Mr. Clark Fortney
Senior Software Engineer

Medical Device Safety in a Connected World

IoT Expo June 6-8 2017

BATTELLE

Clark Fortney

My Background

- 20 years designing systems & software for medical devices at Battelle.
- Practitioner of cybersecurity principles, not a cyber expert.

Goal and Approach

Share strategies and techniques for developing connected embedded systems while reducing vulnerability to cybersecurity threats.

Present techniques in medical development framework that are generally applicable to any embedded product.

About Battelle

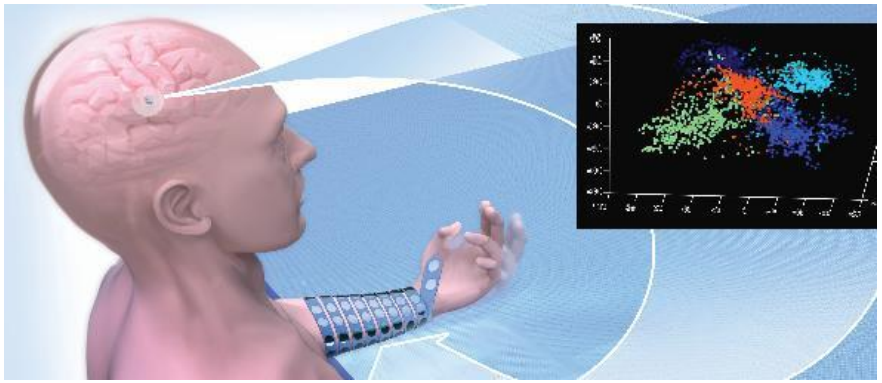
- Global R&D enterprise located in *Columbus, OH*
- *Non-profit, charitable trust* formed in 1929 by the Will of Gordon Battelle to *provide contract R&D for the betterment of the world*
- More than *20,000 employees* in over *100 world-wide locations*
- Serving customers across Consumer, Industrial & Medical; Energy & Environment; National Security and Laboratory Management
- Net income invested in science & technology, education and charity

BATTELLE

Contract Research: Health

Battelle develops advances that benefit patients, providers and payers to ensure better outcomes.

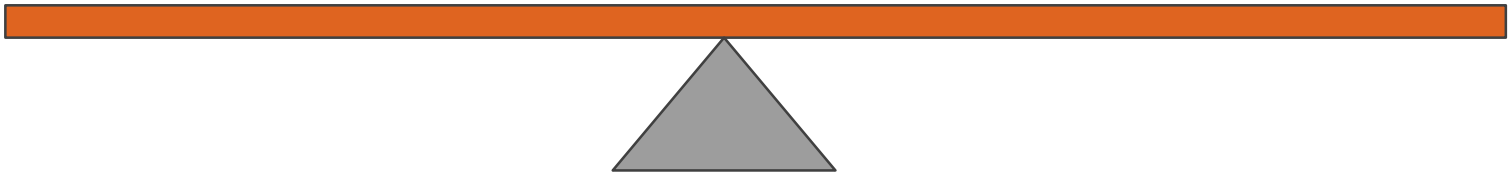
- Healthcare analytics
- Regulatory, toxicology and behavioral studies
- Medical device technologies



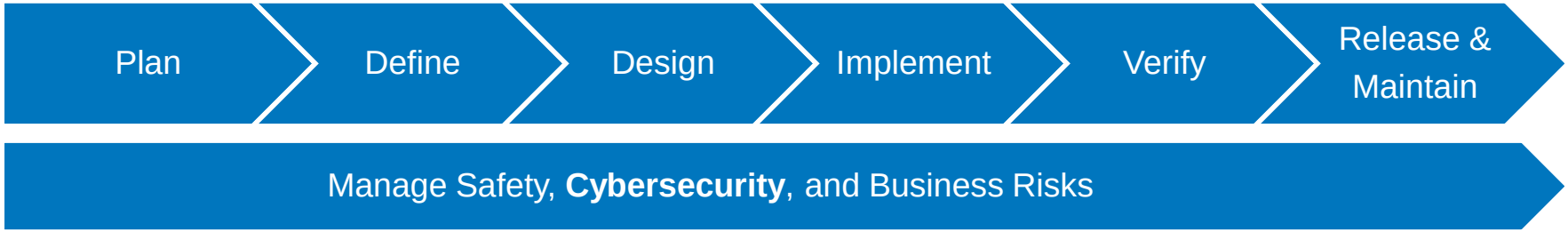
Benefits of Connected Medical Devices vs. Cybersecurity & Safety *Challenges*

- Help patients manage their treatments
- Check that meds are taken regularly
- Monitor vital signs or device performance
- Better outcomes from improved communications

- Growing expectation that every gadget is connected
- Marketing vs really beneficial
- Deciding when user benefits of connecting outweigh risks
- Designing devices to withstand cyber threats during product life



Address Cybersecurity Risks *Throughout* Product Lifecycle



- Most cyber weaknesses in a system are the *result of poor design choice*, not implementation bugs.
- Making secure design choices *up front is critical*.
- Add a *cybersecurity engineer* to your team and involve them at each stage of the development process.
- Cybersecurity risk management should *integrate* with your company's *overall risk management plan*.

BATTELLE

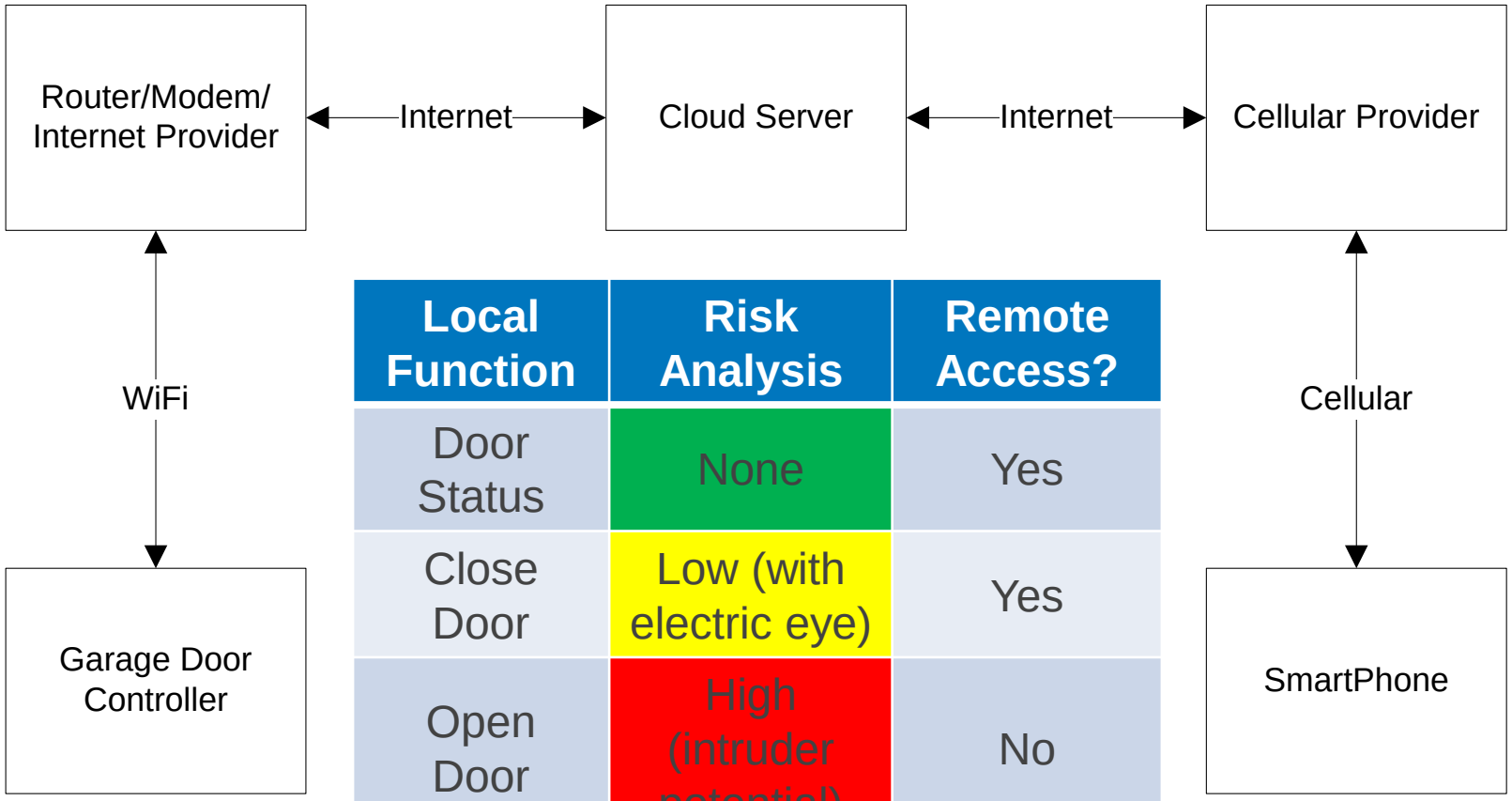
Plan for Cybersecurity

- Learn from cybersecurity engineers and incorporate learnings into development by all engineers.
- Establish cybersecurity checkpoints and integrate them throughout development process.
- Good reference materials from National Institute of Standards (NIST)
  - https://www.nist.gov/topics/cybersecurity
  - https://www.nist.gov/cyberframework

Analyze Cybersecurity Threats During Requirement & Architecture Definition

- Analyze potential threats during requirements definition.
  - Weigh risks vs. benefits.
  - Don’t give remote control over critical functions.
- Review system and software architecture against cybersecurity best practices.
- Conduct Cyber Threat Assessment, *then*:
- Refine architecture or add risk controls to reduce risks to acceptable level.

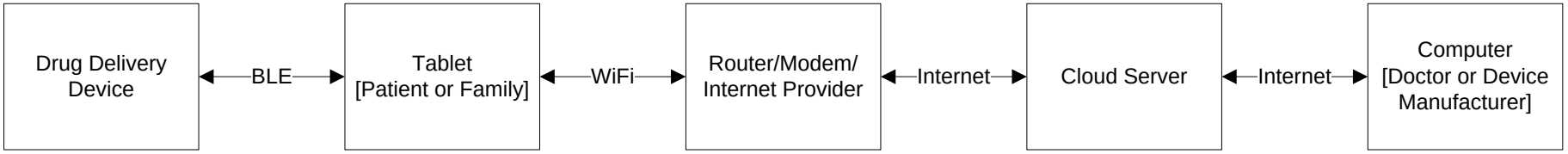
Remote Functions vs. Risk for Smartphone Enabled Garage Door



Local Function	Risk Analysis	Remote Access?
Door Status	None	Yes
Close Door	Low (with electric eye)	Yes
Open Door	High (intruder potential)	No

BATTELLE

Remote Functions vs. Risk for Connected Drug Delivery Device



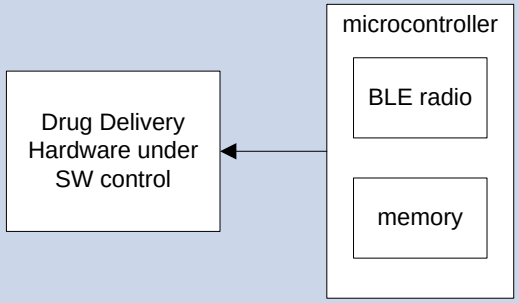
Local Function	Risk Analysis	Remote Access?
Next dose reminder	None	Yes
Read dose history	Low (privacy*)	Yes (encrypt)
Set drug delivery rate	High (over/under dose)	No
Set dose volume	High (over/under dose)	No
Start/stop drug delivery	High (over/under dose)	No

*Since BLE (Bluetooth Low Energy) is short range, it may be possible to associate the data with an individual even if the data sent doesn't contain personal identity information.

BATTELLE

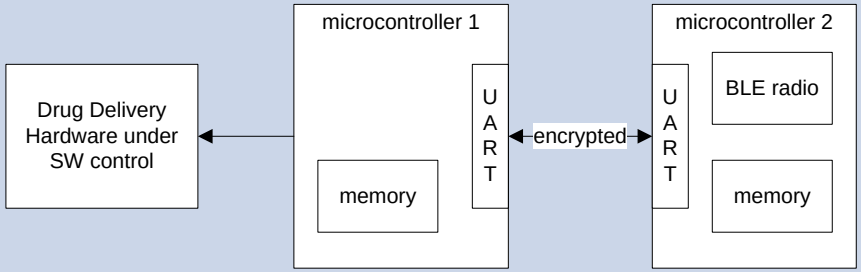
System Architecture Changed to Reduce Susceptibility to BLE Attack

Original Design



- Hack on BLE could corrupt memory and compromise proper drug delivery.
- Heavy load on BLE could effectively result in denial drug delivery service.
- Most BLE chips use ARM Cortex M0, which don't have Memory Protection Unit (MPU).
- Some newer radios have MPU, which may enable safer single chip solution.

More Secure Design



- BLE functionality provided in 2nd micro prevents BLE hack from impacting drug delivery control.
- Micro 1 can shut off UART during critical operations to prevent denial of service.
- Encrypt communications between micros.
- Application level encryption layered on top of standard BLE OTA encryption for extra protection.

BATTELLE

Incorporate Design Elements to Enhance Cybersecurity

- Take advantage of built-in security features (FLASH protection; disable JTAG).
- Use application level encryption for vulnerable communications inside device and outside.
- Incorporate runtime checks on program and data integrity.
- Review system and software design against cybersecurity best practices.

Search for Known Vulnerabilities in 3rd Party Hardware & Software components

- Search National Vulnerability Database (https://nvd.nist.gov/) for known vulnerabilities of 3rd party software components
- Review manufacturer errata reports for hardware components
- Evaluate risks associated with known issues for hardware and software components.
  - Add risk controls to reduce risks to acceptable level, or find better component.

Perform Software Coding Checks

- Review software modules against general coding checklists and cybersecurity coding best practices.
- Run static analysis tools on code.
- Test for memory leaks.
- Perform rigorous and challenging software unit testing.

Conduct Cyber Vulnerability Assessment & Testing

- Conduct fuzz testing of interfaces (e.g. BLE, USB) and resolve vulnerabilities discovered.
- Conduct cyber penetration testing of product.
- Perform Vulnerability Assessment and add risk controls to reduce risks to acceptable level.

Implement post release threat monitoring & firmware security updates

- After product release, periodically:
  - Check for new 3rd party component vulnerabilities.
  - Revisit product vulnerability assessment considering advancements in threat capabilities.
- Develop and verify firmware updates to resolve bugs and to address newly found vulnerabilities.
- Provide means to securely update firmware, possibly in field if overall risk profile can be maintained.

Address Cybersecurity Risks *Throughout* Product Lifecycle

- Incorporate cybersecurity at *each stage of development*, and post product release.
- Include a *cybersecurity engineer* on the product team.
- Ensure that exposed external interfaces and product functions are *worth the effort* required to provide them without compromising safety or privacy.

The Internet of *Great* Things,

not

the Internet of *Dangerous* Things

BATTELLE

It can be done

800.201.2011 | solutions@battelle.org | www.battelle.org