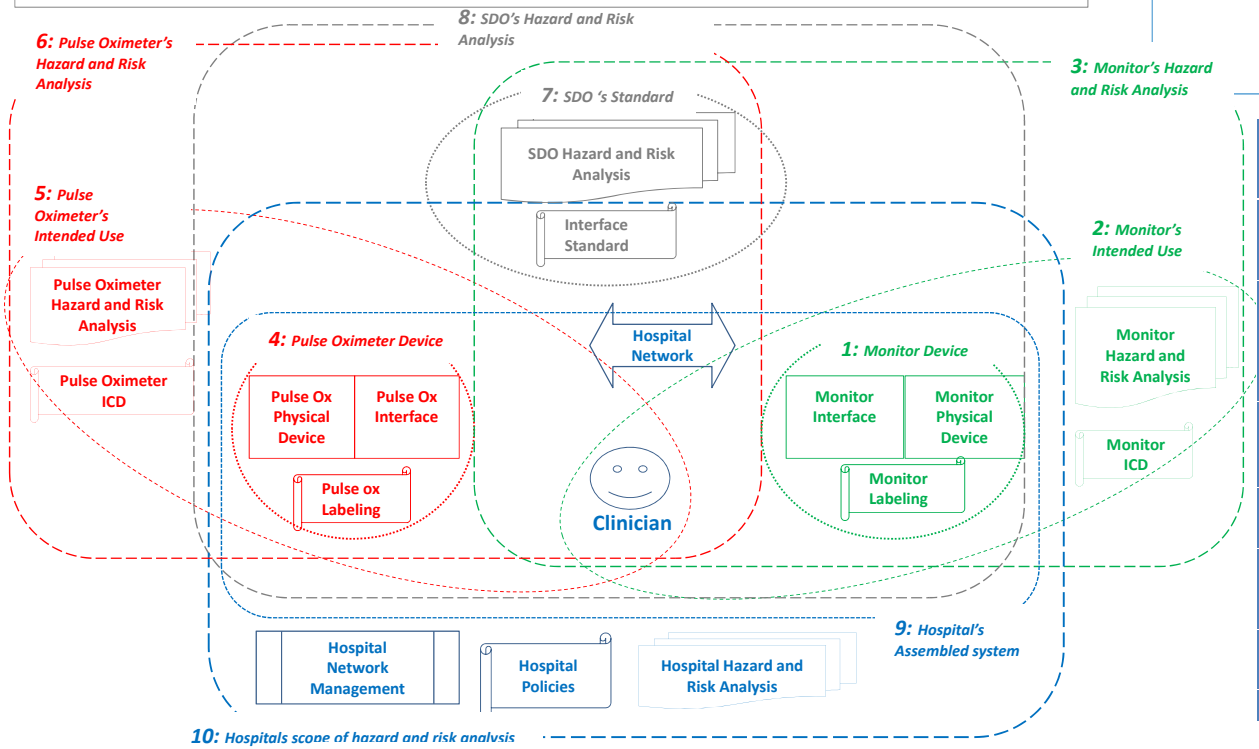
What is the interoperable system scope and its components?

The definition of a system depends on one's point of view:

1: Monitor instantiation in the hospital
2: Monitor scope of labeling, marketing claims, user manuals, and intended use from device manufacturers
3: Monitor manufacturer's system for the scope of hazard and risk analysis
4: Pulse oximeter instantiation in the hospital
5: Pulse oximeter manufacturer's scope of labeling, marketing claims, user manuals, and intended use
6: Pulse oximeter manufacturer's scope for hazard and risk analysis
7: Scope of delivered standard from a Standards Development Organization (SDO)
8: SDO's scope for hazard and risk analysis
9: Hospital's scope of the assembled system
10: Hospital's scope of hazard and risk analysis, quality assurance, and non-FDA regulatory compliance



What is Safe Interoperability?

There are many definitions of interoperability in health care. QMDI has determined that safe MD PnP interoperability is defined by what the Systems Engineering discipline calls Dynamic Interoperability; which implies exchange of data with defined:

- **Syntax (the format of the message)**
- **Semantics (the meaning of the message)**
- **Context (what was happening when the message was sent)**
- **State of the sender and receiver. This includes:**
  - **State of the sender defines the context and intent of the sender's message**
  - **State of the receiver defines the result the sender expects to effect on the receiver**
  - **Safety and hazard information, including the expected results when information is missing, corrupted, incomplete, late, wrong, or the devices are unexpectedly disconnected**

Interoperability Level (Turnitsa*)	Technical Example	Necessary Framework	Information Shared between sub-systems	Organizational Goals	Integrated Solution Scope	Healthcare Use
6: Conceptual	**FDA cleared product**	Business and Engineering processes	Budget, Schedule, Specifications, Requirements	Same product, an integrated system from multiple vendors	Single System	Cleared Medical Device product
5: Dynamic	**Medical Device Plug-and-Play**	**State Model**	**Intention and Expected Effect of both Sender and Receiver**	**Assemble a system for the same clinical purpose from different sub-systems vendors**	**Assembled System of sub-systems**	**One (or more) Clinical Scenarios**
4: Pragmatic	HDO Implemented IHE domain	Workflow	Information + Context	Use different systems in the same workflow	Connected, but separate systems sharing data	Inter- or intra-organization process and procedures
3: Semantic	HL7	Ontology	Information + Meaning	Use data the same way	Complete Data Records	Shared Patient Medical Records
2: Syntactic	Current Time as defined by NTP	Data Structure	Information	Use the same data records	Single Clinical Event Record	Data fields in messages, databases, or API's
1: Technical	32-bit BigEndian Integer	Binary Field Definition	Bits and bytes	Use the same data media	Hardware component	Computer and Network infrastructure
0: None	N/A	None	N/A	N/A	N/A	N/A

* Turnitsa, Charles., Extending the Levels of Conceptual Interoperability Model. Summer Computer Simulation Conference. 2005.

Interoperability Hazards and Risk Mitigations

1) Device Warning Communication

Device Use Warnings are defined by the manufacturer for hazards and mitigations implemented internally to the device. Only the device itself can be relied on to recognize hazardous situations, and the manufacturer must define the risk mitigation. Other ICE sub-systems should, but cannot be assumed to always be able to communicate device failures to the user/operator.. For example:

- PCA software app. If connectivity is lost from necessary physiological sensors, the IV Pump fail-safe mode is to rely on clinician monitoring of patient vital signs.
- IV Pump. If connectivity to a PCA control interlock is lost, the fail-safe mode is to stop infusing morphine and notice the clinician/operator.

2) Technical Interactions Monitoring

These are technology and infrastructure conditions that may affect the performance of both connected and un-connected devices (e.g. power, bandwidth, jitter, latency). These properties are measurable, but cannot be mitigated by the ICE system automatically because the steps necessary to ensure the safety of a patient with degraded or non-functioning devices can only be made by a clinician. It is conceivable that CDS applications could be developed to aid in the decision making processes when infrastructure failures are detected taking into account the clinical scenario, last known physiological state of patient, medical goals, etc… However these would be regulated medical devices themselves.

- Network monitoring infrastructure records and reports available network bandwidth and packet loss.

3) Interoperability Interaction Prevention

These are hazards that are created by interoperability and are unique to systems of interoperable sub-systems. These can be identified, measured, and controlled by ICE sub-systems – with the proper application of Systems Engineering. For example:

- Two devices cannot safely implement the same control parameter over a third device. If there are two sources of controller sending commands, then neither can reliably know the current state of the controlee.
- Operator overrides of safety conditions must have only one source within the assembled system.

4) Physiological effect on the patient caused by multiple devices

Some of these can be known from the device capability and operation. For example:

- A blood pressure cuff on the same arm as a pulse oximeter. When the cuff constricts the blood flow on that arm, the SpO_2 data from the fingertip will be compromised.

All medical devices (sub-systems) are always responsible for their own safe operation