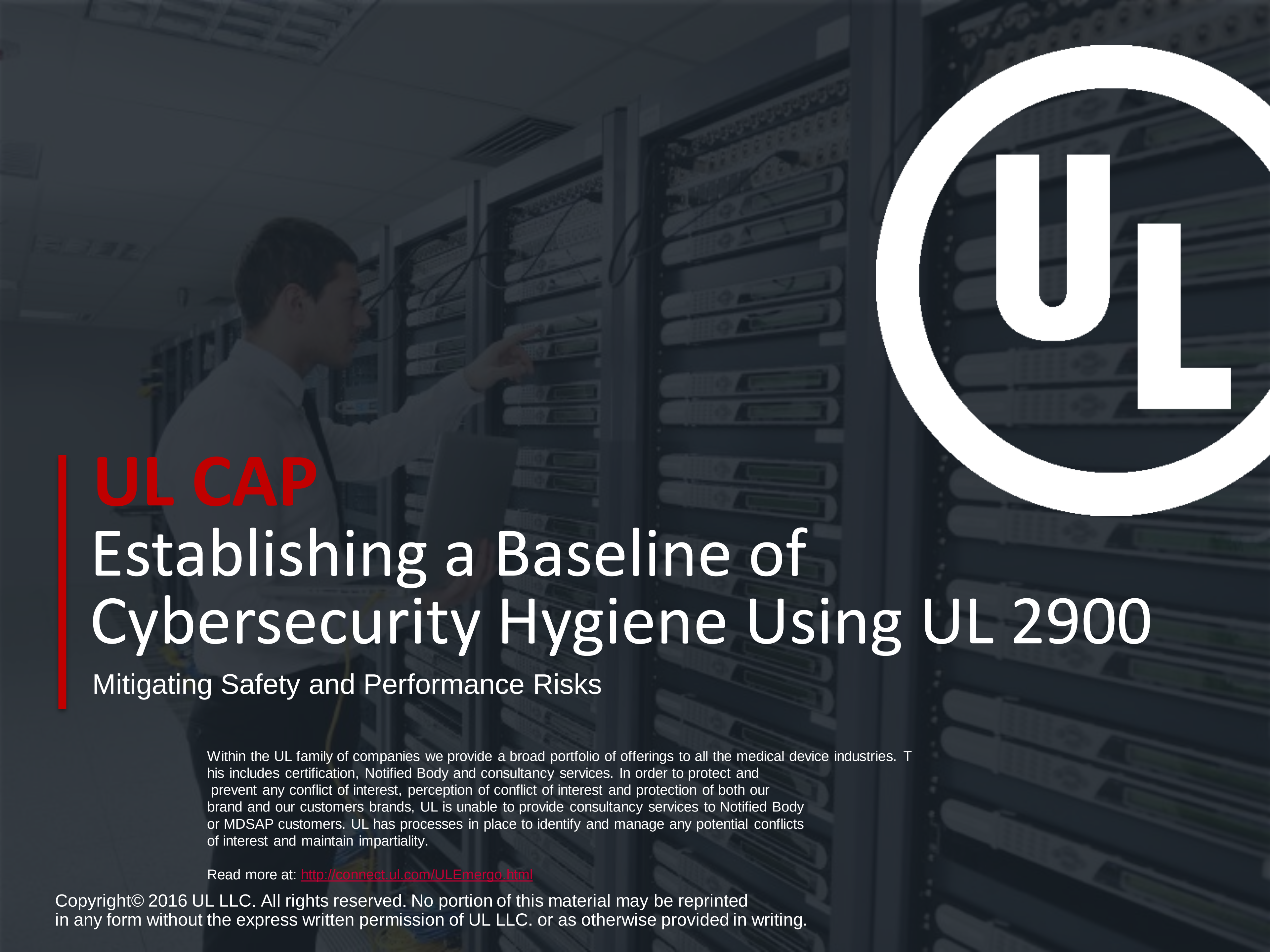


UL CAP

Establishing a Baseline of Cybersecurity Hygiene Using UL 2900

Mitigating Safety and Performance Risks

Within the UL family of companies we provide a broad portfolio of offerings to all the medical device industries. T his includes certification, Notified Body and consultancy services. In order to protect and prevent any conflict of interest, perception of conflict of interest and protection of both our brand and our customers brands, UL is unable to provide consultancy services to Notified Body or MDSAP customers. UL has processes in place to identify and manage any potential conflicts of interest and maintain impartiality.

Read more at: http://connect.ul.com/ULEmergo.html

History of UL – the early use of electricity

“On opening day, President Grover Cleveland ignited 100,000 incandescent lamps by pressing a single button.”

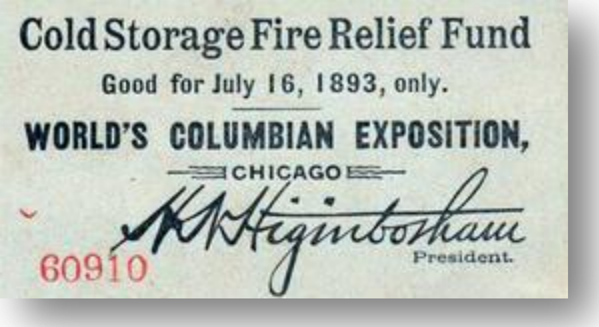
https://www.element14.com/community/community/news/blog/2013/05/06/chicago-world-s-fair-120th-anniversary-lighting-use-of-ac-first-night-time-football-game

Unintended consequences of new technology

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)

https://chicagology.com/columbiaexpo/fair058/



Cold Storage Fire Relief Fund

Good for July 16, 1893, only.

WORLD'S COLUMBIAN EXPOSITION,

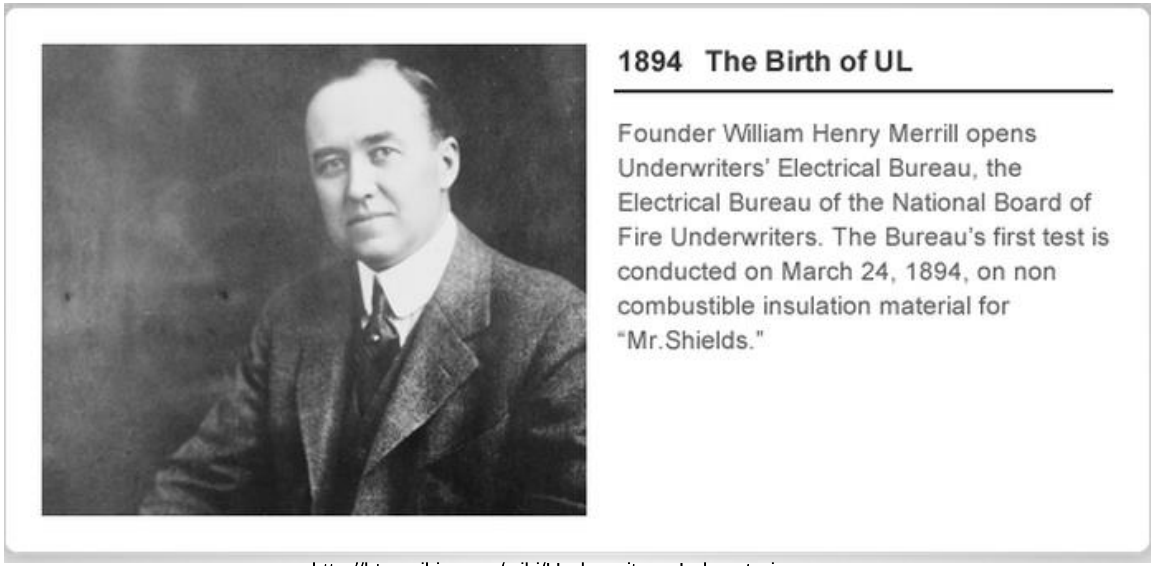
CHICAGO

H N Higinbotham

President.

60910

The origins of UL



1894 The Birth of UL

Founder William Henry Merrill opens Underwriters' Electrical Bureau, the Electrical Bureau of the National Board of Fire Underwriters. The Bureau's first test is conducted on March 24, 1894, on non combustible insulation material for "Mr.Shields."

http://htm.wikia.com/wiki/Underwriters_Laboratories

“Know by test and state the facts”

Today UL has many roles spanning the globe

Testing

Training

Inspection

Standards Development

Certification

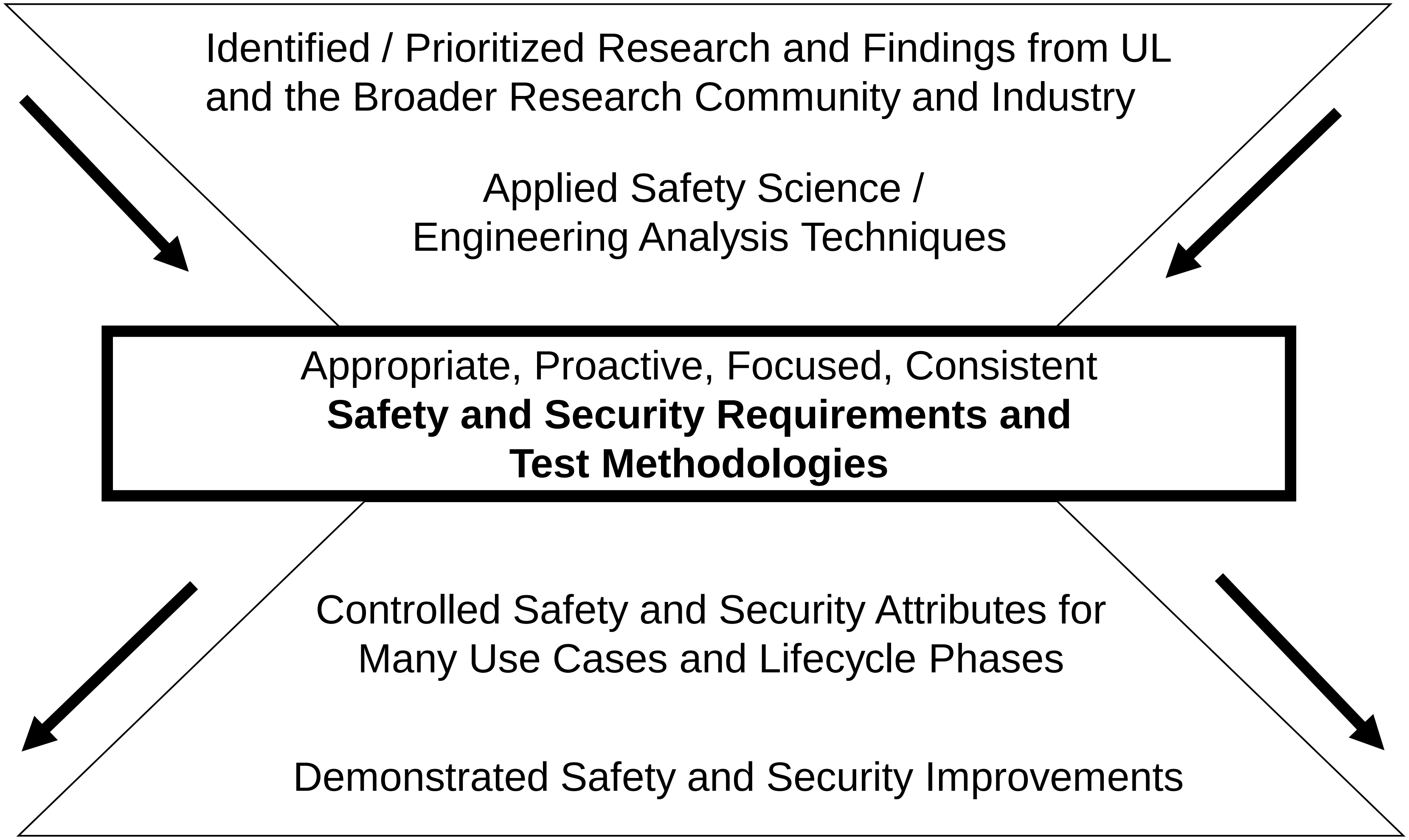
Research

Advisory

Audit

Maintain strict firewalls to avoid any CoI

UL strategy for safety and security standards



Identified / Prioritized Research and Findings from UL
and the Broader Research Community and Industry

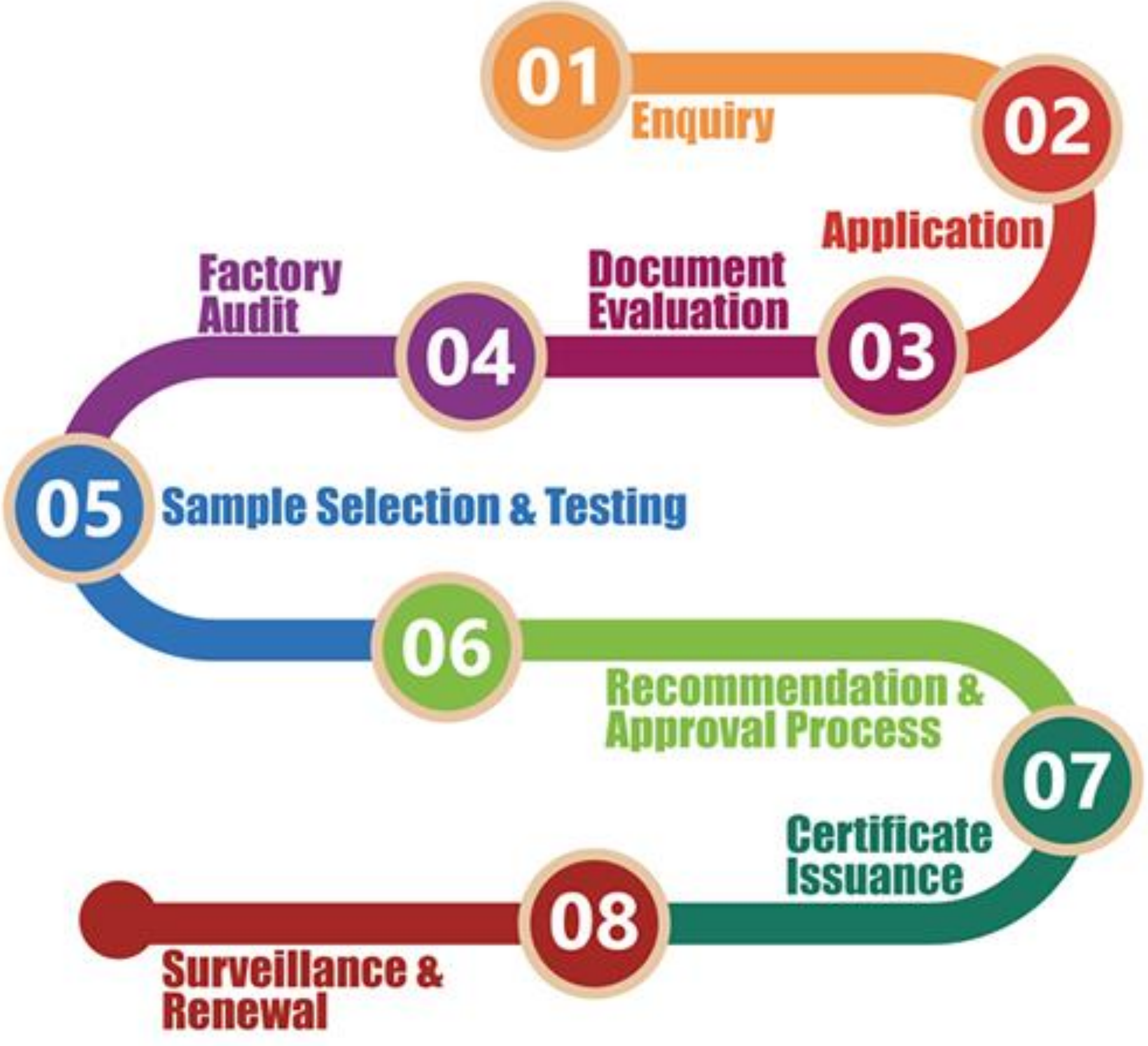
Applied Safety Science /
Engineering Analysis Techniques

Appropriate, Proactive, Focused, Consistent
Safety and Security Requirements and
Test Methodologies

Controlled Safety and Security Attributes for
Many Use Cases and Lifecycle Phases

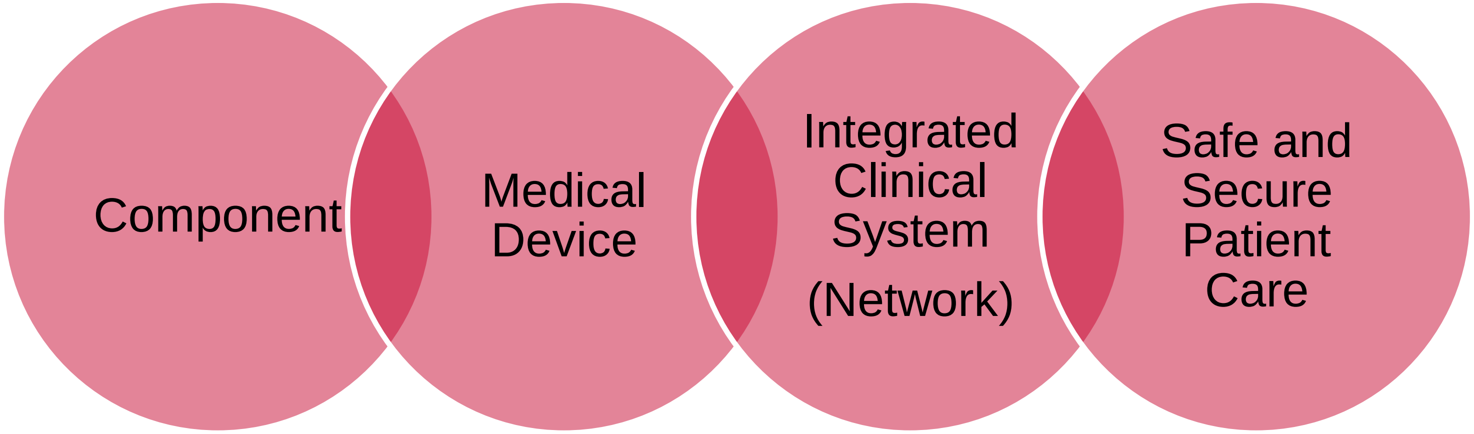
Demonstrated Safety and Security Improvements

Certification in the context of standards

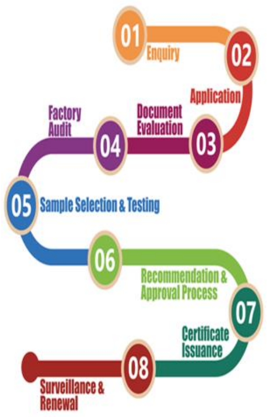


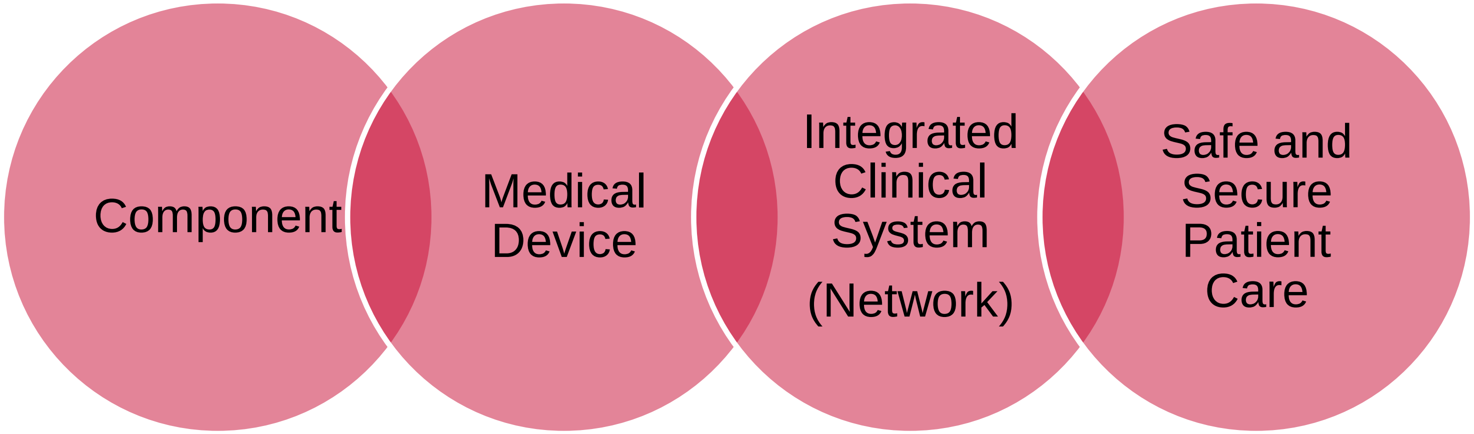
https://www.cidbholdings.com.my/webv2/index.php/technical-services/construction-product-certification

“Certification” can address safety and security concerns that span the supply chain



Certifications can help manage supply chain risk





Component

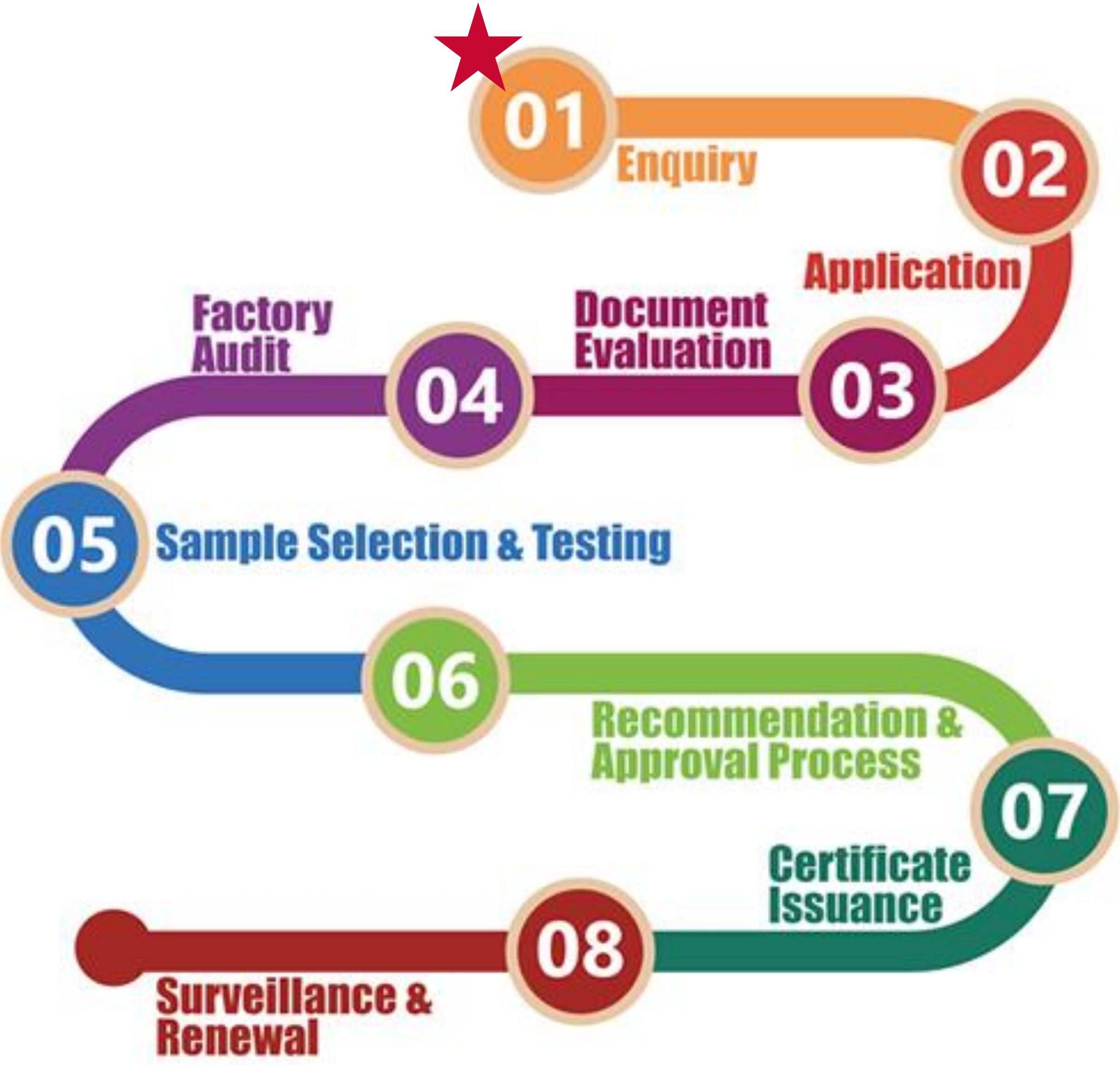
Medical Device

Integrated Clinical System

(Network)

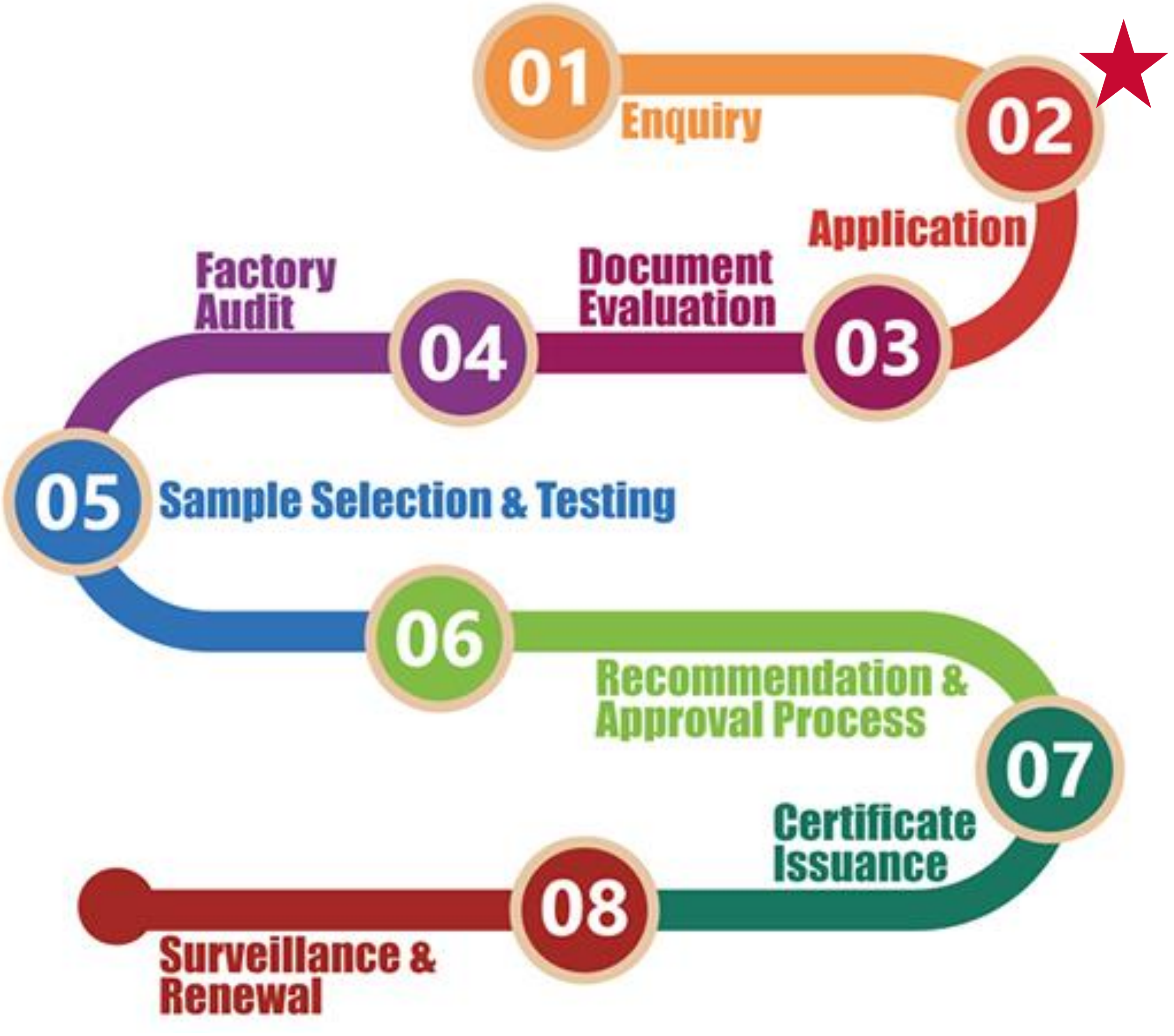
Safe and Secure Patient Care

01 – Megatrends drive interest (electricity, security)



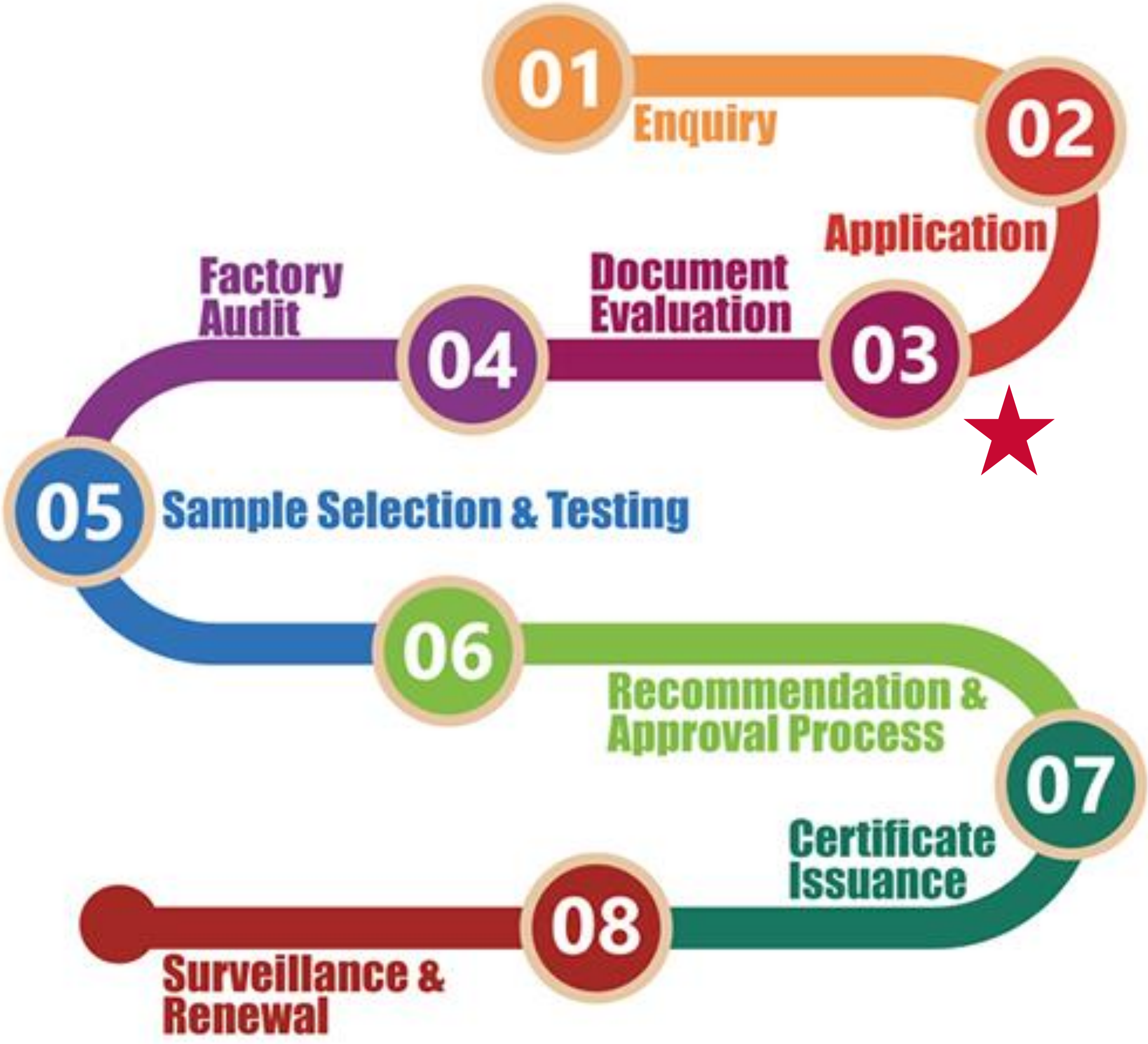
https://www.cidbholdings.com.my/webv2/index.php/technical-services/construction-product-certification

02 – Procurement language drives engagement



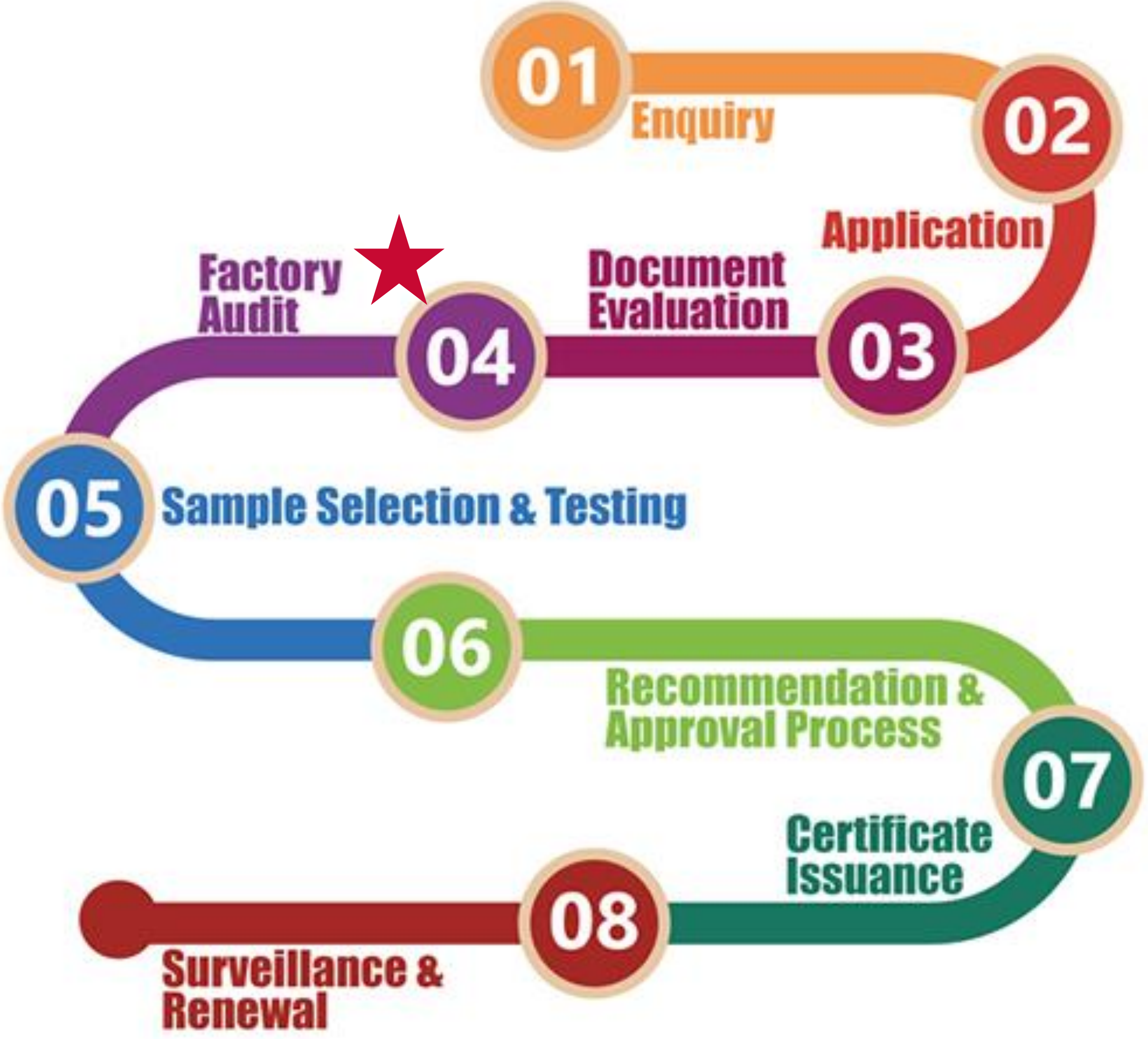
https://www.cidbholdings.com.my/webv2/index.php/technical-services/construction-product-certification

03 – A trust model drives sharing of sensitive IP



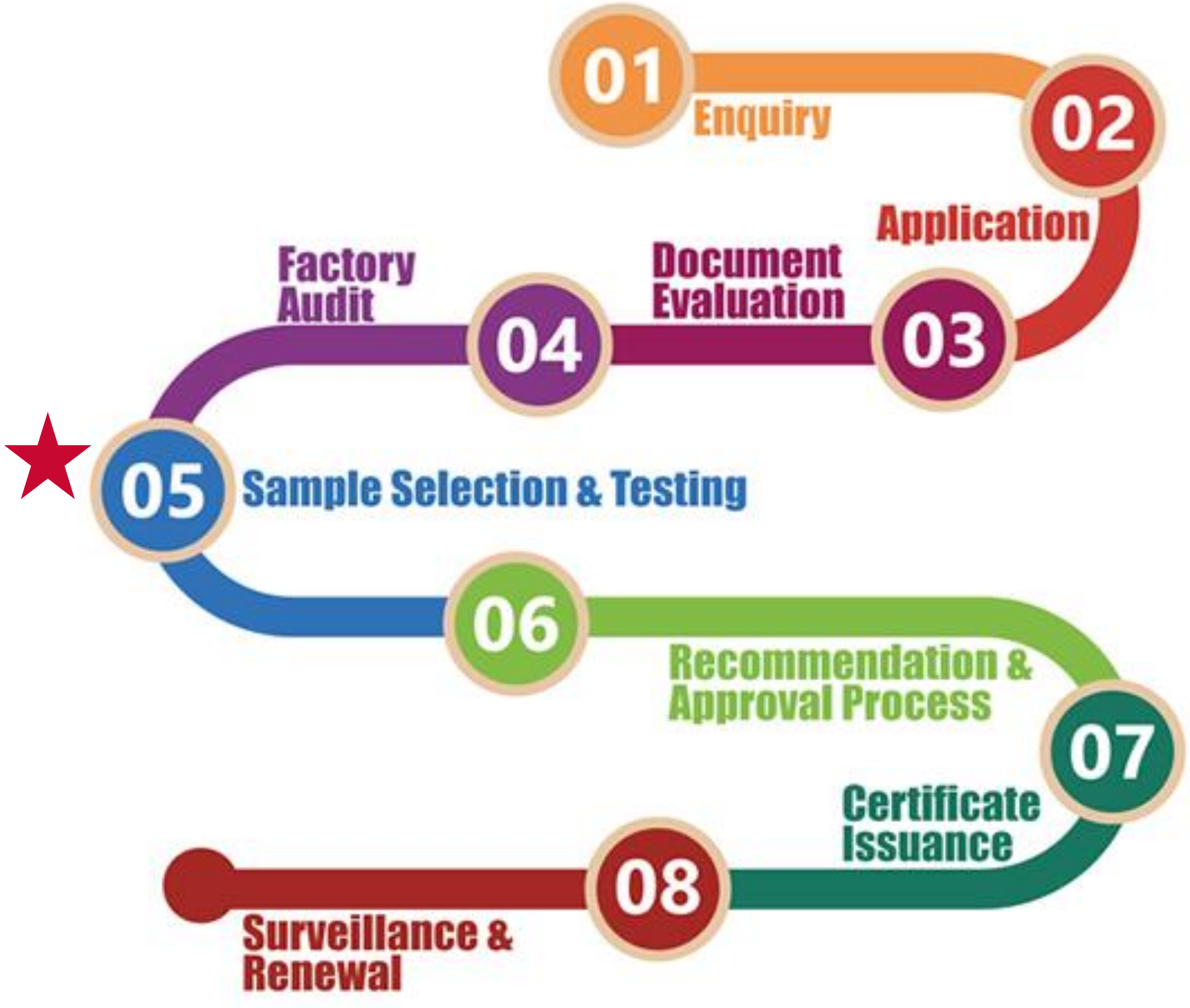
https://www.cidbholdings.com.my/webv2/index.php/technical-services/construction-product-certification

04 – Design, development, & manufacturing are considered



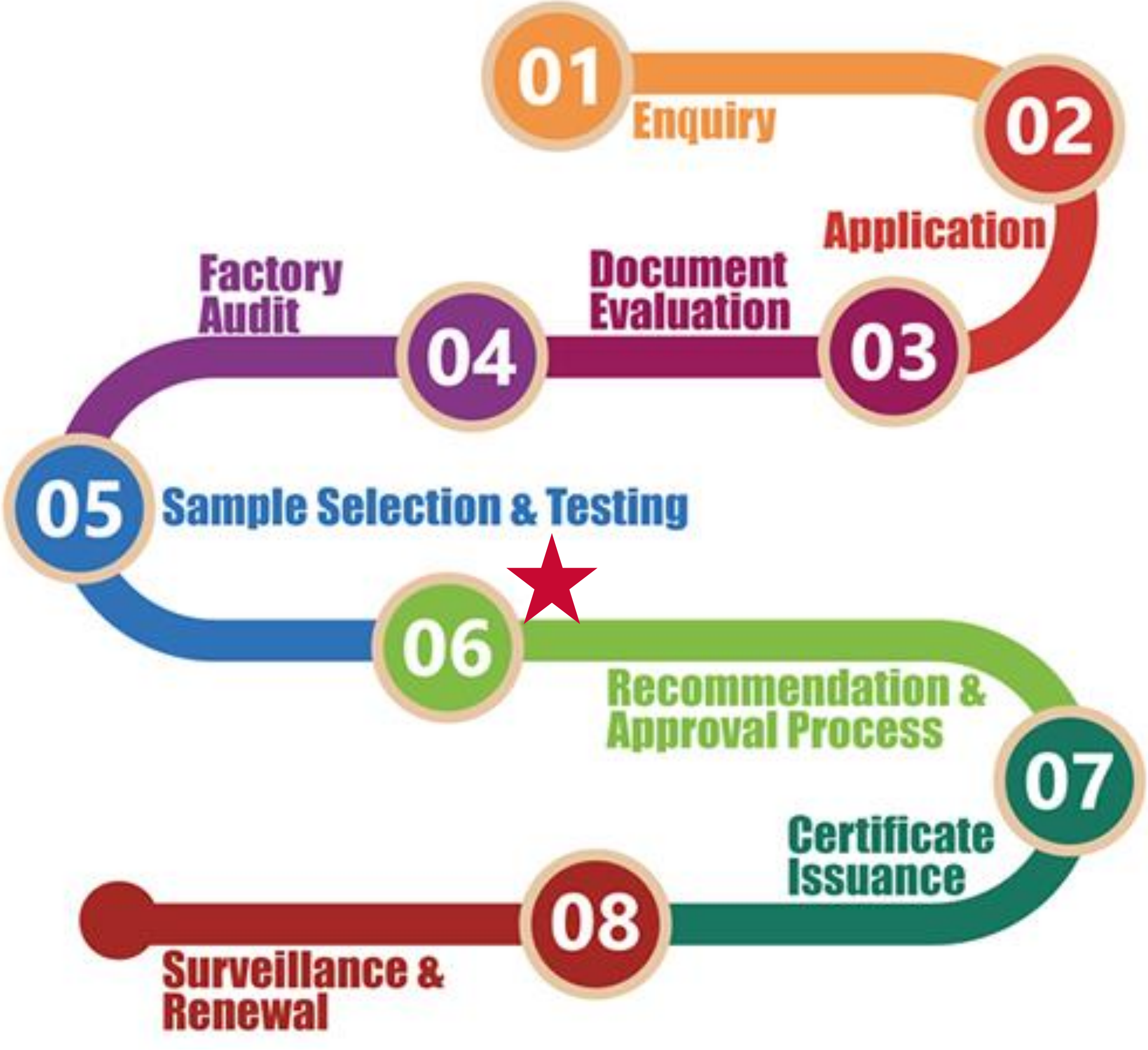
https://www.cidbholdings.com.my/webv2/index.php/technical-services/construction-product-certification

05 – Testing is based on Safety Science research



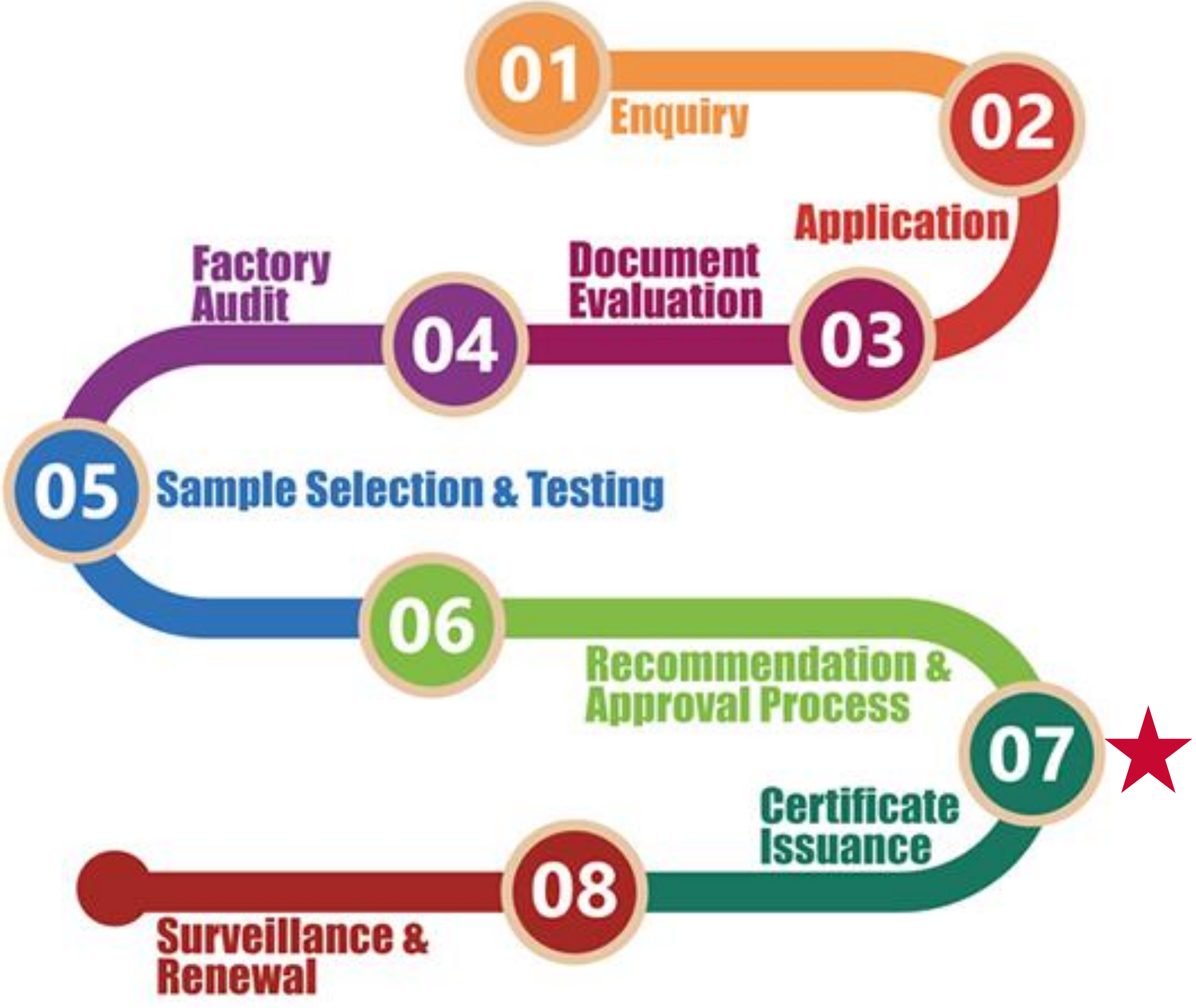
https://www.cidbholdings.com.my/webv2/index.php/technical-services/construction-product-certification

06 – Collaboration to meet mutual safety and security goals



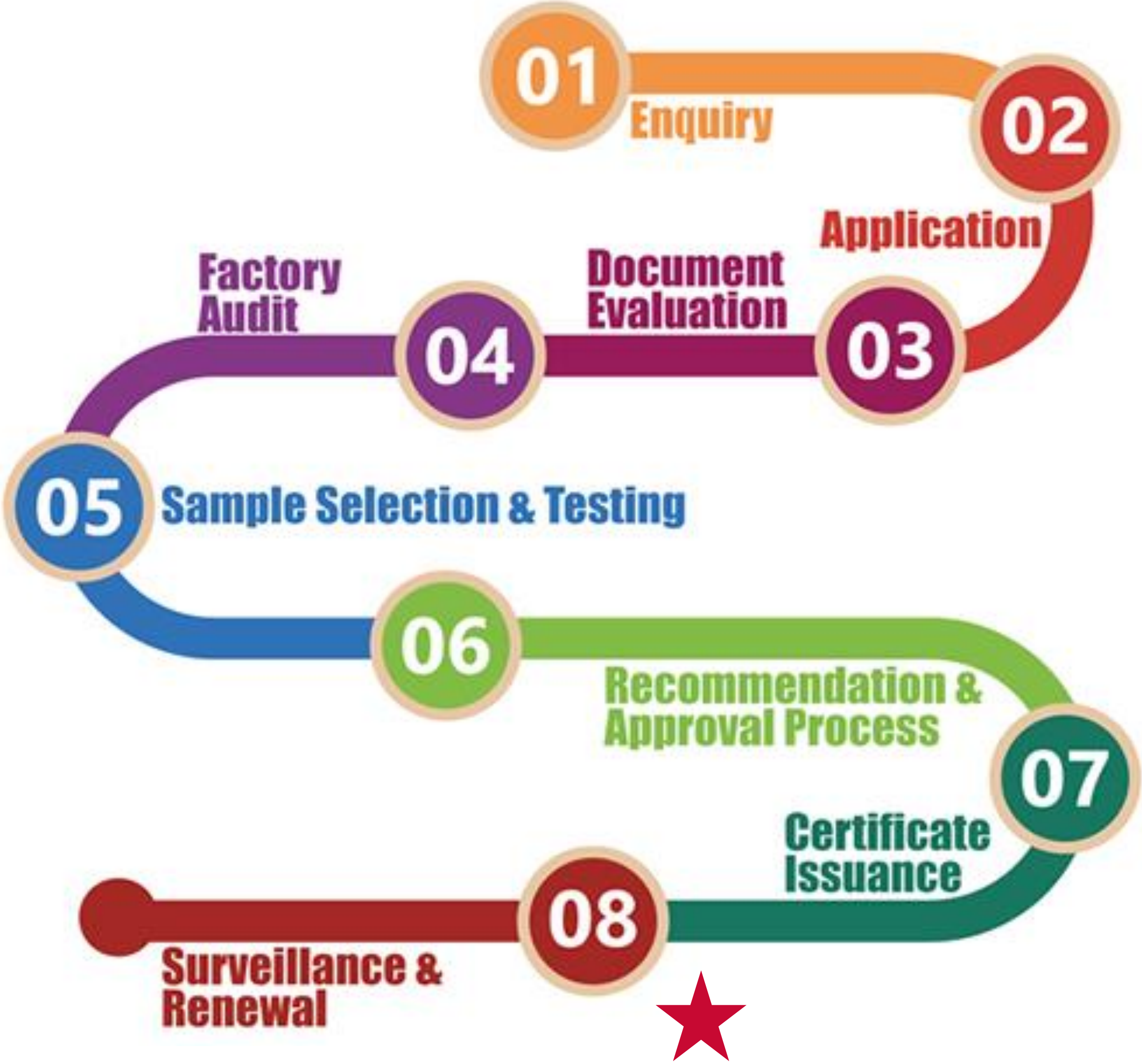
https://www.cidbholdings.com.my/webv2/index.php/technical-services/construction-product-certification

07 – Demonstrates due diligence to the market



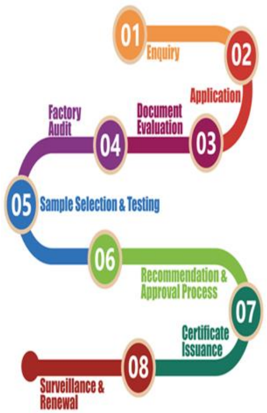
https://www.cidbholdings.com.my/webv2/index.php/technical-services/construction-product-certification

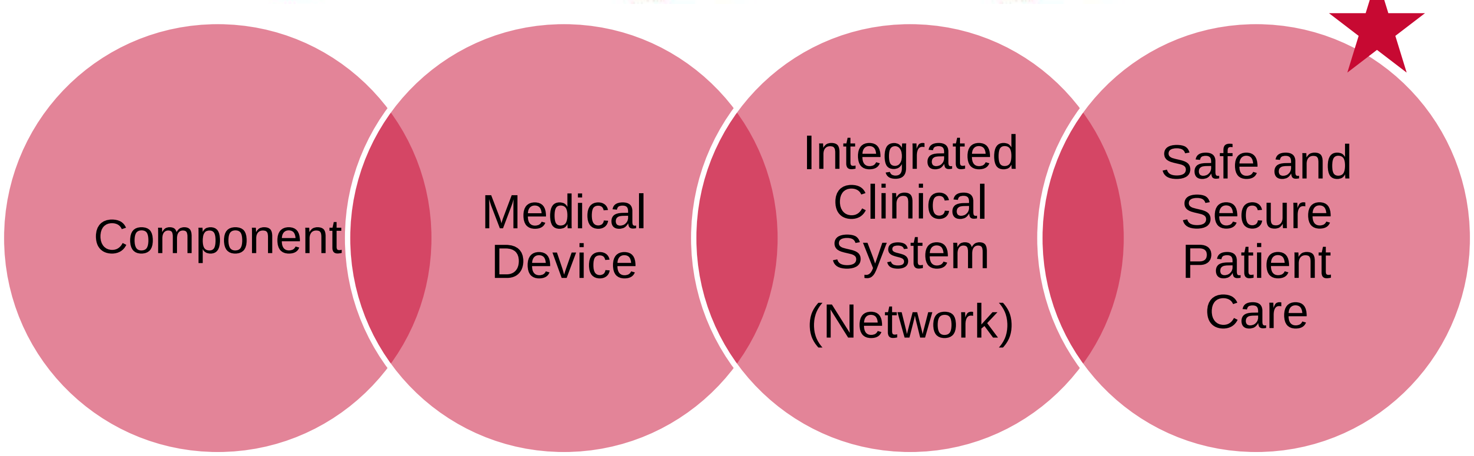
08 – Engages the full product lifecycle



https://www.cidbholdings.com.my/webv2/index.php/technical-services/construction-product-certification

Certification drives sharing of safety and security critical information across the supply chain…resulting in improved patient care





Component

Medical Device

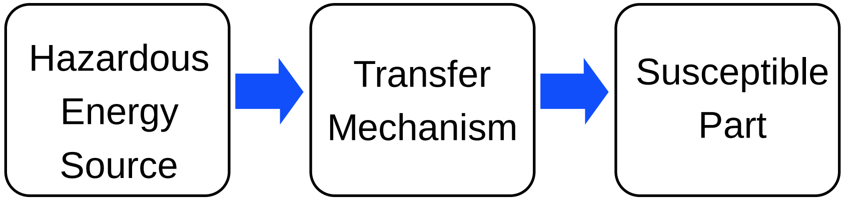
Integrated Clinical System

(Network)

Safe and Secure Patient Care

Key aspects of risk are identified and disclosed

HBSE Premise

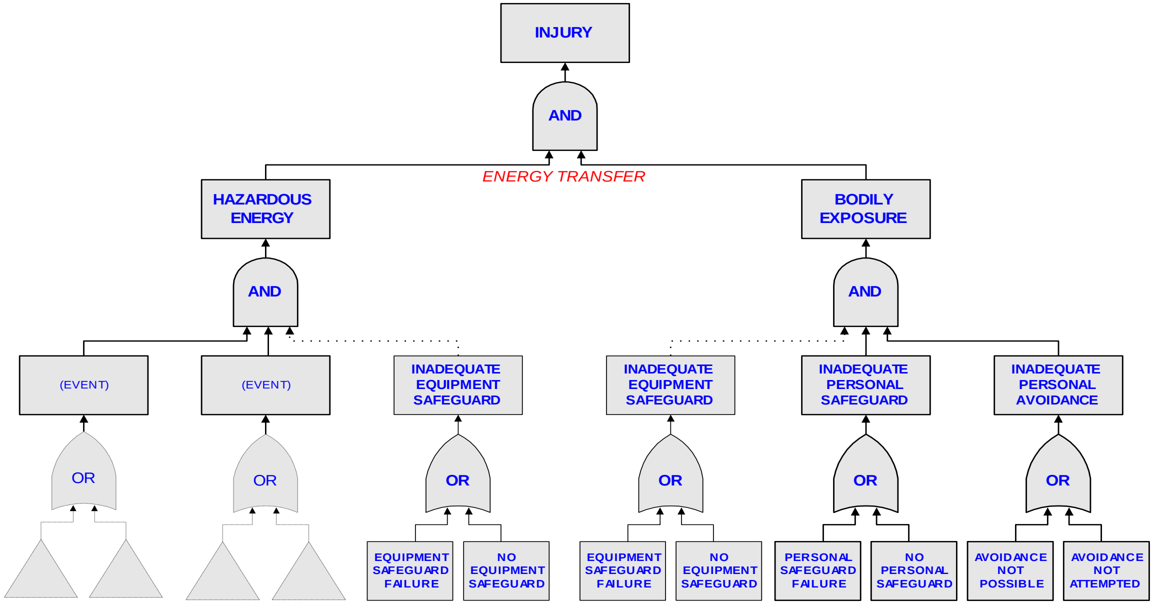


Hazardous Energy Source

Transfer Mechanism

Susceptible Part

Fault Tree Analysis



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

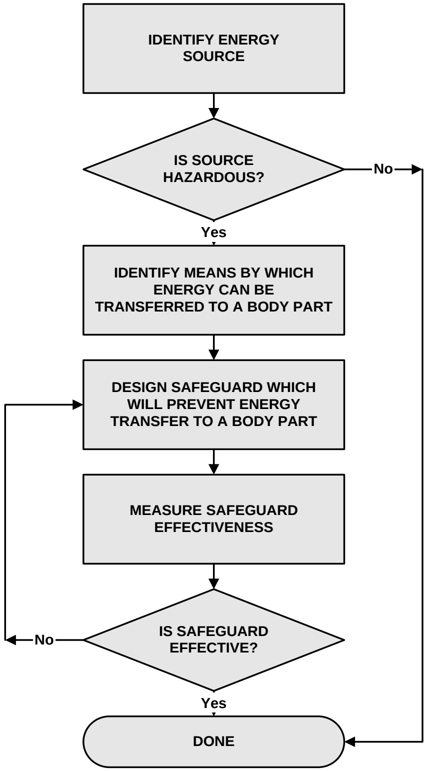
PERSONAL SAFEGUARD FAILURE

NO PERSONAL SAFEGUARD

AVOIDANCE NOT POSSIBLE

AVOIDANCE NOT ATTEMPTED

Risk Management



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

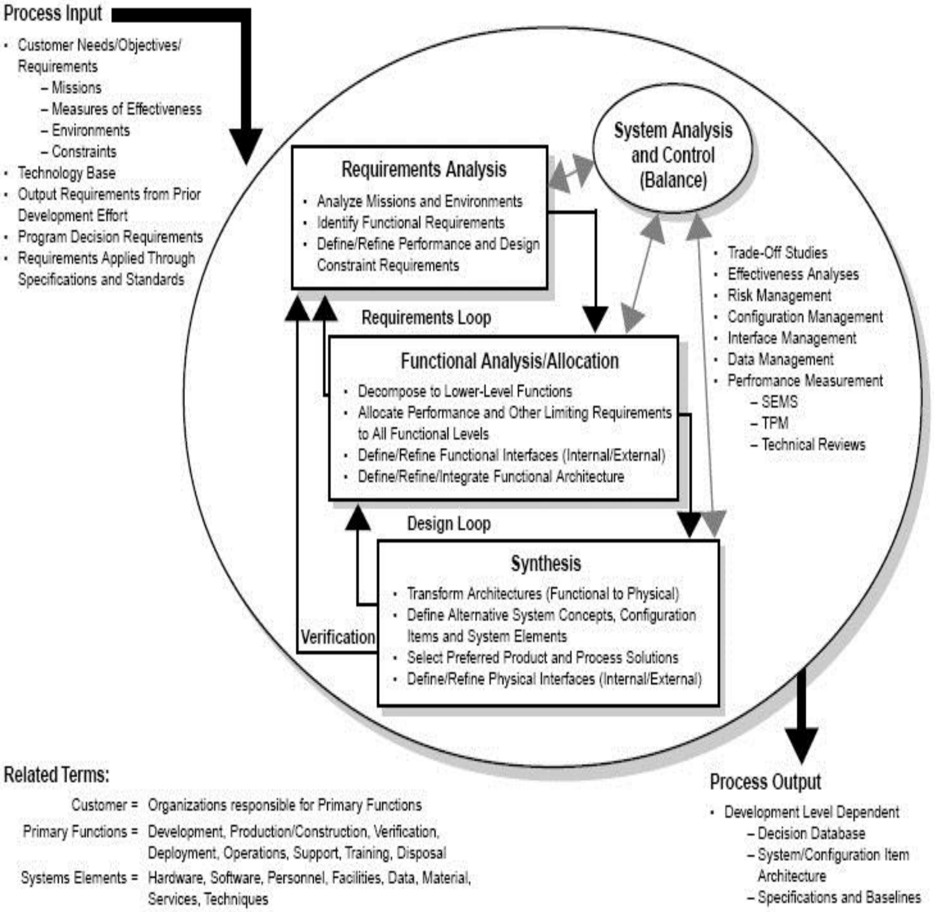
IS SAFEGUARD EFFECTIVE?

No

Yes

DONE

The potential impact of a component in the context of the whole system can be realized



Process Input

- Customer Needs/Objectives/ Requirements
  - Missions
  - Measures of Effectiveness
  - Environments
  - Constraints
- Technology Base
- Output Requirements from Prior Development Effort
- Program Decision Requirements
- Requirements Applied Through Specifications and Standards

System Analysis and Control (Balance)

Requirements Analysis

- Analyze Missions and Environments
- Identify Functional Requirements
- Define/Refine Performance and Design Constraint Requirements

Requirements Loop

Functional Analysis/Allocation

- Decompose to Lower-Level Functions
- Allocate Performance and Other Limiting Requirements to All Functional Levels
- Define/Refine Functional Interfaces (Internal/External)
- Define/Refine/Integrate Functional Architecture

Design Loop

Synthesis

- Transform Architectures (Functional to Physical)
- Define Alternative System Concepts, Configuration Items and System Elements
- Select Preferred Product and Process Solutions
- Define/Refine Physical Interfaces (Internal/External)

Verification

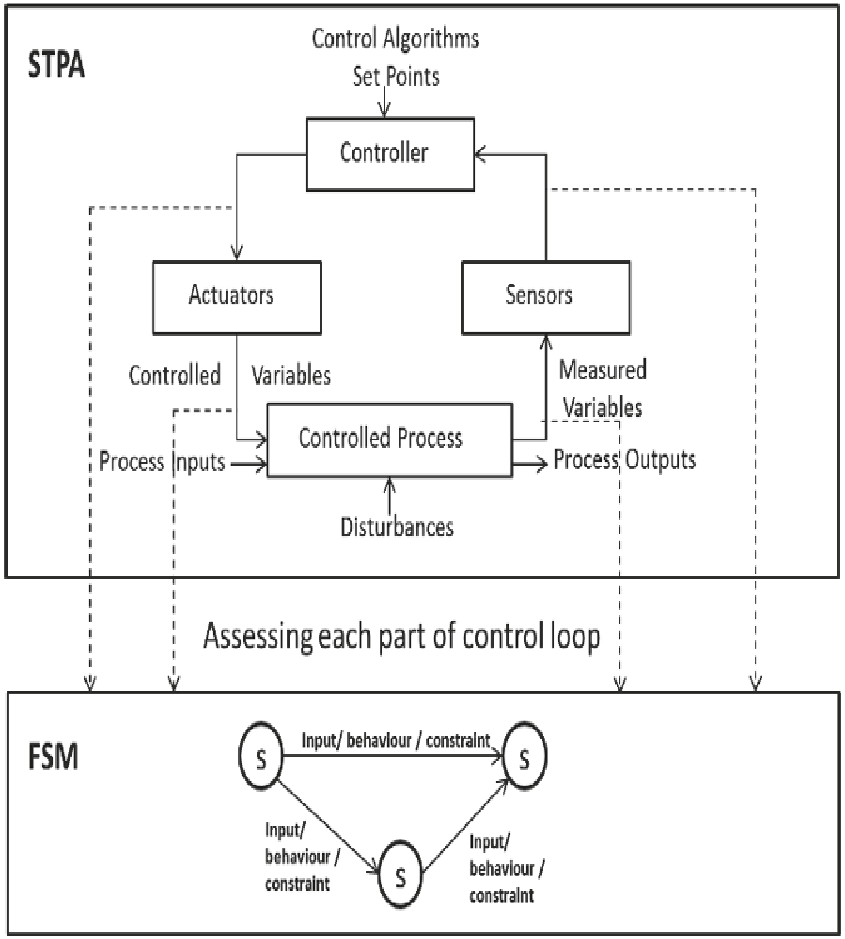
- Trade-Off Studies
- Effectiveness Analyses
- Risk Management
- Configuration Management
- Interface Management
- Data Management
- Perfromance Measurement
  - SEMS
  - TPM
  - Technical Reviews

Process Output

- Development Level Dependent
  - Decision Database
  - System/Configuration Item Architecture
  - Specifications and Baselines

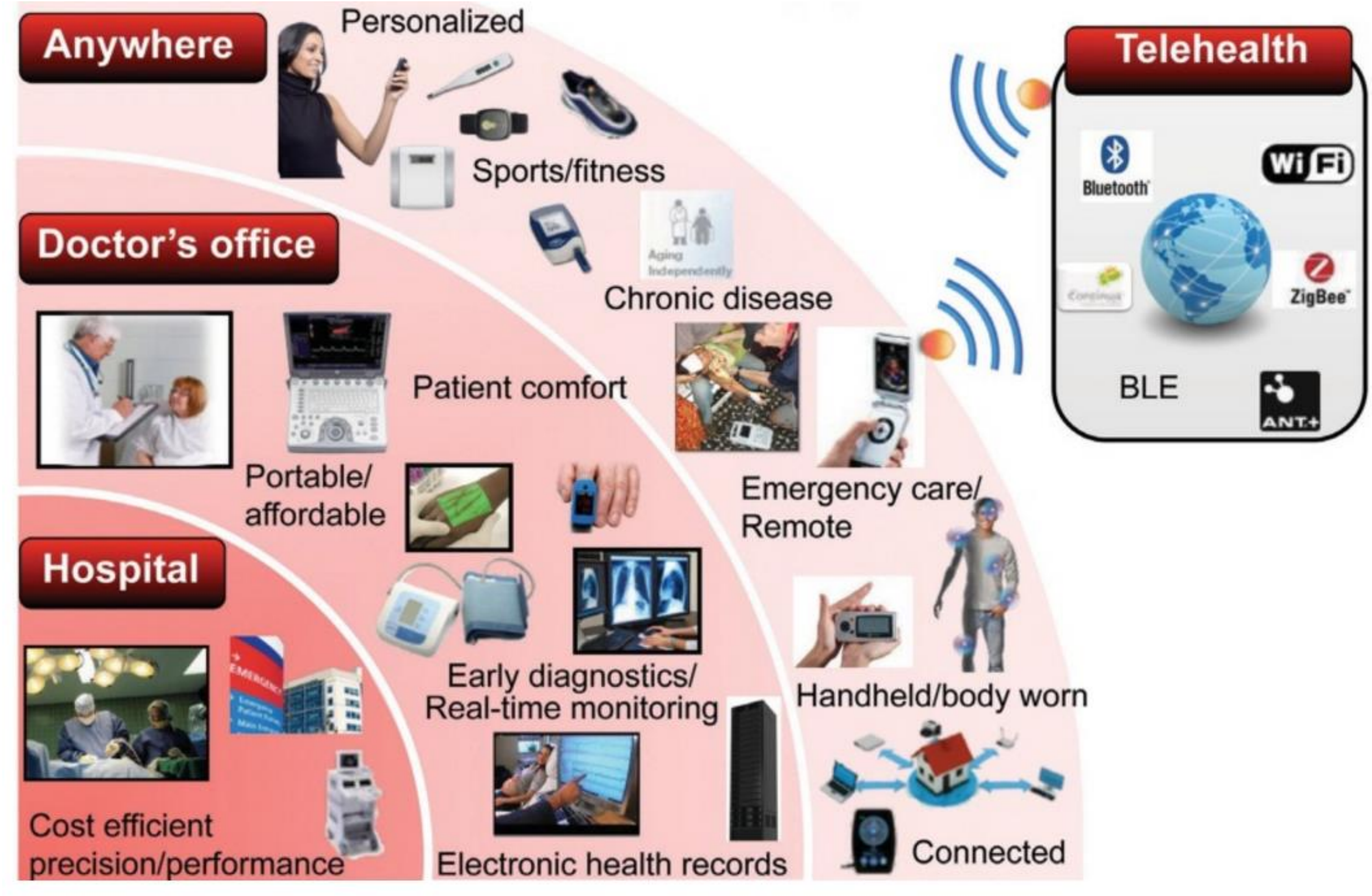
Related Terms:

Customer =	Organizations responsible for Primary Functions
Primary Functions =	Development, Production/Construction, Verification, Deployment, Operations, Support, Training, Disposal
Systems Elements =	Hardware, Software, Personnel, Facilities, Data, Material, Services, Techniques



Integrating State Machine Analysis with System-Theoretic Process Analysis; Abdulkhaleq and Wagoner

Effectively managing such risks can stimulate marketplace innovation



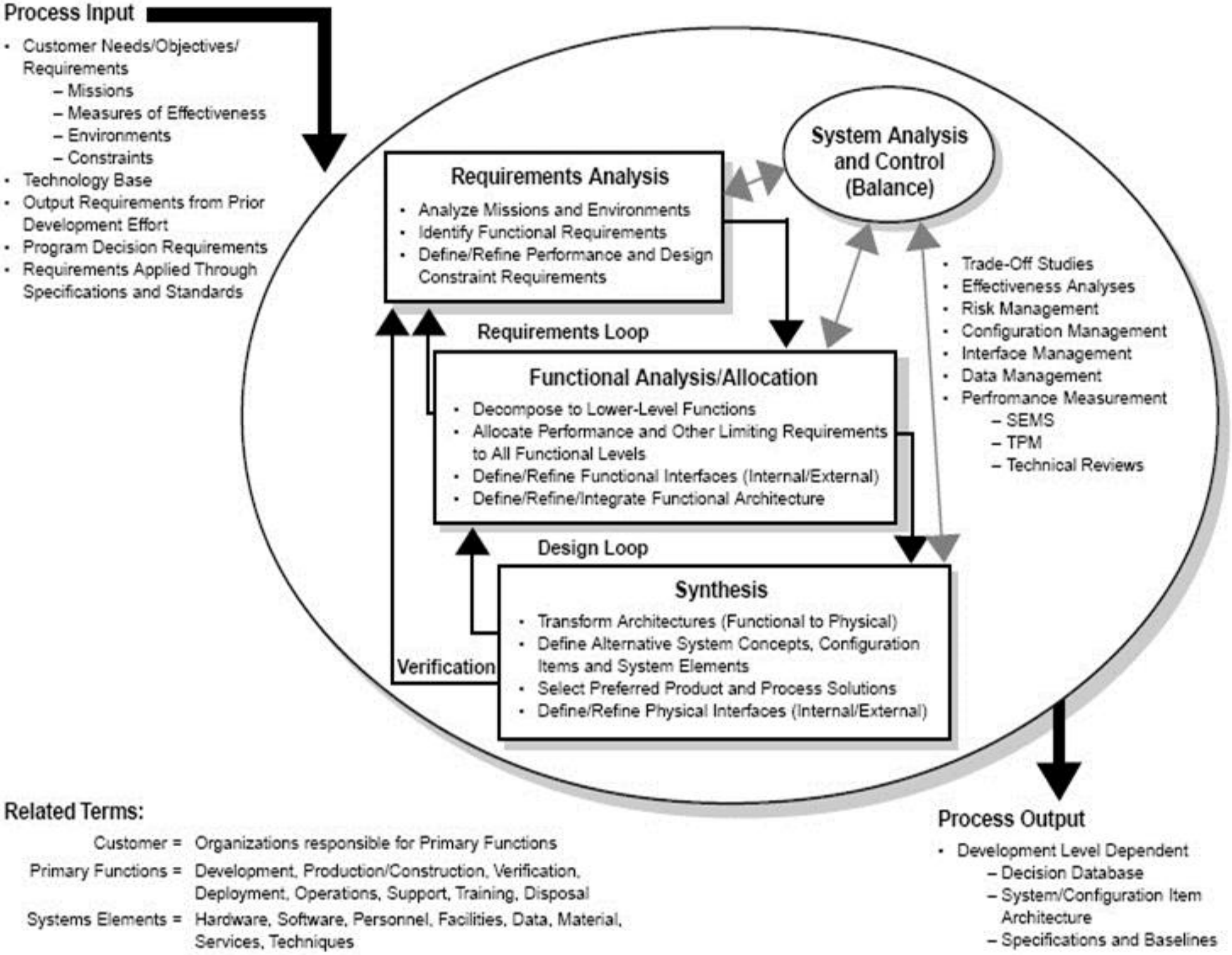
Source: TI Medical

The unique risks of new technology are sometimes not readily apparent

What’s unique about healthcare technologies?

- Patient safety is the most important “asset”
- It is not an issue of just individual patients but also whole populations of patients
    - Cyber-attack causing a drug overdose to a patient (individual impact or multiple patients on same device type / network)
    - Ransomware for EHR (population impact)
    - Malicious tampering with clinical trials (potential individual impact and population impact [delay of new treatment on the market])
- Product risk profiles can be very diverse making risk factors difficult to normalize (e.g. some medical products intentionally expose people to radiation)
- Medical IoT and Telehealth are moving elements of the “practice of medicine” from the hospital into the home.

Fully understanding risk involves thinking about the whole system, not just the device



Process Input

- Customer Needs/Objectives/ Requirements
  - Missions
  - Measures of Effectiveness
  - Environments
  - Constraints
- Technology Base
- Output Requirements from Prior Development Effort
- Program Decision Requirements
- Requirements Applied Through Specifications and Standards

Requirements Analysis

- Analyze Missions and Environments
- Identify Functional Requirements
- Define/Refine Performance and Design Constraint Requirements

System Analysis and Control (Balance)

- Trade-Off Studies
- Effectiveness Analyses
- Risk Management
- Configuration Management
- Interface Management
- Data Management
- Perfromance Measurement
  - SEMS
  - TPM
  - Technical Reviews

Functional Analysis/Allocation

- Decompose to Lower-Level Functions
- Allocate Performance and Other Limiting Requirements to All Functional Levels
- Define/Refine Functional Interfaces (Internal/External)
- Define/Refine/Integrate Functional Architecture

Synthesis

- Transform Architectures (Functional to Physical)
- Define Alternative System Concepts, Configuration Items and System Elements
- Select Preferred Product and Process Solutions
- Define/Refine Physical Interfaces (Internal/External)

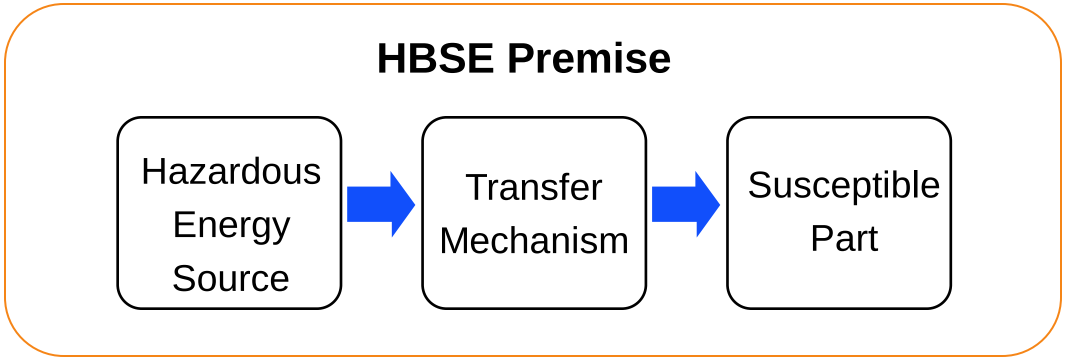
Process Output

- Development Level Dependent
  - Decision Database
  - System/Configuration Item Architecture
  - Specifications and Baselines

Related Terms:

Customer =	Organizations responsible for Primary Functions
Primary Functions =	Development, Production/Construction, Verification, Deployment, Operations, Support, Training, Disposal
Systems Elements =	Hardware, Software, Personnel, Facilities, Data, Material, Services, Techniques

How do we identify critical control structures in systems?

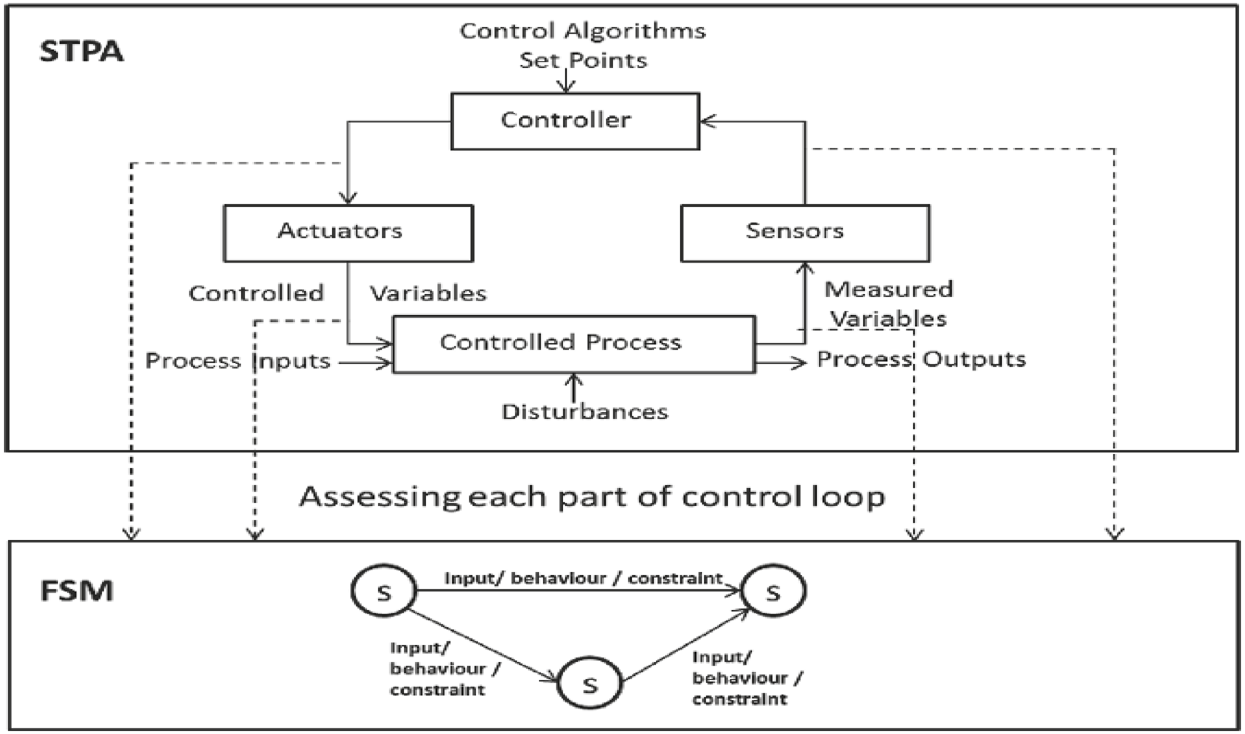


HBSE Premise

Hazardous Energy Source

Transfer Mechanism

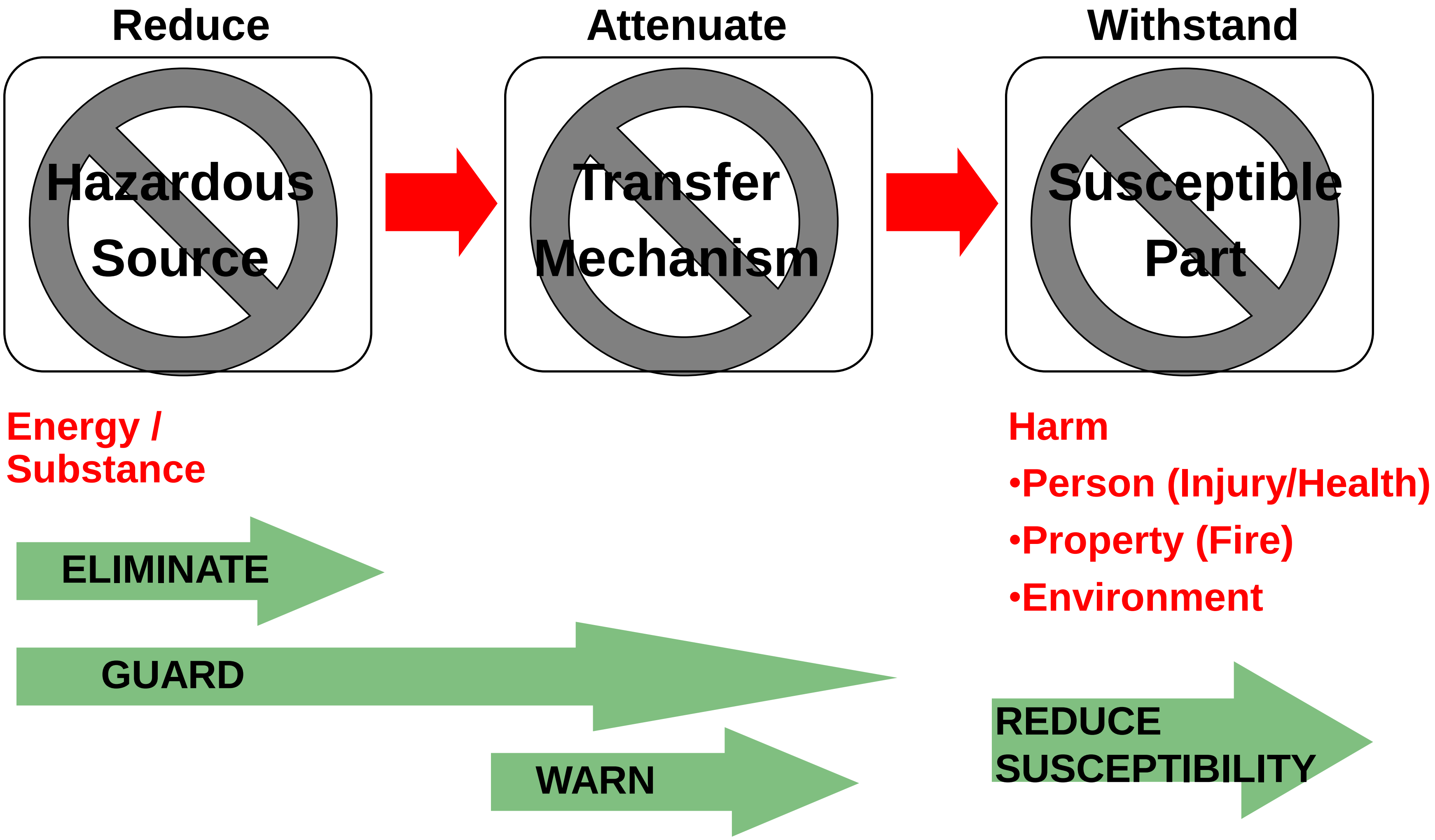
Susceptible Part



Integrating State Machine Analysis with System-Theoretic Process Analysis; Abdulkhaleq and Wagoner

How do we protect such systems?

Eliminate, Guard, Warn or Reduce Susceptibility to Hazard



Reduce

Hazardous Source

Attenuate

Transfer Mechanism

Withstand

Susceptible Part

Energy / Substance

Harm

- Person (Injury/Health)
- Property (Fire)
- Environment

ELIMINATE

GUARD

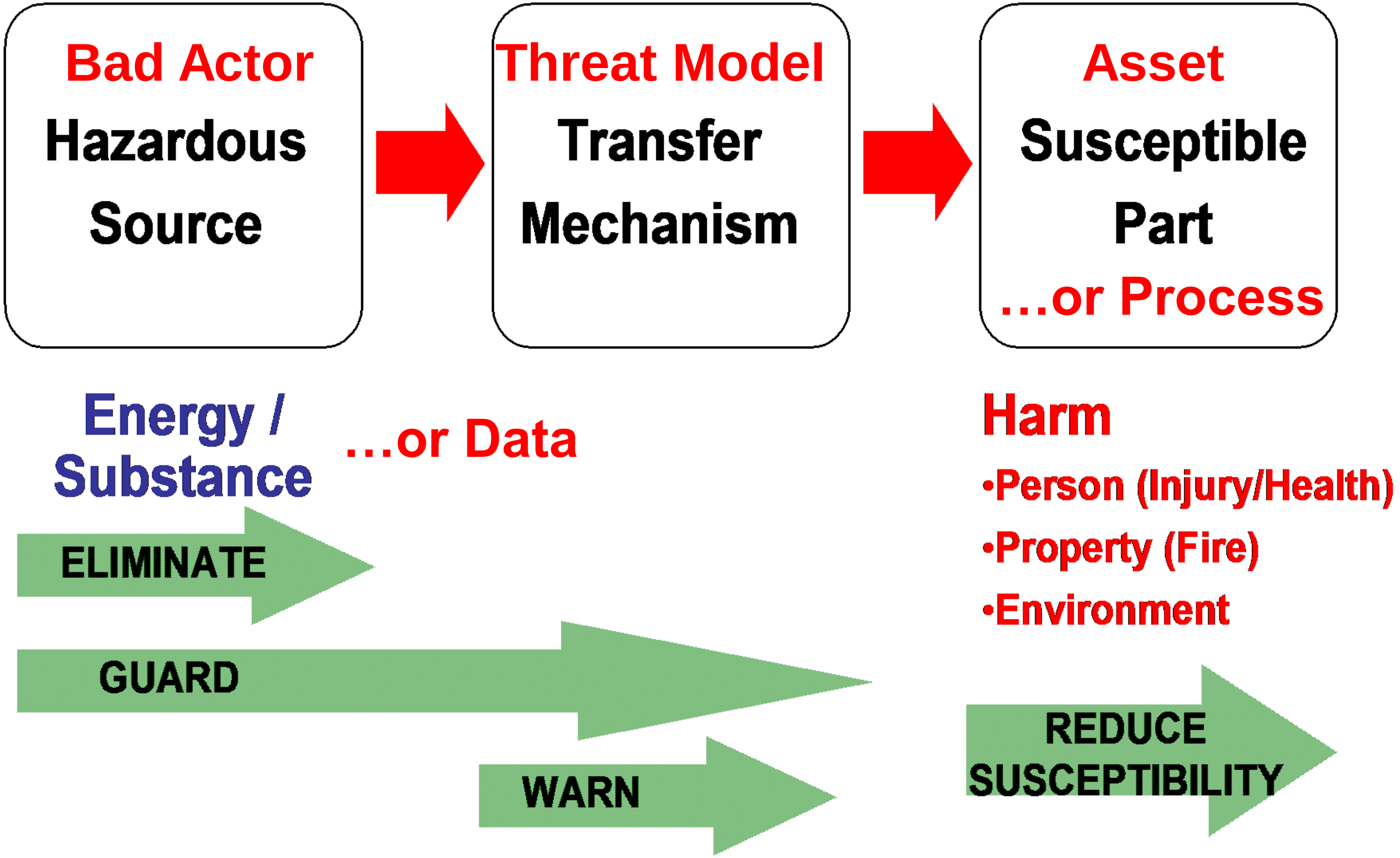
WARN

REDUCE SUSCEPTIBILITY

Determining criticality

- **Safety Critical Function: protective**
  - Relied on for safety
  - Reduces / maintains risk at tolerable level
- **Failure of SCF results in increased risk** (+)
  - Even if not explicitly designed for reliance on safety
  - DO what intended <u>and</u> NOT DO what NOT intended
- **Risk > tolerable level: attention warranted**…
  - Application-specific
  - Risk-based decisions
  - Additional safety requirements / risk controls – reliability, performance, protective functionality, etc.

Focusing on security expands the "asset" base beyond just device-specific injury



Bad Actor

Hazardous Source

Threat Model

Transfer Mechanism

Asset

Susceptible Part

…or Process

Energy / Substance

…or Data

Harm

- Person (Injury/Health)
- Property (Fire)
- Environment

ELIMINATE

GUARD

WARN

REDUCE SUSCEPTIBILITY

Data Breaches

Data Breaches 66%

IDC Research shows that 66% of networks will have an IoT security breach by 2018

Unplanned Downtime

Loss of Production

Harm to Assets

Damage to Reputation

Guidance Documents

- ISO/IEC TR 15443
- ITU-T CYBEX 1500 series
  - CVE / NVD
  - CWE (CWRAF/CWSS, SANS CWE Top 25 / OWASP Top 10) and CAPEC

- ISO/IEC 27000 series
- ISO/IEC 15408
- ISO/IEC DIS 20243 /O-TTPS
- FISMA
- HIPAA
- IEC 62443

- IEC 80001
- AAMI TIR 57
- PCI
- SANS 20 CSC
- Cyber Essentials (UK)
- US-CERT

- Top 35 mitigation strategies (AU)
- NIST Cybersecurity Framework & SP 800-53r4 security controls
- DHS C^3 VP & CRR
- SAE AS5553 & 6174

**Source: IDC Research, Inc.*

Data Breaches

Data Breaches 66%

IDC Research shows that 66% of networks will have an IoT security breach by 2018

How do you demonstrate that you’ve actually implemented these best practices, etc?

Unplanned Downtime

Loss of Production

Harm to Assets

BREACH

Damage to Reputation

Guidance Documents

- ISO/IEC TR 15443
- IT[illegible]0 series
  - CVE / NVD
  - CWE (CWRAF/CWSS, SANS CWE Top 25 / OWASP Top 10) and CAPEC

- ISO/IEC 27000 series
- ISO/IEC 15408
- ISO/IEC DIS 20243 /O-TTPS
- FISMA
- HIPAA
- IEC 62443

- IEC 80001
- [illegible]
- SANS 20 CSC
- Cyber Essentials (UK)

- Top 35 mitigation strategies
- [illegible]
- NIST Cybersecurity Framework & SP 800-53r4 security controls
- DHS C^3 VP & CRR
- SAE AS5553 & 6174

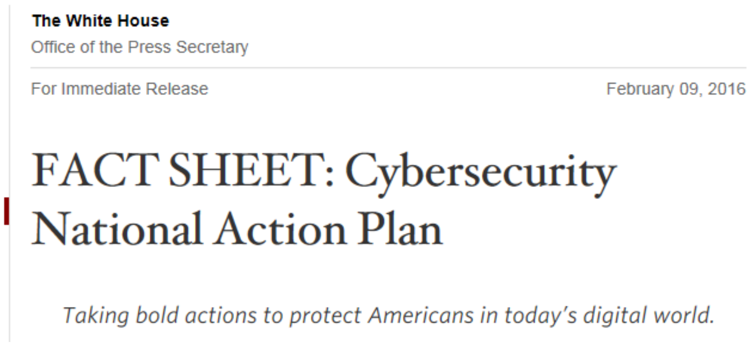
Testable technical criteria

- Improve **cyber hygiene** across all industry verticals
- Transparent, repeatable, reproducible testing across industries

Better Security

Improved Testing

History of UL CAP - CYBERUL



The White House
Office of the Press Secretary

For Immediate Release February 09, 2016

FACT SHEET: Cybersecurity National Action Plan

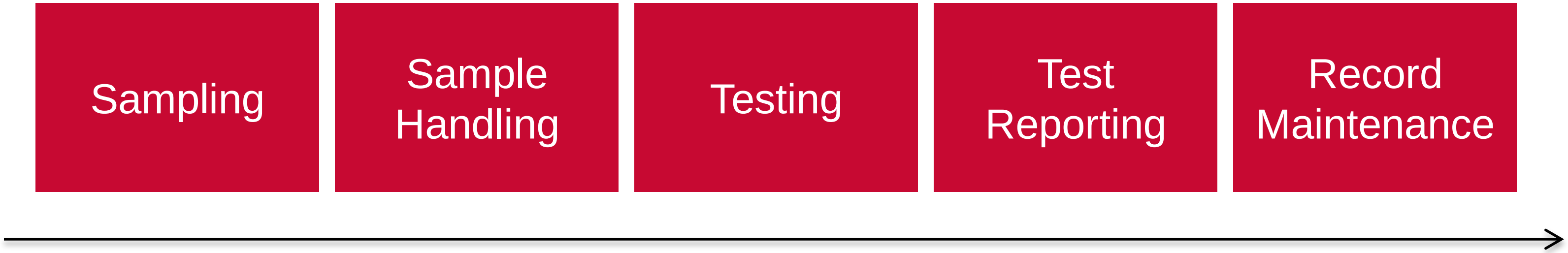
Taking bold actions to protect Americans in today's digital world.

- The Department of Homeland Security is collaborating with UL and other industry partners to develop a **Cybersecurity Assurance Program** to test and certify networked devices within the "Internet of Things," whether they be refrigerators or medical infusion pumps, so that when you buy a new product, you can be sure that it has been certified to meet security standards.

President Obama: *Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"*

Michael Daniel **(Special Assistant to the President and Cybersecurity Coordinator):**
"An Underwriters Laboratories-type safety certification could serve as a basic model for driving Internet of Things product security … "

Testable, repeatable, reproducible



Sampling

Sample Handling

Testing

Test Reporting

Record Maintenance

Sampling plan & sampling documentation

Sample identification & protection of sample integrity

Monitoring the quality and repeatability of test results

Test conditions & test results with estimated uncertainty

Ensure record integrity & security

Compliance across all workflow steps

- Validation of analytical methods & procedures
- Equipment calibration testing & maintenance

- Qualification of material
- Traceability
- Control of nonconforming testing

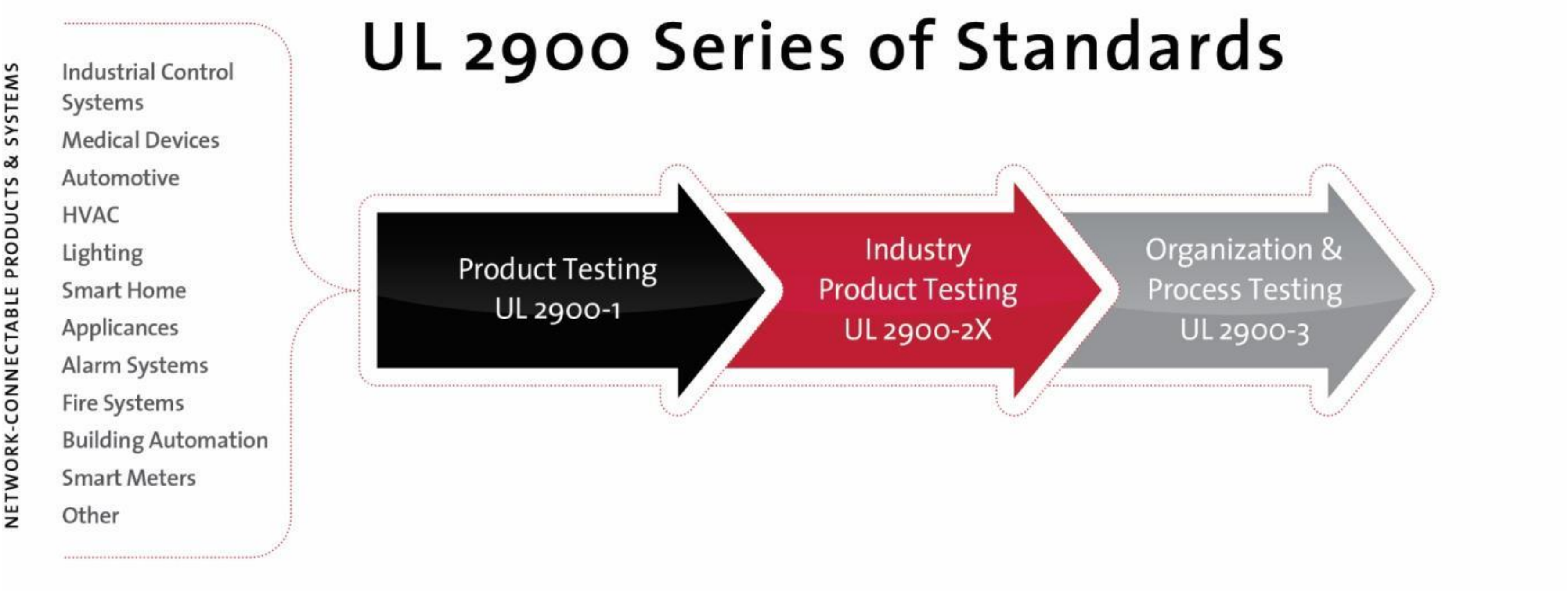
- Qualification of personnel
- Controlled environmental conditions
- Written procedures

Compliance across the laboratory

Documentation control, corrective actions, complaint handling, supplier & subcontractor management, non-conflicting organizational structure, internal audits

recreated from http://www.labcompliance.com/pictures/tutorial/iso17025/17025-requirements-500.jpg

UL 2900 Standards

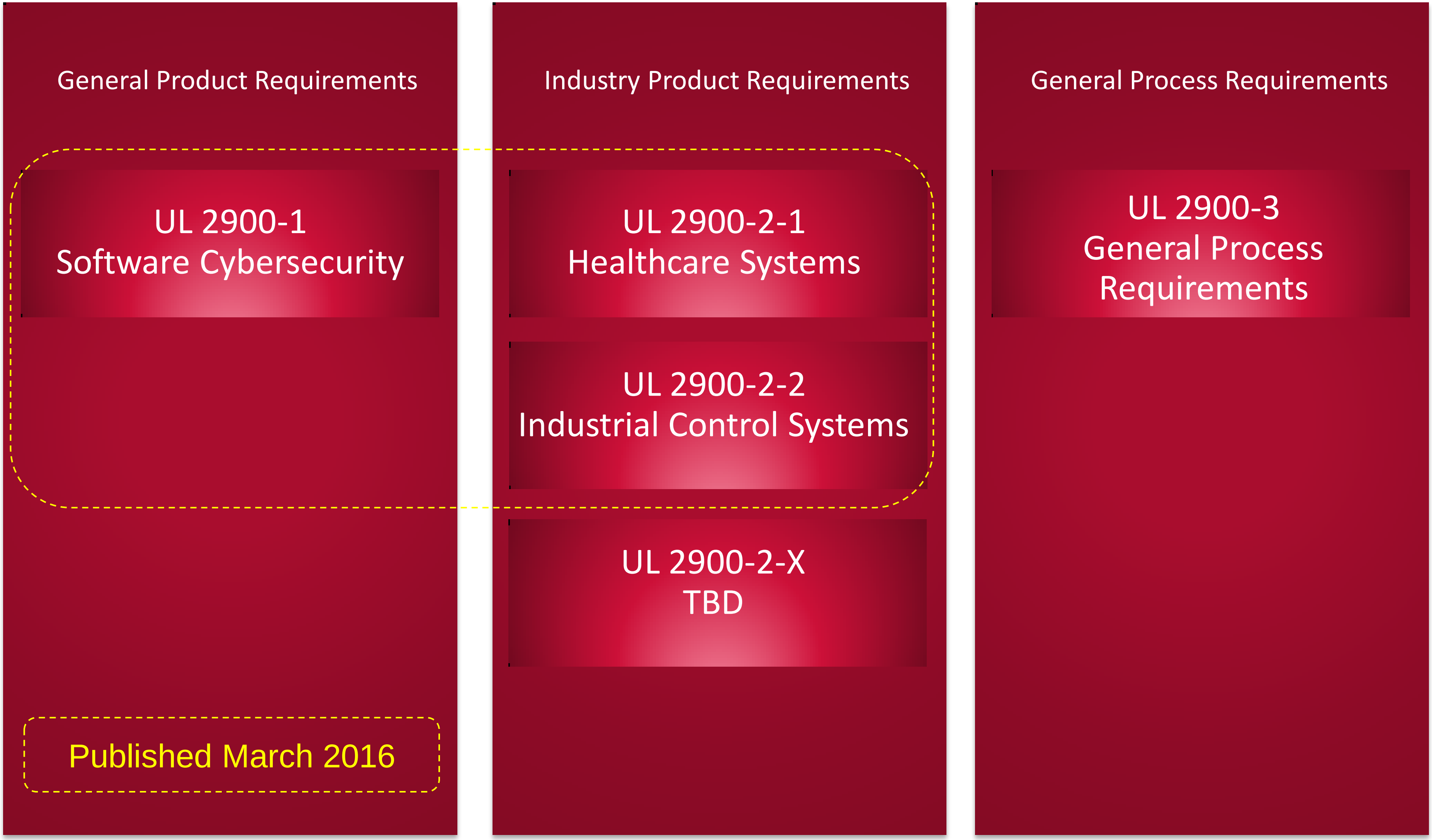

UL 2900 Series of Standards
NETWORK-CONNECTABLE PRODUCTS & SYSTEMS
Industrial Control Systems
Medical Devices
Automotive
HVAC
Lighting
Smart Home
Applicances
Alarm Systems
Fire Systems
Building Automation
Smart Meters
Other
Product Testing UL 2900-1
Industry Product Testing UL 2900-2X
Organization & Process Testing UL 2900-3

Vulnerabilities and Exploits

Software Weaknesses

Security Controls

UL 2900 Standards



General Product Requirements

UL 2900-1
Software Cybersecurity

Published March 2016

Industry Product Requirements

UL 2900-2-1
Healthcare Systems

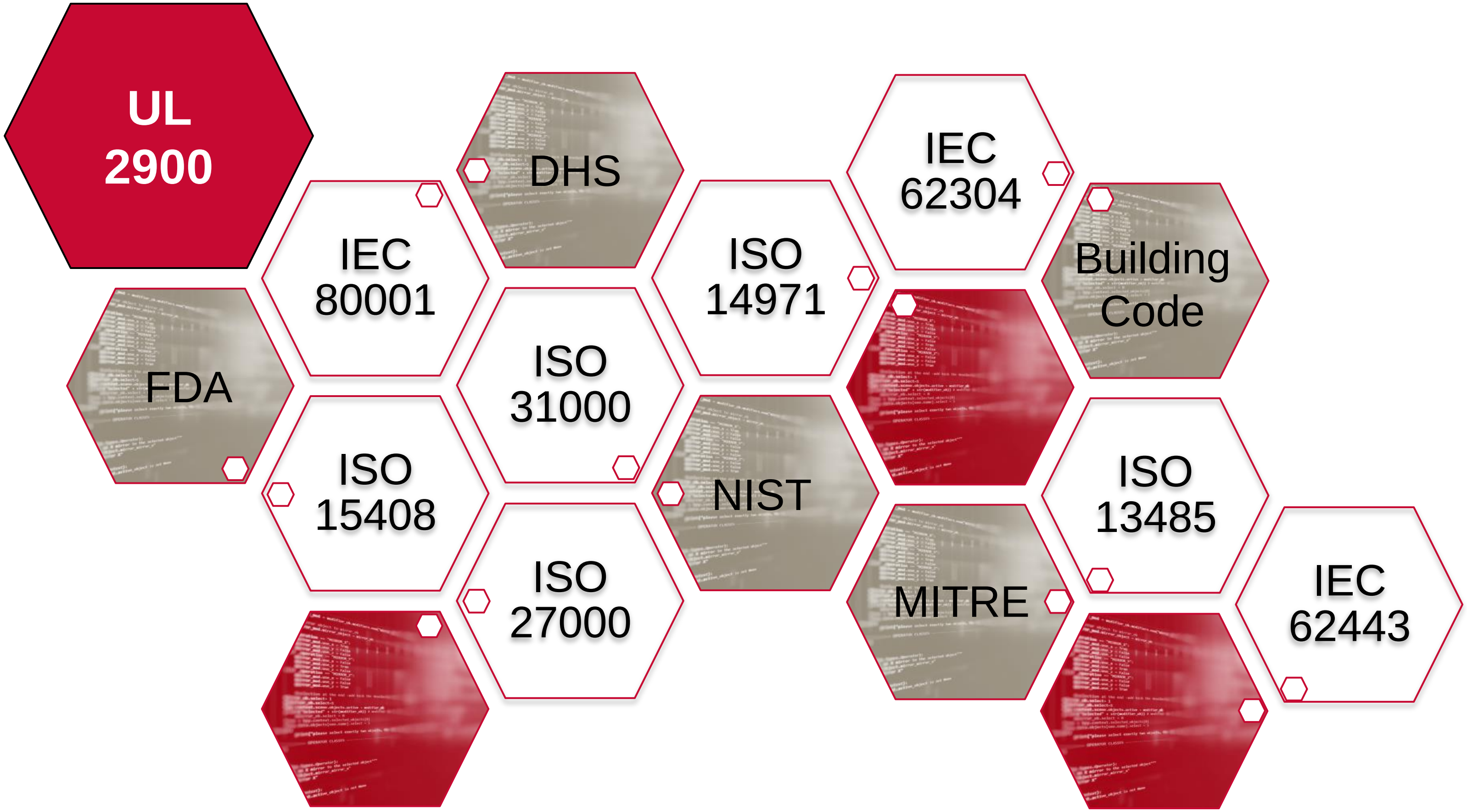
UL 2900-2-2
Industrial Control Systems

UL 2900-2-X
TBD

General Process Requirements

UL 2900-3
General Process Requirements

Leverages many existing standards & frameworks



UL 2900

DHS

IEC 62304

IEC 80001

ISO 14971

Building Code

FDA

ISO 31000

ISO 15408

NIST

ISO 13485

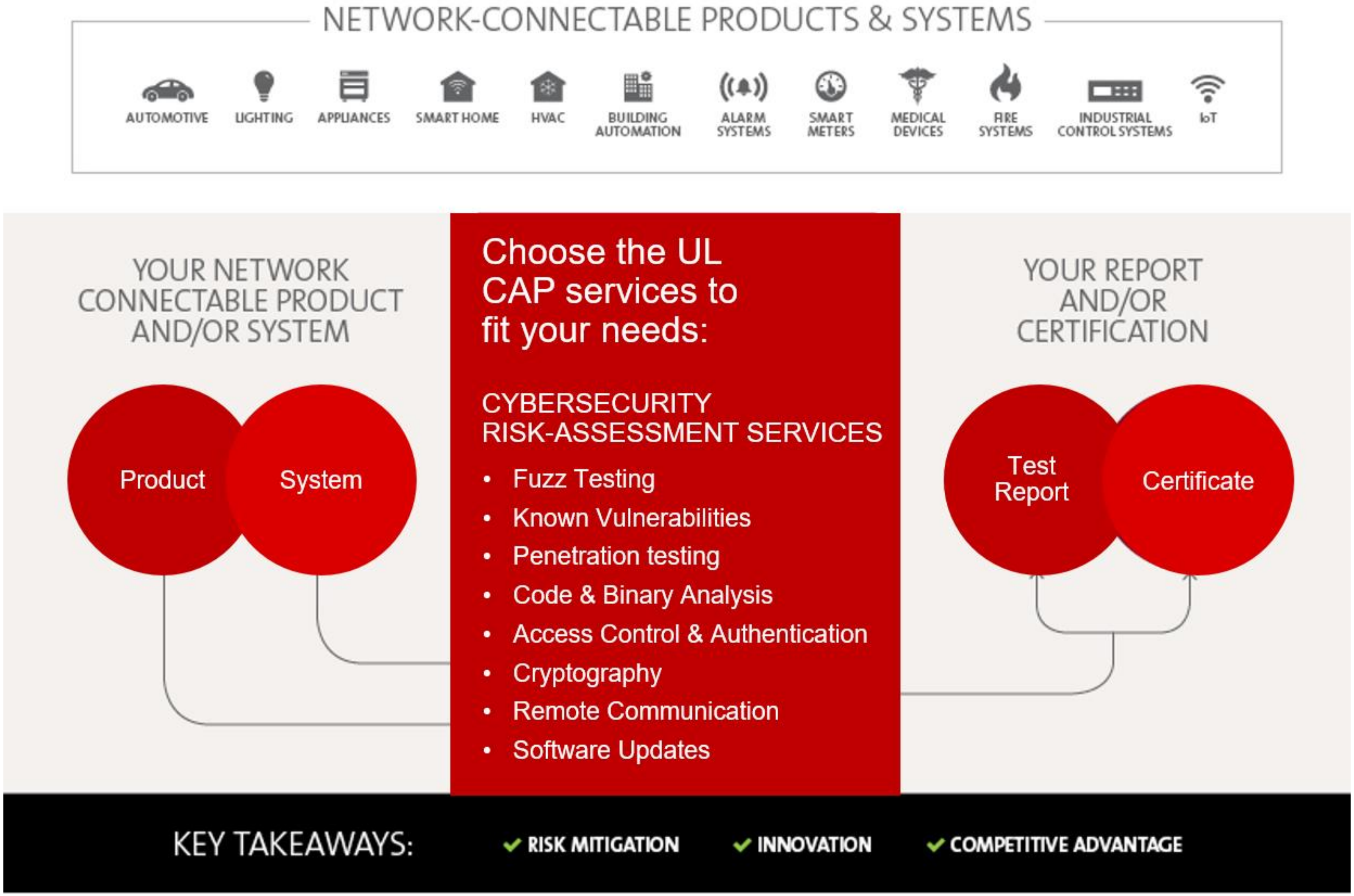
ISO 27000

MITRE

IEC 62443

…and many more…

What is UL CAP?



NETWORK-CONNECTABLE PRODUCTS & SYSTEMS

AUTOMOTIVE · LIGHTING · APPLIANCES · SMART HOME · HVAC · BUILDING AUTOMATION · ALARM SYSTEMS · SMART METERS · MEDICAL DEVICES · FIRE SYSTEMS · INDUSTRIAL CONTROL SYSTEMS · IoT

YOUR NETWORK CONNECTABLE PRODUCT AND/OR SYSTEM

Product

System

Choose the UL CAP services to fit your needs:

CYBERSECURITY RISK-ASSESSMENT SERVICES

- Fuzz Testing
- Known Vulnerabilities
- Penetration testing
- Code & Binary Analysis
- Access Control & Authentication
- Cryptography
- Remote Communication
- Software Updates

YOUR REPORT AND/OR CERTIFICATION

Test Report

Certificate

KEY TAKEAWAYS: ✓ RISK MITIGATION ✓ INNOVATION ✓ COMPETITIVE ADVANTAGE

What is UL CAP trying to accomplish

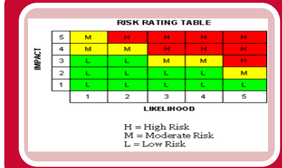
UL Cybersecurity Assurance Program (**UL CAP**) will be **Product Oriented & Industry Specific** with these goals:

- Reduce software vulnerabilities
- Reduce weaknesses, minimize exploitation
- Address known malware
- Increase security awareness

Product service offerings apply to:

- Connectable Products
- Products Eco-Systems (supply chain)
- Products System Integration (supply chain)
- Critical IT Infrastructure Integration (supply chain)

CAP for Healthcare Products (UL 2900-2-1)



RISK RATING TABLE

IMPACT					
5	M	H	H	H	H
4	M	M	H	H	H
3	L	L	M	M	H
2	L	L	L	L	M
1	L	L	L	L	L
	1	2	3	4	5

LIKELIHOOD

H = High Risk
M = Moderate Risk
L = Low Risk

Uses Existing Risk Management Processes

- ISO 14971 Product-centric risk management
- IEC 80001 Network-centric risk management

Uses Existing QMS

- ISO 13485 Quality management
- ISO 27000 Security management

Requirement Analysis
Design
Implementation
Testing
Evolution
SDLC
Software/System Development Life Cycle - SDLC

Uses Existing SDLC

- IEC 62304 Medical device life cycle processes
- ISO 15408 Secure development lifecycle processes

Aligned With Regulatory Processes

- FDA Pre- and Post-Market Guidance
- ISO 15026 Assurance Case Structure

CAP tools help establish BOM showing software components from libraries and SOUP

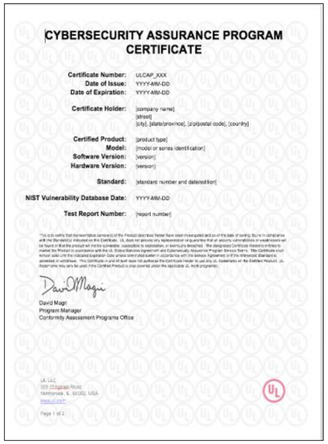
Manage patches

NIST CSF
NVD CVSS,
CWSS,
CAPEC, etc

In process for use in hospital procurement processes to:

- reduce vulnerabilities
- reduce malware
- increase security awareness and preparedness

Disclosure of Results Support the Supply Chain



CYBERSECURITY ASSURANCE PROGRAM
CERTIFICATE

Certificate Number:	ULCAP_XXX
Date of Issue:	YYYY-MM-DD
Date of Expiration:	YYYY-MM-DD
Certificate Holder:	[company name] [street] [city], [state/province], [zip/postal code], [country]
Certified Product:	[product type]
Model:	[model or series identification]
Software Version:	[version]
Hardware Version:	[version]
Standard:	[standard number and date/edition]
NIST Vulnerability Database Date:	YYYY-MM-DD
Test Report Number:	[report number]

This is to certify that representative sample(s) of the Product described herein have been investigated and as of the date of testing, found in compliance with the Standard(s) indicated on this Certificate. UL does not provide any representation or guarantee that all security vulnerabilities or weaknesses will be found or that the product will not be vulnerable, susceptible to exploitation, or eventually breached. The designated Certificate Holder is entitled to market the Product in accordance with the UL Global Services Agreement and Cybersecurity Assurance Program Service Terms. This Certificate shall remain valid until the indicated Expiration Date unless terminated earlier in accordance with the Service Agreement or if the referenced Standard is amended or withdrawn. This Certificate in and of itself does not authorize the Certificate Holder to use any UL trademarks on the Certified Product. UL trademarks may only be used if the Certified Product is also covered under the applicable UL mark programs.

DaviMagi

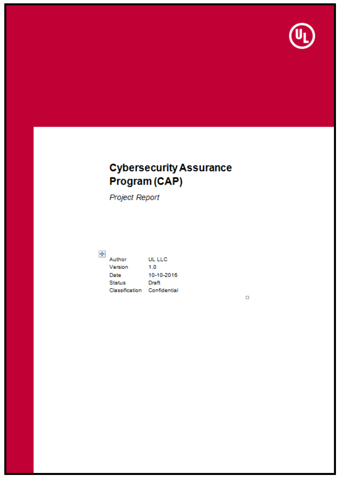
David Magri
Program Manager
Conformity Assessment Programs Office

UL LLC
333 Pfingsten Road
Northbrook, IL 60062, USA
www.ul.com

Page 1 of 2

Public

Manufacturer
Product CM
NVD version
UL DB version
Etc…



Cybersecurity Assurance Program (CAP)

Project Report

Author	UL LLC
Version	1.0
Date	10-10-2016
Status	Draft
Classification	Confidential

Private

Manufacturer
Product CM
Attack surface
Threat model
Vulnerabilities
Security assurance claims, arguments, and evidence
Etc…

Certificate Information Use Cases

Certificate

- identify products available in the market that satisfy the security requirements of UL 2900

- confirm the “known vulnerabilities” evaluated by reference of the NVD version used and date of certification

- determine whether the product certification is continuing to be maintained or has reached its end of certificated life

Test Report Information Use Cases
- entirely at the discretion of the manufacturer

Test Report

- Manufacturers use report data for internal continuous improvement processes

- Manufacturers use full report or excerpts from report to support regulatory submissions

- Manufacturers use report or excerpts to support their customers' needs (e.g. for integrators to develop any needed compensating controls)

UL Cybersecurity Assurance Program Details

Vulnerability Assessment aims to evaluate known vulnerabilities of a product.

Known Vulnerability Testing: – All software binaries, including executables and libraries, in a product are assessed for known vulnerabilities at the time of evaluation. The vulnerabilities are identified from the NIST National Vulnerability Database (NVD).

Malware Testing: The product is inspected for malware which may exist in the software deliverables of the product.

Fuzz Testing: All external interfaces and communication protocols of the product is evaluated using generational fuzz testing techniques, if available, and template-based fuzz testing techniques otherwise. The product is evaluated for unexpected behavior based on the customer's specifications.

Robustness Evaluation aims to test the product's resilience against unexpected or malformed input.

Weakness Analysis

- ○ Common Weakness Enumerations (CWE): The product shall not contain any software weakness identified from CWE/SANS Top 25 Most Dangerous Software Errors, CWE/SANS on the cusp list or OWASP Top 10 2013 web application software weaknesses.
- ○ Static Code Analysis: Static analysis of all compiled executables and libraries of the product, in order to look for known malware and vulnerabilities
- ○ Static Binary and Byte Code Analysis: Static binary and byte code analysis of all compiled or intermediate binary executables and libraries of the product.

Penetration Testing: Evaluation of a product to identify vulnerabilities and software weaknesses.

Network Port and Service Testing

Wireless Testing: If a product has wireless communications technologies, the product is evaluated to identify vulnerabilities and software weaknesses through wireless access points.

Risk Assessment: Analysis by the vendor of the security risk(s) for the product.

Common Vulnerability Scoring System (CVSS): Provides a means for prioritizing CVEs in terms of exploit potential.

Common Weakness Scoring System (CWSS): Provides a means for prioritizing CWEs based on their technical impact.

Common Attack Pattern Enumeration and Classification (CAPEC): List of large number of attack patterns which are a description of common methods for exploiting software.

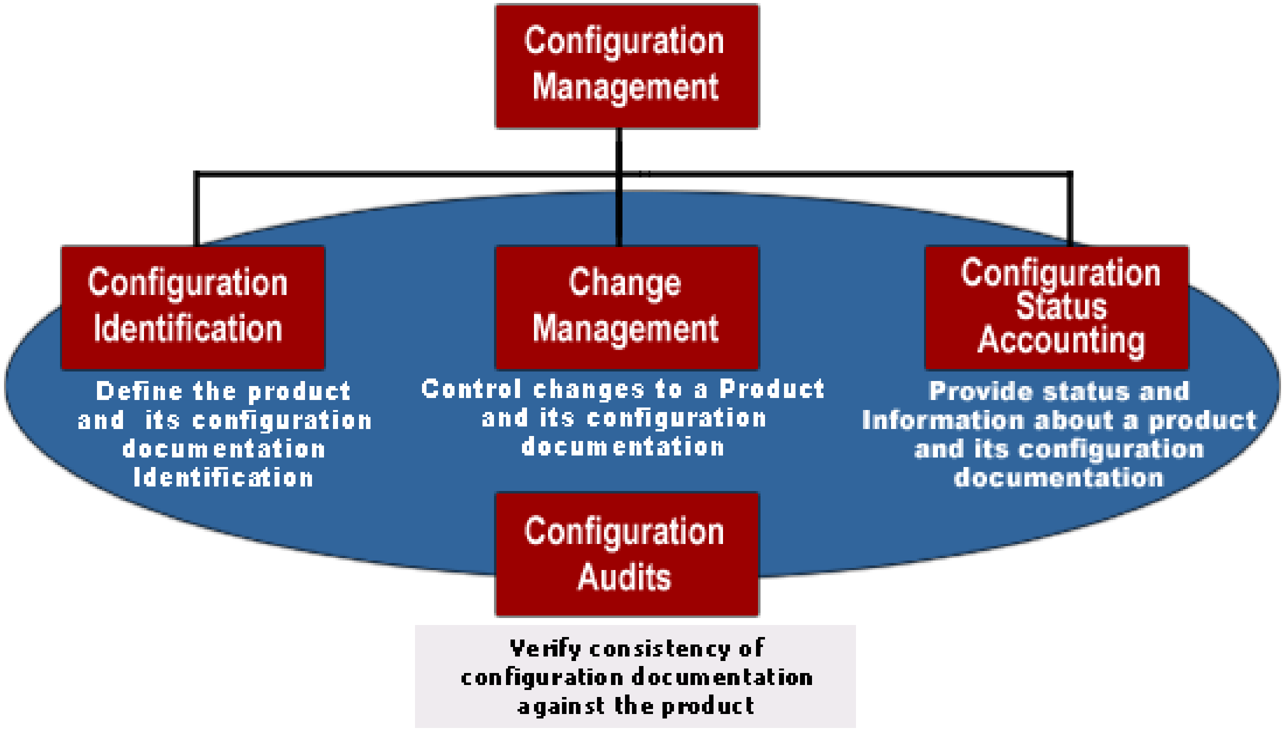
Organizational Assessment

Patch Management

SDLC

Wireless

Managing through the constantly changing threat landscape


Configuration Management
Configuration Identification
Define the product and its configuration documentation Identification
Change Management
Control changes to a Product and its configuration documentation
Configuration Status Accounting
Provide status and Information about a product and its configuration documentation
Configuration Audits
Verify consistency of configuration documentation against the product

http://ops.fhwa.dot.gov/freewaymgmt/publications/cm/handbook/chapter1.htm

Example CM strategy X.Y; where X represents critical changes and Y represents non-critical changes.

PRESS RELEASE

U.S. Department of Veteran Affairs and UL Sign CRADA for Medical Devices Cybersecurity Standards and Certification Approaches

--CRADA Project Will Support Improvement of Veterans Patient Safety and Security through Use of UL Cybersecurity Assurance Program—

NORTHBROOK, Ill., June 16, 2016 — The U.S. Department of Veteran Affairs (VA) and UL (Underwriters Laboratories), a global safety science organization, today announced a signed Cooperative Research and Development Agreement Program (CRADA) for medical devices cybersecurity standards and certification approaches. As part of the Federal Technology Transfer Act of 1986, the CRADA mechanism was established to encourage the creation of teams to solve technological and industrial problems for the greater benefit of the country.

This CRADA project will support improvement of Veterans patient safety and security through the use and verification of UL's Cybersecurity Assurance Program (CAP). Working with UL, the VA's Office of Information & Technology will refine existing and emerging standards and practices related to network connectable medical devices, medical device data systems and related health information technology. Both parties expect the project to accelerate the sharing of medical device cybersecurity information, standards and lifecycle requirements towards creating a safety certification framework for Veterans.

medicalsolutions.ul.com

Thank you