# Promoting Safe Medical Device Interoperability

Anura Fernando – Principal Engineer

Underwriters Laboratories

January 26, 2015

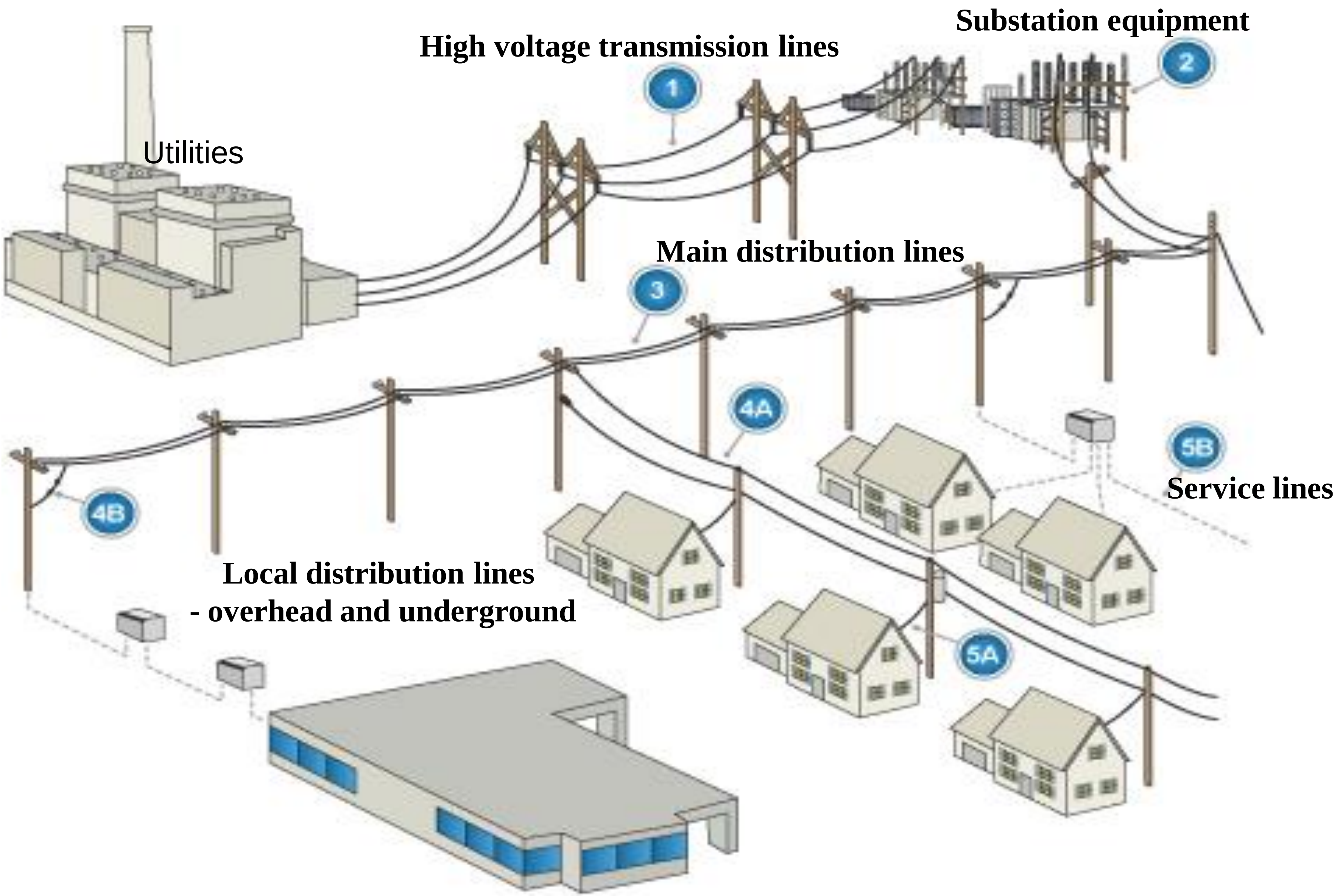
# Data…the new “electricity” for product safety engineers

In the 1890’s as fires began plaguing American cities:

A member of the National Board of Fire Underwriters was quoted during that time as saying, “Better buildings are burning in a greater ratio than ever before…and there are mysterious causes at work that we do not understand. I believe (the cause) to be electricity” (Bezane, 1994)

**We now understand electrical safety fairly well, but do we fully understand all of the safety issues associated with the distribution and utility of *data*?**

# Networks are networks



Utilities

High voltage transmission lines

Substation equipment

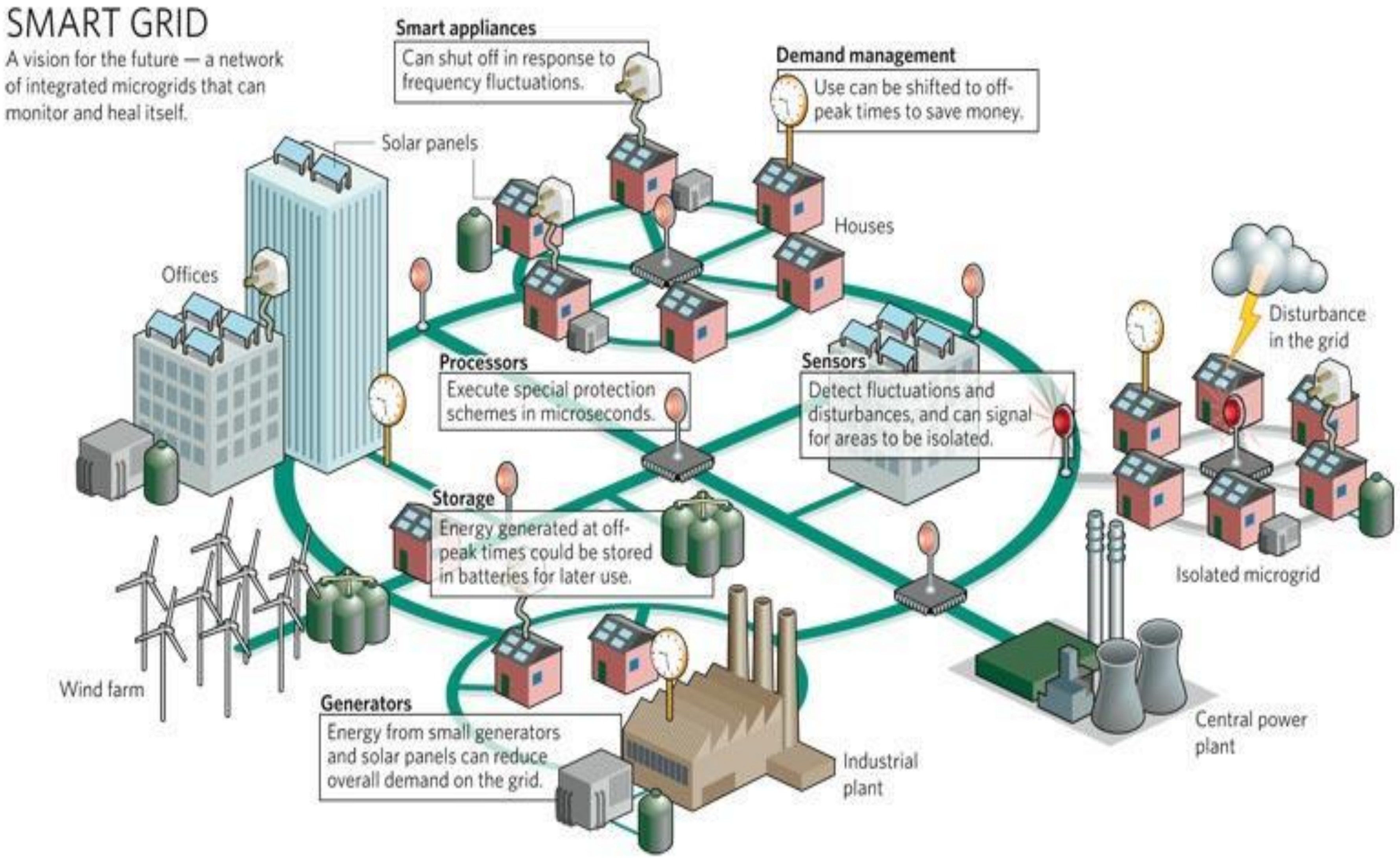
Main distribution lines

Service lines

Local distribution lines
- overhead and underground

http://www.dteenergy.com/images/restorationGraphic.jpg

# But there are many Use Cases to be considered…



SMART GRID

A vision for the future — a network of integrated microgrids that can monitor and heal itself.

**Smart appliances**

Can shut off in response to frequency fluctuations.

**Demand management**

Use can be shifted to off-peak times to save money.

**Processors**

Execute special protection schemes in microseconds.

**Sensors**

Detect fluctuations and disturbances, and can signal for areas to be isolated.

**Storage**

Energy generated at off-peak times could be stored in batteries for later use.

**Generators**

Energy from small generators and solar panels can reduce overall demand on the grid.

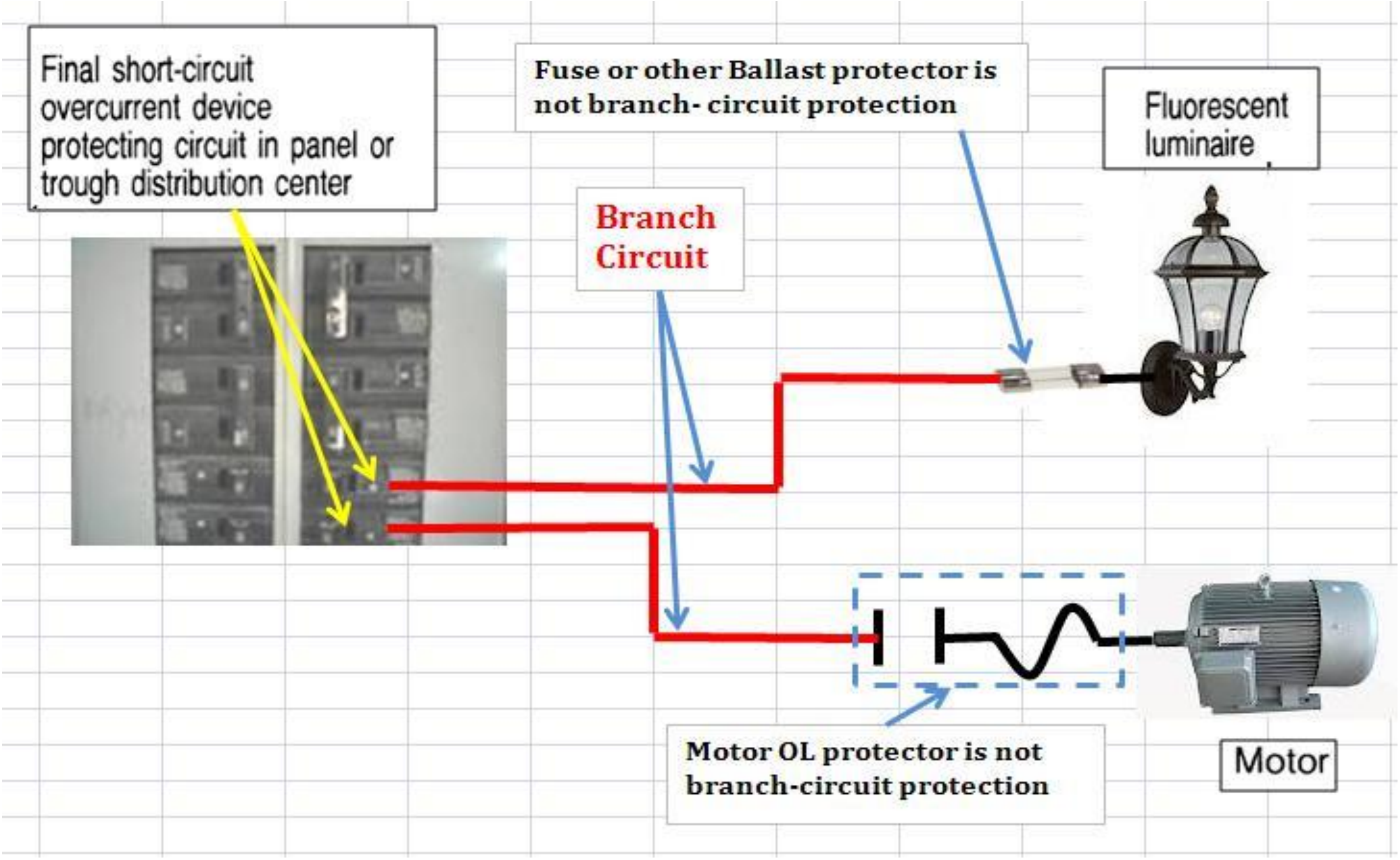
http://energyinformative.org/wp-content/uploads/2012/01/smart-grid.jpg

# …and layers of complexity to be tested

Entertainment
Lighting
Power Distribution
Cooking

http://www.bishopriccompanies.com/custom-homes/electrical/

# …and more layers…



Final short-circuit overcurrent device protecting circuit in panel or trough distribution center

Fuse or other Ballast protector is not branch- circuit protection

Fluorescent luminaire

Branch Circuit

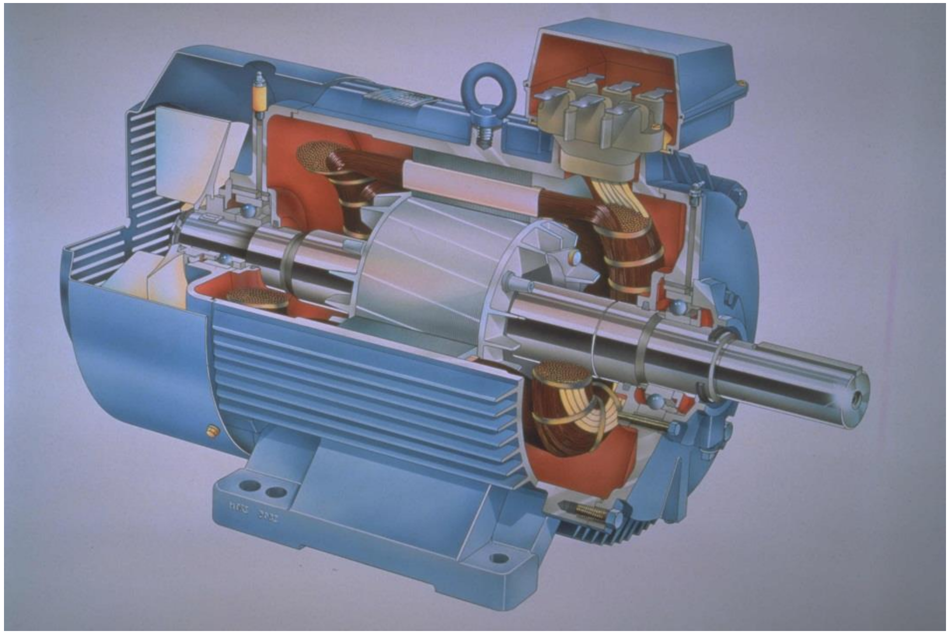
Motor OL protector is not branch-circuit protection

Motor

http://alihassanelashmawy.blogspot.com/2011/12/nec-article-100-branch-circuit.html

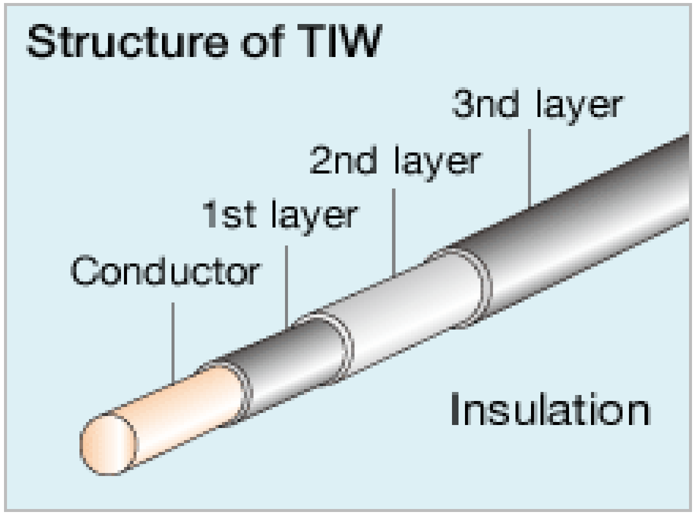
# …and more layers…

http://news.thomasnet.com/fullstory/Post-Top-Luminaire-Base-optimizes-safety-during-maintenance-599980



http://www.mindconnection.com/library/electrical/motorslip.htm

# …and more layers…



http://www.totoku.com/products/electric_wires/wires/tiw/

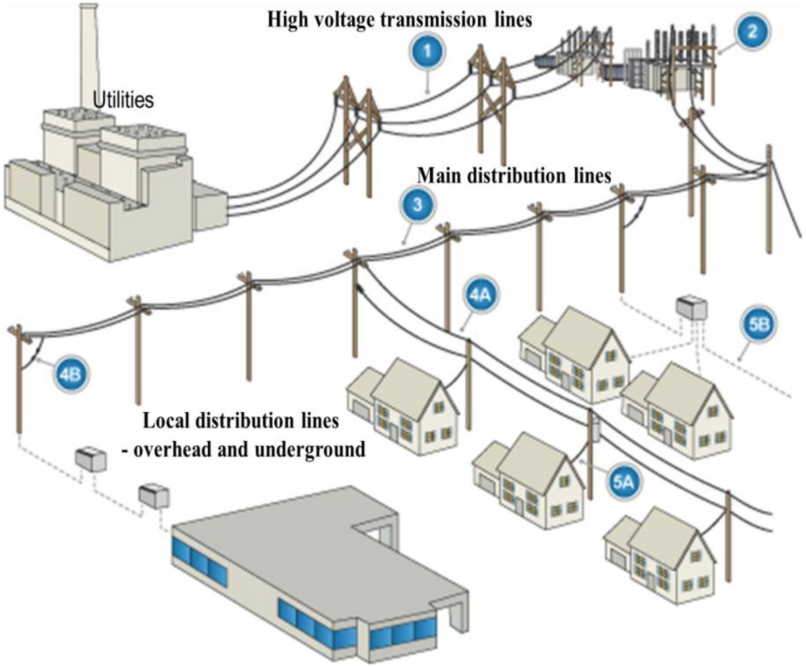
http://www.wencosimplex.com/wire_strippers.htm

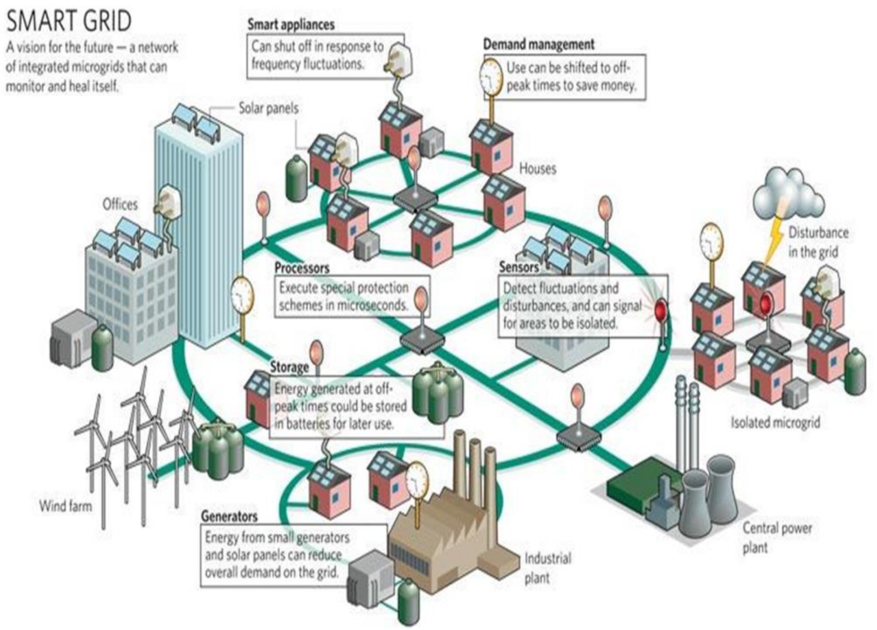
# But the point is

**Every “component” could be a “system”**

**and**

**every “system” could be a “component.”**





A vision for the future — a network of integrated microgrids that can monitor and heal itself.

Smart appliances: Can shut off in response to frequency fluctuations.

Demand management: Use can be shifted to off-peak times to save money.

Processors: Execute special protection schemes in microseconds.

Sensors: Detect fluctuations and disturbances, and can signal for areas to be isolated.

Storage: Energy generated at off-peak times could be stored in batteries for later use.

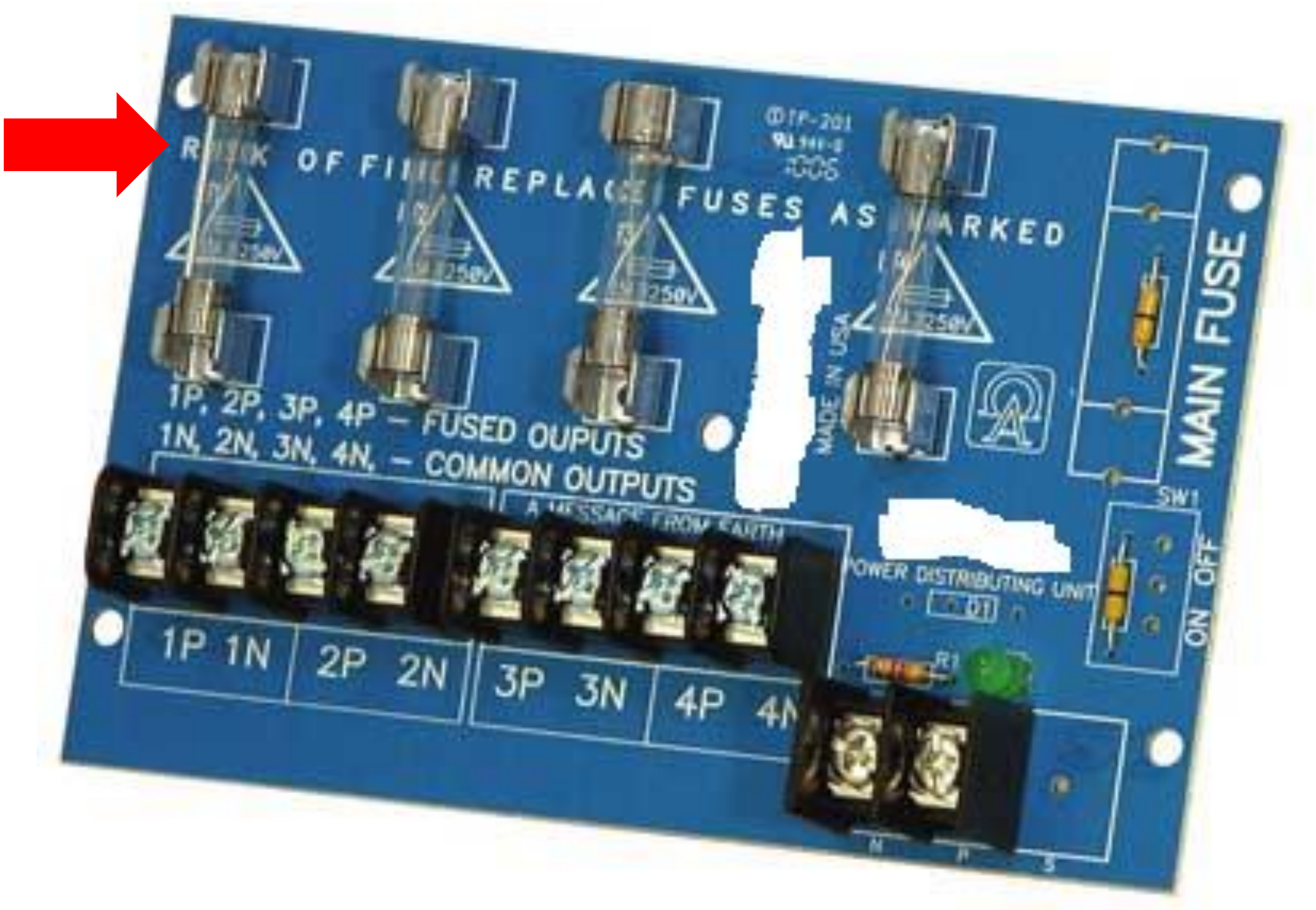
Generators: Energy from small generators and solar panels can reduce overall demand on the grid.

# So, “component” testing has to meet “system” safety objectives.

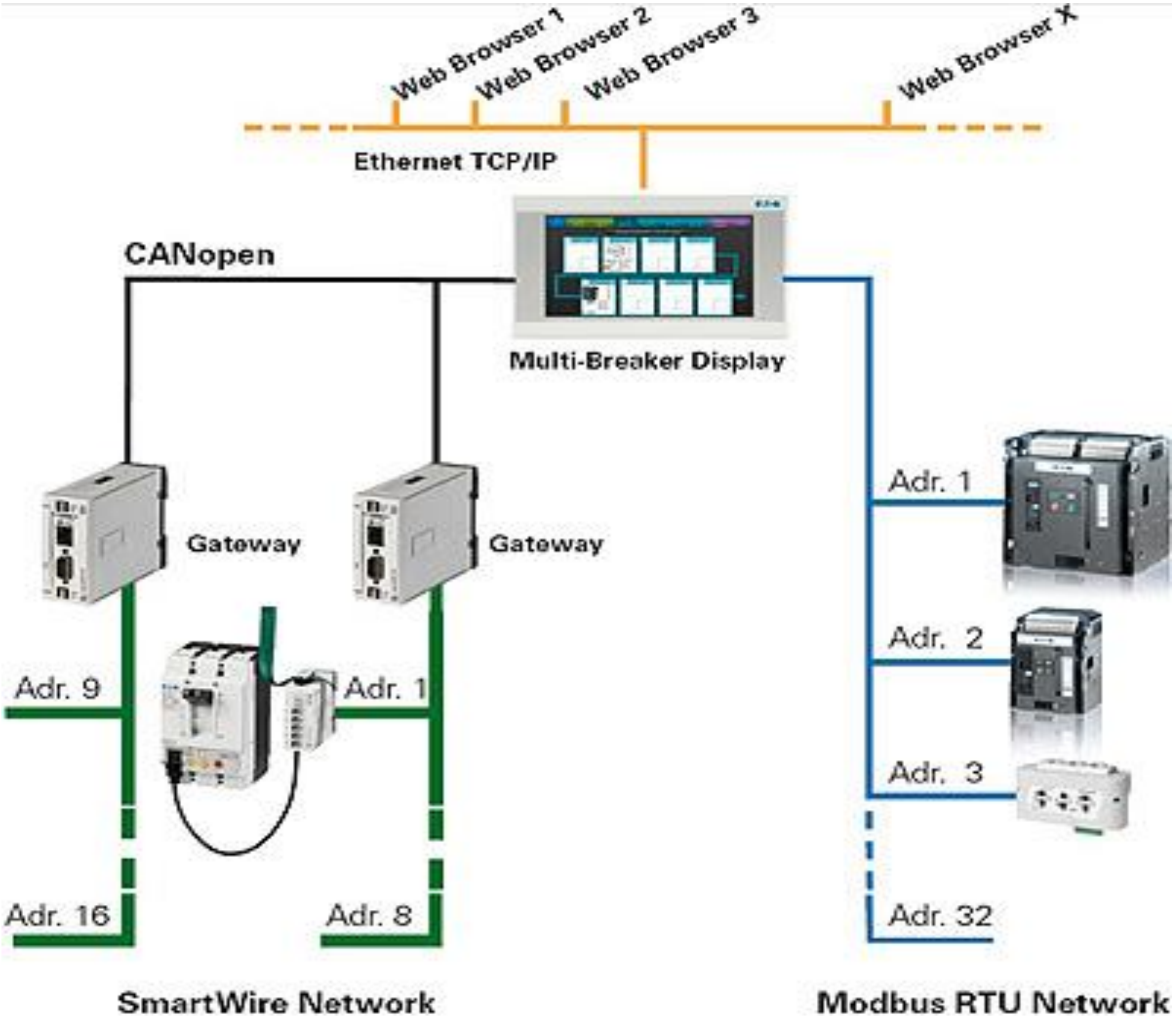
http://www.bob937.com/bobsstupidnews/Story.aspx?id=1445467

http://www.punjabkesari.com/health/health_files/electricshock.gif

# And “component” capabilities must satisfy “system” requirements.


R     K OF FI     REPLA     FUSES AS     ARKED
1P, 2P, 3P, 4P – FUSED OUPUTS
1N, 2N, 3N, 4N, – COMMON OUTPUTS
MADE IN USA
MAIN FUSE
SW1
ON OFF
POWER DISTRIBUTING UNIT
1P 1N
2P 2N
3P 3N
4P 4N

# Even many “basic electrical” risks are now mitigated by software-based electronic controls (e.g. web-enabled circuit breakers)



www.moeller.net

# Lessons Learned for E/E/PE Systems Safety

**VS**

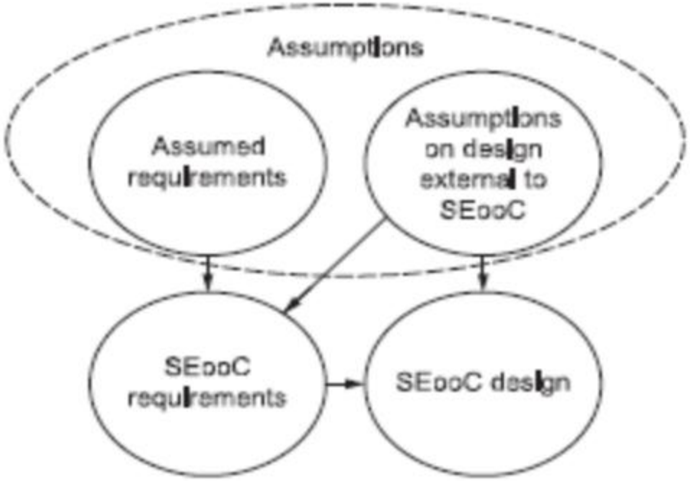
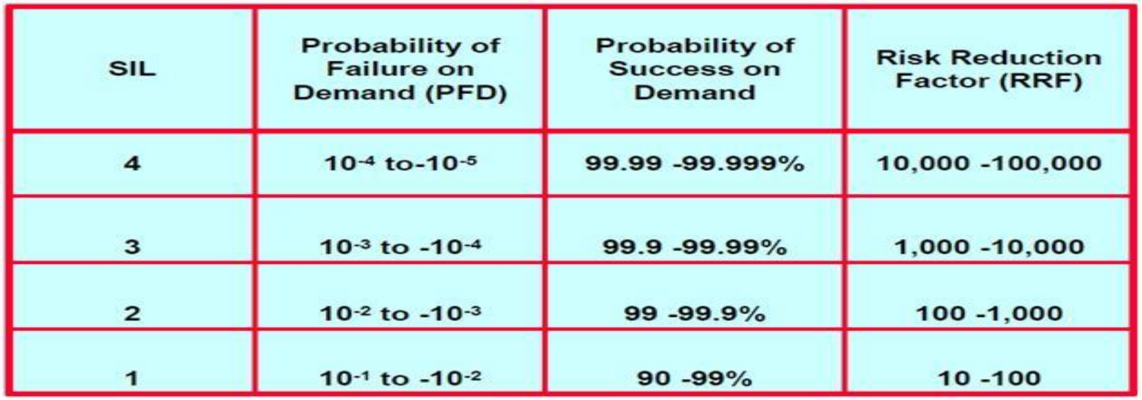


**Figure 18 — Relationship between assumptions and SEooC development**

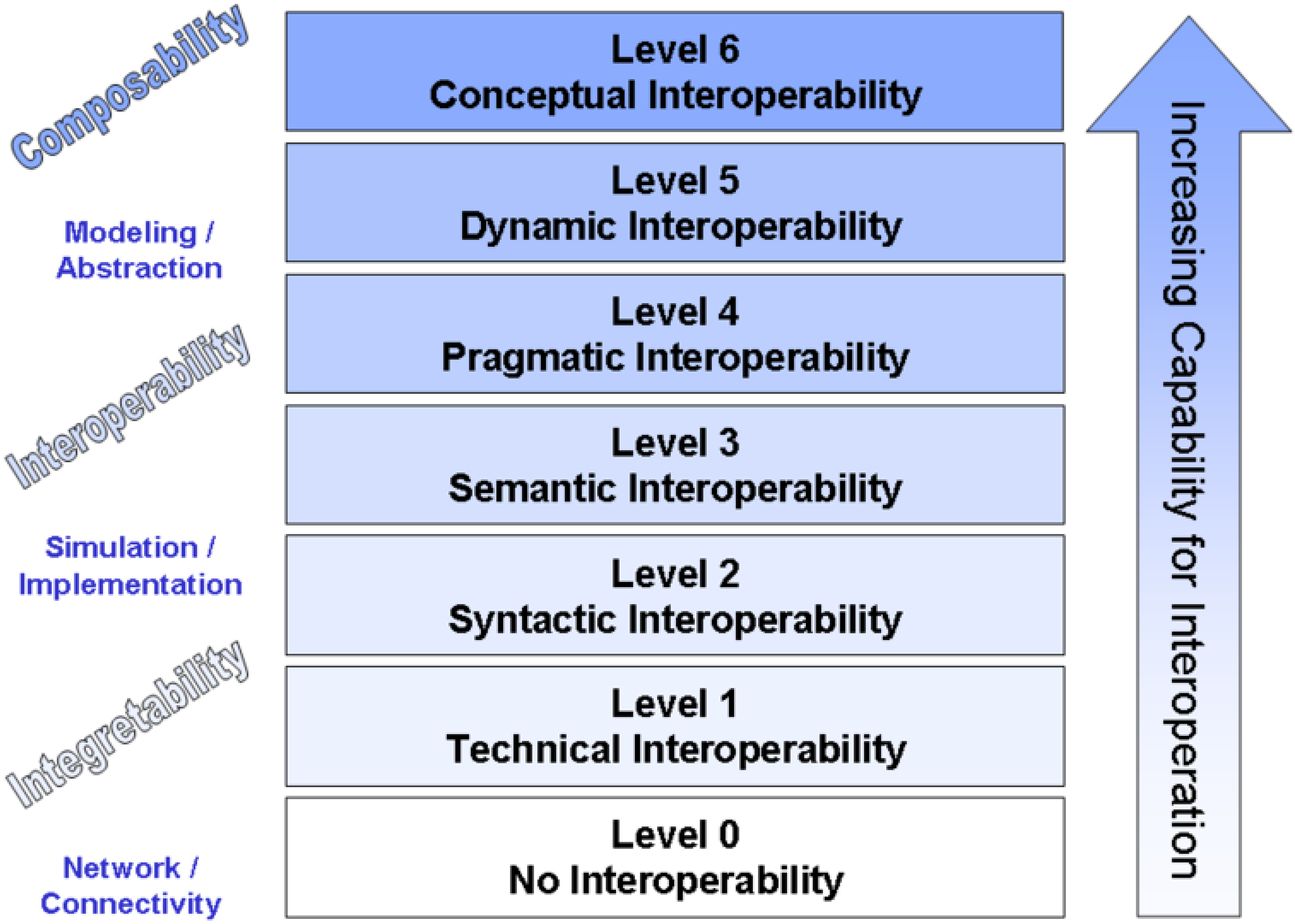
Reference: ISO 26262



| SIL | Probability of Failure on Demand (PFD) | Probability of Success on Demand | Risk Reduction Factor (RRF) |
|---|---|---|---|
| 4 | $10^{-4}$ to-$10^{-5}$ | 99.99 -99.999% | 10,000 -100,000 |
| 3 | $10^{-3}$ to -$10^{-4}$ | 99.9 -99.99% | 1,000 -10,000 |
| 2 | $10^{-2}$ to -$10^{-3}$ | 99 -99.9% | 100 -1,000 |
| 1 | $10^{-1}$ to -$10^{-2}$ | 90 -99% | 10 -100 |

http://www.piping-engineering.com/sil-safety-integrity-level-overview.html

# In order to achieve “interoperability”



Composability

Modeling / Abstraction

Interoperability

Simulation / Implementation

Integretability

Network / Connectivity

Level 6
Conceptual Interoperability

Level 5
Dynamic Interoperability

Level 4
Pragmatic Interoperability

Level 3
Semantic Interoperability

Level 2
Syntactic Interoperability

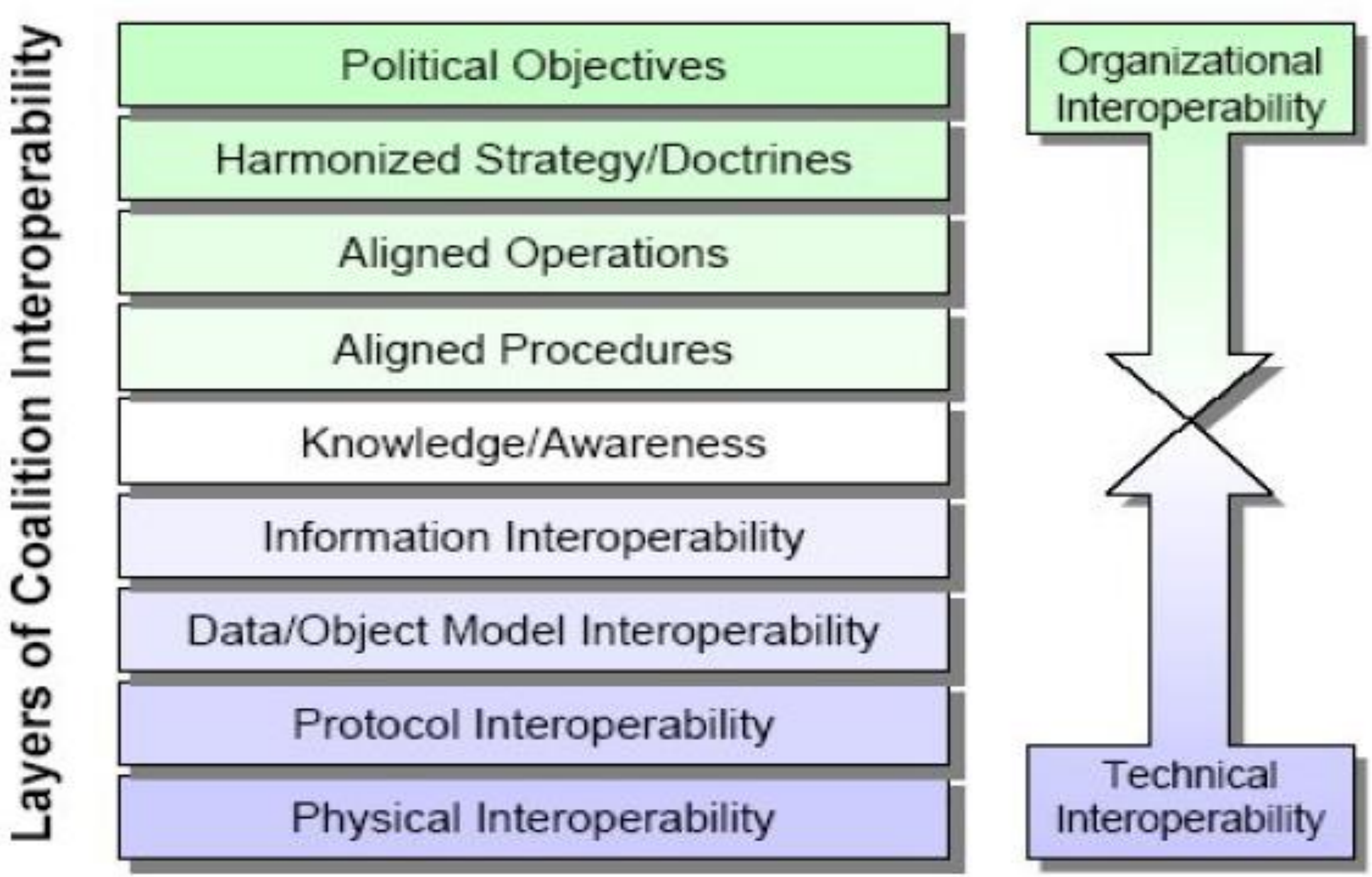
Level 1
Technical Interoperability

Level 0
No Interoperability

Increasing Capability for Interoperation

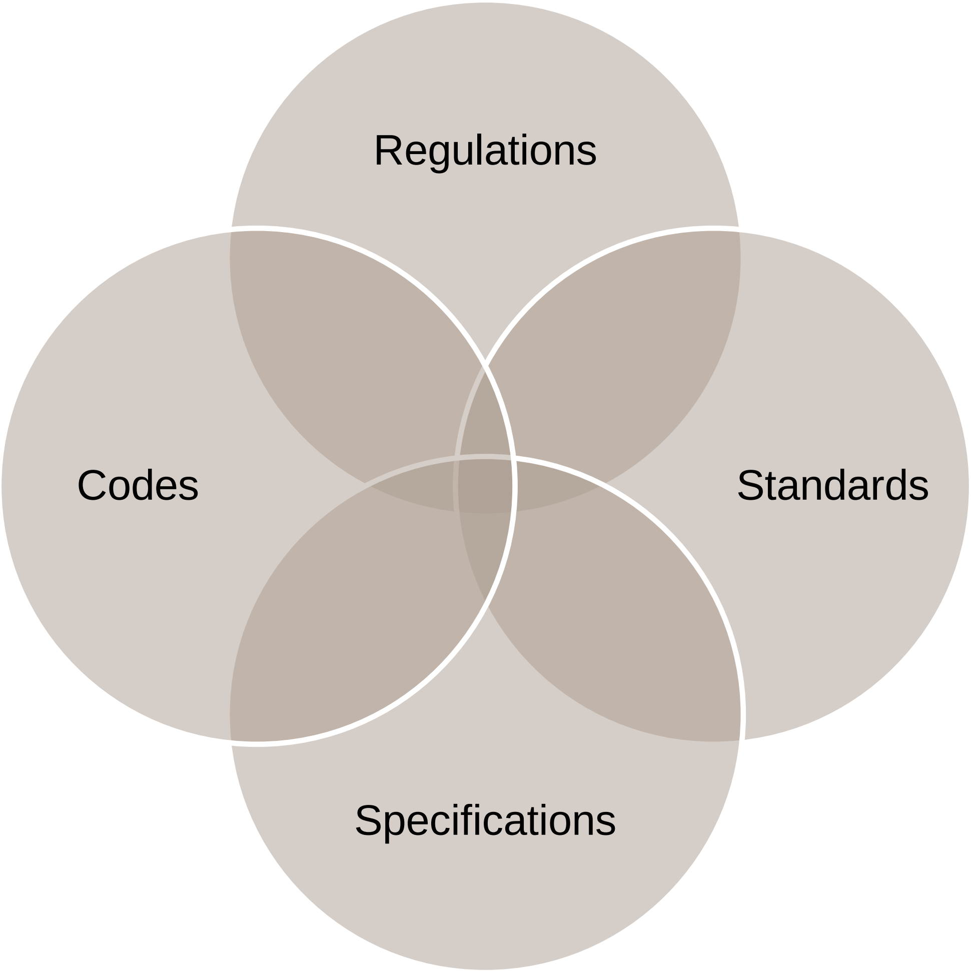
Andreas Tolk, first use in <<Tolk A, Diallo SY, Turnitsa CD, Winters LS (2006) "Composable M&S Web Services for Net-centric Applications," Journal for Defense Modeling & Simulation (JDMS), Volume 3 Number 1, pp. 27-44, January 2006>>, also used in << Tolk A: "What comes after the Semantic Web, PADS Implications for the Dynamic Web," Proceedings of the 20th ACM/IEEE/SCS Workshop on Principles of Advanced and Distributed Simulation (PADS 2006), Singapore, May 2006, pp. 55-62

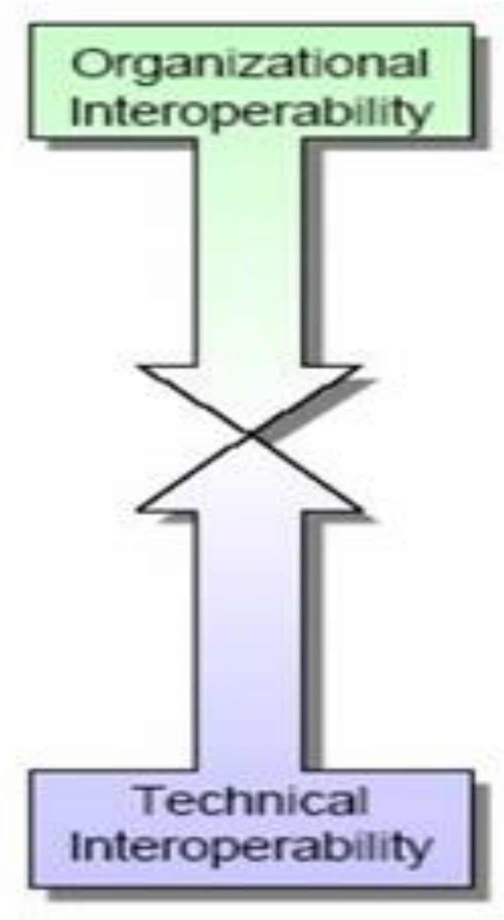
# In order to realize safe “interoperability”


Layers of Coalition Interoperability
Political Objectives
Harmonized Strategy/Doctrines
Aligned Operations
Aligned Procedures
Knowledge/Awareness
Information Interoperability
Data/Object Model Interoperability
Protocol Interoperability
Physical Interoperability
Organizational Interoperability
Technical Interoperability

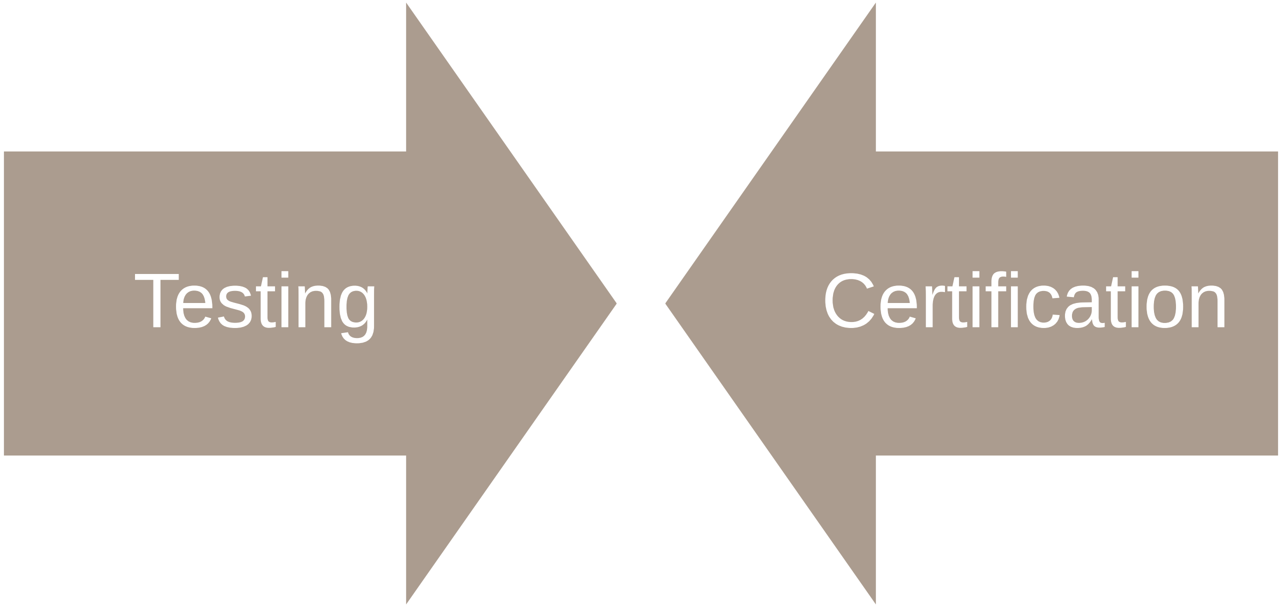
[Tolk 03] Tolk, Andreas. “Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability.” 8th International Command and Control Research and Technology Symposium (ICCRTS), Washington, D.C., June 17-19, 2003. Washington DC: Command and Control Research Program (CCRP), 2003

# Drivers for alignment of “safety thinking” are necessary





# Demonstration of conformance to drivers via

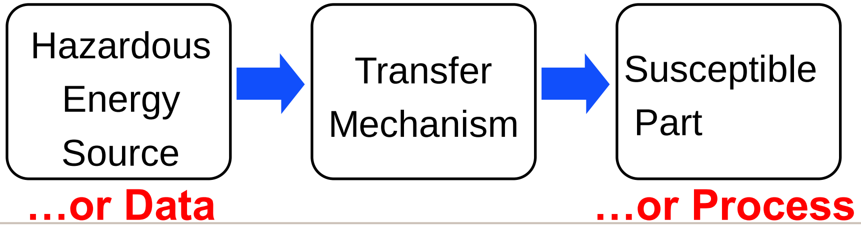


Testing

Certification

# Risk management for standardization and testing

## HBSE Premise



Hazardous Energy Source

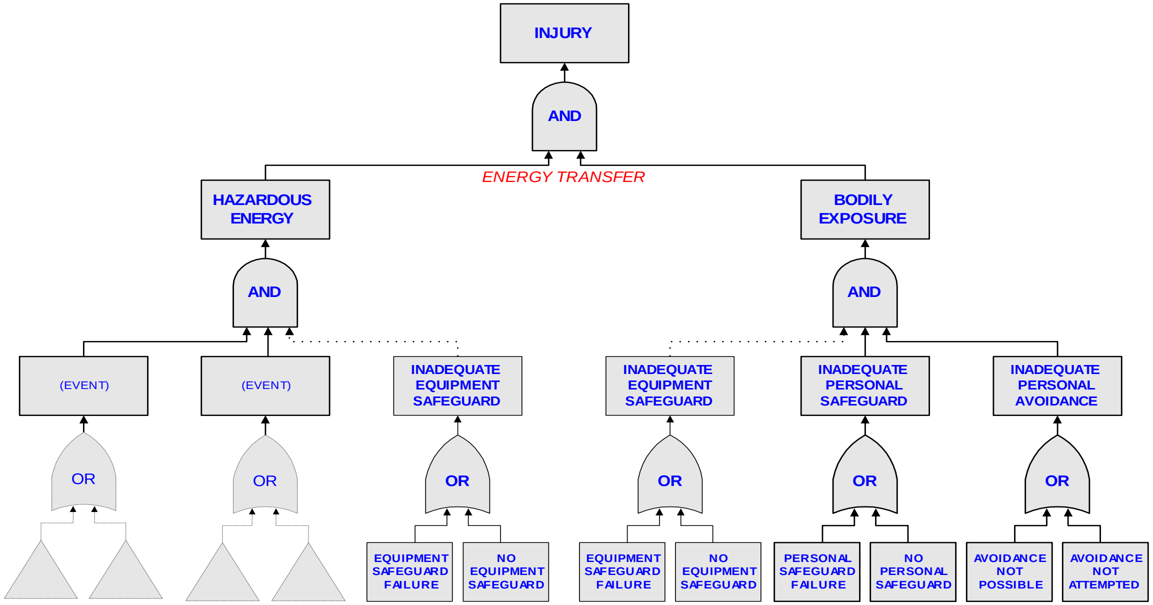
Transfer Mechanism

Susceptible Part

…or Data

…or Process

## HBSE Standard Injury Fault Tree



INJURY

AND

ENERGY TRANSFER

HAZARDOUS ENERGY

BODILY EXPOSURE

AND

AND

(EVENT)

(EVENT)

INADEQUATE EQUIPMENT SAFEGUARD

INADEQUATE EQUIPMENT SAFEGUARD

INADEQUATE PERSONAL SAFEGUARD

INADEQUATE PERSONAL AVOIDANCE

OR

OR

OR

OR

OR

OR

EQUIPMENT SAFEGUARD FAILURE

NO EQUIPMENT SAFEGUARD

EQUIPMENT SAFEGUARD FAILURE

NO EQUIPMENT SAFEGUARD

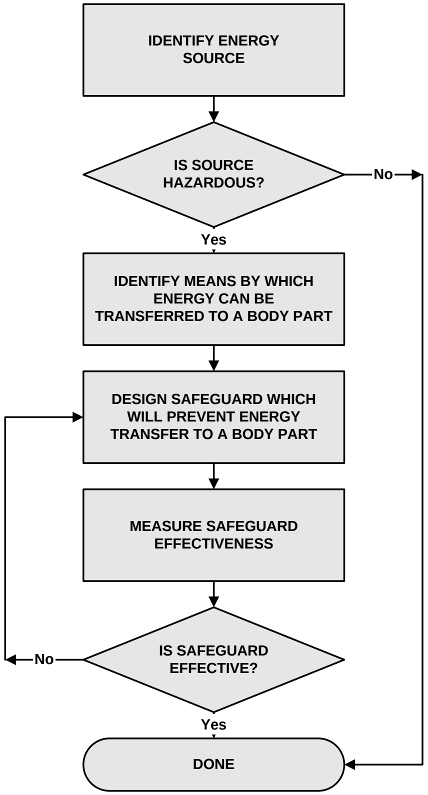
PERSONAL SAFEGUARD FAILURE

NO PERSONAL SAFEGUARD

AVOIDANCE NOT POSSIBLE

AVOIDANCE NOT ATTEMPTED

## HBSE Process



IDENTIFY ENERGY SOURCE

IS SOURCE HAZARDOUS?

No

Yes

IDENTIFY MEANS BY WHICH ENERGY CAN BE TRANSFERRED TO A BODY PART

DESIGN SAFEGUARD WHICH WILL PREVENT ENERGY TRANSFER TO A BODY PART

MEASURE SAFEGUARD EFFECTIVENESS

IS SAFEGUARD EFFECTIVE?

No

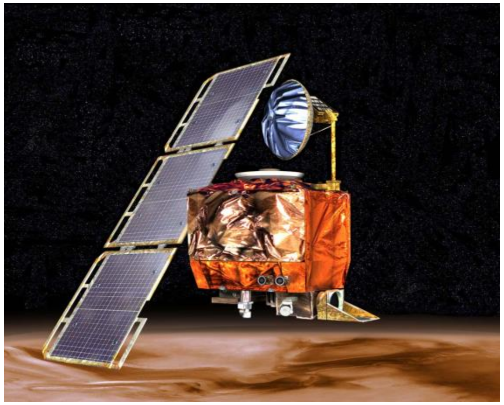
Yes

DONE

# Regardless of the application domain, system testing and certification should strive to address:

- Responsibility / Accountability (Ownership of the System)
- The Potential for Miscommunication (Requirements)
- Incomplete Understanding of Technology (Failure Modes)
- Inadequate Risk Controls for Random Faults (incl. CCF)
- Ineffective Project Management Metrics (Safety Detractors)

# …otherwise…

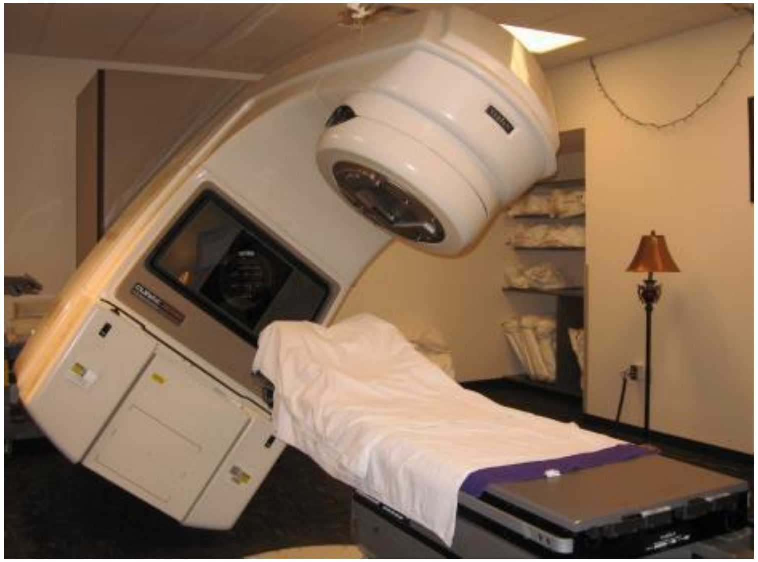


Mars Climate Orbiter

- Mismatched units

Ariane 5

Floating point value too large to be represented by signed integer



Therac - 25

- “unlikely” sequence of keystrokes

- Integrated re-used sw into incompatible hardware (no interlocks)

- Improper V&V – no pre-release integration testing

http://50quidsoundboy.net/wp-content/uploads/2011/05/thumb-21367-radiation_therapy.jpg

# AAMI/UL 2800 Problem Statement

- Risk exists in both the “absence of interoperability” as well as the “presence of interoperability”

- UL noticed a “healthcare megatrend” aligned with its public safety mission, and an opportunity to significantly reduce unnecessary deaths due to the “absence of interoperability” by providing a means to demonstrate safety during the “presence of interoperability.”

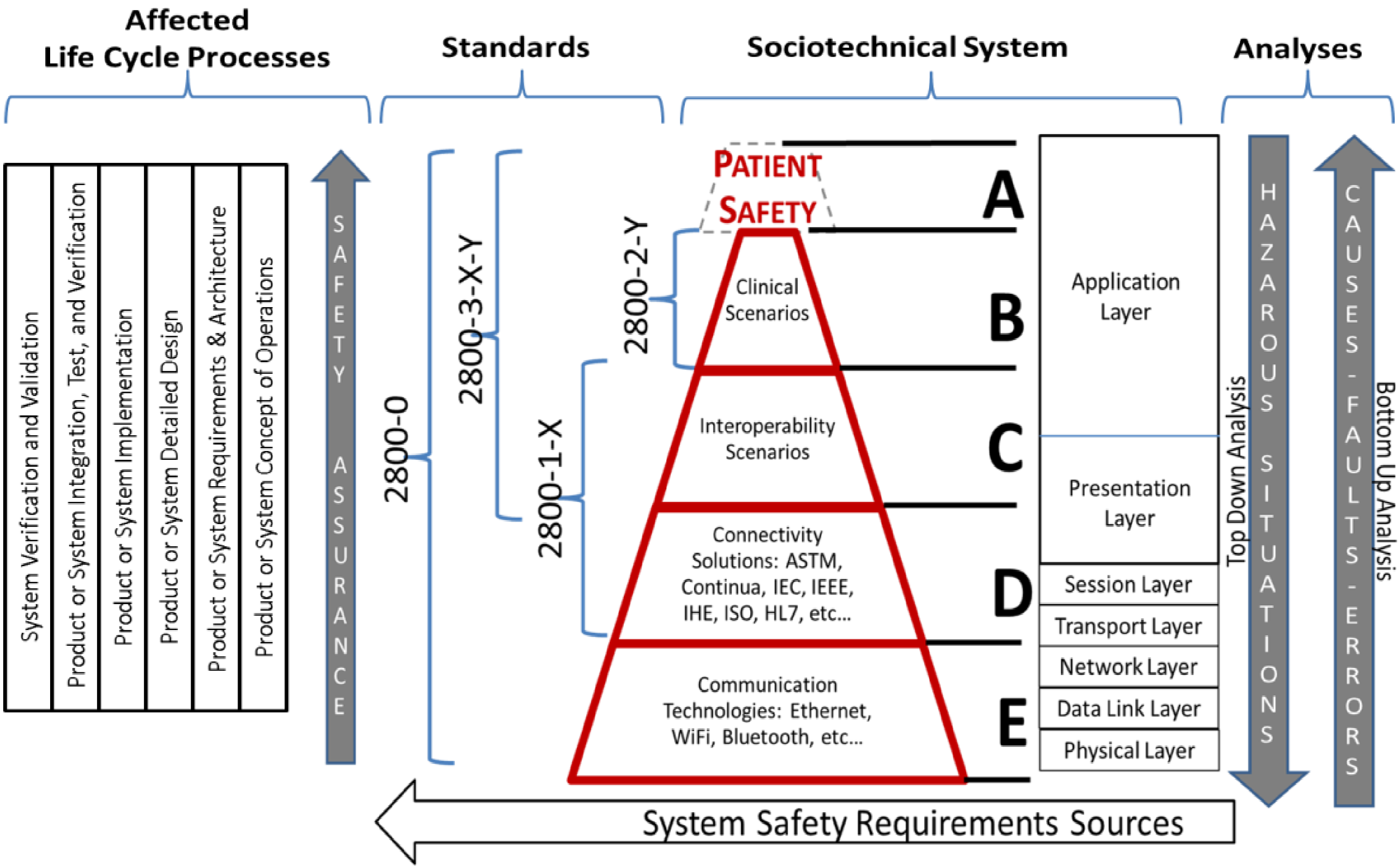
- Safety-focused architecture standardization work had already begun under ASTM efforts, however, testing and certification of conformance was missing. Such testing and conformance certification seemed to be a necessary part of the ecosystem that could aslo support regulation.

# Objectives of AAMI/UL 2800

## Safety, Security, and Essential Performance Objectives:

- Identification of common functional components/capabilities to be found in medical interoperable systems for which safety/security requirements will be enumerated
- Correct patient and user identification
- Component authentication (i.e. to facilitate plug and play interoperability, ensuring trusted composition)
- Clinical app logic execution safety (partitioning, non-interference) coordination (incl. mechanisms to manage complexity) with appropriate statement and realization of system safety requirements
- General mechanisms for establishing traceability of adverse event to root cause (ie. data provenance)
- Fail-safe or fail-operational (fault tolerant) risk-associated state determinism
- General requirements on “Real time” capabilities (i.e. Response time < Hazard time)
- Time synchronization
- Characterization of interface safety requirements for testing under normal operating conditions as well as failure mode and stress conditions
- Safety-related QoS metrics (e.g. bandwidth, latency, etc…)
- Partitioning mechanisms for data and time partitioning for both application execution and communication
- Unambiguous descriptions of interoperability architectures and component interface
- Consistent and unambiguous interpretation of physiological, clinical, and patient data as well as control signals

# AAMI/UL 2800 Promotes Safe Interoperability



Affected Life Cycle Processes
Standards
Sociotechnical System
Analyses
System Verification and Validation
Product or System Integration, Test, and Verification
Product or System Implementation
Product or System Detailed Design
Product or System Requirements & Architecture
Product or System Concept of Operations
SAFETY ASSURANCE
2800-0
2800-3-X-Y
2800-1-X
2800-2-Y
PATIENT SAFETY
Clinical Scenarios
Interoperability Scenarios
Connectivity Solutions: ASTM, Continua, IEC, IEEE, IHE, ISO, HL7, etc...
Communication Technologies: Ethernet, WiFi, Bluetooth, etc...
A
B
C
D
E
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Top Down Analysis
HAZAROUS SITUATIONS
CAUSES - FAULTS - ERRORS
Bottom Up Analysis
System Safety Requirements Sources

# Thank You

For more information please visit:

www.ul.com/eHealth