NSF
NSF-ISR
Registered to ISO 13485

Simplexity®
PRODUCT DEVELOPMENT

BEST PRACTICES IN MEDICAL DEVICE SOFTWARE & FIRMWARE DESIGN

Katie Elliott, Expert Firmware Engineer

Dorota Shortell, CEO

January 14, 2021

PRESENTERS

Katie Elliott

- Expert Firmware Engineer
- Simplexity Quality Lead

Dorota Shortell

- CEO

AGENDA

- Motivation for software process
- Phase-based device and software development
  - Planning and Requirements
  - Architecture and Feasibility
    - Safety classifications
    - Risk Analysis
  - Detailed Design
  - Design Verification and Transfer
- Case Studies
- Best Practices Summary
- Q&A

FAILURES DUE TO SOFTWARE BUGS

- Toyota – unintended acceleration
  - Source code analysis
    - Memory corruption
    - Thousands of global variables
    - Overly complex, untestable, and unmaintainable functions – spaghetti code

- Inadequate software engineering process
  - Failure to use automotive software reliability coding standards
  - Failure to follow even Toyota’s inadequate rules
  - Safety not considered during design
  - No peer/code review

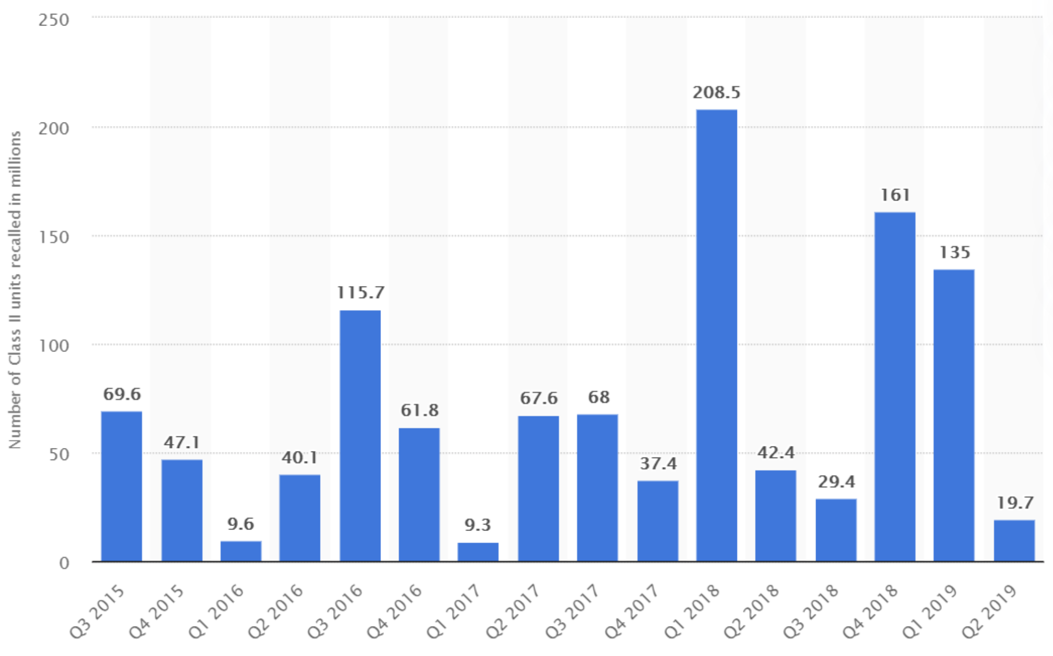
SW FAILURES IN MEDICAL DEVICES

Example recalls from 2019 due to software defects

- Smiths Medical– Syringe pumps – malfunctioning alarms and potential interruption of therapy
- Zimmer Biomet – ROSA Brain Robotic surgery system – software issue that incorrectly positions the robotic arm causing risk of patient injury
- Medtronic – Remote Controllers for MiniMed insulin pumps – potential cybersecurity risk

Device recalls have significantly increased in recent years

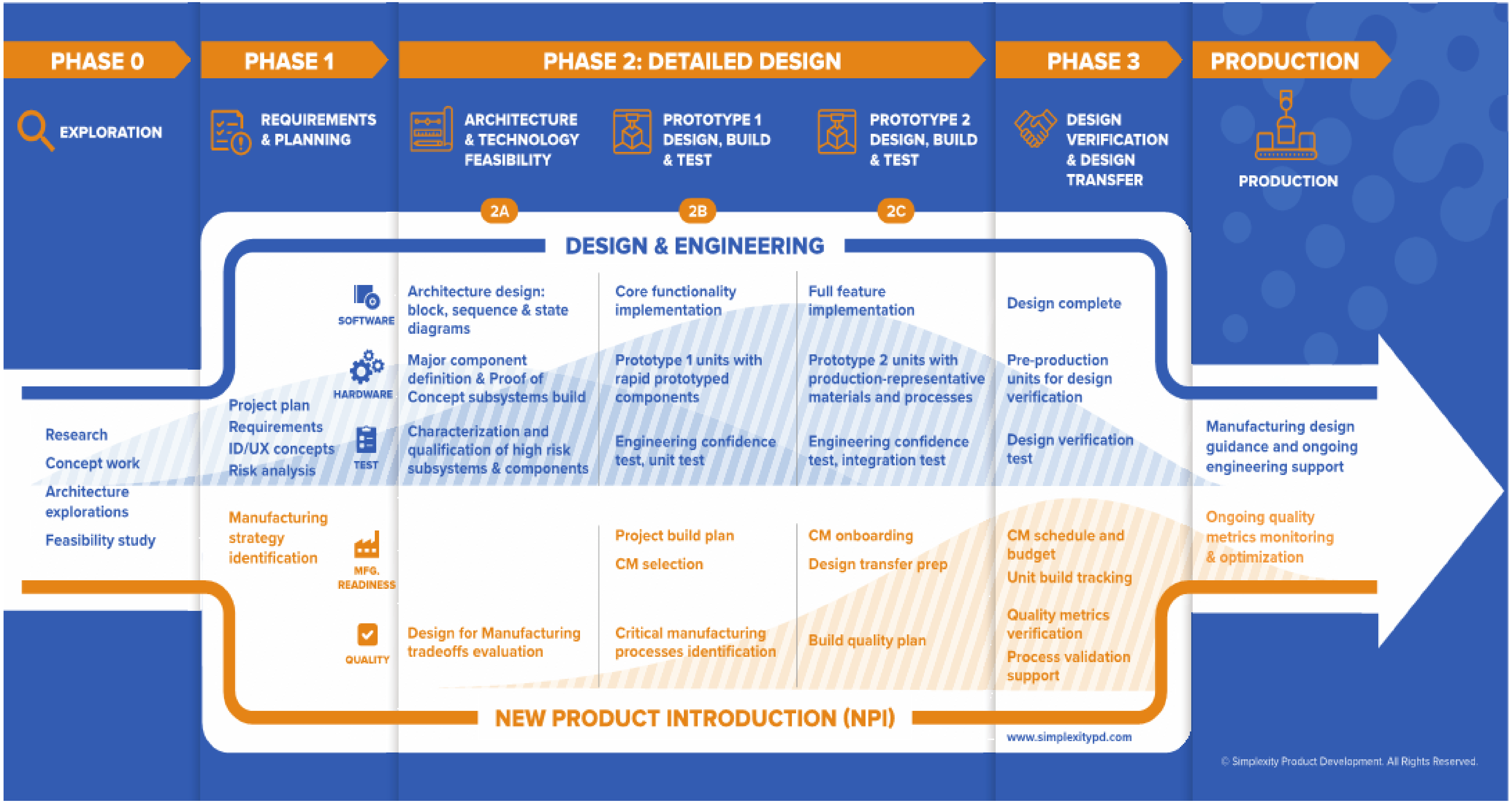
- Software the largest driver of medical device recalls
- Increased complexity of devices and software



© Statista 2020

PRODUCT DEVELOPMENT PHASES

Simplexity®
PRODUCT DEVELOPMENT



PHASE 0
EXPLORATION

PHASE 1
REQUIREMENTS & PLANNING

PHASE 2: DETAILED DESIGN
2A ARCHITECTURE & TECHNOLOGY FEASIBILITY
2B PROTOTYPE 1 DESIGN, BUILD & TEST
2C PROTOTYPE 2 DESIGN, BUILD & TEST

PHASE 3
DESIGN VERIFICATION & DESIGN TRANSFER

PRODUCTION
PRODUCTION

DESIGN & ENGINEERING

Phase 0:
- Research
- Concept work
- Architecture explorations
- Feasibility study

Phase 1:
- Project plan
- Requirements
- ID/UX concepts
- Risk analysis
- Manufacturing strategy identification

SOFTWARE
HARDWARE
TEST
MFG. READINESS
QUALITY

2A:
- Architecture design: block, sequence & state diagrams
- Major component definition & Proof of Concept subsystems build
- Characterization and qualification of high risk subsystems & components
- Design for Manufacturing tradeoffs evaluation

2B:
- Core functionality implementation
- Prototype 1 units with rapid prototyped components
- Engineering confidence test, unit test
- Project build plan
- CM selection
- Critical manufacturing processes identification

2C:
- Full feature implementation
- Prototype 2 units with production-representative materials and processes
- Engineering confidence test, integration test
- CM onboarding
- Design transfer prep
- Build quality plan

Phase 3:
- Design complete
- Pre-production units for design verification
- Design verification test
- CM schedule and budget
- Unit build tracking
- Quality metrics verification
- Process validation support

Production:
- Manufacturing design guidance and ongoing engineering support
- Ongoing quality metrics monitoring & optimization

NEW PRODUCT INTRODUCTION (NPI)

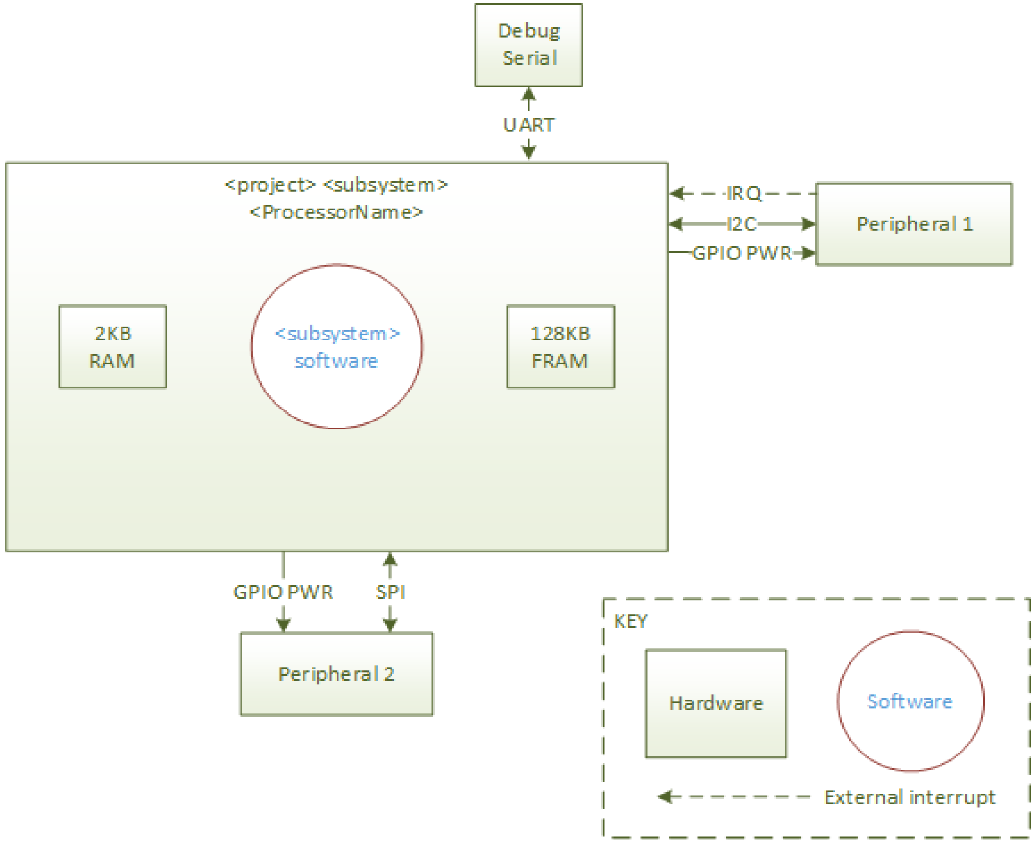
www.simplexitypd.com

PHASE 1: REQUIREMENTS AND PLANNING

- Project Development Plan
- Software Development Plan
  - Determine software development life-cycle model – Agile? Waterfall? Incremental?
  - Identify milestones and associated features
- Product Requirements Document
- Software Requirements Specification
  - Functions and capabilities
  - Security
  - Usability
  - Risk control measures

PHASE 2A: ARCHITECTURE & FEASIBILITY

- Map requirements to high-level architectural description of SW
  - Describe interfaces between software and internal/external components
- IEC 62304 terms
  - **Software System** – top level, composed of 1 or more SW items
  - **Software Item** – any identifiable part of a program, composed of 1 or more units
  - **Software Unit** – the lowest level that is not decomposed
- Perform initial SW Risk Analysis



DEVICE CLASSIFICATION

Simplexity® PRODUCT DEVELOPMENT

FDA devices

- **Class I** – lowest risk
  - Adhesive bandages, IV stand, glasses
- **Class II** – moderate risk
  - Syringes, surgical masks, powered wheelchair
- **Class III** – highest risk
  - Heart valves, implantable neuromuscular stimulator, breast implants

ISO 13485 devices

- **Class I** – lowest risk
  - Eyeglasses, stethoscopes, crutches
- **Class IIa** – low to medium risk
  - Syringes, surgical gloves, hearing aids, diagnostic ultrasound
- **Class IIb** – medium to high risk
  - Surgical lasers, defibrillators
- **Class III** – highest risk
  - Cardiovascular catheters, hip-joint implants, prosthetic heart valves

SOFTWARE SAFETY CLASSIFICATION

FDA software levels of concern

- **Minor**: failures unlikely to cause injury to patient or operator
- **Moderate**: failures could directly result in minor injury to patient or operator
- **Major**: failures could directly result in death or serious injury to patient or operator

IEC 62304 Software Safety Classification

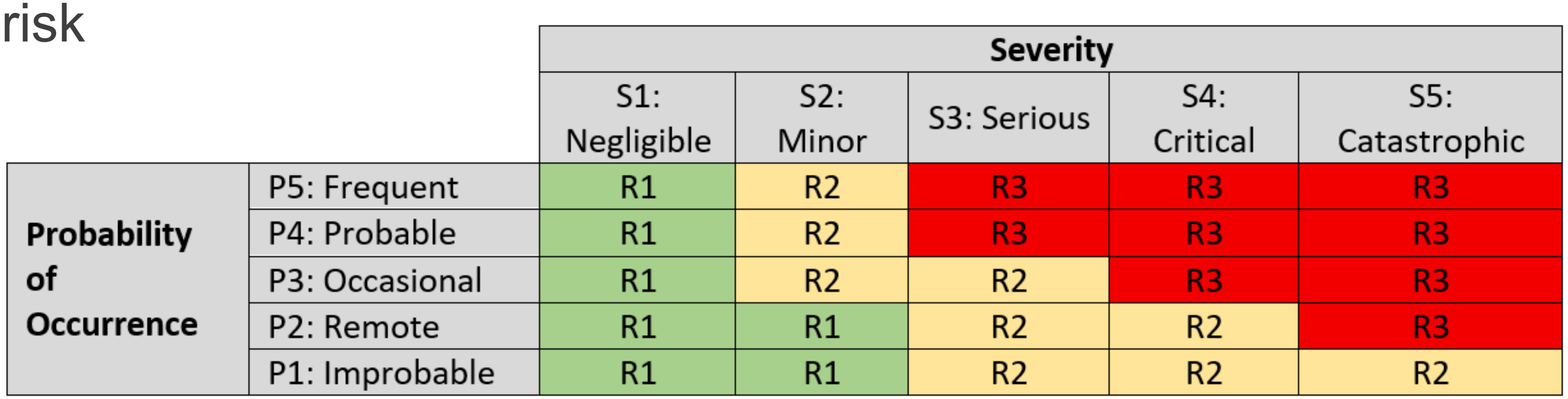
- **Class A**: SW can't contribute to hazardous situation causing harm
- **Class B**: SW can contribute to hazardous situation and resulting harm is non-serious injury
- **Class C**: SW can contribute to hazardous situation and resulting harm is death or serious injury

RISK ANALYSIS

- **Risk = combination of probability of occurrence and severity of harm**

- Hazard analysis – top-down approach
  - Required by ISO 14971 and the FDA
  - Identify hazards (sources of harm)
  - Define hazardous situations and associated harm
  - Estimate risk

- Failure Modes and Effects Analysis (FMEA) – bottom-up approach
  - Identify failure modes
  - List effects of each failure
  - Estimate risk



		Severity				
		S1: Negligible	S2: Minor	S3: Serious	S4: Critical	S5: Catastrophic
Probability of Occurrence	P5: Frequent	R1	R2	R3	R3	R3
	P4: Probable	R1	R2	R3	R3	R3
	P3: Occasional	R1	R2	R2	R3	R3
	P2: Remote	R1	R1	R2	R2	R3
	P1: Improbable	R1	R1	R2	R2	R2

- Use Risk Controls to reduce risk

SW RISK ANALYSIS AND MITIGATION

- Identify **software items** that could contribute to a hazardous situation
- Identify causes of those items contributing to a hazardous situation

- Risk Controls
  - For each case where a SW item contributes to a hazardous situation define a risk control measure (mitigations)
  - Risk control measures can be implemented in
    - hardware
    - software
    - working environment
    - user instruction
  - If the risk control measure is in software, ***add it to the software requirements specification***

PHASE 2B/2C: DETAILED DESIGN

Detailed design

- Flesh out details of architecture – divide items identified in the architecture into SW units with enough detail to allow implementation to proceed
- **Design reviews before implementation**

Unit implementation and testing

- Actual coding! Convert designs to source code and runnable binaries for test
- Always utilize source code control
- **Code reviews before integration**

Software Integration and testing

- Integrate SW units into progressively larger subsystems and test them

Feature complete by end of phase

PHASE 3: VERIFICATION AND TRANSFER

Release candidate software build

- Prepare candidate release for formal software verification
- Include release notes with known issues and fixed defects

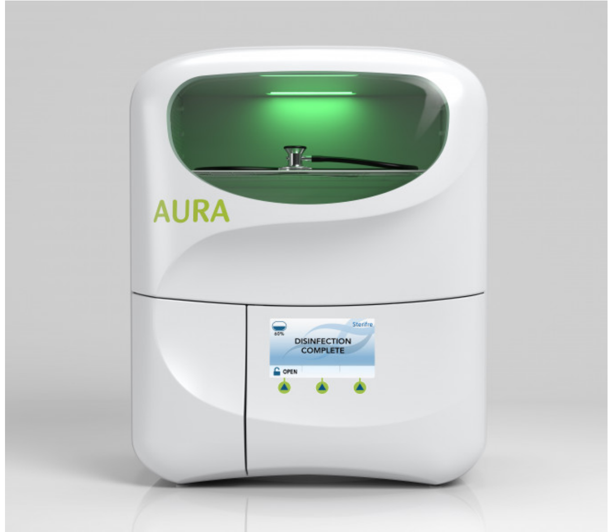
Release software verification protocols

- Software Verification Testing
  - System-level testing of the software/firmware
  - Formal testing done by independent testers (NOT the engineers who wrote the code)
  - Any bugs found logged in issue tracking system
  - Performed along with system design verification testing

CASE STUDY: Sterifre MEDICAL

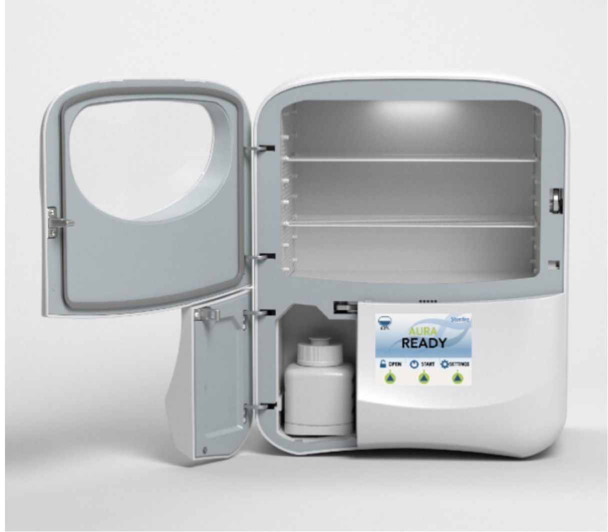
THE PRODUCT: AURA

- Initial target market: hospitals, clinics, long term care
- Patented core technology. The first automated point-of-care disinfection system, replacing the use of disinfectant wipes and sprays
- Broad material compatibility with broad-spectrum efficacy and zero chemical residue, no environmental impact, eliminates employee chemical exposure
- Plug-and-play set-up offers a fast and flexible, no installation required comprehensive turnkey solution



SIMPLEXITY'S ROLE

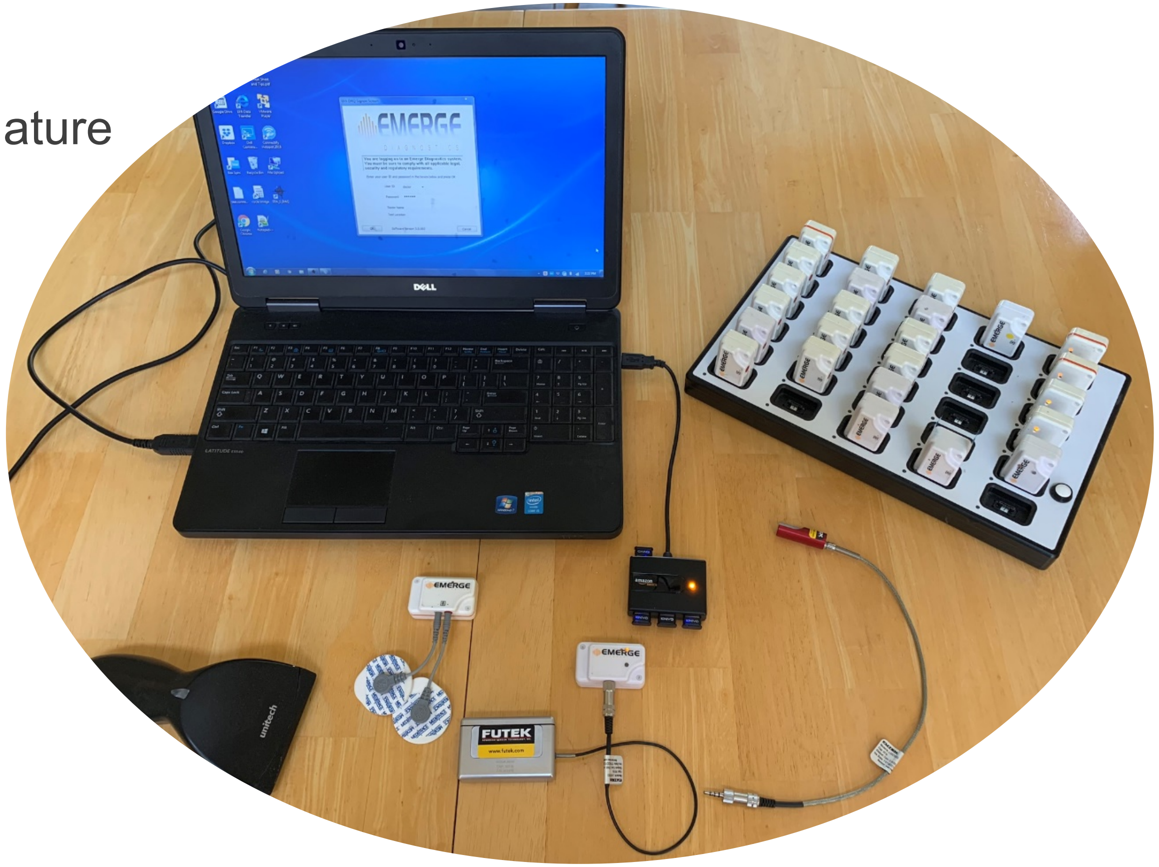
- Redesigning AURA for simplicity, improved reliability, scaled manufacturing cost reduction, noise reduction, and reduced product weight
- This will be an EPA registered product
- Full product design, prototyping, manufacturing support, & production ramp
- Embedded firmware, electrical, mechanical, systems, and quality engineering, supported by dedicated project managers and a New Product Introduction (NPI) team



CASE STUDY: EMERGE DIAGNOSTICS

THE PRODUCT

- The Electrodiagnostic Functional Assessment (EFA) Test objectively diagnoses and identifies the location, extent, nature and age of soft tissue injuries, including
  - Range of motion
  - Functional assessment
  - Pinch strength
  - Grip strength
  - Electromyography (EMG)



SIMPLEXITY'S ROLE

- Assist with development of the sensors and charger, including mechanical, electrical, firmware, and quality engineering
- Assist with providing process documentation such as the development plan, requirements specifications, architecture description, hazard analysis, FMEA, design and code reviews

BEST PRACTICES

1. Use a phase-gate development process – create a project plan, define requirements, develop the architecture, detailed design and implementation, verify and validate
2. Design your specifications so that they are easily tested for verification and validation, but still cover all safety aspects
3. Perform Software Risk Analysis along with Hazards Analysis during the architecture phase and identify software risk controls
4. Use design and code reviews to enforce company or industry design and coding standards
5. Test early and often - automate unit and integration testing as much as possible

THANK YOU FOR ATTENDING!

Katie Elliott & Dorota Shortell

Simplexity Product Development

SimplexityPD.com

info@simplexitypd.com

Sources:

- Sterifre Medical
- Emerge Diagnostics
- Toyota Article
- Quarterly Medical Device Recalls Graph
- Medical Device Recalls