ENGINEERING HIGH-PERFORMANCE MEDICAL ROBOTICS SOLUTIONS

Technical Risk Considerations & How to Mitigate

September 19, 2023

PRESENTERS

Tom Amlicke
Technical Director
Robotics Practice

MEDACUITY

Michael Chalupa
Principal Field Application Engineer

BlackBerry | QNX

Hasnat Ashiq
Regional Field Application Engineer Manager

rti

PRESENTED BY

MEDACUITY

BlackBerry | QNX

rti

Technical Risk Considerations & How to Mitigate

PRESENTED BY

MEDACUITY

BlackBerry QNX

rti

TECHNICAL RISK MANAGEMENT
TOP THREE CONSIDERATIONS

1

SAFETY | RELIABILITY | PERFORMANCE
Are you reducing your development risks by building with functional safety?

2

SECURITY RISK MANAGEMENT
How are real-world examples shaping effective risk management strategies?

3

DATA CONNECTIVITY
How can you design for interoperable and scalable data flow while ensuring reliable and secure communications?
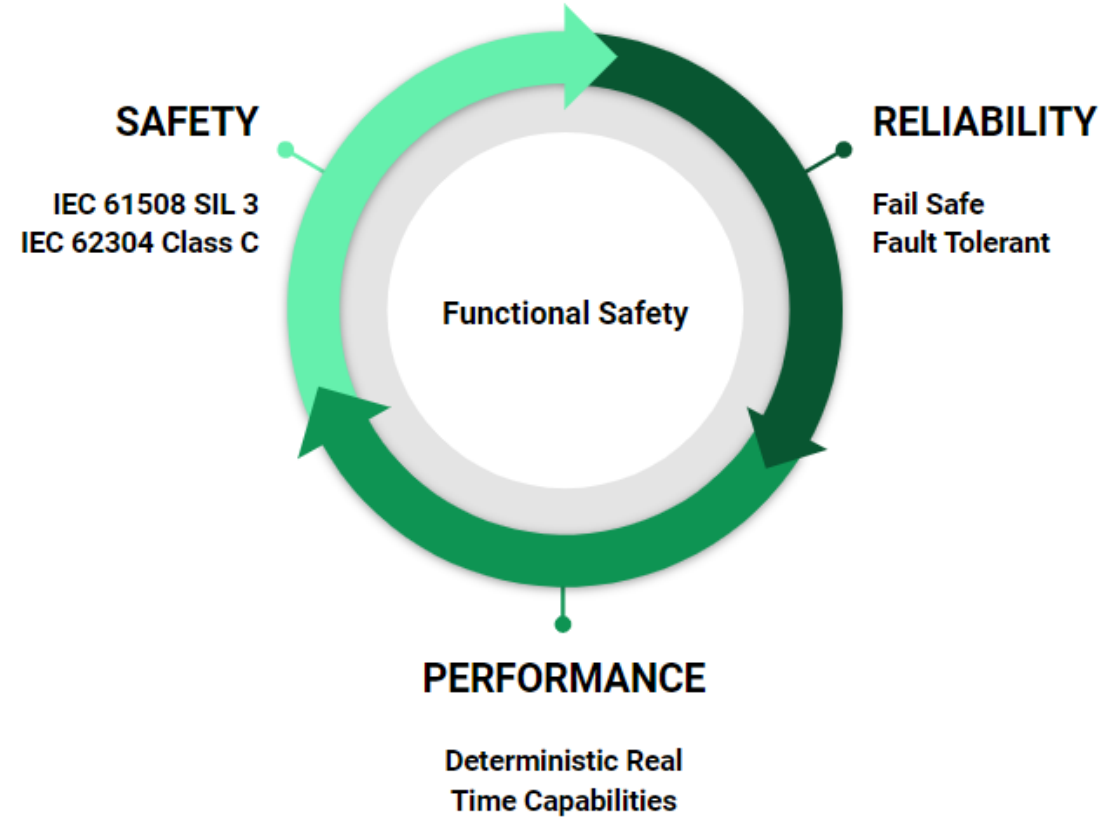
1 | SAFETY | RELIABILITY | PERFORMANCE

Are you reducing your development risks by building with functional safety?

Technical Risk Considerations & How to Mitigate

BUILDING WITH FUNCTIONAL SAFETY

Manage your development lifecycle by building with functional safety from the get-go.

SAFETY

IEC 61508 SIL 3
IEC 62304 Class C

Functional Safety

RELIABILITY

Fail Safe
Fault Tolerant

PERFORMANCE

Deterministic Real
Time Capabilities

PRESENTED BY

MEDACUITY

BlackBerry QNX

rti

SAFETY | RELIABILITY | PERFORMANCE
FUNCTIONAL SAFETY FOR SURGICAL ROBOTICS

❑ Advanced surgical robotic systems to be certified to IEC 62304 Class C as it has a higher level of criticality and risk if it malfunctions, potentially causing harm to patients or users.

❑ In practical terms, building software with functional safety for this standard typically involves:
  ▪ Risk analysis
  ▪ Meeting safety requirements
  ▪ Validation and verification
 ▪ Traceability
  ▪ Documentation

SAFETY | RELIABILITY | PERFORMANCE

PATH OF LEASE RESISTANCE: GO-TO-MARKET

- ❑ Building on the right products and platforms starts with knowing which ecosystem partners are best suited for your needs from the beginning.

- ❑ **Production-ready** COTS reduces time needed to conduct your testing, validation, and documentation.

- ❑ Invest in comprehensive technical risk management processes.

- ❑ Developing with modular design.

SAFETY | RELIABILITY | PERFORMANCE
RELIABLE REAL-TIME SYSYTEM ARCHITECTURE
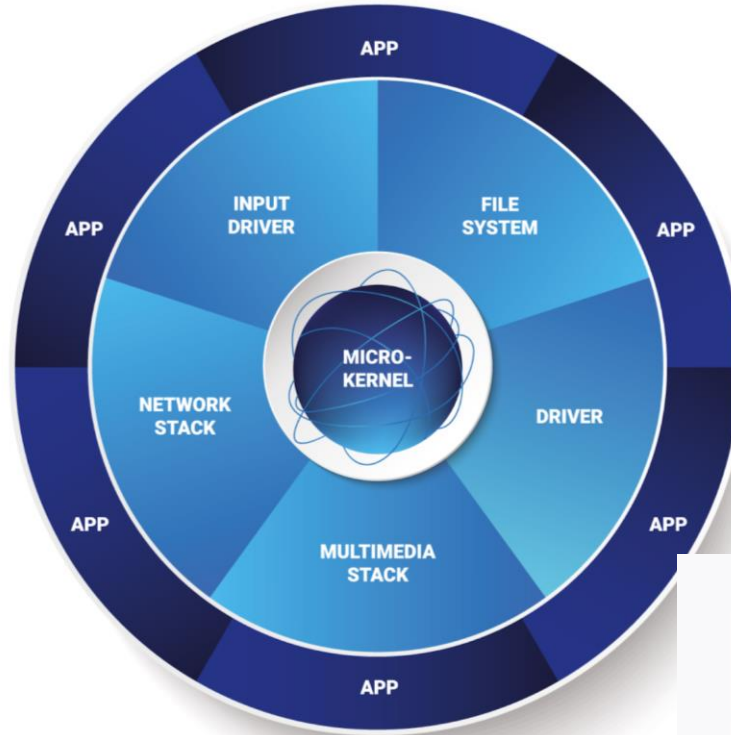
- ❑ Safe Reliable Fail-Safe Systems
- ❑ Performant Deterministic Real-Time Application: Low Latency
- ❑ Secure by Design
  - ▪ There's no safety without security!

2 | SECURITY RISK MANAGEMENT

How are real-world examples shaping effective risk management strategies?

Technical Risk Considerations & How to Mitigate

PRESENTED BY

MEDACUITY

BlackBerry QNX

rti

SECURITY RISK MANAGEMENT
WHY SHOULD I CARE?

Beyond FDA legislation (21 CFR820.30(g)) and Guidance

COST
- ❑ Intra-Organizational Inefficiencies from the Wrong Approach to Cybersecurity
- ❑ Fees and Fines Due resulting from Data Breaches or Adverse Patient Events
- ❑ Opportunity Cost if a Product Misses a Critical Schedule Milestone
- ❑ SLA and Contractual Losses due to Missed Contract Stipulations

HARM
- ❑ Patient Injury/Death due to Ineffective Cyber Controls and Practices
- ❑ Damage to Business Reputation as Events are Publicized
- ❑ Risk of Introducing Vulnerabilities to Connected Customer Systems
- ❑ Negligence Could Lead to Potential Personal Liability for Executives

SECURITY RISK MANAGEMENT
REAL WORLD EXAMPLES

- ❑ Large hospital system refuses to approve an installation of a medical device due to weak MDS2* documentation and lack of mature cybersecurity risk management.
- ❑ Mature infusion pump incorporates changes requiring a 510(k) that results in an emergency security risk assessment.
- ❑ A security risk assessment reveals serious medical device vulnerabilities with:
  - WiFi
  - Bluetooth
  - Unprotected Kiosk
  - Unprotected access to PHI and PII
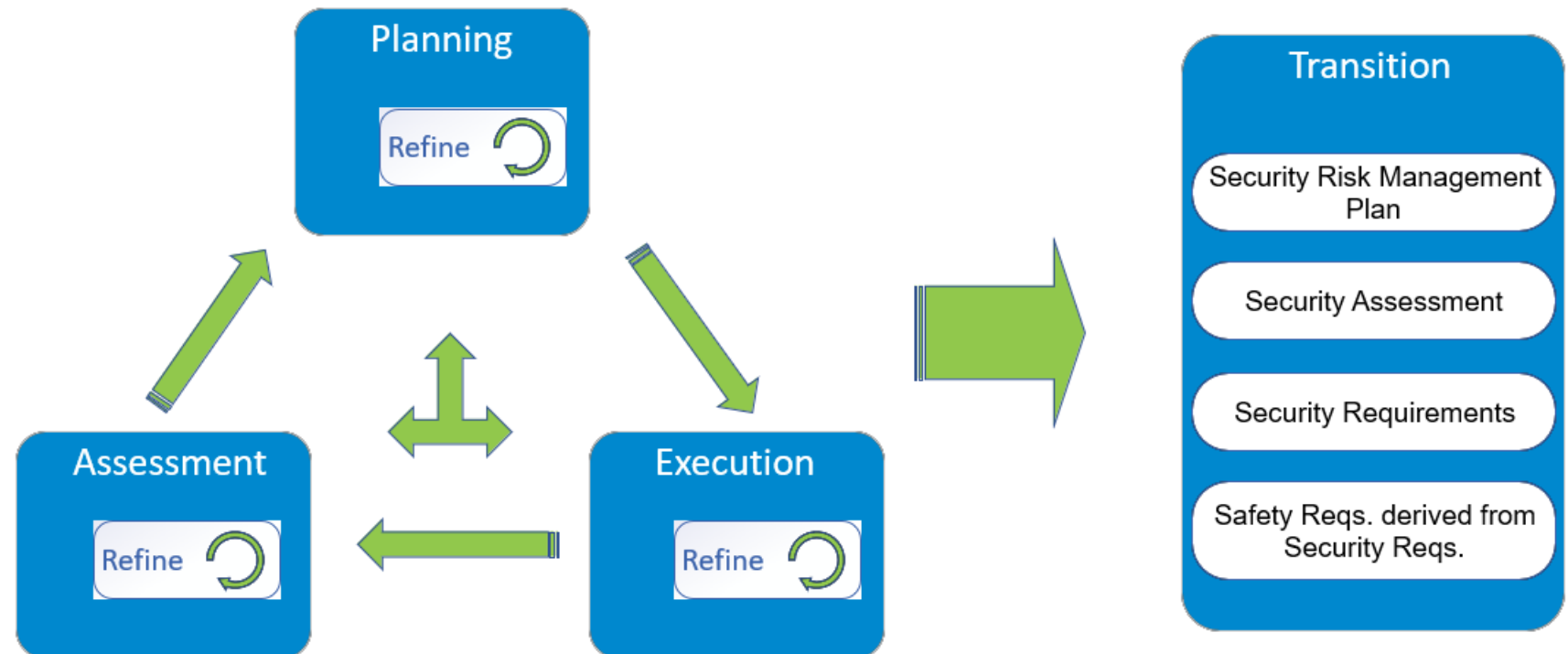
* Manufacturer Disclosure Statement for Medical Device Security

SECURITY RISK MANAGEMENT
APPROACH: SECURITY RISK MANAGEMENT

Ongoing Iterative Process

- Assessment
- Planning
- Execution
- Ongoing Evaluation
- Transition

OUTPUT: SAMPLE RISK ASSESSMENT

Exploit ID (Life Cycle-Index)	Threat ID	Threat Event	Vulnerability ID	Vulnerability	Assets	Impact Description	Safety Impact (Risk ID or N/A)	CVSS v3.1 Base Score	Security Risk Level	Security Risk Controls (Requirements)	Modified CVSS v3.1 Base Score	Modified Security Risk Level	Residual Security Risk Acceptability Justificat
						Threat Model Exploits		**Scoring before Security Controls Applied**		**Mitigations**	**Scoring with Security Risk Controls in place**		
LC1-001	THR-0004	With physical access, a threat actor can tamper with/install software and/or malware	VLN-0012	Unsigned firmware leads to undetectable tampering	AST-0108 - Application & Firmware Image AST-1001 - MCU Firmware INF-0114 - Internal Hard Drive INF-1004 - MCU Debug Interface	Installation of alterred firmware leads to availability issues resulting in delay of therapy. This can also lead to integrity issues resulting in incorrect therapy/potential patient harm.	<ID or N/A>	6.1	Medium	MIT-0030 - System performs a power on self-test (POST) MIT-0038 - Access to site and functional locations is badge controlled. MIT-0053 - Digital Signatures	2.9	Low	
LC1-002	THR-0004	With physical access, a threat actor can tamper with/install software and/or malware	VLN-0011	Unsigned software leads to undetectable tampering	AST-0107 - OS and Drivers AST-0110 - COTS Components INF-0111 - Service KB INF-0114 - Internal Hard Drive INF-0117 - Operator Display	Installation of alterred OS, drivers, and/or application software leads to availability issues resulting in delay of therapy. This can also lead to integrity issues resulting in incorrect therapy/potential patient harm. Incorrect OS and/or drivers can lead to future information disclosure.	<ID or N/A>	8.4	High	MIT-0030 - System performs a power on self-test (POST) MIT-0038 - Access to site and functional locations is badge controlled. MIT-0053 - Digital Signatures	3.9	Low	
LC1-003	THR-0007	A threat actor loads valid firmware on the wrong processor	VLN-0050	Lack of firmware signatures/identifying marks prevents firmware from being associated with a specific processing element	AST-1001 - MCU Firmware INF-1004 - MCU Debug Interface	Installation of incorrect firmware leads to availability issues resulting in delay of therapy. This can also lead to integrity issues resulting in incorrect therapy/potential patient harm.	<ID or N/A>	7.7	High	MIT-0030 - System performs a power on self-test (POST) MIT-0045 - Encrypted and signed system manifest MIT-0053 - Digital Signatures	3.9	Low	
LC1-004	THR-0009	A threat actor tampers with material obtained from suppliers prior to them being received	VLN-0012	Unsigned firmware leads to undetectable tampering	AST-0101 - Computer BIOS AST-0110 - COTS Components	Installation of software/firmware items that have been tampered with leads to confidentiality, safety, integrity, and possibly availability issues.	<ID or N/A>	6.8	Medium	MIT-0024 - Software / firmware integrity value is provided to the supplier/CM for verification of file integrity. MIT-0053 - Digital Signatures MIT-0055 - Supplier Qualification	2.3	Low	
					AST-0103 - Drive encryption keys AST-0104 - X509 Certs/Private Keys								

Template Header | Header | Life Cycle | Trust Zones | Assets | Interfaces | Threats | Vulnerabilities | Mitigations | Security Risk Assesment | Assessment Report | Threat Sources | CVSS 3.1 Metrics

**Technical Risk
Considerations &
How to Mitigate**

SECURITY RISK MANAGEMENT
DEMO CYBERSECURITY
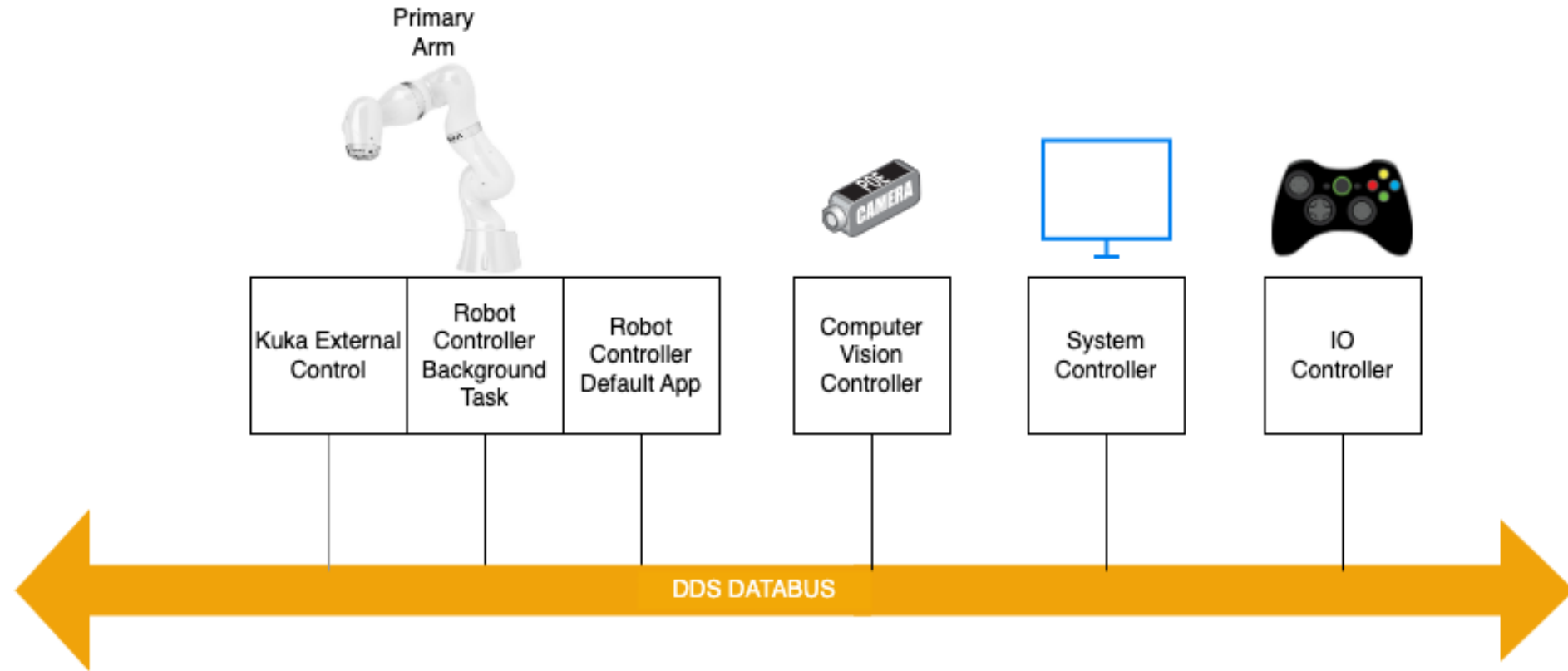
3 | DATA CONNECTIVITY

How can you design for interoperable and scalable data flow while ensuring reliable and secure communications?

INTEGRATED TECHNOLOGIES POWERING THE FUTURE OF SURGICAL ROBOTICS

ENGINEERING HIGH-PERFORMANCE MEDICAL ROBOTICS SOLUTIONS

Technical Risk Considerations & How to Mitigate

PRESENTED BY

MEDACUITY
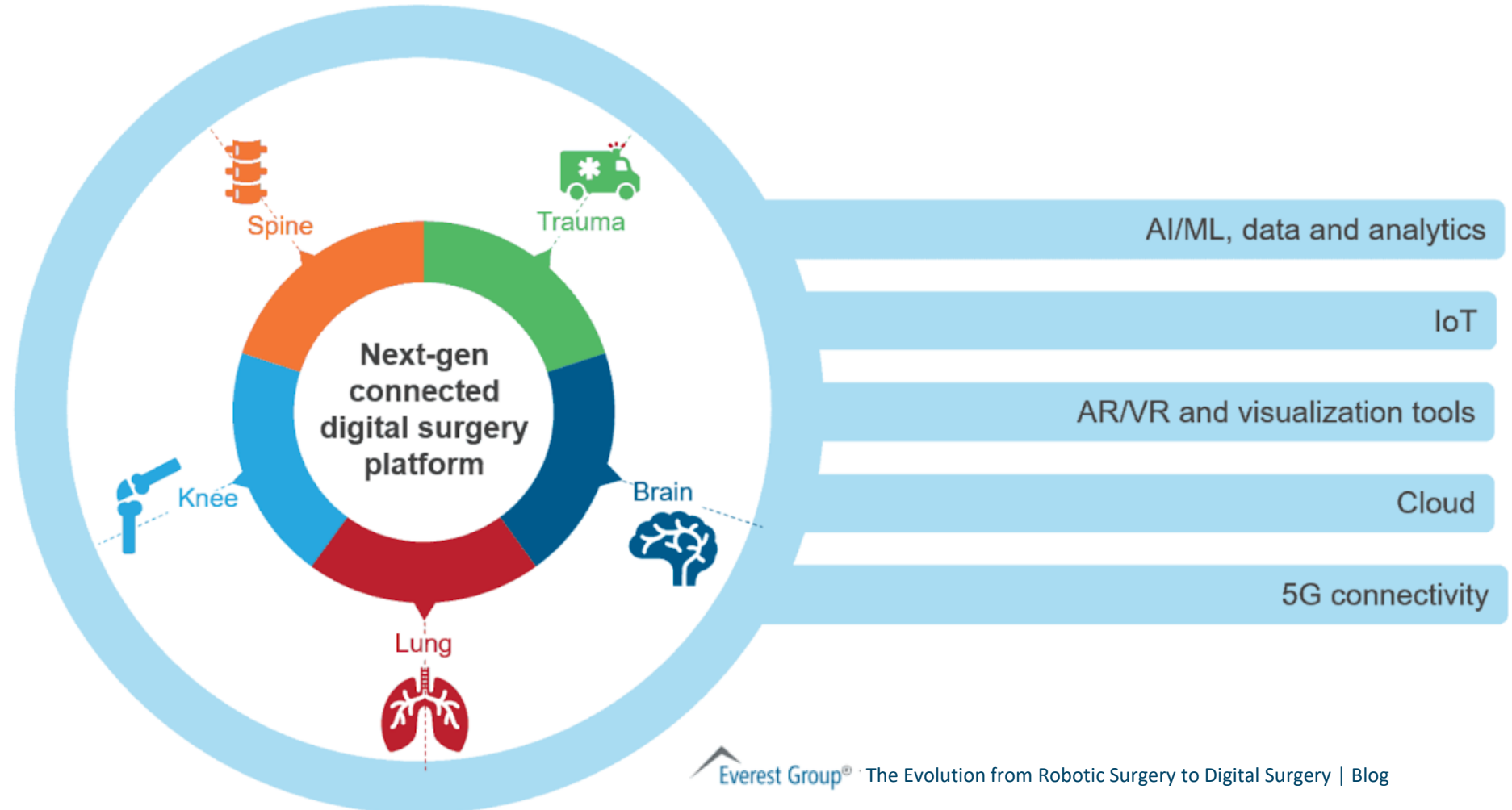
BlackBerry | QNX

rti

- Spine
- Trauma
- Knee
- Next-gen connected digital surgery platform
- Brain
- Lung

- AI/ML, data and analytics
- IoT
- AR/VR and visualization tools
- Cloud
- 5G connectivity

Everest Group® · The Evolution from Robotic Surgery to Digital Surgery | Blog

ENGINEERING HIGH-PERFORMANCE MEDICAL ROBOTICS SOLUTIONS

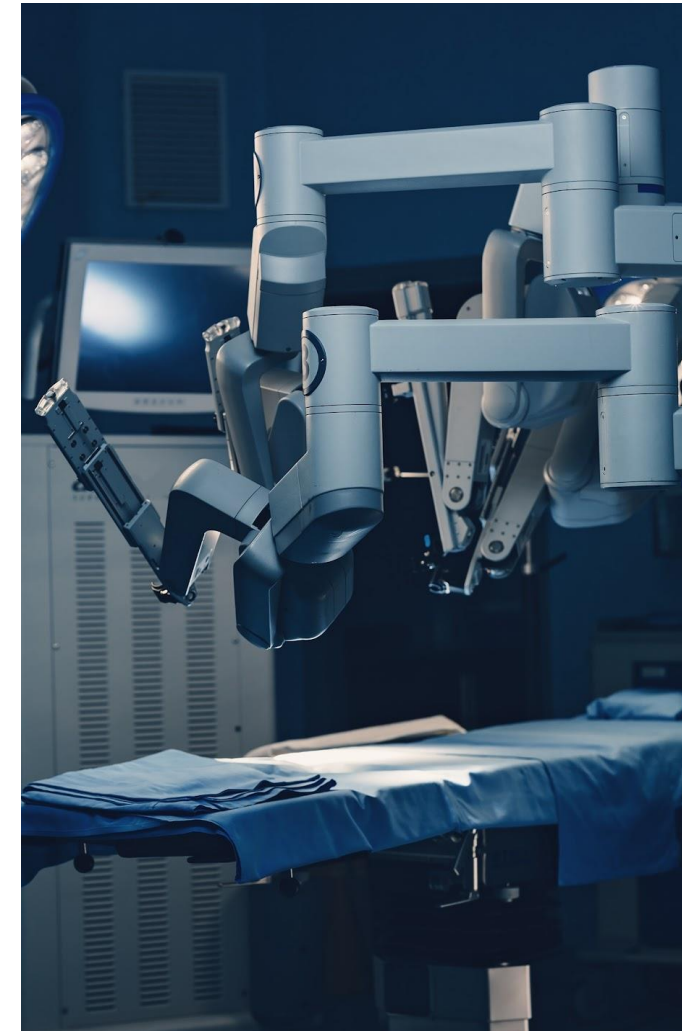**Technical Risk Considerations & How to Mitigate**

PRESENTED BY

MEDACUITY

BlackBerry | QNX

rti

DATA CONNECTIVITY

SURGICAL ROBOTICS: CONNECTIVITY REQUIREMENTS

- Flexible interoperability (instruments, devices, video, data)

- Reliable, real-time performance across distributed system

- Secure communications

- Platform for real-time intelligence / guidance

ENGINEERING HIGH-PERFORMANCE MEDICAL ROBOTICS SOLUTIONS

Technical Risk Considerations & How to Mitigate

PRESENTED BY

MEDACUITY

BlackBerry | QNX

rti

DESIGN CHALLENGES IN DISTRIBUTED CONNECTIVITY
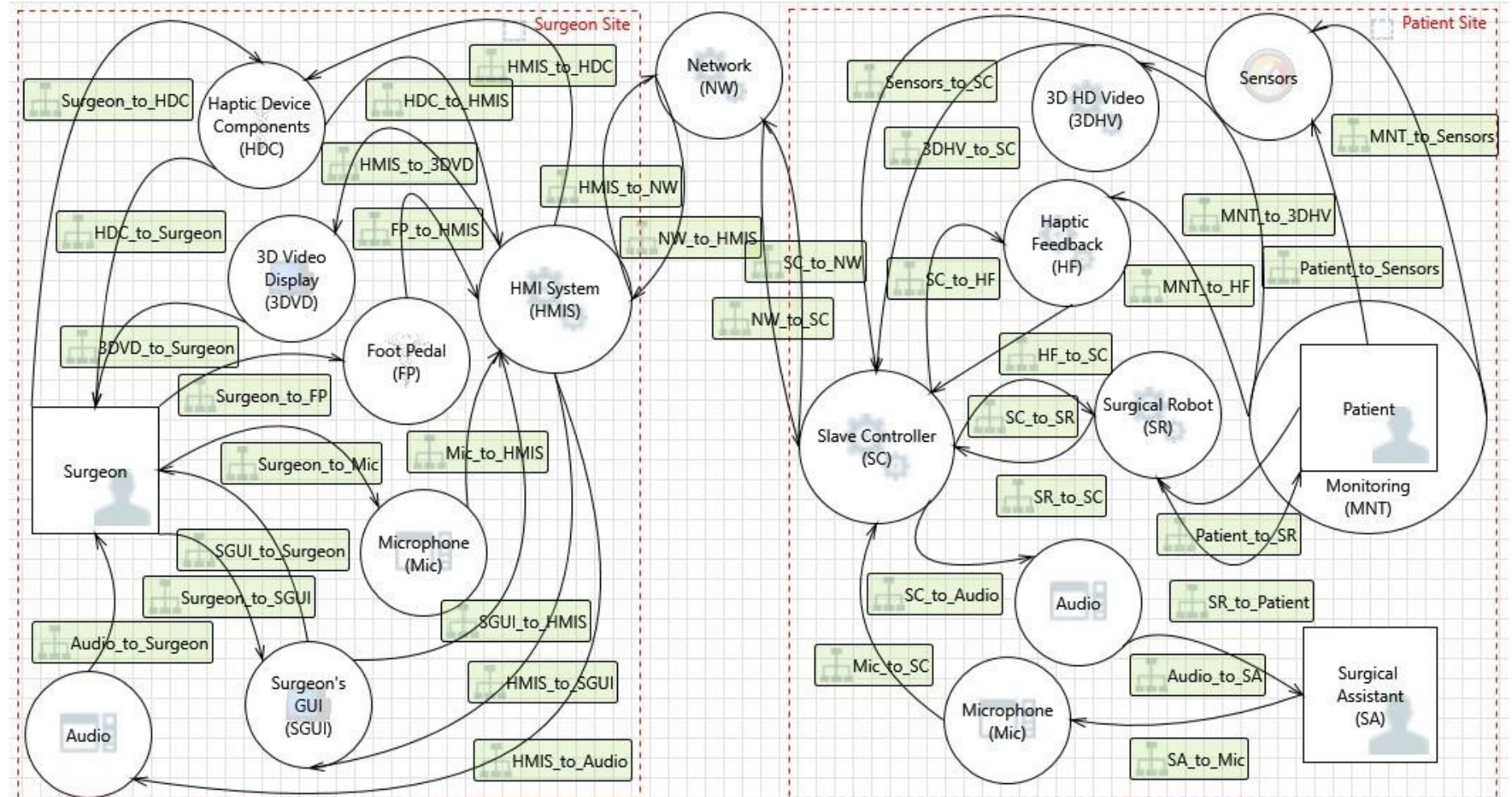# PERFORMANCE, RELIABILITY, SCALABILITY, CYBERSECURITY

Md. Rashid Al Asif, Khondokar Fida Hasan, Md Zahidul Islam, Rahamatullah Khondoker, "STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems", *Sustainable Technologies for Industry 4.0 (STI) 2021 3rd International Conference on*, pp. 1-6, 2021

DATA DISTRIBUTION SERVICE (DDS)

STANDARDS-BASED MIDDLEWARE FOR SCALABLE, RELIABLE, SECURE CONNECTIVITY

- Data-Centric
- Decentralized/ Decoupled
- Low-Latency
- Quality of Service
- Security by Design
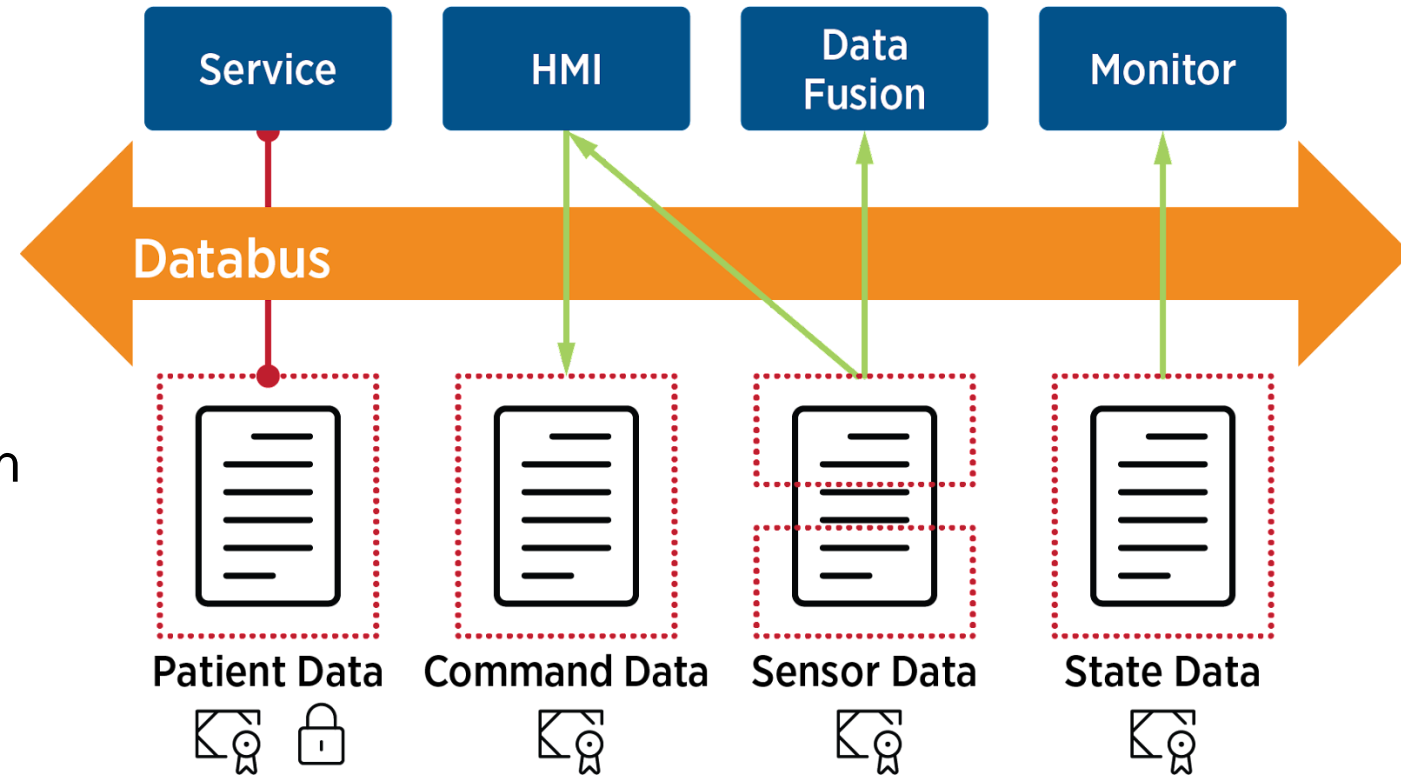
TECHNOLOGY ECOSYSTEM

Why it makes sense for your next medical robotics development effort and your business.

WHY A TECHNOLOGY ECOSYTEM?

Working with synergistic technology ecosystem partners will simplify development and reduce risk.

YOUR QUESTIONS

THANK YOU

Check out our demo!

TOM AMLICKE
tamlicke@medacuity.com

MICHAEL CHALUPA
mchalupa@blackberry.com

HASNAT ASHIQ
hasnat@rti.com

BACK-UP

ENGINEERING HIGH-PERFORMANCE MEDICAL ROBOTICS SOLUTIONS

Technical Risk Considerations & How to Mitigate

PRESENTED BY

MEDACUITY

BlackBerry | QNX

rti

ABOUT
MEDACUITY

MEDACUITY

Specialized software engineering firm **trusted by global companies and innovators,** large and small

Delivering **custom software solutions** for MedTech, Life Sciences, and Robotics

- ISO 13485 & 27001 Certified
- IEC 62304 & ISO 14971 Compliant

300+ Completed Projects

100+ Software Engineers

10+ Average Years Experience

90% Repeat Business Rate

CONTACTS

Tom Amlicke
Technical Director, Robotics Practice
tamlicke@medacuity.com

Shawn Vanseth
Director, Robotics Practice
svanseth@medacuity.com

medacuity.com

PRESENTED BY

MEDACUITY

BlackBerry | QNX

rti

ABOUT

BLACKBERRY | QNX

BlackBerry | QNX

Trusted supplier of **safe and secure operating systems, hypervisors, frameworks and development tools.**

Technology is **trusted in more than 235 million vehicles** and is deployed in **embedded systems** around the world

Industries: Automotive, **medical devices**, industrial controls, transportation, heavy machinery, **robotics**

CONTACTS

Michael Chalupa
mchalupa@blackberry.com

Winston Leung
wileung@blackberry.com

blackberry.qnx.com/en/company

ENGINEERING HIGH-PERFORMANCE MEDICAL ROBOTICS SOLUTIONS

Technical Risk Considerations & How to Mitigate

PRESENTED BY

MEDACUITY

BlackBerry | QNX

rti

ABOUT
REAL-TIME INNOVATIONS

rti

RTI is the largest software framework company for autonomous systems.

CONTACTS

Hasnat Ashiq
Regional FAE Manager
Hasnat@rti.com

Darren Porras
Market Development Manager, Healthcare
dporras@rti.com

www.rti.com