The Real-World Challenges of Medical Device Cybersecurity:

MITIGATING VULNERABILITIES

timesys

A LYNX SOFTWARE TECHNOLOGIES COMPANY

ICS

ICS

Milton is a certified PMP and Scrum Master with a background in software architecture, medical device product development and program management. He has 20 years in product development with 10 years in software consulting and 15 years working with Class II and Class III medical device manufacturers.

Director of Medical Programs and Cybersecurity for ICS

Milton Yarberry

timesys

A LYNX SOFTWARE TECHNOLOGIES COMPANY

Maciej has more than 25 years of experience in embedded computing with a focus on embedded Linux and real-time systems. The creator of Timesys University embedded Linux workshops and the co-host of LinuxLink Radio, Maciej has also authored numerous embedded Linux and industry articles.

Vice President of EMEA Business Development & Technical Sales

Maciej Halasz


The Real-World Challenges of
Medical Device Cybersecurity:
MITIGATING VULNERABILITIES
TODAY'S
WEBINAR
INTRODUCING
ICS

Agenda

From Abstract:

“Recap the process for managing vulnerabilities
Identify the categories of vulnerabilities and solutions
Describe the methods for applying mitigations

- *OS*
- *Kernel mode drivers*
- *Open source*
- *Custom application software*

Provide an overview of Software Bill of Materials (SBOM) and explain why it’s relevant but challenging

Discuss Cybersecurity reporting to the FDA including the handling of CVEs and the role of Penetration testing”

Milton

1. Recent industry change – key events
2. Key process for managing vulnerabilities with some key elements
3. Vulnerabilities and solutions
4. Organization of outputs for FDA

Maciej

1. Methods for mitigating vulnerabilities
2. SBOM management
3. Vulnerability monitoring
4. OS Long-term maintenance

Questions

ICS

About ICS

Established in 1987, Integrated Computer Solutions, Inc. (ICS) delivers **innovative software solutions** with a full suite of services to accelerate development of successful next-gen products.

ICS is **headquartered outside Boston** in Waltham, Mass. with offices in California, Canada and Europe. Currently 160 people.

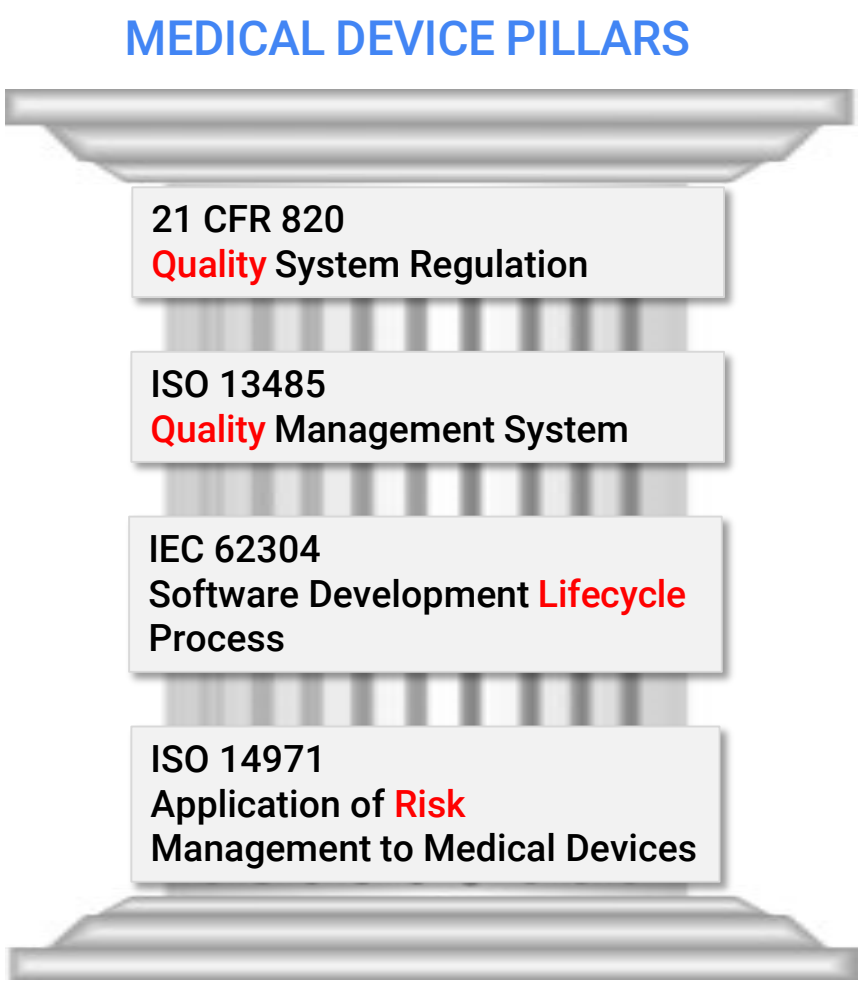
Boston UX is ICS' design studio, specializing in intuitive touchscreen and multimodal interfaces for high-impact embedded and connected devices.

Delivering a Full Suite of Medtech Services

- IEC 62366-UX/UI Design
- Human Factors Engineering
- Custom Frontend and Backend Software Development
- Development with IEC 62304-Compliant Platform
- Low-code Tools that Convert UX Prototype to Product
- Medical Device Cybersecurity
- AWS and Azure Cloud Services and Analytics
- ISO 14971-Compliant Hazard Analysis
- Software Verification Testing
- Complimentary Software Technology Assessment

Key Events for Medical Device Cybersecurity

Regulations, Guidance, Standards



Key Events for Medical Device Cybersecurity

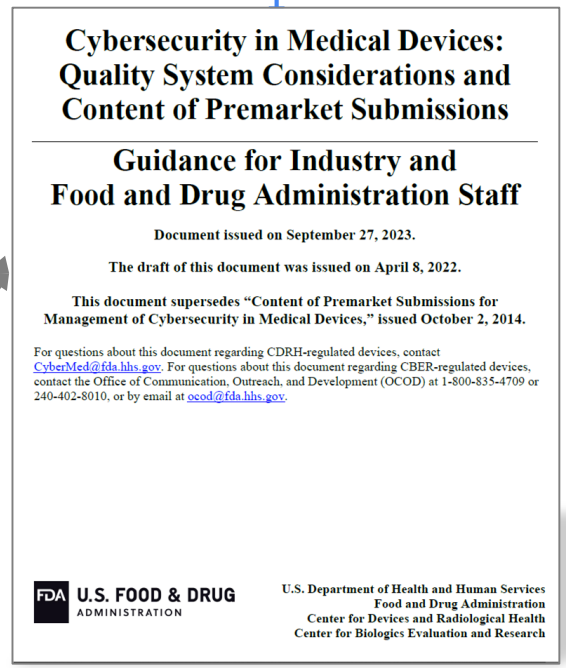
Regulations, Guidance, Standards

MEDICAL DEVICE PILLARS

- 21 CFR 820
  Quality System Regulation
- ISO 13485
  Quality Management System
- IEC 62304
  Software Development Lifecycle Process
- ISO 14971
  Application of Risk Management to medical devices

PATCH Act (524B)
Passes Congress

December 29, 2022



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

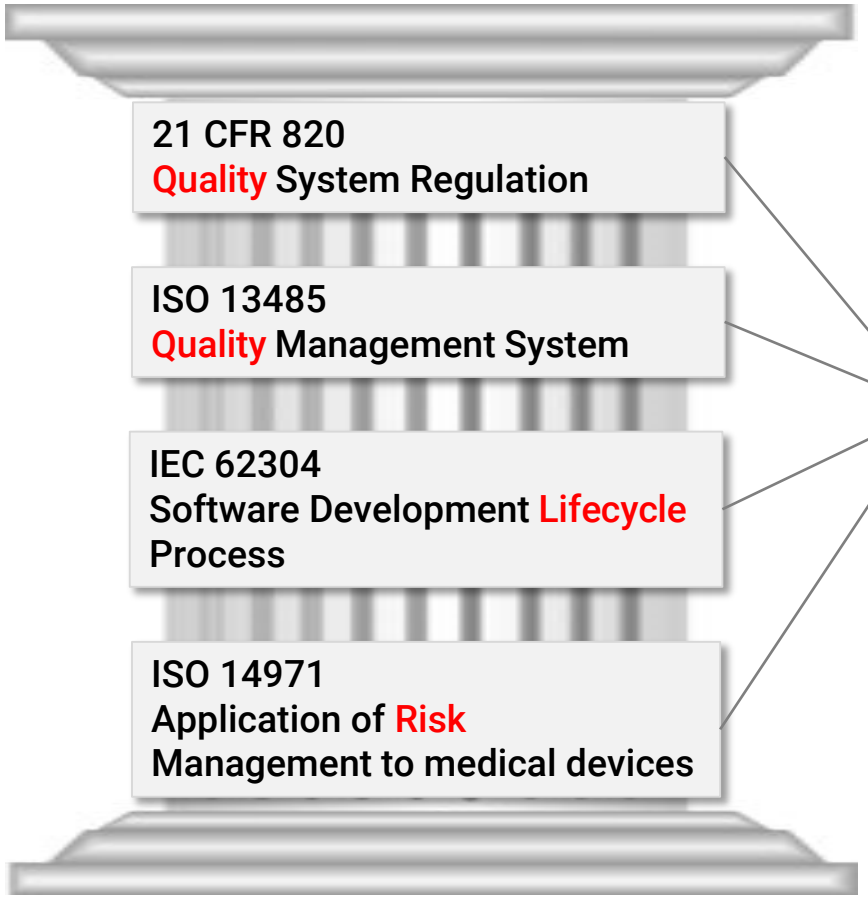
FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

Key Events for Medical Device Cybersecurity

Regulations, Guidance, Standards

MEDICAL DEVICE PILLARS



PATCH Act (524B)
Passes Congress

December 29, 2022

Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 240-402-8010, or by email at ocod@fda.hhs.gov.

Enforced Oct 2023

FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

Key Events for Medical Device Cybersecurity

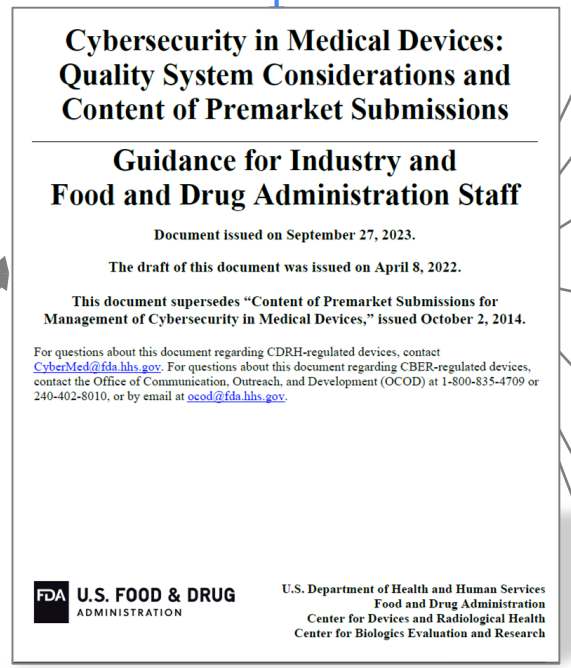
Regulations, Guidance, Standards

MEDICAL DEVICE PILLARS

- 21 CFR 820 Quality System Regulation
- ISO 13485 Quality Management System
- IEC 62304 Software Development Lifecycle Process
- ISO 14971 Application of Risk Management to medical devices

PATCH Act (524B) Passes Congress

December 29, 2022



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

FDA U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

CYBERSECURITY RECENT

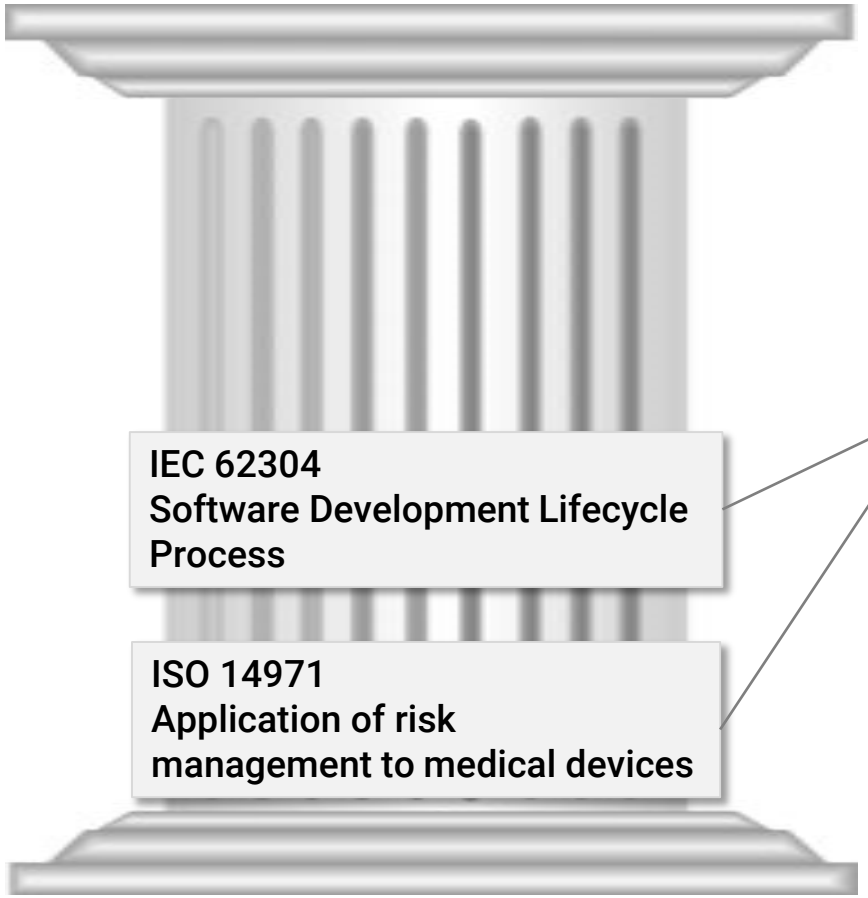
- ISA 62443 Security for industrial automation and control systems
- ISO 81001 5-1 Health Software IT Security
- NIST Cybersecurity Framework NIST CSF - NIST800-30 Risk assessment
- UL 2900 1-1 UL Standard for Safety Software Cybersecurity for Network-Connectable Products
- TIR57 Principles for medical device security - Risk management
- TIR97 Principles for medical device security – Post-market risk management for device manufacturers
- AAMI SW96

ICS

Key Events for Medical Device Cybersecurity

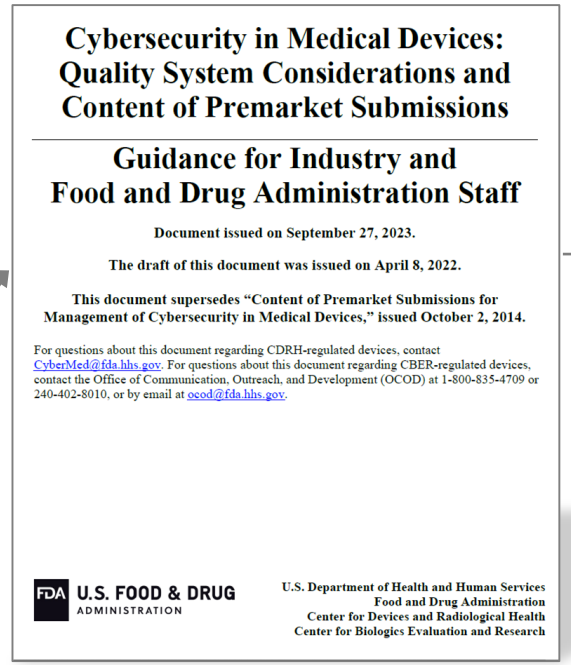
Regulations, Guidance, Standards

MEDICAL DEVICE PILLARS



IEC 62304
Software Development Lifecycle Process

ISO 14971
Application of risk management to medical devices



Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions

Guidance for Industry and Food and Drug Administration Staff

Document issued on September 27, 2023.

The draft of this document was issued on April 8, 2022.

This document supersedes "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices," issued October 2, 2014.

For questions about this document regarding CDRH-regulated devices, contact CyberMed@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.

FDA U.S. FOOD & DRUG ADMINISTRATION

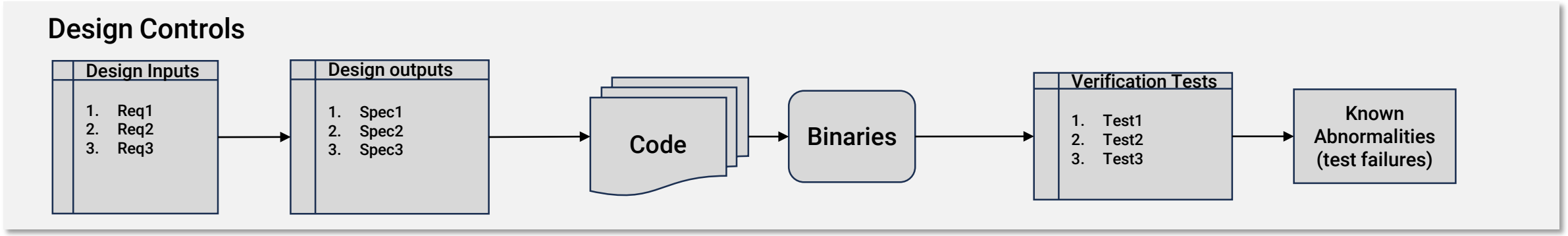
U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

SPDF

Secure
Product
Development
Framework

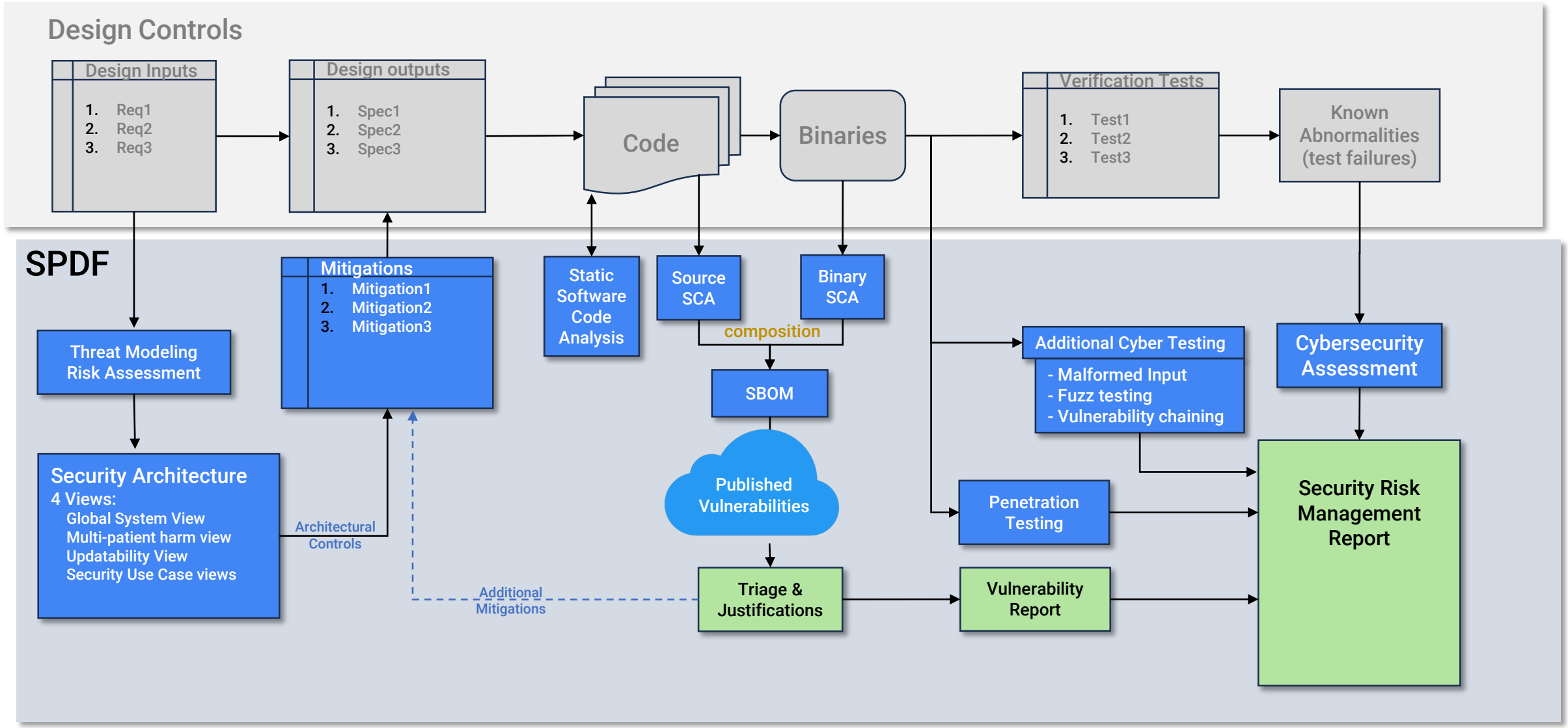
Cybersecurity Process

Traditional Design Control Process for Medical Devices



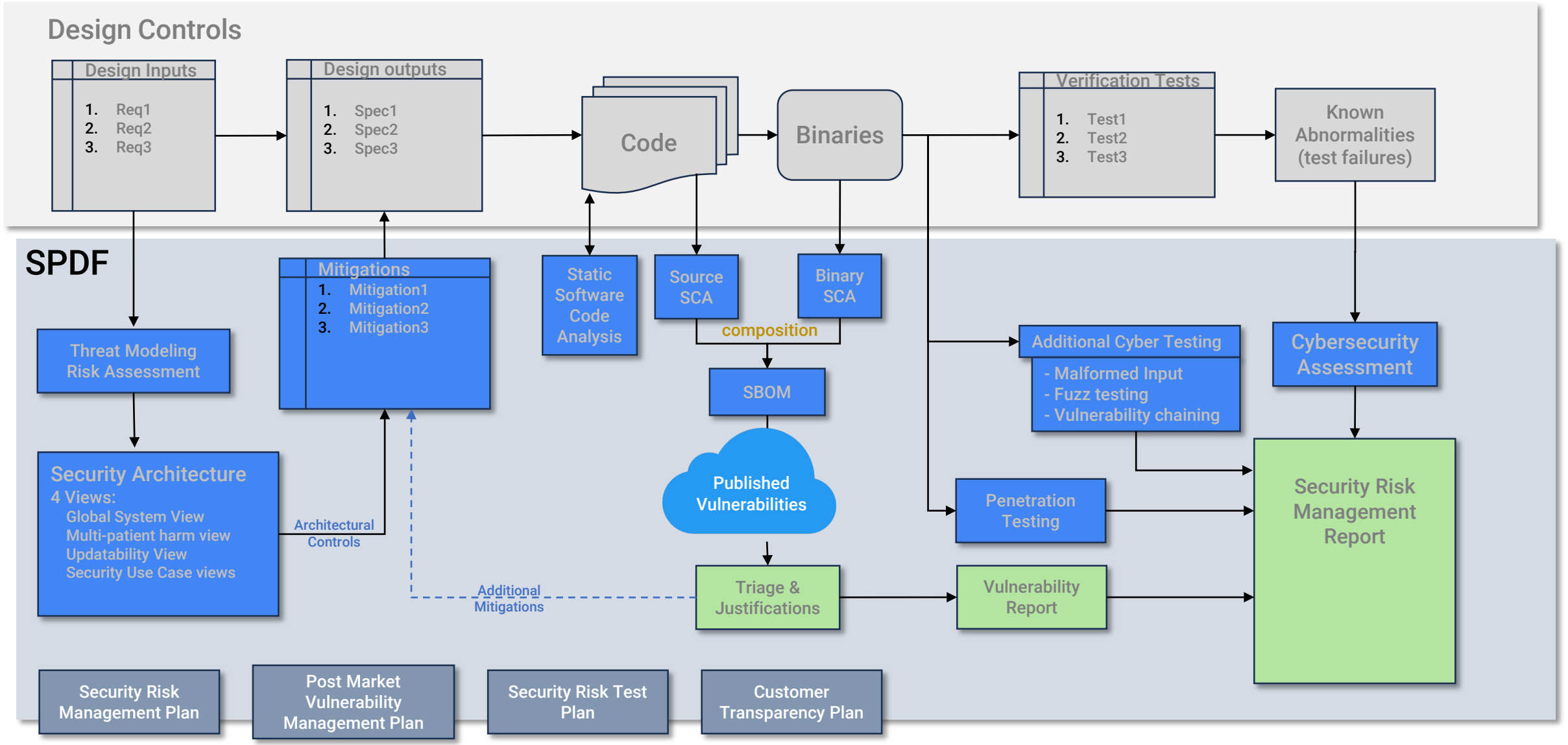
Cybersecurity Process

Secure Product Development Framework (SPDF)



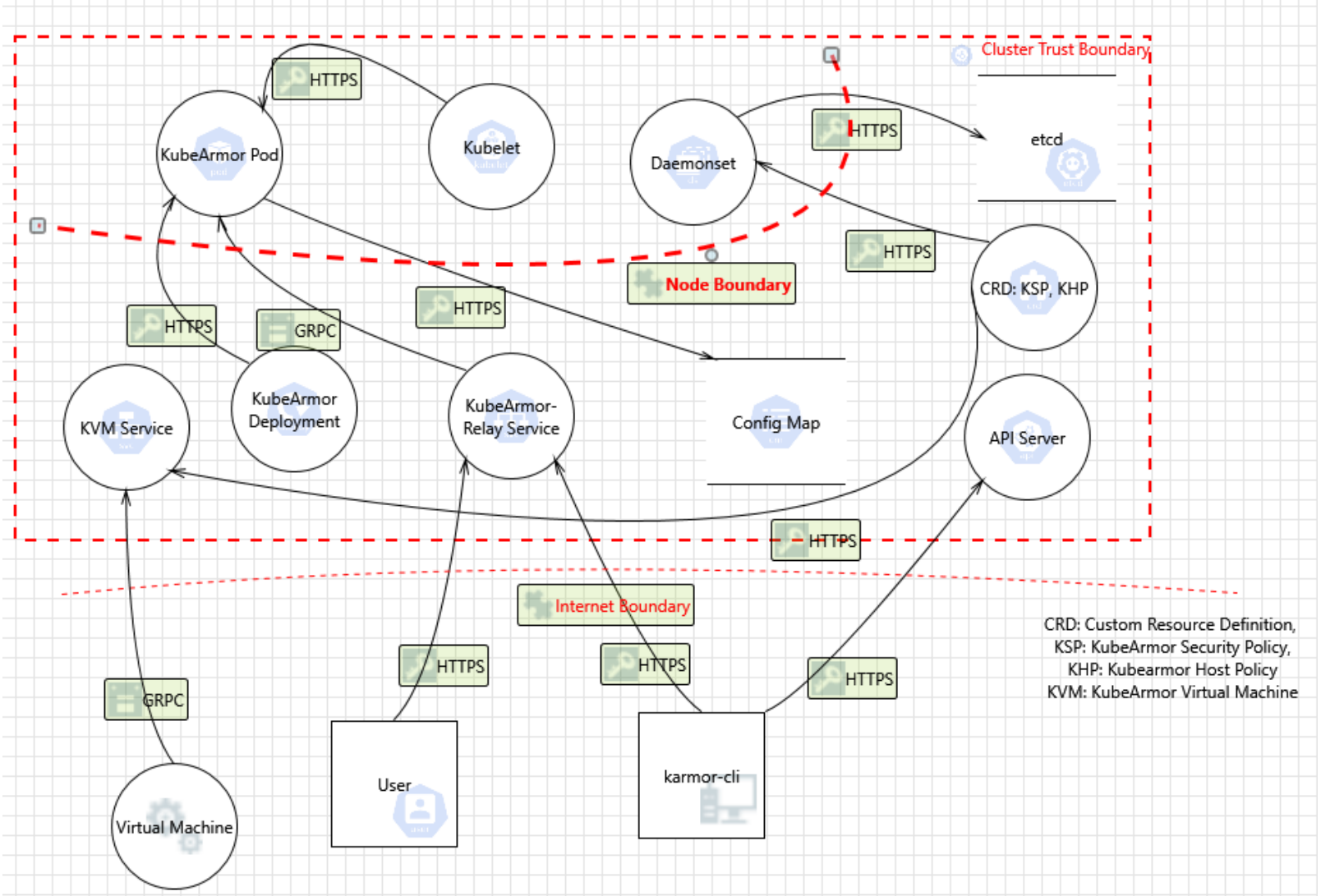
Cybersecurity Process

SPDF Planning



Threat Modeling

- Asset based method to identify threats
- Notionally data flow driven
- Based on trust boundaries, assets and communication



4 Architectural Views

1. Global System View
   - Threat model can satisfy this view
   - External and Internal connections
   - Includes support systems
     - SW update, Service
     - Cloud DB servers, Backups

2. Multi-Patient Harm View
   - Large scale exploits
     - DB compromised
     - Ransomware
     - Denial of service
   - Centralized infrastructure
     - Common servers
     - Common networks
   - Show the architecture controls that address scaled exploits
     - i.e. what locks are there on
       - Backend cloud server
       - The shared network
       - Historical results on a device

3. Updatability View
   - Diagram of the architectural controls when updating software/firmware
     - Chain of Trust – where did it come from
     - Secure boot – prevent unauthorized running
     - Roll-back if failure

4. Secure Use Case Views
   - Scenario centric
   - Use centric
   - Corner cases
     - Manufacturing
     - Stolen credentials
   - Swim lane or component diagram, but for chosen scenarios
   - Example: Service access

ICS

Asset List

Assets are a key part of the risk analysis

Developing an understanding of all the Assets (an Asset List) and how Threats and Vulnerabilities operate on Assets.

What's in an Asset List?

- All hardware
  - Servers, Co-processors, Processing cores, Communication relays, I/O interface, Network servers, Networks
- All software
  - Applications, Operating Systems, Data
- But don't forget
  - Communication interfaces/protocols
  - Support files (language, updates, logs, configurations)
  - Encryption keys, credentials, certificates

ICS

Security Control Categories

Vulnerabilities and Solutions

Control Category: Vulnerabilities	Solutions
Authentication:	
Authorization:	
Cryptography:	
Code integrity: **Data integrity:** **Execution integrity:**	
Confidentiality:	
Event Detection and Logging:	
Resiliency and Recovery:	
Software Updates:	

ICS

Security Control Categories Vulnerabilities and Solutions

Control Category: Vulnerabilities	Solutions
Authentication: • Invalid system (remote or subsystem) • Invalid user	
Authorization: • Unauthorized use	
Cryptography: • Confidentiality violations	
Code integrity: unauthorized code **Data integrity:** altered data **Execution integrity:** SQL injection	
Confidentiality: • Accessing patient info	
Event Detection and Logging: • Hacking attempts	
Resiliency and Recovery: • Denial of Service, therapy dependencies	
Software Updates: • Provision for Secure and timely updates	

Security Control Categories Vulnerabilities and Solutions

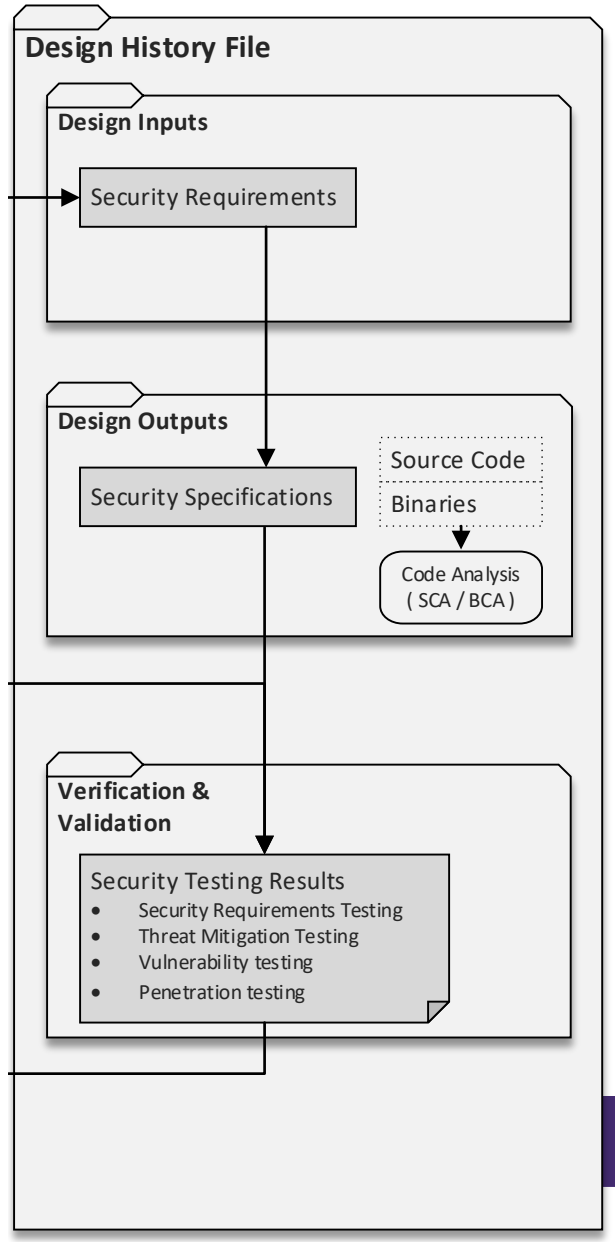
Control Category: Vulnerabilities	Solutions	
Authentication: • Invalid system (remote or subsystem) • Invalid user	System Authentication – CA and PKI User logins, Multi-factor Authentication	
Authorization: • Unauthorized use	Role based permissions	
Cryptography: • Confidentiality violations	Network encryption Database encryption Drive encryption	Key Management PKI
Code integrity: unauthorized code **Data integrity:** altered data **Execution integrity:** SQL injection	Root of Trust, Process monitoring Hashing/CRC Parsing controls, Host based intrusion	
Confidentiality: • Accessing patient info	PHI, PII, HIPAA	
Event Detection and Logging: • Hacking attempts	Security event detection Security Logs	Non-repudiation
Resiliency and Recovery: • Denial of Service, therapy dependencies	Trusted environments, Sub-system Isolation	
Software Updates: • Provision for Secure and timely updates	Ability to update in field Installation validation	Distribution infrastructure Update failure contingencies

ICS

Cybersecurity Outputs - Where does everything go?

Deliverables
Security Risk System Description
Plans
Risk Management Plan
Risk Test Plan
Vulnerability Management Plan
Customer Transparency Plan
Assessment
Threat Model
Asset List
Risk Assessment
Security Architecture
Architecture views
Global, Multi-Patient, Updatability, Use Case
Post Production file
SBOM (Software Bill of Materials)
CVE Assessment
Security Risk Management Report
Security Requirements
Security Specifications
SCA Analysis

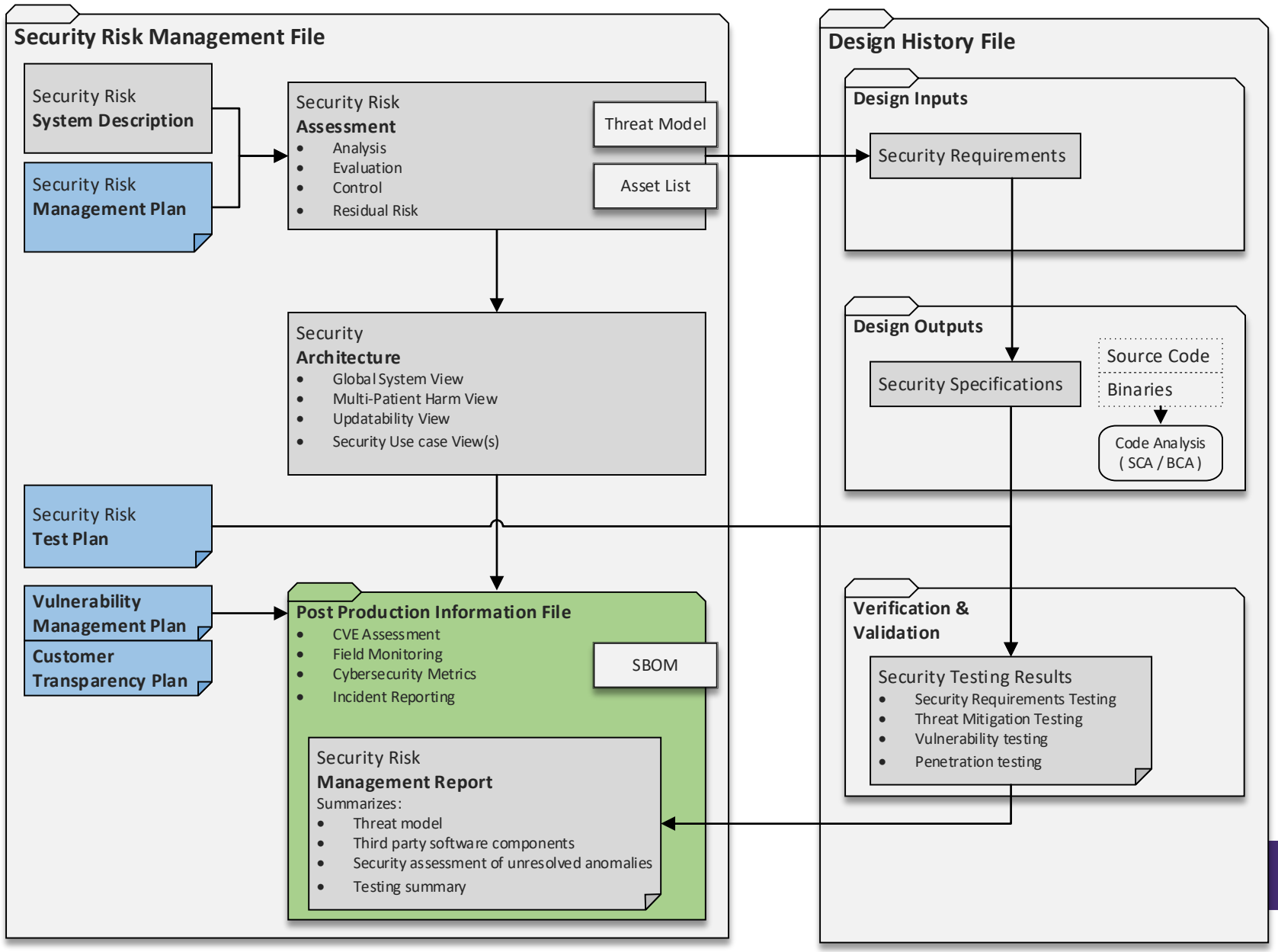
Additional efforts
Field Monitoring
Incident Reporting
SBOM updates



Cybersecurity Outputs - Where does everything go?

Deliverables
Security Risk System Description
Plans
Risk Management Plan
Risk Test Plan
Vulnerability Management Plan
Customer Transparency Plan
Assessment
Threat Model
Asset List
Risk Assessment
Security Architecture
Architecture views
Global, Multi-Patient, Updatability, Use Case
Post Production file
SBOM (Software Bill of Materials)
CVE Assessment
Security Risk Management Report
Security Requirements
Security Specifications
SCA Analysis

Additional efforts
Field Monitoring
Incident Reporting
SBOM updates



The Real-World Challenges of Medical Device Cybersecurity:

MITIGATING VULNERABILITIES

TODAY'S WEBINAR

INTRODUCING

timesys

A LYNX SOFTWARE TECHNOLOGIES COMPANY


timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

About timesys

A LYNX SOFTWARE TECHNOLOGIES COMPANY

What do we do?

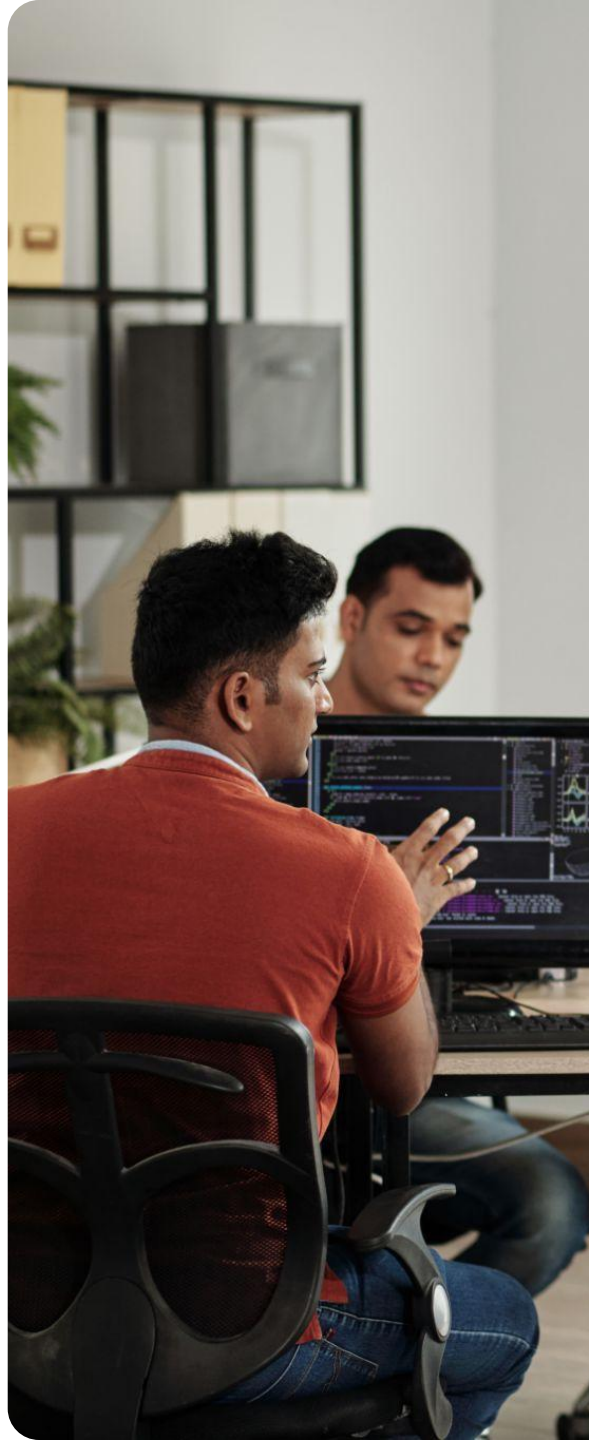
We expand your embedded Linux device capabilities by leveraging our 25+ years of experience and expertise as industry pioneers, so you can free up engineering resources, increase productivity, be confident in your core open source OS and security feature implementation, and minimize OEM risks, for the entire lifecycle of your devices.

Building, Securing, and Maintaining embedded platforms for you

1000+ Customers & Software Projects

Embedded OS Software Security Thought Leaders

20+ Years Embedded Linux Experience



open source embedded software platforms

(Linux Yocto, Buildroot, Debian/Ubuntu, Android, and Timesys Factory)

timesys

timesys

A LYNX SOFTWARE TECHNOLOGIES COMPANY

The Real-World Challenges of Medical Device Cybersecurity

-Mitigating Vulnerabilities

Maciej Halasz

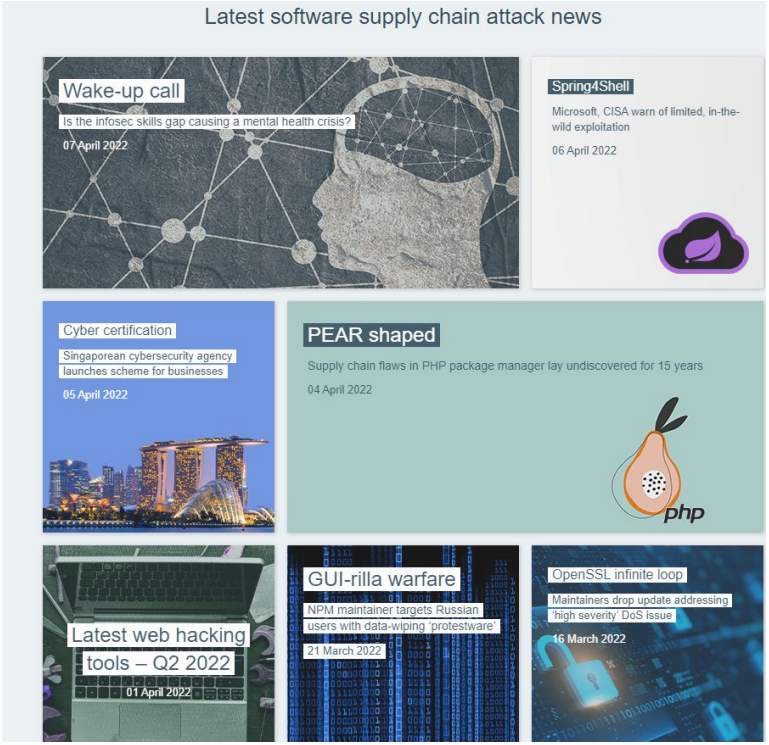
Software Supply Chain Attacks in the News

Protestware

- Devs wanting to make a point, are self-sabotaging open source, protesting both countries and corporations
- node-ipc, es5-ext

Hijacks - drop password-stealer DLLs, cryptominers

- typosquatting / brandjacking
  - Django vs. Diango, Djanga, Djago, and Dajngo
  - klown pretends to be UAParser.js
  - noblox.js-proxies vs. proxied
- repo jacking & chainjacking
- version 2 squatting: “fake” new versions
  - new versions of coa & rc libs published to npm



Hidden malware: look like comments but execute code, or smuggling hidden backdoors with homoglyphs and invisible Unicode characters

timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

Software Supply Chain: Open Source Eating the World

2008 Gartner report on the state of open source software:

"if you don't think you use it, then you use it; and

if you think you do use it, then you use lots more of it than you know."

The Hidden & Exponential Challenges of Dependencies:

- direct: libraries code is directly calling into
- transitive: libraries that your dependencies are linked against (dependencies of dependencies)

Example: sqlite requires dependencies like readline & zlib; readline requires glibc & ncurses, etc.

Will Attackers Target IT or Embedded Devices?

🔮 55.7 billion connected IoT devices; 80B ZB data

📱 embedded products = larger and more vulnerable attack surface

🔒 air gaps can't provide adequate security for processed data

Good news and bad news

👍 Attacks focused on widely used/downloaded packages on *poorly designed* embedded systems

👎 As IT gets harder to attack, hackers will focus on Embedded targets

timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

Medical Device Using OSS and Embedded Linux

Imaging	Diagnostics	Therapeutic	Proactive Health
			
CT Scanner	ECG	Infusion Pumps	Fitness Equipment
Ultrasound	Patient Monitoring	Defibrillators	Restorative Therapy
MRI	Home Monitoring	Ventilators	TeleHealth
Digital X-Ray	Bedside Terminals		
Retinal Scanners	Self diagnostic station		

timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

timesys

A LYNX SOFTWARE TECHNOLOGIES COMPANY

So What Things Should Product Companies Be Doing?

EO 14028: SBOM is gaining momentum

THE WHITE HOUSE
WASHINGTON

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

(v) providing, when requested by a purchaser, artifacts of the execution of the tools and processes described in subsection (e)(iii) and (iv) of this section, and making publicly available summary information on completion of these actions, to include a summary description of the risks assessed and mitigated;

(vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and performing audits and enforcement of these controls on a recurring basis;

(vii) providing a purchaser a Software Bill of Materials (SBOM) for each product directly or by publishing it on a public website;

(viii) participating in a vulnerability disclosure program that includes a reporting and disclosure process;

- CISA shows that **Build-based SBOM are better** than other types but each type has limitations.
- **Vigiles** is a Design- and Build-based **SBOM Management tool**.
- NEW Vigiles **supports industry-standard** SPDX and CycloneDX SBOM types.

CISA has compiled a table listing the benefits and disadvantages of various types of SBOMs:

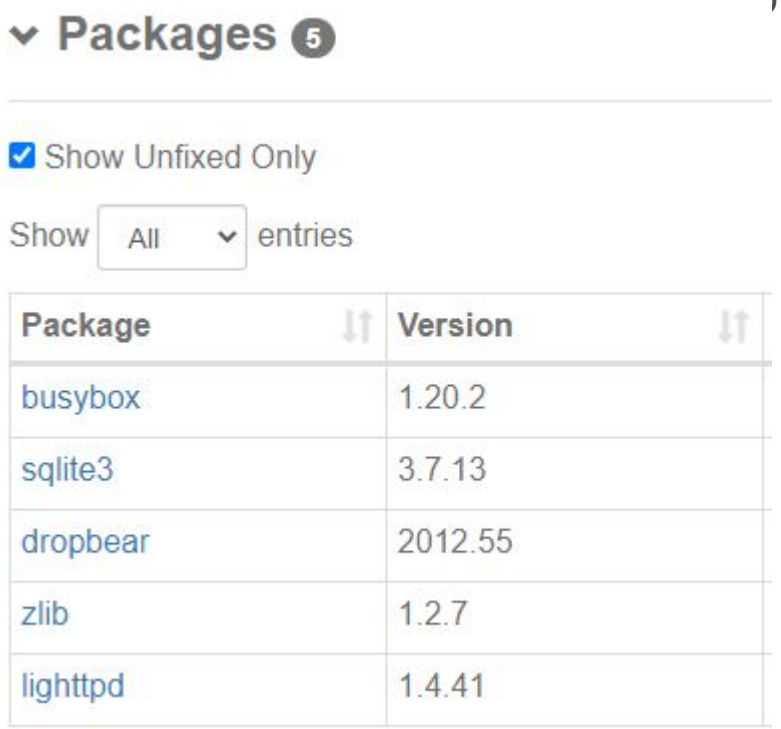
SBOM Type	Benefits	
Design	ighlight incompatible components ahead of licensing purchase or acquisition - Defines approved or recommended included component list for developer use	- This may be very di enerate - Unlikely to identify as muc as found in a Source or Build SBOM
Source	- Provides visibility without access to build process - Can facilitate remediation of vulnerabilities at the source - Can provide a view into the dependency tree / hierarchy of the included components	- Can highlight components and vulnerabiliti that never run or compiled out in deployed cod - May not include runtime, plugin, or dynamic components, like appserver or platform libraries - May require references to other SBOMs for completeness
Build	- Increases confidence that the SBOM representation of the product artifact is correct due to information available during the build and/or CI/CD processes - Provides visibility into more components than just source code - Increased trust by enabling signing of the SBOM and product artifact by the same build workflow	- Potentially have to change build process to generate this SBOM - Highly dependent on the build environment in which the build is executed - May be difficult to capture indirect and/or runtime dependencies - May not contain the correct versions of dynamically linked dependencies
Analyzed	ovides visibility without an active de environment, such as legacy firmware ar - Does not need access to build proces - Can help verify SBOM data from other sources - May find hidden dependencies missed by other SBOM Type creation tools	- May be prone to o or approximations if the tool i decompose or recognize components precisely - May depend on heuristics or context-specific risk factors
Deployed	- Highlights software components installed on a system, including other configurations and system components used to run an application	- May require changing install and deploy processes to generate - May not accurately reflect the software's runtime environment, as components may reside in inaccessible code
Runtime	- Provides visibility to understand what is in use when the system is executing - Not only provides SBOM information on components in a system, but can highlight how components are used and what they do	- Collected during system execution and may involve additional overhead - Period of time window may miss specific artifacts that are not invoked during the time interval used

https://docs.google.com/document/d/1PsUhUQ_L-lNymD9p613zP0_MiT1Boag68TP3aiwZ4R8/edit#

1. Understand What is in Your Product

- Need for accurate SBOMs
  - Importance of integrating directly into your build system / CI process
- NTIA minimum elements of SBOM driven by Executive Order
- Standardization for interoperability: SPDX, CycloneDX

SPDX format




```
SPDXVersion: SPDX-2.2
DataLicense: CC0-1.0
SPDXID: SPDXRef-DOCUMENT
DocumentName: imx-image-core
DocumentNamespace:
https://linuxlink.timesys.com/vigiles/spdxdocs/imx-image-core-18044d5f-999d-4
94c-a6e9-c399b57f41a9
LicenseListVersion: 3.13
Creator: Organization: Timesys Corporation
Creator: Tool: VigilesManifestExporter-1.0
Created: 2022-05-03T19:08:38Z
CreatorComment: <text>This document was auto-generated by
VigilesManifestExporter tool.</text>

PackageName: busybox
SPDXID: SPDXRef-busybox-1.33.1
PackageVersion: 1.33.1
PackageDownloadLocation:
https://busybox.net/downloads/busybox-1.33.1.tar.bz2;name=tarball
FilesAnalyzed: false
PackageLicenseConcluded: NOASSERTION
PackageLicenseDeclared: GPLv2 AND bzip2-1.0.4
PackageCopyrightText: NOASSERTION
ExternalRef: SECURITY cpe23Type
cpe:2.3:a:busybox:busybox:1.33.1:*:*:*:*:*:*:*
PackageSupplier: Organization: OpenEmbedded ()
```

SBOM Management in Vigiles

End user

SBOM Generation

CI/CD Auto generated Build Systems

- Yocto
- Buildroot
- OpenWRT
- Factory

Import

SPDX
CycloneDX
CSV

Ecosystem

Languages
Other OS
Containers

SBOM Wizard

SBOM DashBoard

- SBOM Depot
- Product SBOM
- Compliance
- Vulnerability
- Alerts

Search CVEs

- ✓ Producing your NTIA compliant device SBOM
- ✓ SBOM generation wizard and/or ability to import externally generated SBOM
- ✓ Automated accurate SBOM generation anytime during your development lifecycle for major Linux build system including **Yocto, Buildroot, PetaLinux, Wind River Linux, PTXdist, OpenWrt, and Timesys Factory**
- ✓ Manage software supply chain risks leveraging detailed SBOM
- ✓ Intuitively track and manage SBOMs across various products and releases
- ✓ Automatic scan of your SBOM against our curated vulnerabilities database creates an immediate CVE report
- ✓ View side-by-side SBOM comparison with searchable SBOM and CVE sections
- ✓ Export your SBOM in SPDX and CycloneDX formats, official international open standards for SBOMs

SBOM Compliance

VIGILES®

- Create **license compliance** policies
- Get notified when a **New Package** is added to your chain of linked SBOMs
- Check if your SBOM is **NTIA compliant**

timesys

A LYNX SOFTWARE TECHNOLOGIES COMPANY

2. Validate the Provenance and Integrity of Your Software Components

- Where does each software component come from?
- Starting with a “vetted” release
- Verify signatures, or, at a minimum, verify hash
- Perform Static Code Analysis
- More:
  - Have commit signing as a mandatory configuration.
  - Enable static code scanning and open source scanning across your repositories.
  - Before any software is updated, run the changes through a code checking review and signing process by another party; this can guard against unintentional oversights and insider threats.

Software provenance

- Off-The-Shelf Software (OTS Software):
  - A generally available software component, used by a medical device manufacturer for which the manufacturer cannot claim complete software life cycle control (Definition from the FDA)
- Commercial Off-The-Shelf Software (COTS Software):
  - OTS software that comes from a commercial supplier
  - Typically binary, commercial software distribution (e.g. VxWorks, Windows, RedHat)
  - Binary, commercial components (e.g. drivers, FPGA algorithms, AI components)
- Software of Unknown Provenance (SOUP Software):
  - Software component that is already developed and widely available, and that has not been developed, to be integrated into the MEDICAL DEVICE (also known as "Off-The-Shelf Software"), or previously developed software for which adequate records of the development process are not available
  - Need to document each software component used in the Medical Device
  - Applies to Embedded, Open Source Linux

SOUP ingredients

- Definition can vary between companies
- Typically include:
  - Software name
  - Version
  - License
  - Origin
  - Author
  - Description
  - Intended use
  - Functional group
- Also may include
  - Safety Classification
  - Design Limitation
- Often sought by our customers: assistance in evaluating SOUP or OTS software compliance to MDR or FDA demands

How do companies fail?

Based on FDA Pre-Market Submission review, many FDA submissions fail around proper documentation, including:

- No software documentation provided
- Missing description
- Missing validation
- Missing traceability information
- Missing list of anomalies

3. Understand Vulnerabilities in Software Components

- Monitoring the SBOM as part of DevSecOps
- Defining a process and owner for addressing vulnerabilities
  - Cadence for pulling in security fixes
    - Challenges of upgrade breaking applications?
    - Challenges of frozen software from silicon vendors?
  - Field update process
- Picking LTS releases: 15 year product lifecycle

U-boot and the Linux kernel

linux_kernel	5.15.35	0	8	4	1	11
u-boot	2022.01	0	0	0	0	0

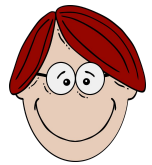
linux_kernel	4.19.239	1	14	20	2	18
u-boot	2020.01	1	3	0	0	0

u-boot	2018.01	16	7	2	0	0
linux_kernel	4.4.302	2	29	54	4	22

Package	Version	Unfixed				
u-boot	2013.01	14	6	3	0	0
linux_kernel	3.16.85	4	92	128	8	28

timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

Vigiles high-level architecture overview



End user

SBOM Generation

CI/CD Auto generated Build Systems

- Yocto
- Buildroot
- OpenWRT
- Factory

Import
SPDX
CycloneDX
CSV

Ecosystem
Languages
Other OS
Containers

SBOM Wizard

SBOM DashBoard

- SBOM Depot
- Product SBOM
- Compliance
- Vulnerability
- Alerts

Search CVEs

VIGILES®

Vigiles Scan

Curated vulnerability database
(NVD, Security Bulletins/Mailing list, Issue trackers: Debian/Ubuntu/Github, SoC advisories) + Patch/Fix Tracker

Notifications / Alerts (for new CVEs)

CVE Dashboard
- Summary + CVE details
- Filter / Prioritize
- Fix and mitigate info
- Triage, collaborate, track
- Downloadable reports, SPDX SBOM and more...

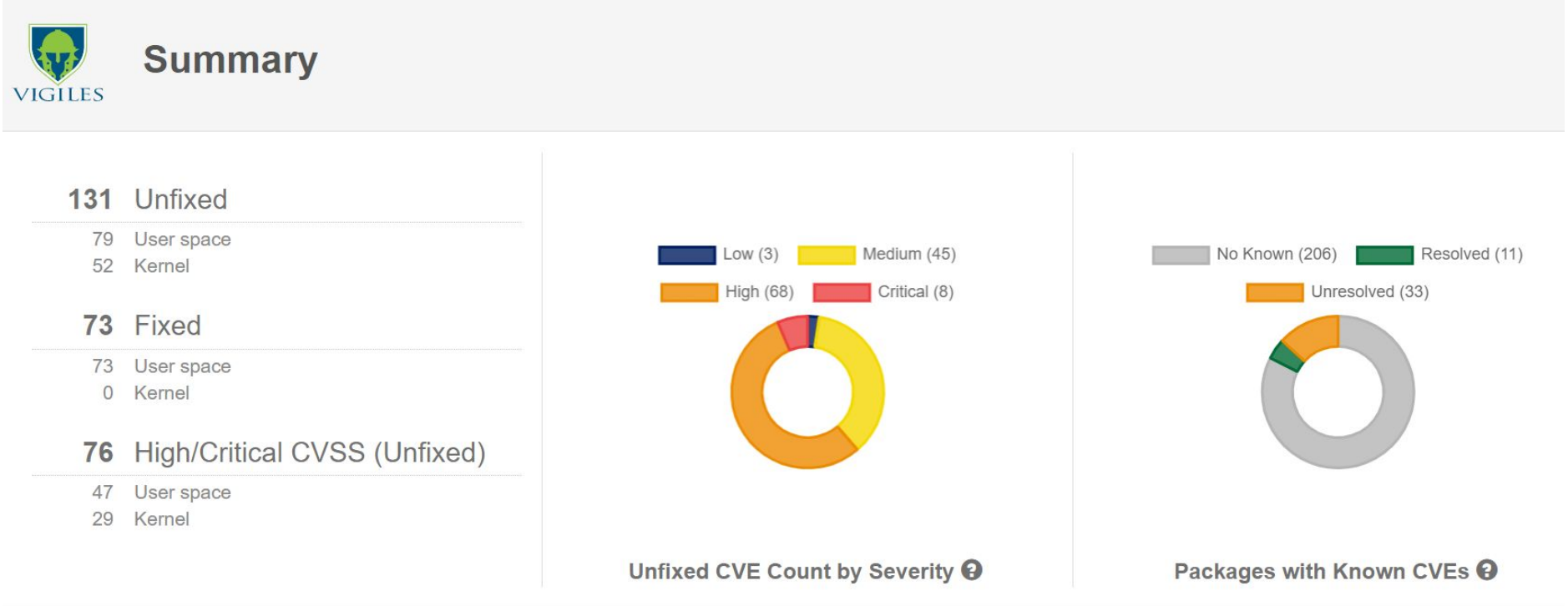
Desktop / Rest API CVE report

SBOM / Product management tools

Intelligent curation algorithms
+
Timesys Security research team

timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

Vulnerability Monitoring & Remediation

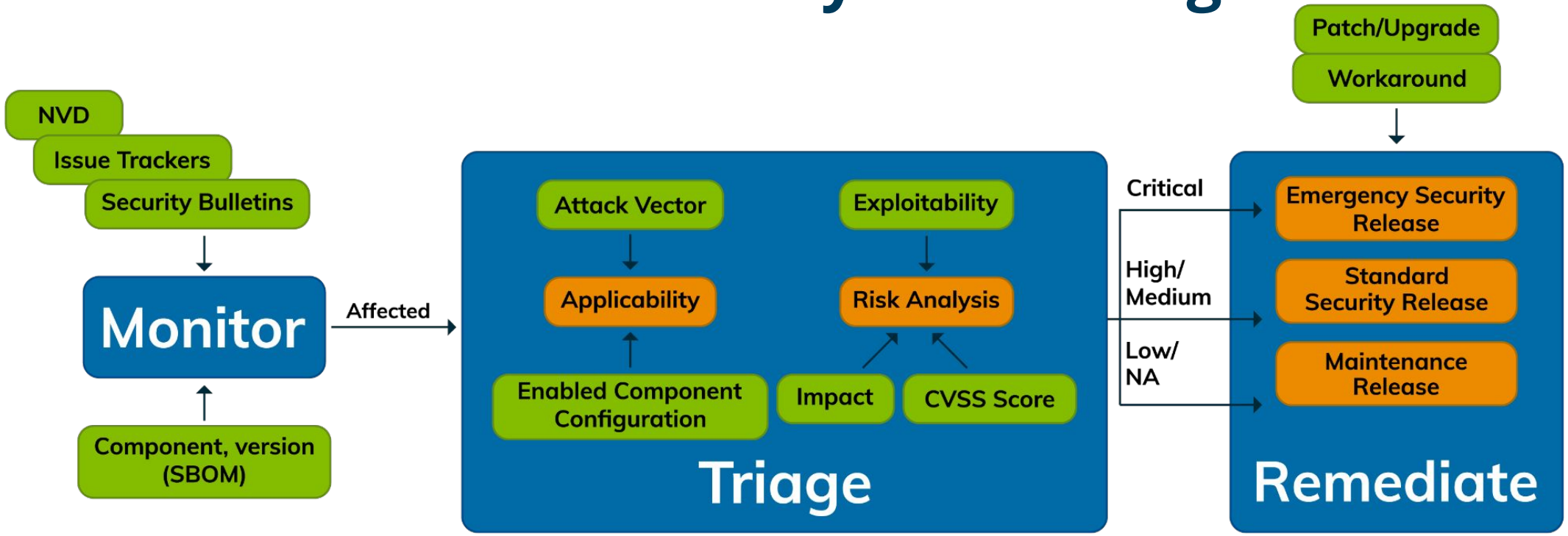


Industry's first SBOM management, CVE monitoring and remediation tool targeted at embedded Linux and Open Source RToS

- Continuously scans thousands of vulnerabilities curated by Timesys
- Filters CVEs based on your actual product configurations
- Monitors fixes across all of your product branches
- Powerful triage and collaboration tools accelerate fixes

timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

Recommended Vulnerability Monitoring Workflow



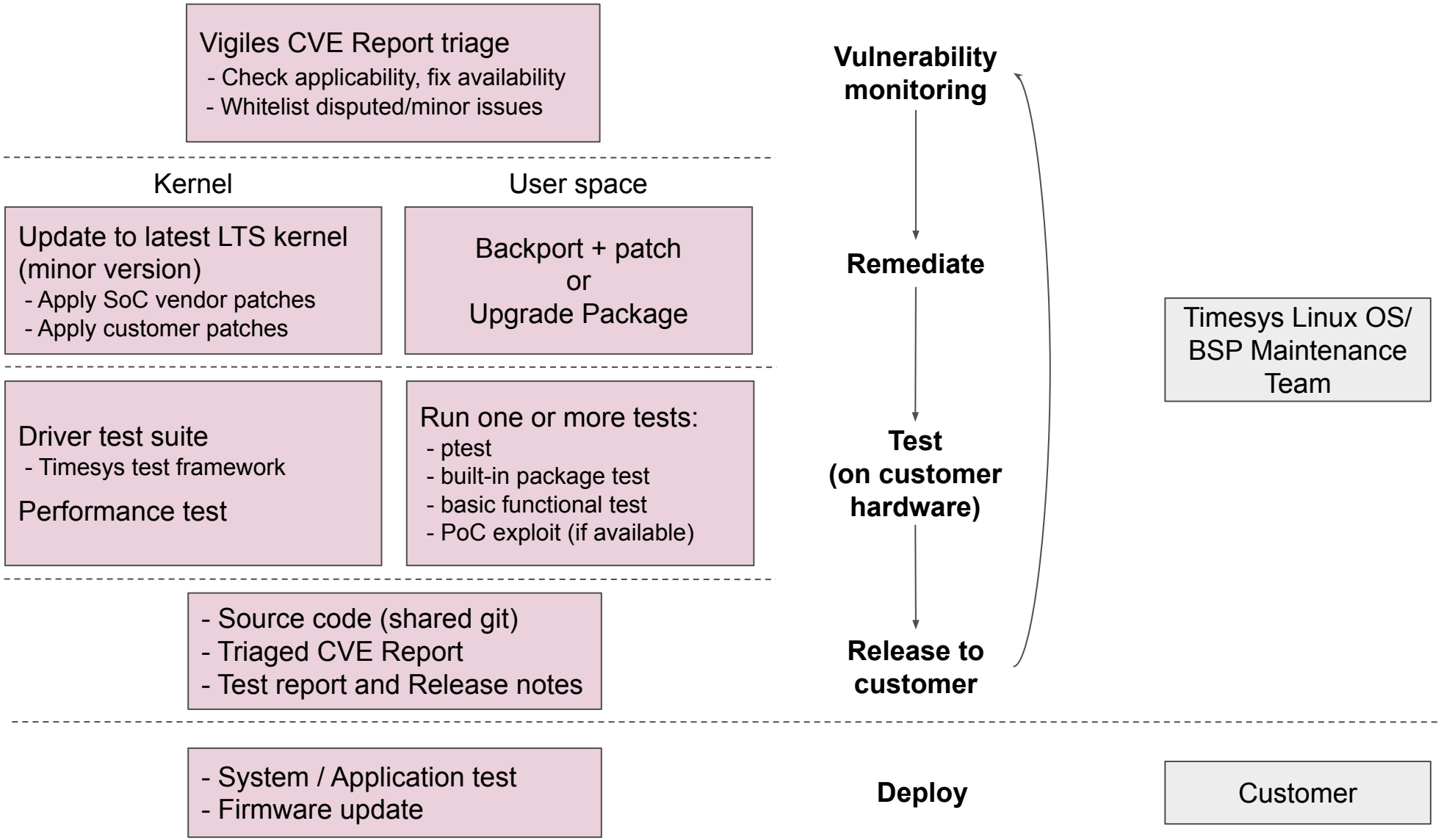
- Generate Device SBOM(s)
- Go through OSS Vulnerability feeds
- Determine which CVEs might apply

- Determine valid CVEs to perform risk analysis on
- Perform risk analysis to triage how urgently the applicable CVEs need to be addressed
- Document triage efforts

- Gather and validate remediation option information
- Coordinate remediation efforts
- Document remediation

timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

Linux OS/BSP Maintenance workflow: How Timesys does it



4. Communicate, Remediate and Mitigate

French hospital group disconnects Internet after hackers steal data

By **Bill Toulas** April 25, 2022 10:48 AM 1

The GHT Coeur Grand Est. Hospitals and Health Care group has disconnected all incoming and outgoing Internet connections after discovering they suffered a cyberattack that resulted in the theft of sensitive administrative and patient data.

FDA

Appendix: Sample Cybersecurity Vulnerability Safety Communication

NOT REAL – MOCK-UP OF CYBER COMMUNICATION – NOT REAL

Your Brand X Insulin Pump May Be Affected by X Cybersecurity Risk

*Medical devices, like other computer systems, can be vulnerable to security risks, potentially impacting the safety and effectiveness of the device. These are **cybersecurity risks**.*

Content current as of:
Month/Day/Year

Español | 简体中文 | 한국어 | Tagalog | Việt

Contact your health care provider right away if you think your Brand X insulin pump settings or insulin delivery changed unexpectedly.

An unauthorized person (someone other than a patient, patient caregiver, or health care provider) could potentially connect wirelessly to a nearby **Brand X** insulin pump. This unauthorized person could change the pump's settings to either over-deliver insulin to a patient, leading to low blood sugar (hypoglycemia), or stop insulin delivery, leading to high blood sugar (hyperglycemia) and diabetic ketoacidosis.

The FDA recommends people who have affected **Brand X** insulin pumps update the software on their devices to protect them from these risks.

Why do medical devices fail?

Software related recalls are growing (based on FDA records)

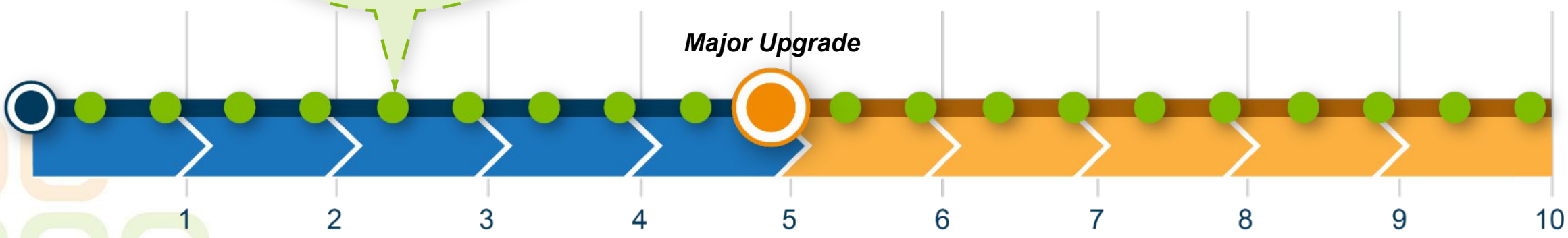
- Example - Insulin pump
  - Cybersecurity vulnerability
  - Exposure - ability to connect remotely to a device and change its settings
  - Risk - over deliver insulin to a patient
  - Result - recall of 4000+ devices
- Solution
  - CVE monitoring process
    - Knowing which software components are affected in your product ASAP
    - Generate reports, communicate
  - Cybersecurity maintenance process
    - Triage security information
    - Implement remediation steps
    - Rollout software updates
    - Generate reports, communicate

Long-term security updates and maintenance for Linux OS/BSPs

We keep your device secure and updated for the full product lifecycle:

- **updates 1-4x/year**
  - minor kernel version upgrade
  - security patches/updates/backports
- **vulnerability alerts, monitoring and management** w/ on-demand reports
- **joint review and analysis** of new vulnerabilities
- implement one **emergency release** if needed
- provide **documentation** of updates and testing

\+ major upgrades (recommended every 3-5 years)



Product Lifecycle (Average: 10 Years)

timesys
A LYNX SOFTWARE TECHNOLOGIES COMPANY

Key Takeaways

1. Understand the software in your product (and all dependencies!)
2. Validate the provenance of your source code
3. Monitor for vulnerabilities in your open source software
4. Communicate, Remediate, and Mitigate

A Framework for Supply Chain Evaluation (courtesy of Cloud Native Computing Foundation)

- Verify Source Code
- Verify Materials
- Protect Build Pipelines
- Protect Artifacts and Deployments

- Use Dependency Scanning Tools
- Employ Static and Dynamic Application Security Testing Tools
- Enable runtime application self-protection
- Automate Software Composition Analysis (SCA)

Al Feczko
VP of Sales & Field Engineering

US / Americas
+1-412-897-2416
Al.Feczko@timesys.com

Maciej Halasz
VP of EMEA Business Development & Technical Sales

EMEA
+48-537-338-080
Maciej.Halasz@timesys.com

Nagamahesh Gamidi
Business Development Manager

APAC
+91-814-754-1239
Nagamahesh.Gamidi@timesys.com

timesys

A LYNX SOFTWARE TECHNOLOGIES COMPANY

ICS

The Real-World Challenges of Medical Device Cybersecurity: MITIGATING VULNERABILITIES

TODAY'S WEBINAR

Q&A