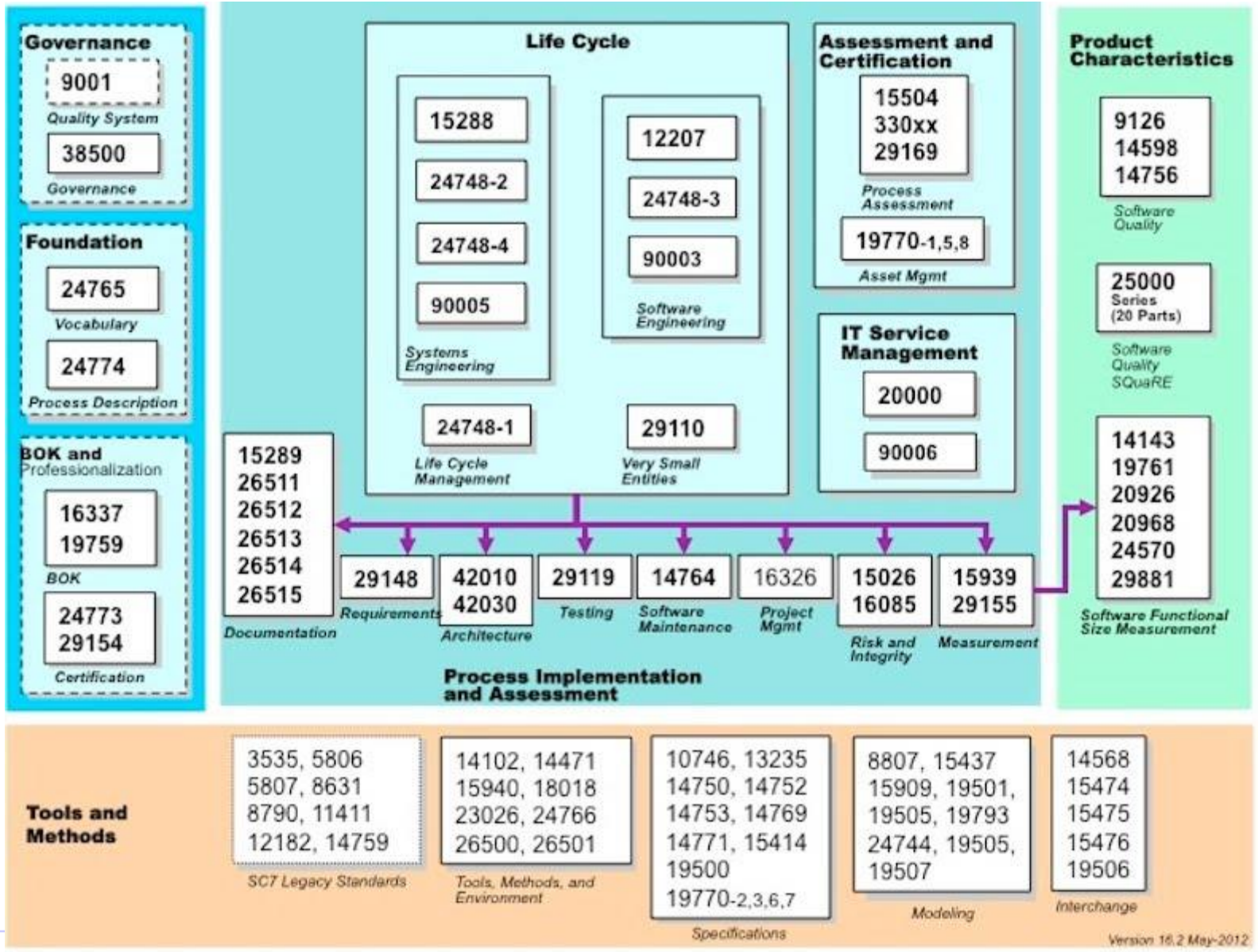
Standards Initiatives – Where We Participate

- International Organization for Standardization (ISO)/
  International Electrotechnical Commission (IEC)
  Joint Technical Committee 1 (JTC 1)
  Subcommittee 7 (SC 7), Software and Systems Engineering
- ISO/IEC JTC 1 SC 27, IT Security Techniques
  - And the US Technical Advisory Group to SC 27
    - International Committee for Information Technology Standards,
      Technical Committee CS1 – Cyber Security
- Object Management Group (OMG)
  Systems Engineering Domain Special Interest Group (SE DSIG)

ISO/IEC JTC 1 SC 7 WG7 – Life Cycle Management

- ISO/IEC 15288: 2015 – System Life Cycle Processes
- IEEE 15288.1-2014 – IEEE Standard for Application of Systems Engineering on Defense Programs
- IEEE 15288.2-2014 – IEEE Standard for Technical Reviews and Audits of Defense Programs
- ISO/IEC/IEEE DIS 12207 – Software Life Cycle Processes
- ISO/IEC TS 24748-1:2016 – Guidelines for Life Cycle Management
- ISO/IEC TR 24748-2:2011 – Guide for Application of 15288
- ISO/IEC TR 24748-3:2011 – Guide for Application of 12207
- ISO/IEC/IEEE 24748-4:2016 – Systems engineering planning
- ISO/IEC PRF TS 24748-6 – System integration engineering
- ISO/IEC/IEEE CD 29148 – Life Cycle Processes – Requirements Engineering
- ISO/IEC/IEEE FDIS 15939 – Measurement Process
- ISO/IEC 16326:201x Working Draft 2 – Project Management

ISO/IEC SC7 Standards Collection



https://sites.google.com/site/isoiecjtc1sc7/

ISO/IEC JTC 1 SC 7 WG4 – Tools and Environments

- Establishment of product lines for development of systems engineering and software tools, creating direct connection between INCOSE PLE working group and SC7'S WG04's standards
- ISO/IEC 26550:2015 – Reference model for product line engineering and management
- ISO/IEC 26551:2016– Tools and methods for product line requirements engineering
- ISO/IEC 26555:2015– Tools and methods for product line technical management

ISO/IEC JTC 1 SC 7 WG 20 - Software and Systems Bodies of Knowledge and Professionalization

- ISO/IEC CD 24773-1 – Certification of Software and Systems Engineering Professionals -- Part 1: General Requirements
- ISO/IEC Draft TR 24773-2 – Certification of Software and Systems Engineering Professionals – Part 2- Guidance Regarding Description of Knowledge, Skills, and Competences in Certification and Qualification Schemes
- ISO/IEC CD 24773-3 – Certification of Software and Systems Engineering Professionals -- Part 3: Systems Engineering Certification

ISO/IEC JTC 1 SC 7 WG 10 – Process Assessment

- ISO/IEC 15504-1:2004 Process assessment — Part 1: Concepts and vocabulary
- ISO/IEC 15504-2:2003 Process assessment — Part 2: Performing an assessment
- ISO/IEC 15504-3:2004 Process assessment — Part 3: Guidance on performing an assessment
- ISO/IEC 15504-4:2004 Process assessment — Part 4: Guidance on use for process improvement and process capability determination
- ISO/IEC 15504-5:2012 Process Assessment — Part 5: An exemplar Process Assessment Model
- ISO/IEC TR 15504-6:2013 Process assessment — Part 6: An exemplar system life cycle process assessment model
- ISO/IEC TR 15504-7:2008 Process assessment — Part 7: Assessment of organizational maturity
- ISO/IEC PDTR 15504-8 Process assessment — Part 8: An exemplar process assessment model for IT service management
- ISO/IEC TS 15504-9:2011 Process assessment — Part 9: Target process profiles
- ISO/IEC TS 15504-10:2011 Process assessment — Part 10: Safety extension

INCOSE

INCOSE has ceased participation in WG 10 due to resource constraints

ISO/IEC JTC 1 SC 7 WG 24 – Life Cycles for Very Small Entities (VSE)

- ISO/IEC TR 29110-1:2016 Life cycles for Very Small Entities – Part 1: O
- ISO/IEC TR 29110-3-1:2015 Life cycles for Very Small Entities – Part 3-1: Assessment Guide
- ISO/IEC TR 29110-5-1-1:2012 Life cycles for Very Small Entities – Part 5-1-1: Management and Engineering Guide: Generic Profile Group: Entry Profile
- ISO/IEC TR 29110-5-1-2:2011 Life cycles for Very Small Entities – Part 5-1-2: Management and Engineering Guide: Generic Profile Group: Basic Profile
- ISO/IEC TR 29110-5-6-1:2015 Life cycles for Very Small Entities – Part 5-6-1: Systems Engineering – Management and Engineering Guide: Generic Profile Group: Entry Profile
- ISO/IEC TR 29110-5-6-2:2014 Life cycles for Very Small Entities – Part 5-6-1: Systems Engineering – Management and Engineering Guide: Generic Profile Group: Basic Profile

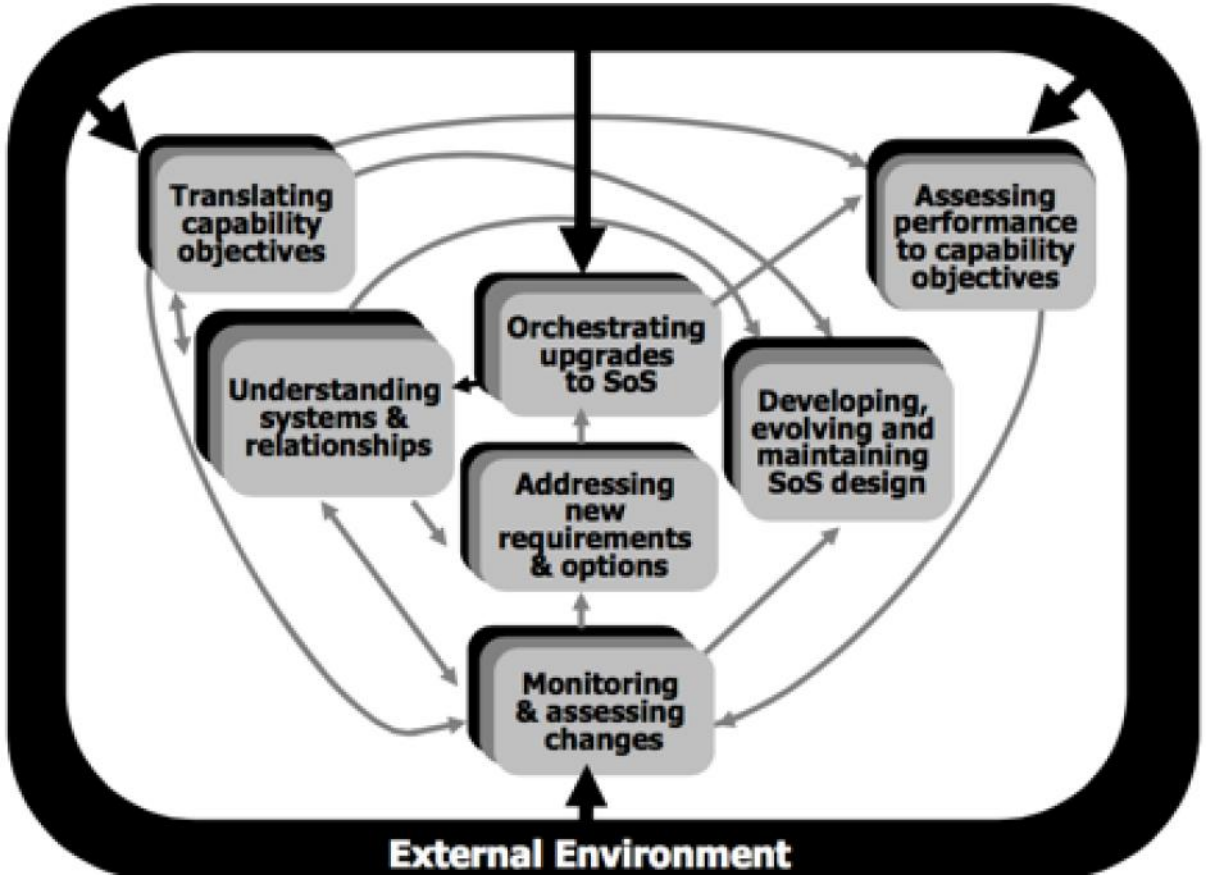
ISO/IEC JTC 1 SC 7 WG 42 – Architecture

- ISO/IEC/IEEE 42010:2011 Architecture description
  - See http://www.iso-architecture.org/ieee-1471/
- ISO/IEC CD 42020 Architecture Processes
- ISO/IEC CD 42030 Architecture Evaluation

SC7 Study Group on System of Systems

- Report completed; now developing proposals for projects
- Analogy – SoSE is to Systems Engineering what i Portfolio Management is to Project Management
- Principal differences – outside of scale / complexity
  - No life-cycle in the classical sense: continuous evolution
  - Asynchronous evolution of components is the rule rather than the exception
  - Architectural ‘frameworks’
  - -> Dynamic reconfiguration?

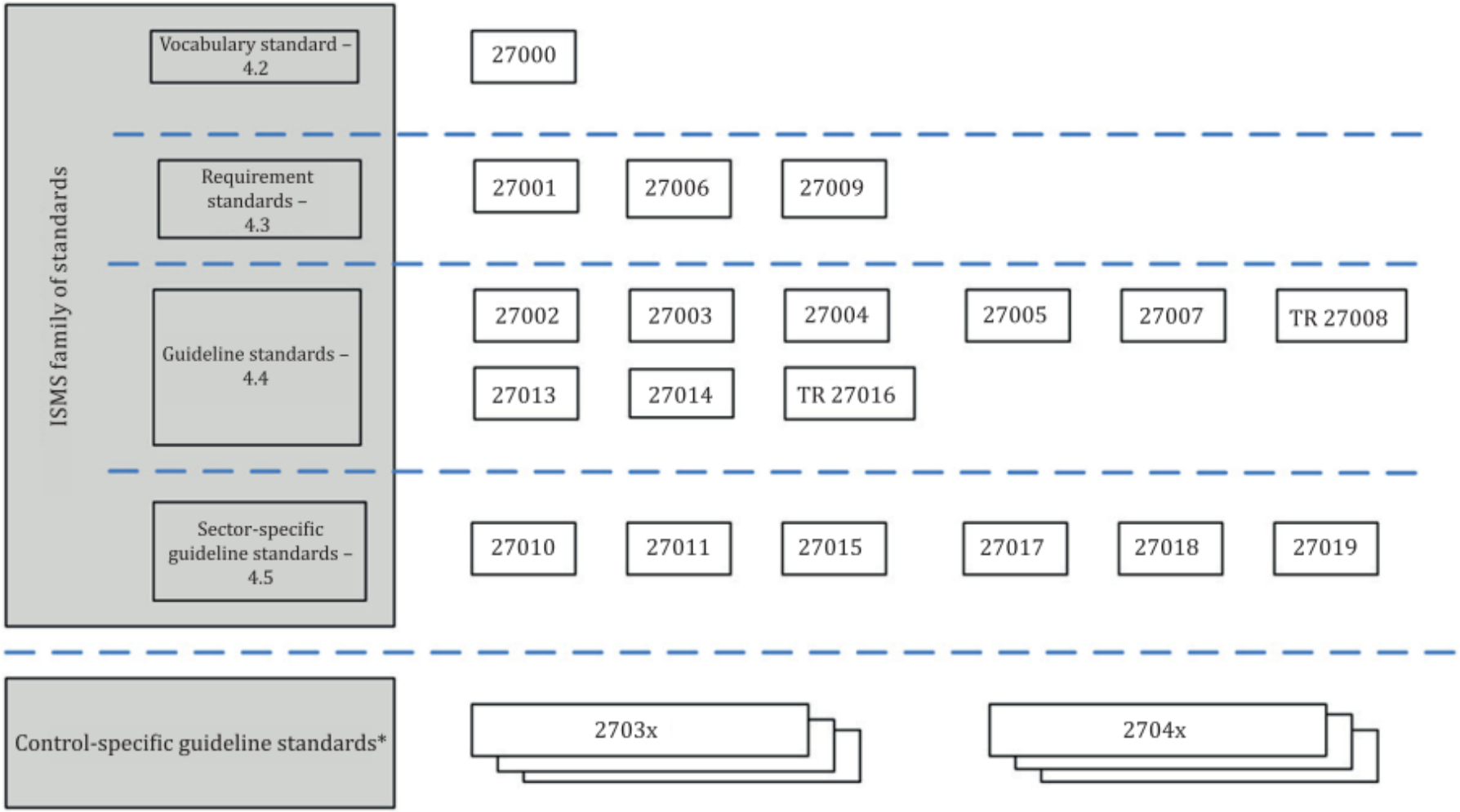
Core elements of Systems Engineering for SoS



ISO/IEC JTC 1 SC 27 WG 1 – Information Security Management Systems

- ISO/IEC 27000 family of standards
  - Provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series). {Source: https://en.wikipedia.org/wiki/ISO/IEC_27000-series}
- ISO/IEC 27000:2016 - Security techniques — Information security management systems — Overview and vocabulary *{Publicly available}*
  - Define requirements for an ISMS and for those certifying such systems,
  - Provide direct support, detailed guidance and/or interpretation for the overall process to establish, implement, maintain, and improve an ISMS,
  - Address sector-specific guidelines for ISMS, and
  - Address conformity assessment for ISMS.

Information Security Management System (ISMS)



Standards in the ISO/IEC 27000 Family (1/2)

- ISO/IEC 27001, Information security management systems — Requirements
- ISO/IEC 27002, Code of practice for information security controls
- ISO/IEC 27003, Information security management system implementation guidance
- ISO/IEC 27004, Information security management — Measurement
- ISO/IEC 27005, Information security risk management
- ISO/IEC 27006, Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007, Guidelines for information security management systems auditing
- ISO/IEC TR 27008, Guidelines for auditors on information security controls
- ISO/IEC 27009, Sector-specific application of ISO/IEC 27001 — Requirements
- ISO/IEC 27010, Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013, Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Standards in the ISO/IEC 27000 Family (2/2)

- ISO/IEC TR 27015, Information security management guidelines for financial services
- ISO/IEC TR 27016, Information security management — Organizational economics
- ISO/IEC 27017, Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- ISO/IEC 27018, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- ISO/IEC 27019, Information security management guidelines based on ISO/IEC 27002 for process
- Related Standard
  - ISO 27799, Health informatics — Information security management in health using ISO/IEC 27002

Why Systems Engineers Should Care

- The controls specified in ISO/IEC 27002 are acknowledged as best practices applicable to most organizations and readily tailored to accommodate organizations of various sizes and complexities. Other standards in the ISMS family of standards provide guidance on the selection and application of ISO/IEC 27002 controls for the information security management system.
- Information security controls should be considered at the systems and projects requirements specification and design stage. Failure to do so can result in additional costs and less effective solutions, and maybe, in the worst case, inability to achieve adequate security.

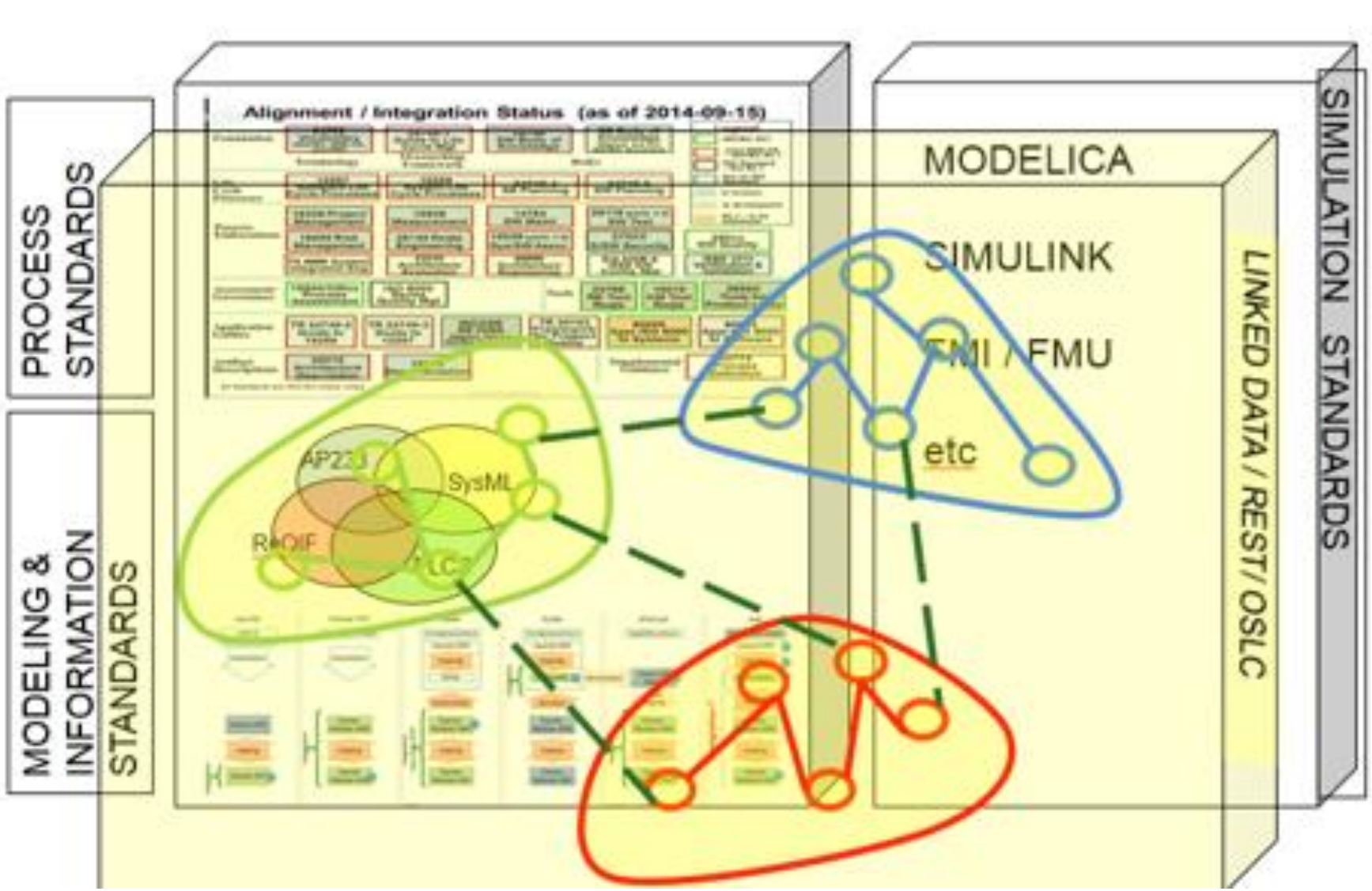
Object Management Group – SE Domain Special Interest Group (SE DSIG)

- OMG Systems Modeling Language (OMG SysML™)
  - Revision underway – Version 2
  - Latest information is available at the official OMG SysML site at http://www.omgsysml.org
- Unified Modeling Language (UML)
  - http://www.omg.org/spec/UML/2.3/
- There is also an effort to develop a safety profile based on SysML
  - Improve the integration of safety engineering with systems engineering and certification
  - Improve consistency and traceability among the different artifacts and promote reasoning based on the safety information.

ISO TC 184 – Automation Systems and Integration

- ISO TC184 SC4 Industrial Data
  - ISO 10303-233:2012, Industrial automation systems and integration -- Part 233: Systems engineering data representation
    - Data models that provide interfaces between domain specific data models such as mechanical, electronic, structural analysis, thermal analysis, manufacturing, etc. e.g. the transform between engineering analysis (AP209, STEP-TAS, STEP-NRF, AP235, etc.) and any AP233 module set.
- ISO TC184 SC5 Architecture, Communications & Integration Frameworks
  - ISO/PAS 19450:2015 - Automation systems and integration — Object-Process Methodology (OPM)
    - Normative document that specifies a generic approach to write standards using OPM for standards such as
      - ISO/CEN 19440 (modeling constructs)
      - ISO/IEC 19782 (positioning of bar codes on products)
      - IEC 62264 (enterprise-control system integration)

ISO 10303-242:2014 – Industrial automation systems and integration – Product data representation and exchange – Part 242: Application protocol: Managed model-based 3D engineering



The Need for Standards

- Earliest standards may have been calendars – needed for agriculture
- Weights and measures – needed for commerce
  - What does the gold weigh that the merchant is using to pay for the length of silk?
- Interchange and interoperability
  - Neighboring towns bought fire hoses and hydrants from different suppliers – large fire required working together
  - This helped establish need for American Standards Association (now American National Standards Institute – ANSI)
- SE Standards
  - Provide a common language among systems engineers
  - Facilitate teaming
  - Basis for competency assessment (CSEP, etc.)

Standardization is …

- "Activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context"
  - ISO/IEC Guide 2:1991
- Important benefits of standardization are improvement of the suitability of products, processes, and services for their intended purposes, prevention of barriers to trade, and facilitation of technological cooperation
  - Variety control
  - Protection of the environment
  - Product protection
  - Mutual understanding
  - Economic performance
  - Trade
  - Usability
    - Compatibility
    - Interchangeability
    - Health
  - Safety

Standardization is … (cont.)

- A standard is a “document, established by consensus and approved by a recognized body, that provides, for common and repeated use, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context”

Standards can have “oddball” effects

- Why are the Space Shuttle solid rocket boosters the size they are?
  - SRBs manufactured by Thiokol at a factory in Utah
    - They had to be shipped by rail to the launch site
  - Railroad line runs through a tunnel in the mountains
  - Tunnel width is based on US standard rail gauge – 4 feet, 8.5 inches
    - Derived from gauge in England
    - Used same jigs and tools for building wagons
  - Wagon wheel spacing based on existing wheel ruts
    - That were made by the Roman legions with their chariots, which were built to standard specifications
  - Chariot wheel spacing accommodates back ends of two warhorses
- Which makes for an interesting requirements trace!

http://madmikesamerica.com/2010/08/interesting-historical-facts/

The First ISO Standard and Technical Committee

- First ISO standard dealt with measuring threads
  - ISO 1:2016 – Geometrical product specifications (GPS) -- Standard reference temperature for the specification of geometrical and dimensional properties
    - "ISO 1:2016 defines the concepts of a reference temperature and of the standard reference temperature, and specifies the standard reference temperature value for the specification of geometrical and dimensional properties of an object. Some examples of geometrical and dimensional properties include size, location, orientation (including angle), form and surface texture of a workpiece."
    - "ISO 1:2016 Standard is also applicable to the definition of the measurand used in verification or calibration."
- ISO/TC 1 Screw threads
  - Standardization of series of internationally interchangeable fastening and traversing screw threads with a minimum variety of basic profiles, pitches and diameters including tolerances and verification. {23 standards have been published}
  - ISO 1:2016 is now maintained by ISO/TC 213 - Dimensional and geometrical product specifications and verification

Standards successes

- At one time, rail gauges were not standardized
  - Rail cars could not be transferred to another line
    - Unload the cargo
- Shipping containers are now standardized – limited number of sizes
  - Transfer from ocean-going cargo ship
  - To railroad
  - To highway trucks
  - Cooperative effort across industries

Potential Impact of Careless Regulation

- Standards have made great contributions over the years
- Sometimes the good intentions of standards developers (or regulators) can cause challenges for systems engineers and other stakeholders.
- Systems engineers need to have the skills — and tenacity — to deal with standards and regulations that might constrain the design space or otherwise impose burdens.
- This phenomenon is illustrated by a video about the frustration of manufacturers of doors and gates; see http://www.youtube.com/watch?v=r5GZDdvYJrE

Tailoring the paperwork, etc. to magnitude of risk

DO-278 / ED109 Assurance Levels

- AL1 Catastrophic: prevents continued safe flight or landing, many fatal injuries
- AL2 Hazardous/Severe: potential fatal injuries to a small number of occupants
- AL3 Major: impairs crew efficiency, discomfort or possible injuries to occupants
- AL4 No equivalent {Ground automation needed something between AL3 & AL5}
- AL5 Minor: reduced aircraft safety margins, but well within crew capabilities
- AL6 No Effect: does not effect the safety of the aircraft at all!

Based on DO-178B / ED-12 Safety Levels

Source: RTCA DO-278 / EUROCAE ED-109 "Guidelines for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance",

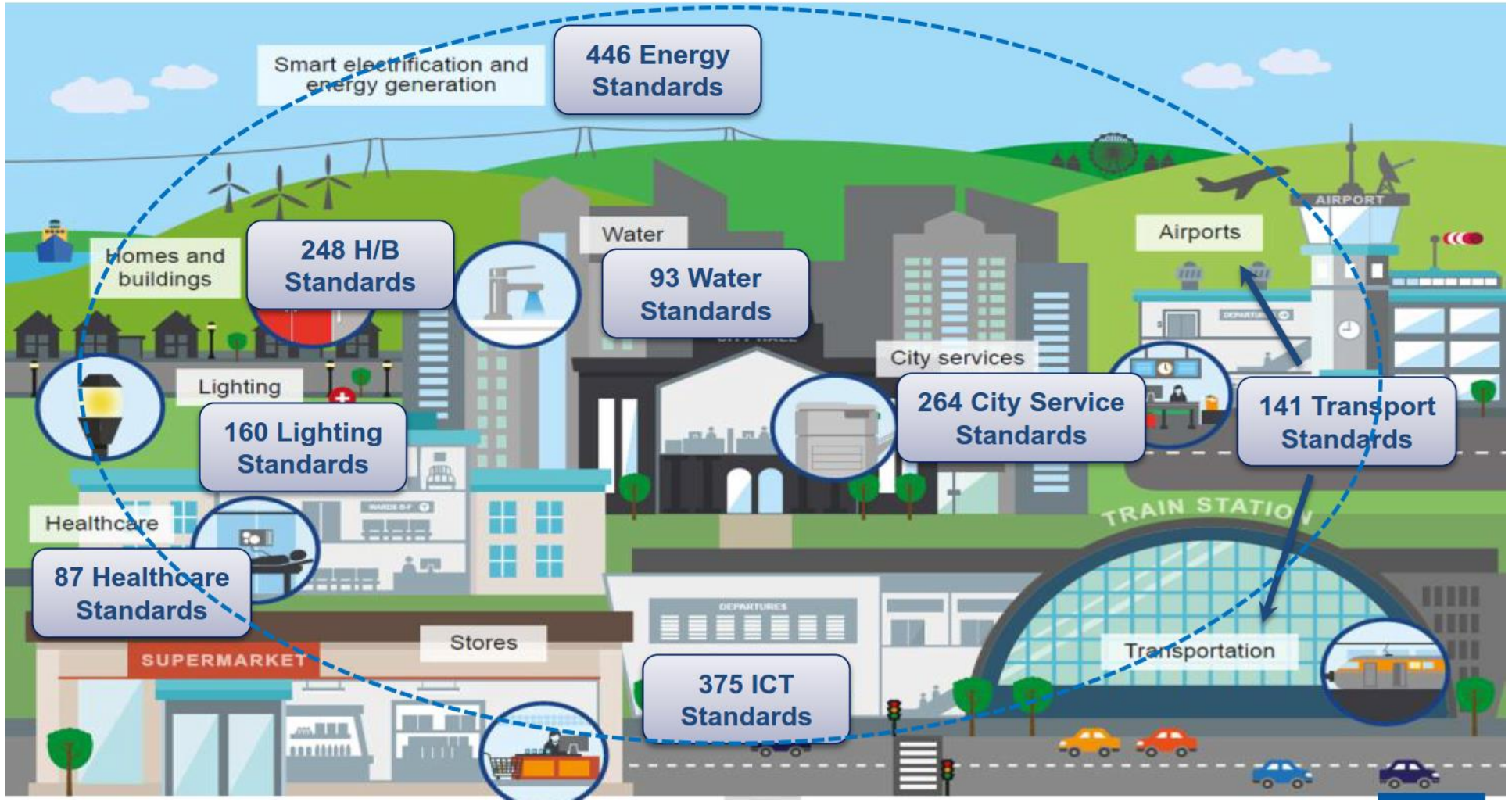
Selecting Standards in Your Requirements

- Strategies for future conformance
  - MIL-STD-490 permits specifying a Draft International Standard (DIS)
- Market surveys to determine the availability of standards
  - Is anybody building to the standards?
- Standards selection
  - There should be a business case for each choice
- Standards profiling — Coordination and tailoring of standards to work together
- Selection of standards-compliant implementations
- Some work is done first in consortia
- Specify timeline for compliance
  - “Will conform to approved standard” once approved

Standards Planning

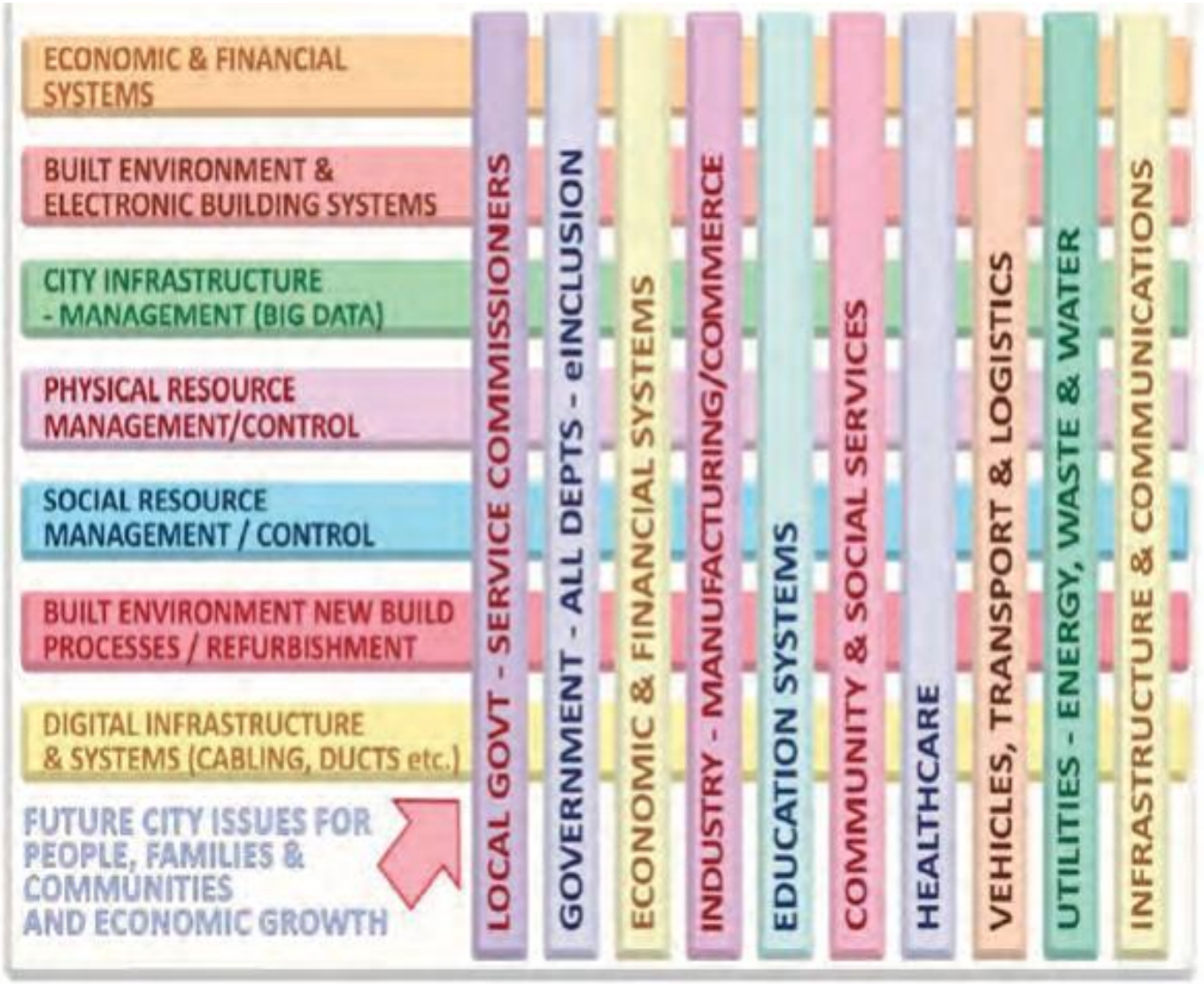
- Assess technical standards to determine
  - How they inhibit or enhance the incorporation of new technologies into system development projects
  - Determine where they are headed and the alignment of these new standards with the life cycles for the systems in the enterprise's current and projected future portfolios
- Identify need for new or updated standards
  - Create a business case
  - Identify resources
  - Which standards organization is best for this objective?

IEC Smart City – 1,814 Standards



INCOSE

Smart City Stakeholders



How Can Someone Acquire a Standard?

- Most standards are not free
  - Use your National Body (ANSI for United States) or ISO
    - ANSI Standards Store - http://www.nssn.org/
  - Contact the Standards Development Organization (SDO)
  - http://www.techstreet.com/ is a good source
- ISO has a site for *some* free standards
  - http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
- ISO has a preview mode – Online Browsing Platform
  - https://www.iso.org/obp/ui/#home
    Or use ISO catalog at http://www.iso.org/iso/home/store/catalogue_ics.htm
  - Typically includes foreword, introduction, definitions, table of contents
    - "Only informative sections of standards are publicly available. To view the full content, you will need to purchase the standard by clicking on the 'Buy' button."

Final thoughts – “Standards Build Trust”