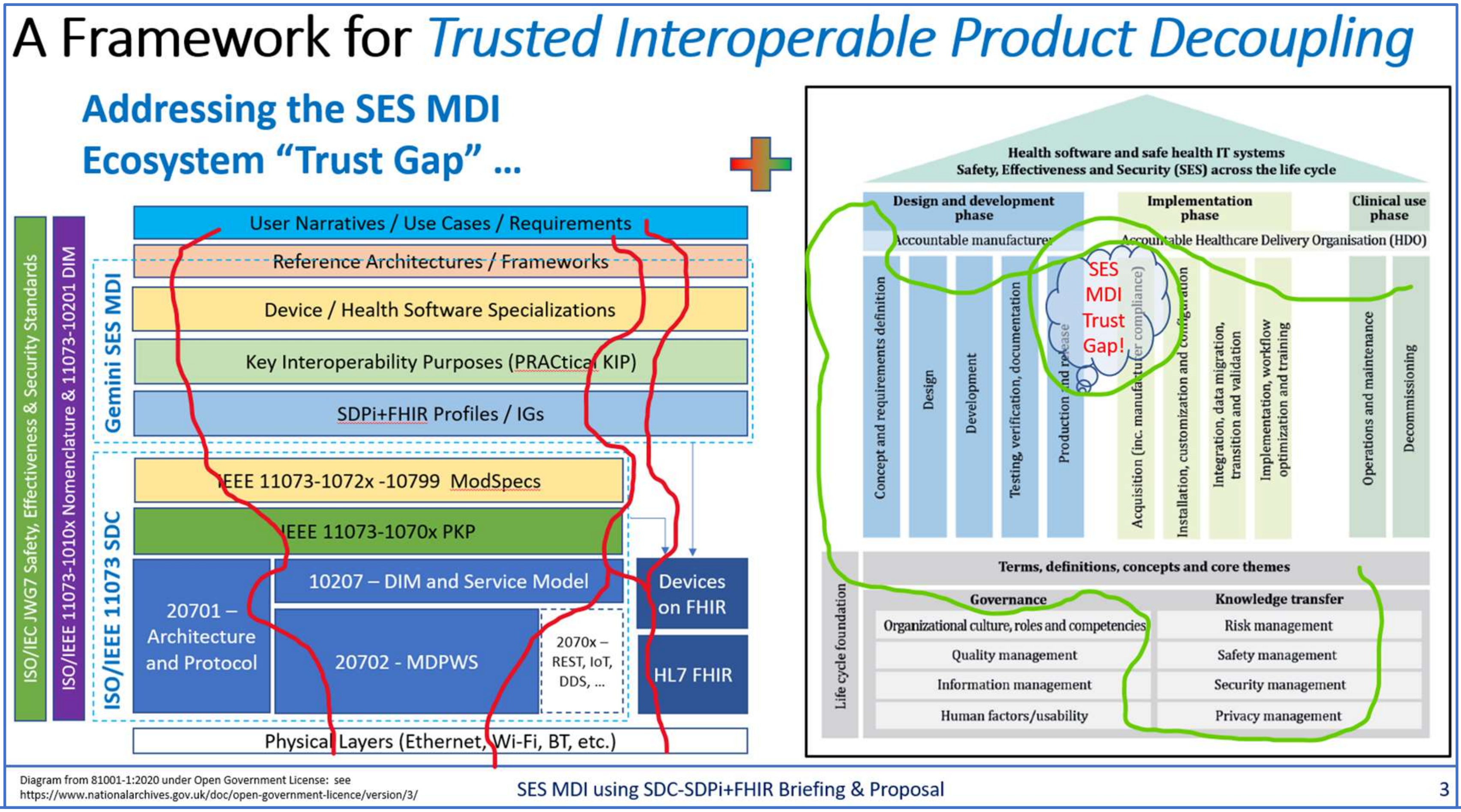
SES MDI using SDC/SDPi+FHIR
Framework & Considerations

Pre-release
Draft 2020.07.23

Establishing a framework for
Trusted Interoperable Product Decoupling

ADD UML MODEL
UPDATE Gardens \Diagram

SES MDI Using SDC/SDPi+FHIR – *The Big Idea*



A Framework for *Trusted Interoperable Product Decoupling*

Addressing the SES MDI Ecosystem “Trust Gap” …

ISO/IEC JWG7 Safety, Effectiveness & Security Standards

ISO/IEEE 11073-1010x Nomenclature & 11073-10201 DIM

Gemini SES MDI

User Narratives / Use Cases / Requirements

Reference Architectures / Frameworks

Device / Health Software Specializations

Key Interoperability Purposes (PRACtical KIP)

SDPi+FHIR Profiles / IGs

ISO/IEEE 11073 SDC

IEEE 11073-1072x -10799 ModSpecs

IEEE 11073-1070x PKP

10207 – DIM and Service Model

20701 – Architecture and Protocol

20702 - MDPWS

2070x – REST, IoT, DDS, …

Devices on FHIR

HL7 FHIR

Physical Layers (Ethernet, Wi-Fi, BT, etc.)

Health software and safe health IT systems
Safety, Effectiveness and Security (SES) across the life cycle

Design and development phase

Implementation phase

Clinical use phase

Accountable manufacturer

Accountable Healthcare Delivery Organisation (HDO)

Concept and requirements definition

Design

Development

Testing, verification, documentation

Production and release

Acquisition (inc. manufacturer compliance)

Installation, customization and configuration

Integration, data migration, transition and validation

Implementation, workflow optimization and training

Operations and maintenance

Decommissioning

SES MDI Trust Gap!

Life cycle foundation

Terms, definitions, concepts and core themes

Governance	Knowledge transfer
Organizational culture, roles and competencies	Risk management
Quality management	Safety management
Information management	Security management
Human factors/usability	Privacy management

Diagram from 81001-1:2020 under Open Government License: see https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/

SES MDI using SDC-SDPi+FHIR Briefing & Proposal 3

Full presentation available @ Gemini SDPi+FHIR “The SES MDI Interoperability Trust Gap” @ https://confluence.hl7.org/x/IQ7xB

Questions to Contemplate …

How to minimize duplication of information & effort?

How to maximize use of work and resources already created?

What is the requirements starting point & ending point?

How to truly integrate SES & MDI … seamlessly?!

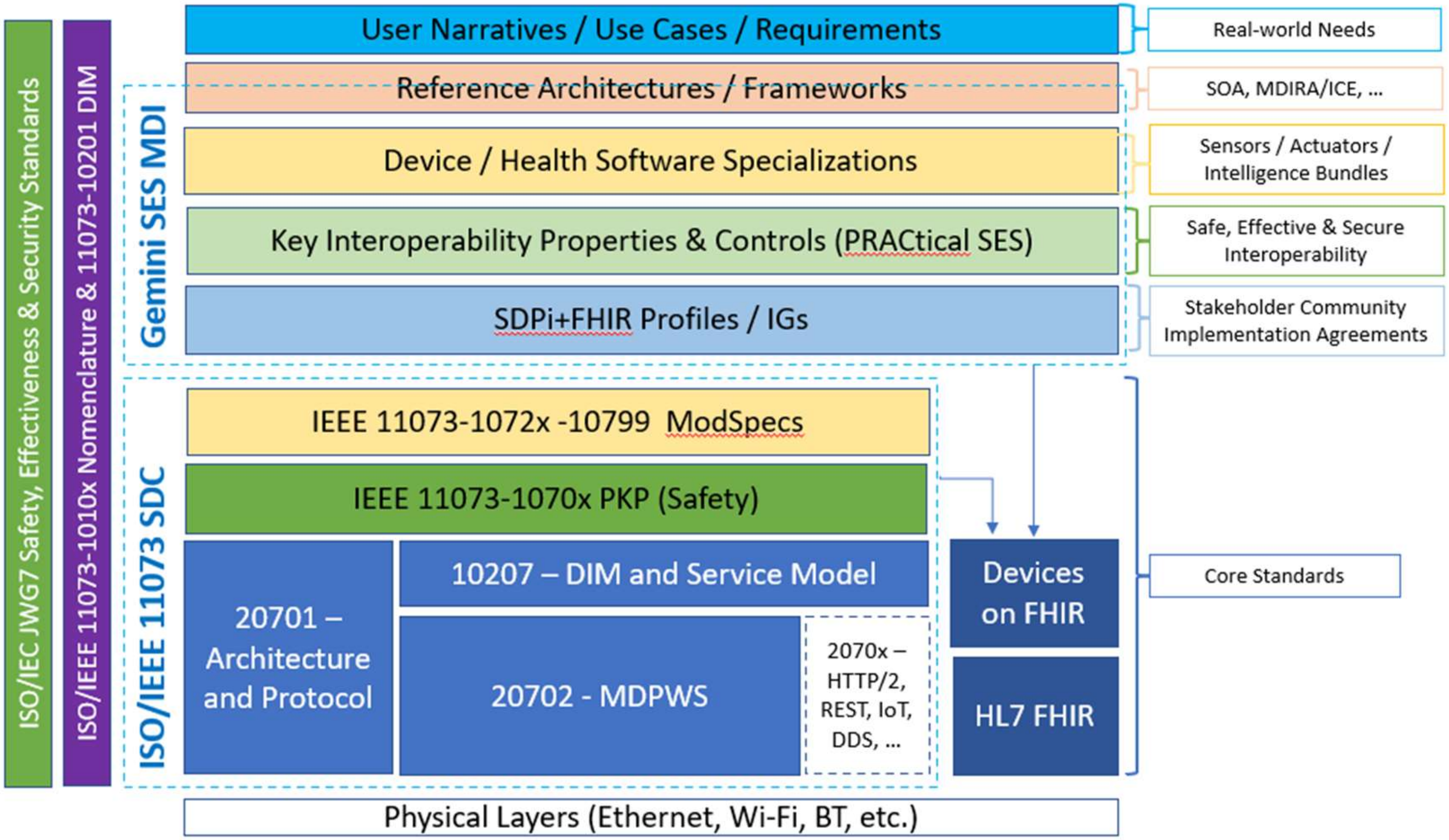
How to craft a framework for SES “PnT” MDI …

… With an achievable starting point & compelling future state?

SES MDI Using SDC/SDPi+FHIR – *The Big Picture*

“Hanging Gardens” Model

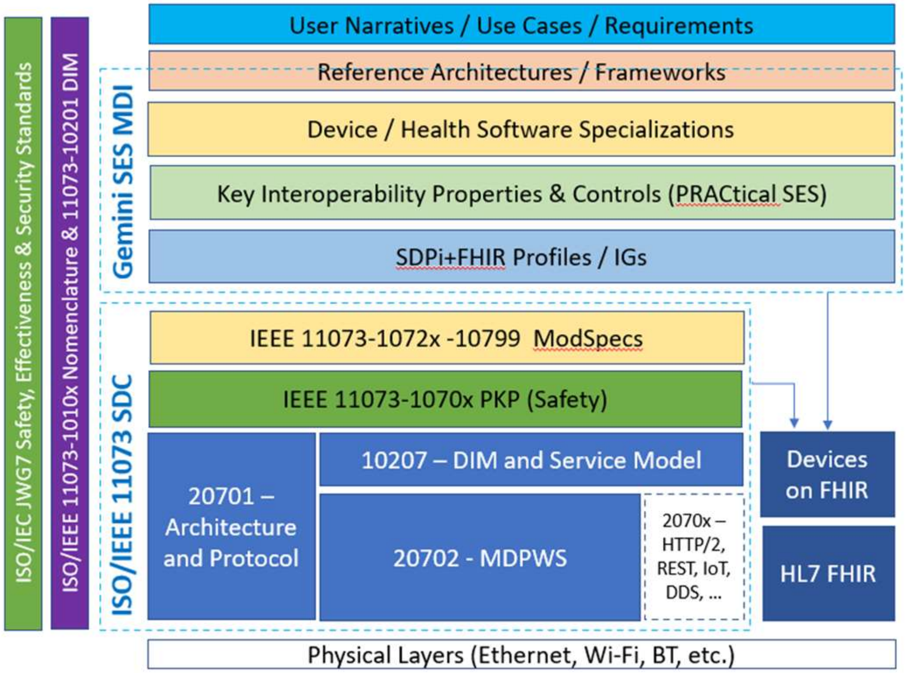
- ✓ Perfect? Not!
- ✓ Useful? Absolutely!!!
- ✓ Provides a common reference point to consider the questions and identify a workable framework
- ✓ Cuts across …
  - Standards
  - Organizations
  - Subject Areas
  - Past/Present/Future
  - ….


ISO/IEC JWG7 Safety, Effectiveness & Security Standards
ISO/IEEE 11073-1010x Nomenclature & 11073-10201 DIM
Gemini SES MDI
ISO/IEEE 11073 SDC
User Narratives / Use Cases / Requirements
Reference Architectures / Frameworks
Device / Health Software Specializations
Key Interoperability Properties & Controls (PRACtical SES)
SDPi+FHIR Profiles / IGs
IEEE 11073-1072x -10799 ModSpecs
IEEE 11073-1070x PKP (Safety)
20701 – Architecture and Protocol
10207 – DIM and Service Model
20702 - MDPWS
2070x – HTTP/2, REST, IoT, DDS, …
Devices on FHIR
HL7 FHIR
Physical Layers (Ethernet, Wi-Fi, BT, etc.)
Real-world Needs
SOA, MDIRA/ICE, …
Sensors / Actuators / Intelligence Bundles
Safe, Effective & Secure Interoperability
Stakeholder Community Implementation Agreements
Core Standards

“Hanging Gardens” Model – *Layer Integration*

Each layer can be characterized by:

- Unique Subject Concepts & Components (Terms)
- Layer-specific Information & Knowledge (UML models)
- Layer API & Capabilities & Requirements (Inter-layer Spec’s)
- Requirements Formalization (Gherkin & ReqIF Spec’s)
- Implementation Trust Logic (SES Assurance Case Spec’s)
- Implementation Technology Logic (MDI Spec’s)



ISO/IEC JWG7 Safety, Effectiveness & Security Standards

ISO/IEEE 11073-1010x Nomenclature & 11073-10201 DIM

Gemini SES MDI

ISO/IEEE 11073 SDC

User Narratives / Use Cases / Requirements

Reference Architectures / Frameworks

Device / Health Software Specializations

Key Interoperability Properties & Controls (PRACtical SES)

SDPi+FHIR Profiles / IGs

IEEE 11073-1072x -10799 ModSpecs

IEEE 11073-1070x PKP (Safety)

20701 – Architecture and Protocol

10207 – DIM and Service Model

20702 - MDPWS

2070x – HTTP/2, REST, IoT, DDS, …

Devices on FHIR

HL7 FHIR

Physical Layers (Ethernet, Wi-Fi, BT, etc.)

Integrating each “hanging garden” can be achieved by “threading” …

horizontally – across layer-specific characterization dimensions

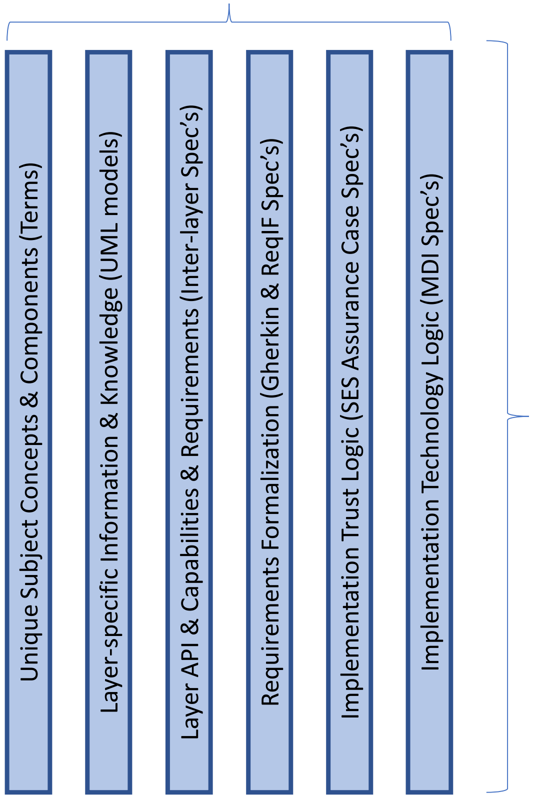
+

vertically – mapping from scenarios to Plug-and-Trust decoupled product interfaces

Layer Characterization: *Horizontal & Vertical*

Horizontal

(Intra-Garden Walkways)



Unique Subject Concepts & Components (Terms)

Layer-specific Information & Knowledge (UML models)

Layer API & Capabilities & Requirements (Inter-layer Spec's)

Requirements Formalization (Gherkin & ReqIF Spec's)

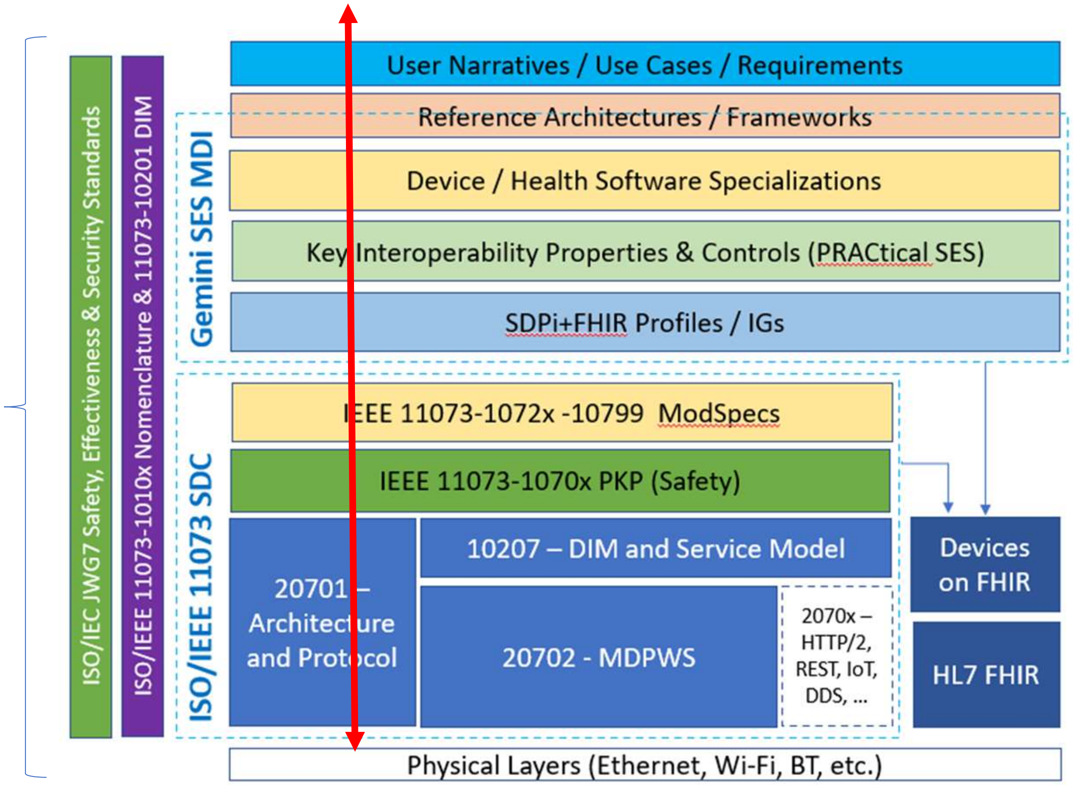
Implementation Trust Logic (SES Assurance Case Spec's)

Implementation Technology Logic (MDI Spec's)

Each Layer Characterized Horizontally & Integrated Vertically

Vertical

(Inter-Garden Stairways)



ISO/IEC JWG7 Safety, Effectiveness & Security Standards

ISO/IEEE 11073-1010x Nomenclature & 11073-10201 DIM

Gemini SES MDI

User Narratives / Use Cases / Requirements

Reference Architectures / Frameworks

Device / Health Software Specializations

Key Interoperability Properties & Controls (PRACtical SES)

SDPi+FHIR Profiles / IGs

ISO/IEEE 11073 SDC

IEEE 11073-1072x -10799 ModSpecs

IEEE 11073-1070x PKP (Safety)

20701 – Architecture and Protocol

10207 – DIM and Service Model

20702 - MDPWS

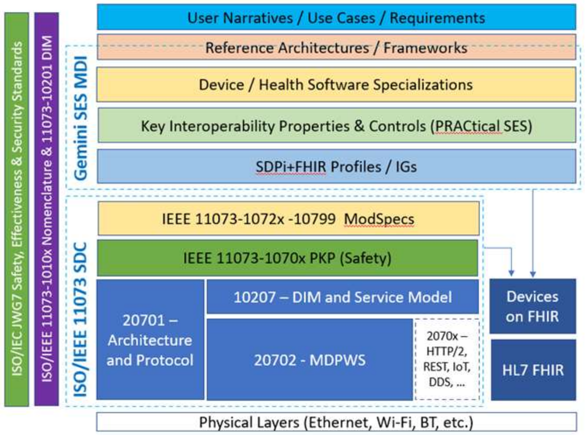
2070x – HTTP/2, REST, IoT, DDS, …

Devices on FHIR

HL7 FHIR

Physical Layers (Ethernet, Wi-Fi, BT, etc.)

Garden Design: *Horizontal Integration*


User Narratives / Use Cases / Requirements
Reference Architectures / Frameworks
Device / Health Software Specializations
Key Interoperability Properties & Controls (PRACtical SES)
SDPi+FHIR Profiles / IGs
Gemini SES MDI
IEEE 11073-1072x -10799 ModSpecs
IEEE 11073-1070x PKP (Safety)
20701 – Architecture and Protocol
10207 – DIM and Service Model
20702 - MDPWS
2070x – HTTP/2, REST, IoT, DDS, …
ISO/IEEE 11073 SDC
Devices on FHIR
HL7 FHIR
Physical Layers (Ethernet, Wi-Fi, BT, etc.)
ISO/IEC JWG7 Safety, Effectiveness & Security Standards
ISO/IEEE 11073-1010x Nomenclature & 11073-10201 DIM

Unique Subject Concepts & Components (Semantics/Terms)

Concepts, terms, definitions, algorithms, frameworks, …

Layer-specific Information & Knowledge (UML models)

Use Case / Activity Diagrams, Sequence Models, Object Models, etc.

Layer API & Capabilities & Requirements (Inter-layer Spec’s)

“API” Specifications, Implementation “Platform” Requirements, etc.

Requirements Formalization (Gherkin & ReqIF Spec’s)

Feature, Rule, Given/When/Then + Specification, SpecRelation (Source, Target), etc.

Implementation Trust Logic (SES Assurance Case Spec’s)

Profiled application of 81001-1, 80001-1, 62304, assurance cases, etc.

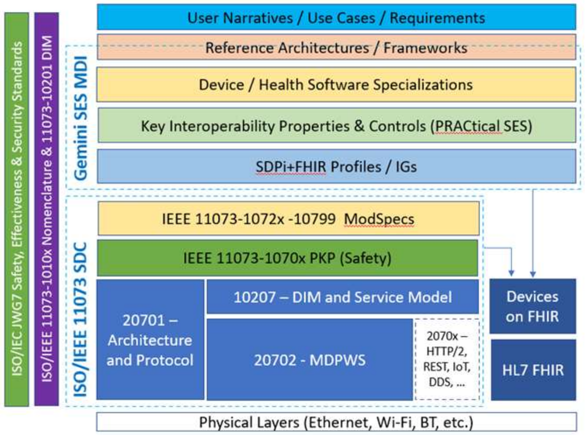
Implementation Technology Logic (MDI Spec’s)

System Actors, Transactions, Messages, Events, Terminology, Value Sets, etc.

INCLUDE MAPPING COMPONENT / ARTIFACTS + standards in scope

Create a UML model showing relationships

Garden Design: *Vertical Integration*



ISO/IEC JWG7 Safety, Effectiveness & Security Standards

ISO/IEEE 11073-1010x Nomenclature & 11073-10201 DIM

Gemini SES MDI

User Narratives / Use Cases / Requirements

Reference Architectures / Frameworks

Device / Health Software Specializations

Key Interoperability Properties & Controls (PRACtical SES)

SDPi+FHIR Profiles / IGs

ISO/IEEE 11073 SDC

IEEE 11073-1072x -10799 ModSpecs

IEEE 11073-1070x PKP (Safety)

20701 – Architecture and Protocol

10207 – DIM and Service Model

20702 - MDPWS

2070x – HTTP/2, REST, IoT, DDS, …

Devices on FHIR

HL7 FHIR

Physical Layers (Ethernet, Wi-Fi, BT, etc.)

Unique Subject Concepts & Components (Semantics/Terms)

Concepts, terms, definitions, algorithms, frameworks, …

Layer-specific Information & Knowledge (UML models)

Use Case / Activity Diagrams, Sequence Models, Object Models, etc.

Layer API & Capabilities & Requirements (Inter-layer Spec’s)

“API” Specifications, Implementation “Platform” Requirements, etc.

Requirements Formalization (Gherkin & ReqIF Spec’s)

Feature, Rule, Given/When/Then + Specification, SpecRelation (Source, Target), etc.

Implementation Trust Logic (SES Assurance Case Spec’s)

Profiled application of 81001-1, 80001-1, 62304, assurance cases, etc.

Implementation Technology Logic (MDI Spec’s)

System Actors, Transactions, Messages, Events, Terminology, Value Sets, etc.

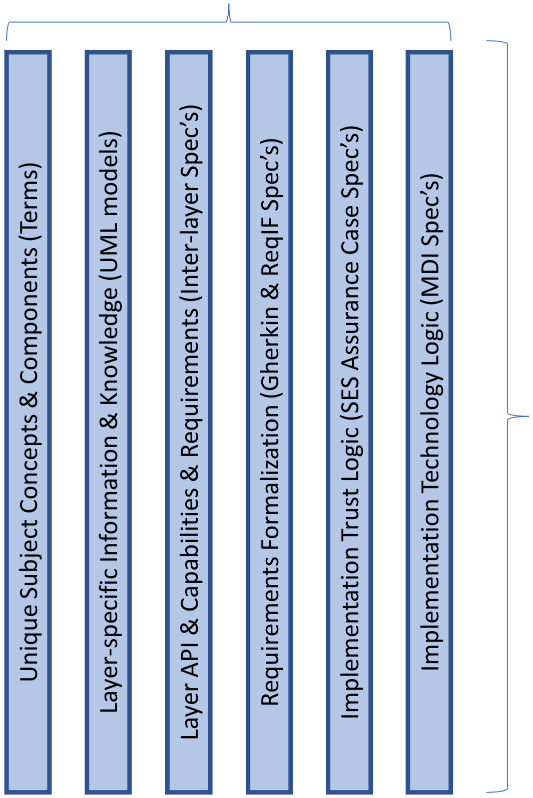
Use Case(s) to SOA to DS to KIP(SES) to SDPi to SDC to SFC

Layer Characterization: *Horizontal & Vertical Model*

CREATE A UML MODEL SHOWING ALL THE BITS THAT GET INTEGRATED HORIZONTALLY & VERTICALLY

Horizontal

(Intra-Garden Walkways)



Unique Subject Concepts & Components (Terms)

Layer-specific Information & Knowledge (UML models)

Layer API & Capabilities & Requirements (Inter-layer Spec's)

Requirements Formalization (Gherkin & ReqIF Spec's)

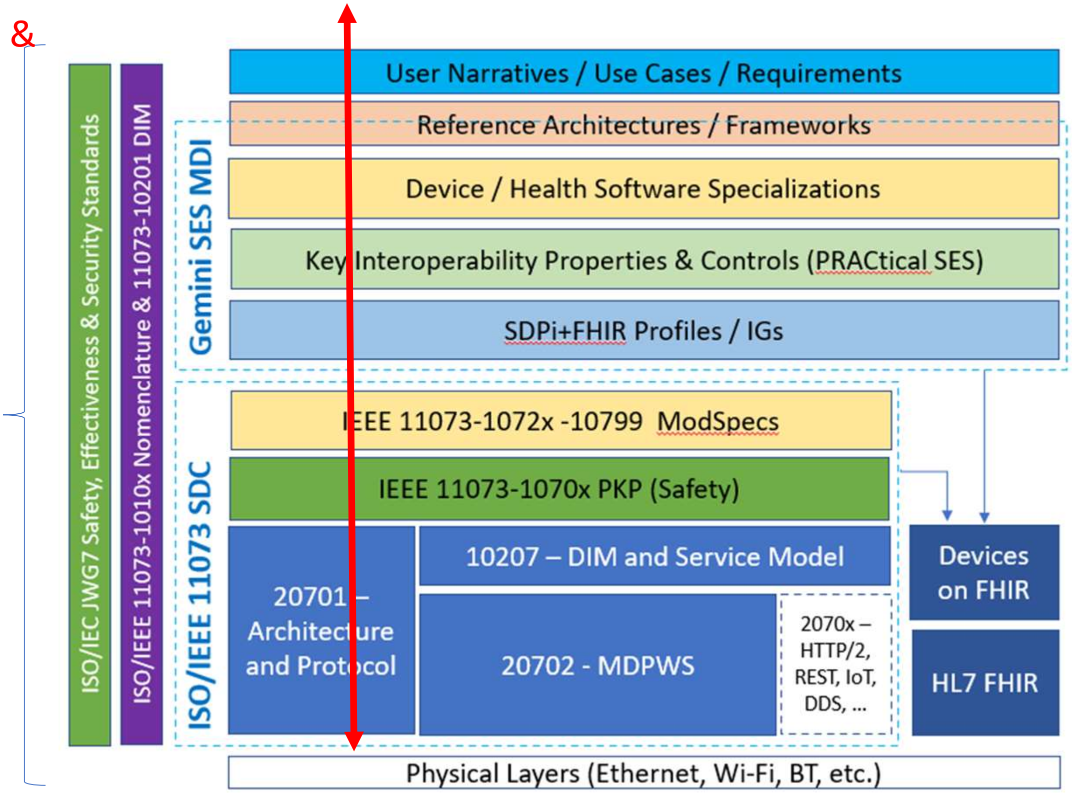
Implementation Trust Logic (SES Assurance Case Spec's)

Implementation Technology Logic (MDI Spec's)

Each Layer Characterized Horizontally & Integrated Vertically

Vertical

(Inter-Garden Stairways)



ISO/IEC JWG7 Safety, Effectiveness & Security Standards

ISO/IEEE 11073-1010x Nomenclature & 11073-10201 DIM

Gemini SES MDI

User Narratives / Use Cases / Requirements

Reference Architectures / Frameworks

Device / Health Software Specializations

Key Interoperability Properties & Controls (PRACtical SES)

SDPi+FHIR Profiles / IGs

ISO/IEEE 11073 SDC

IEEE 11073-1072x -10799 ModSpecs

IEEE 11073-1070x PKP (Safety)

10207 – DIM and Service Model

20701 – Architecture and Protocol

20702 - MDPWS

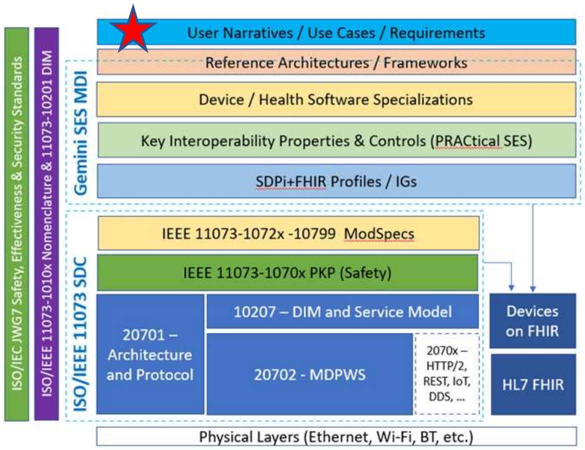
2070x – HTTP/2, REST, IoT, DDS, ...

Devices on FHIR

HL7 FHIR

Physical Layers (Ethernet, Wi-Fi, BT, etc.)

Garden: *Use Case Scenarios*


User Narratives / Use Cases / Requirements
Reference Architectures / Frameworks
Device / Health Software Specializations
Key Interoperability Properties & Controls (PRACtical SES)
SDPi+FHIR Profiles / IGs
IEEE 11073-1072x -10799 ModSpecs
IEEE 11073-1070x PKP (Safety)
20701 – Architecture and Protocol
10207 – DIM and Service Model
20702 - MDPWS
2070x – HTTP/2, REST, IoT, DDS, …
Devices on FHIR
HL7 FHIR
Physical Layers (Ethernet, Wi-Fi, BT, etc.)
ISO/IEC JWG7 Safety, Effectiveness & Security Standards
ISO/IEEE 11073-1010x Nomenclature & 11073-10201 DIM
Gemini SES MDI
ISO/IEEE 11073 SDC

Unique Subject Concepts & Components (Terms)

Narrative Stories, Actors (People & Systems), Scenarios, Activities, …

Layer-specific Information & Knowledge (UML models)

Use Case / Activity Diagrams, Sequence Models, Object Models, etc.

Layer API & Capabilities & Requirements (Inter-layer Spec's)

"API" Specifications, Implementation "Platform" Requirements, etc.

Requirements Formalization (Gherkin & ReqIF Spec's)

Feature, Rule, Given/When/Then + Specification, SpecRelation (Source, Target), etc.

Implementation Trust Logic (SES Assurance Case Spec's)

, etc.

Implementation Technology Logic (MDI Spec's)

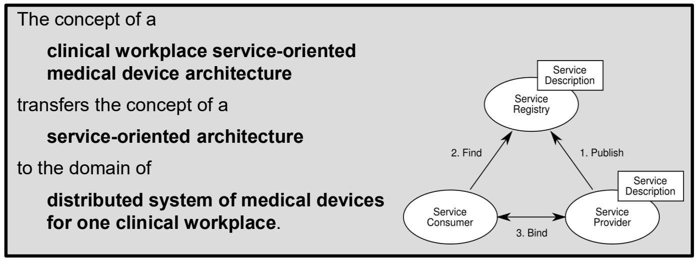
Actors, Transactions, Messages, Events, Terminology, Value Sets, etc.

Update layout to focus on Use Case Stuff – Minimize horizontal / vertical

Add layer Scope / Garden Theme

Garden: *Reference Architectures*

- Architecture layer
- Include: MDIRA/ICE and SDC/SOA examples



The concept of a

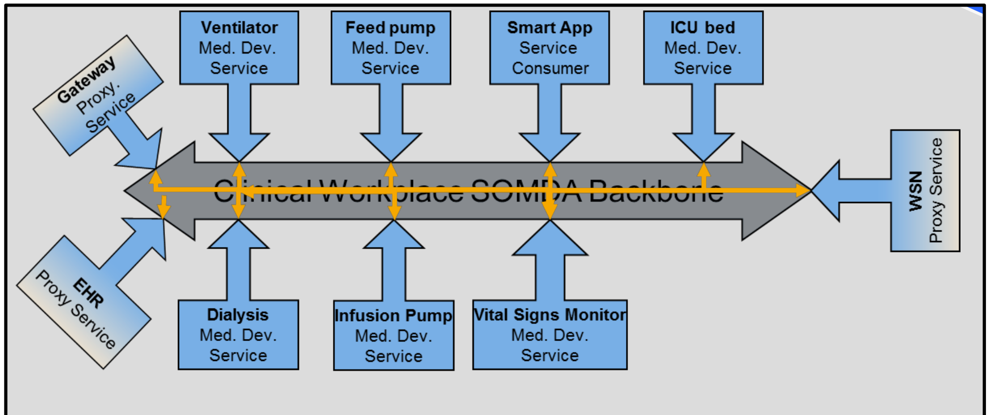
clinical workplace service-oriented medical device architecture

transfers the concept of a

service-oriented architecture

to the domain of

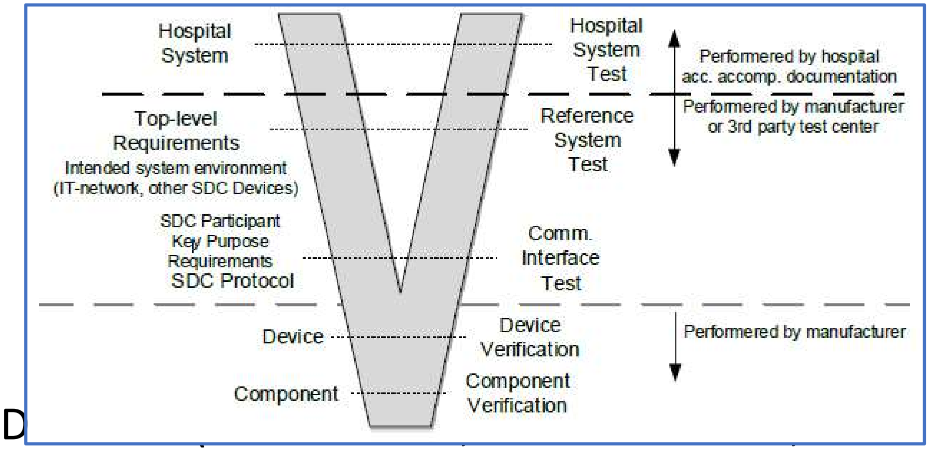
distributed system of medical devices for one clinical workplace.



Ventilator Med. Dev. Service
Feed pump Med. Dev. Service
Smart App Service Consumer
ICU bed Med. Dev. Service
Gateway Proxy. Service
Clinical Workplace SOMDA Backbone
WSN Proxy Service
EHR Proxy Service
Dialysis Med. Dev. Service
Infusion Pump Med. Dev. Service
Vital Signs Monitor Med. Dev. Service

Conceptual view of a SOMDA for a clinical workplace

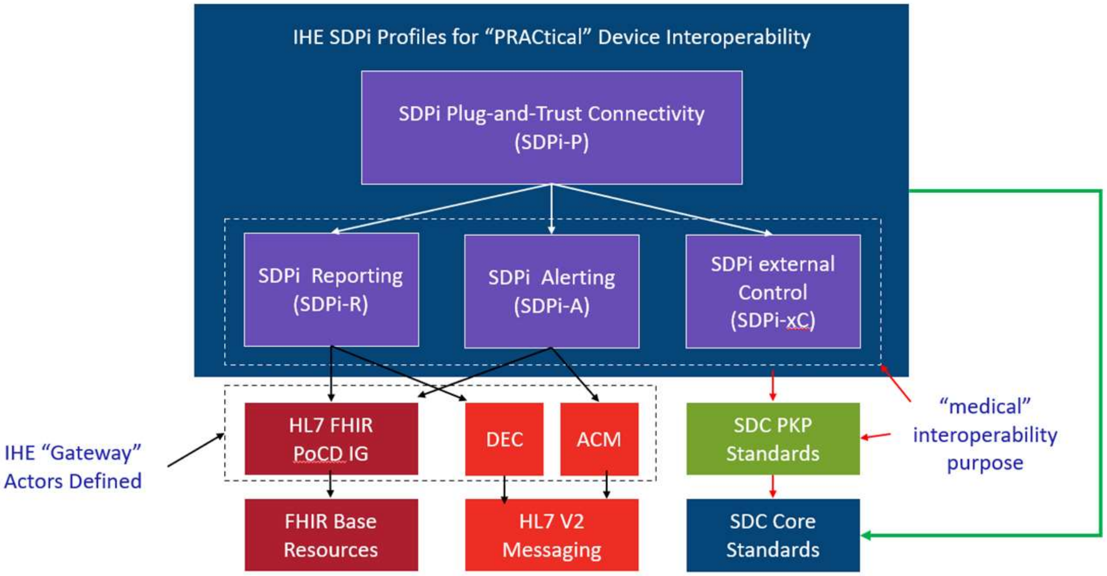
Garden: *Key Interoperability Purposes (SES)*


Hospital System
Top-level Requirements
Intended system environment (IT-network, other SDC Devices)
SDC Participant Key Purpose Requirements SDC Protocol
Device
Component
Hospital System Test
Reference System Test
Comm. Interface Test
Device Verification
Component Verification
Perfomered by hospital acc. accomp. documentation
Perfomered by manufacturer or 3rd party test center
Perfomered by manufacturer

- SES KIP
- Includes:
  - SES profiles @ MDI standards
  - Assurance Case Templates
  - Interoperability model(s)
  - 4 Key Purpose Areas for MDI
  - Profiles for applying SES standards to SDC/SD 62304, etc.)
  - INCLUDE 81001-1 / 80001-1 REQUIREMENTs that are aligned with LIFECYCLE PHASES including RIGHT SIDE STAKEHOLDERS and filling in "open" requirements => provisioned to device (via PKI?) and including arch requirements etc. [baseline PnT + "value added" for enhanced SES] *** Usability of Device Coupling Strategies, PnT, …
- SFC spec includes SES requirements that COULD / MUST be completed in the Deployment RM … + how formalized in the PKI/EKU provisioned at implementation?

Garden: *IHE SDPi*

- IHE SDPi
- IHE TF Constructs:
  - ✓ Use Cases (actors, transactions


IHE SDPi Profiles for "PRACtical" Device Interoperability
SDPi Plug-and-Trust Connectivity (SDPi-P)
SDPi Reporting (SDPi-R)
SDPi Alerting (SDPi-A)
SDPi external Control (SDPi-xC)
IHE "Gateway" Actors Defined
HL7 FHIR PoCD IG
DEC
ACM
SDC PKP Standards
"medical" interoperability purpose
FHIR Base Resources
HL7 V2 Messaging
SDC Core Standards

Garden: *ISO/IEEE 11073 SDC*

- SDC – ModSpecs, PKP, BICEPS, SOMDA, MDPWS
- <? 5 slides or one or … ???>
- <include mapping to TF volumes>
- Integrated Rxxxx
- BICEPS model
- SOMDA Model
- WS-*

Hanging Gardens: *Pulling it all together …*

- SES MDI (TF-1 Appendix A)
  - SFC – Specification / formalization / organization / …
  - Assurance Cases – composable / computable / V&V'able / CA'able
  - SES Requirements – per 81001-1, 80001-1, 60601-x-y, 62304, etc.
  - KIP(Regulatory) – sans implementation tech (see earlier slide)
  - CA @ SFC …

- ACID TEST:
  - ✓Requirement Test: Verify that PKP OID is in a device's security certificate
  - ✓Challenge: Do we know WHY it has to be there? Can we trace that requirement to the initial layer (Scenario?) that mandated its inclusion?

Additional Information

OMG Requirements Interchange Format (ReqIF) “Mapping” Background

OMG ReqIF: Base Model

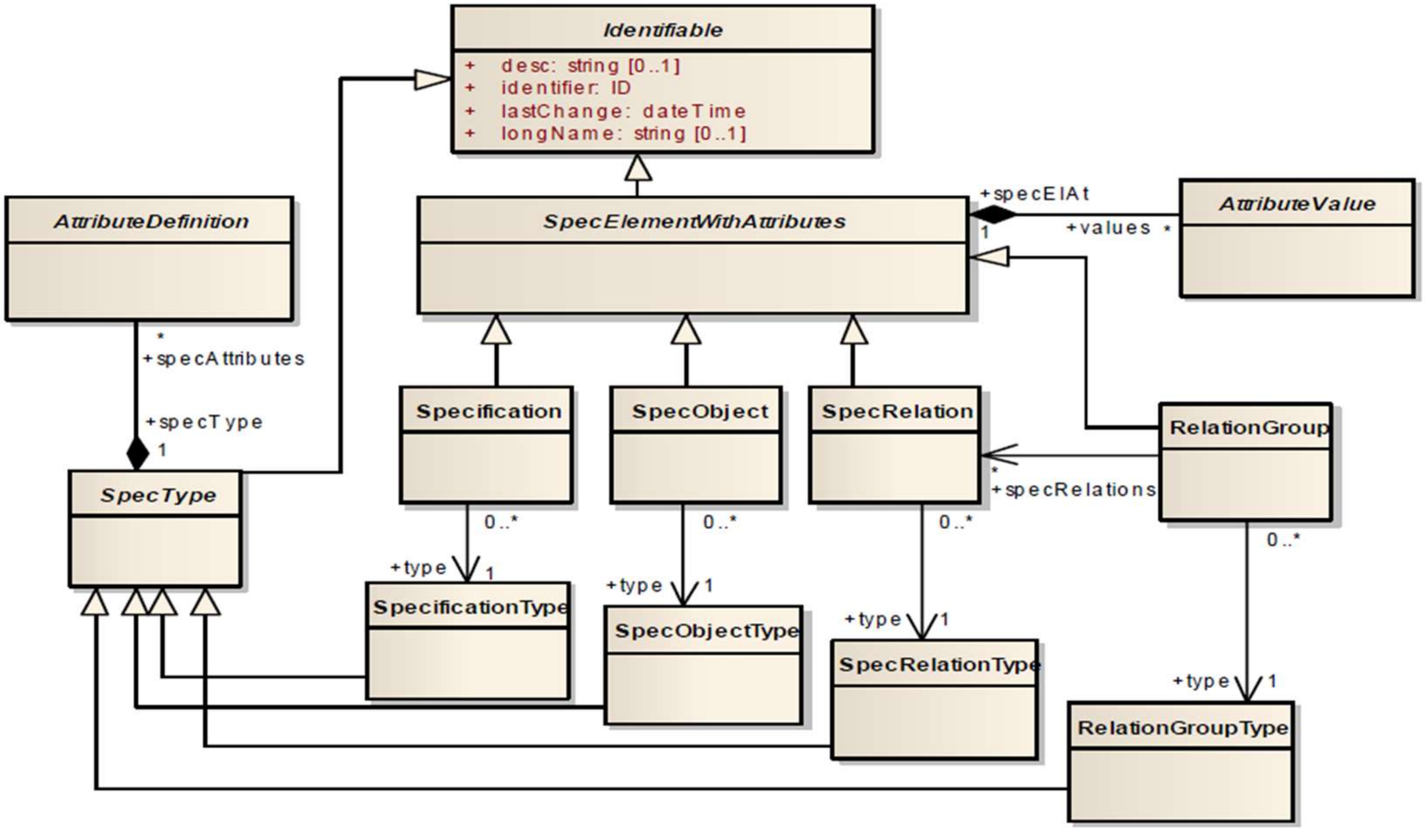
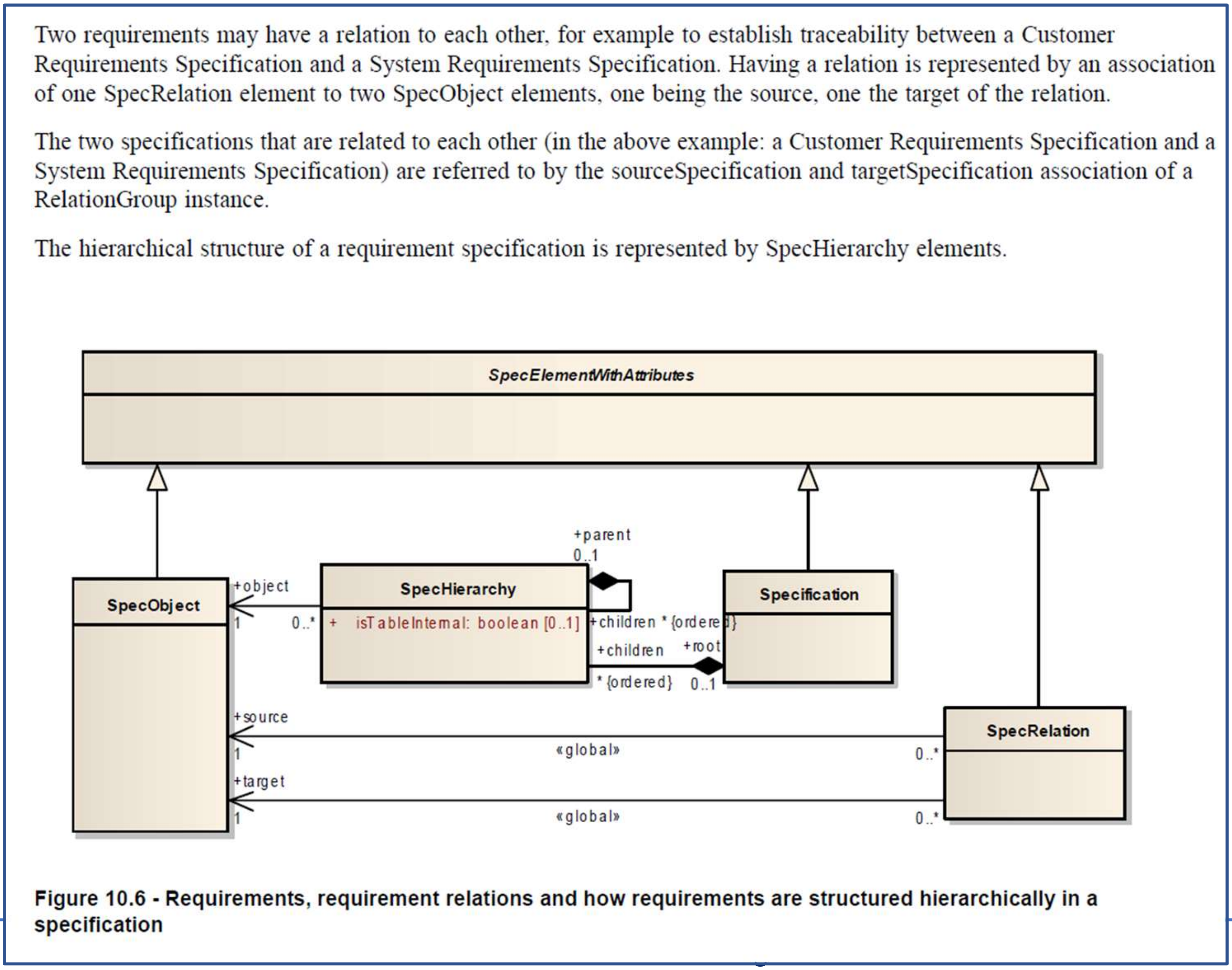


Figure 10.3 - Specification (Specificification), requirement (SpecObject), requirement relation (SpecRelation), relation group (RelationGroup) and associated attributes (AttributeDefinition, AttributeValue)

ReqIF: Requirement Hierarchies & Relationships

“mapping”
between
Source & Target
Requirements



Two requirements may have a relation to each other, for example to establish traceability between a Customer Requirements Specification and a System Requirements Specification. Having a relation is represented by an association of one SpecRelation element to two SpecObject elements, one being the source, one the target of the relation.

The two specifications that are related to each other (in the above example: a Customer Requirements Specification and a System Requirements Specification) are referred to by the sourceSpecification and targetSpecification association of a RelationGroup instance.

The hierarchical structure of a requirement specification is represented by SpecHierarchy elements.

Figure 10.6 - Requirements, requirement relations and how requirements are structured hierarchically in a specification