Safety Considerations of Medical Device Remote Control in the Tele-Critical Care Context

Yi Zhang, Ph.D.

yzhang134@mgh.Harvard.edu

Medical Device Plug-and-Play Program
Massachusetts General Hospital
May 2024

About Me

- PhD in Computer Science (NCSU 2008)
- Computer scientist at the FDA (2008 -2019)

  Research, regulation, and policy making related to medical device software & cybersecurity
- Senior Program Manager at Mass Gen Hospital (2019 – present)

  Research and industrial services on medical device interoperability & digital health

MD PnP Program @ MGH

The Medical Device "Plug-and-Play" Interoperability & Cybersecurity (MD PnP) Program at Mass Gen Hospital was founded in 2004.

- Mission: improve patient care by enabling innovations of safe, secure, and interoperable medical technologies.
- 3,200 sq ft cyber range to support pre-clinical, pre-emptive research and services
- Research portfolios: $40+M federally funded projects on medical device interoperability
- Industrial service portfolios – state gov. recognized digital sandbox

Roadmap

01. Medical Device Remote Control

02. Case Study

03. Safety Considerations

1. Medical Device Remote Control

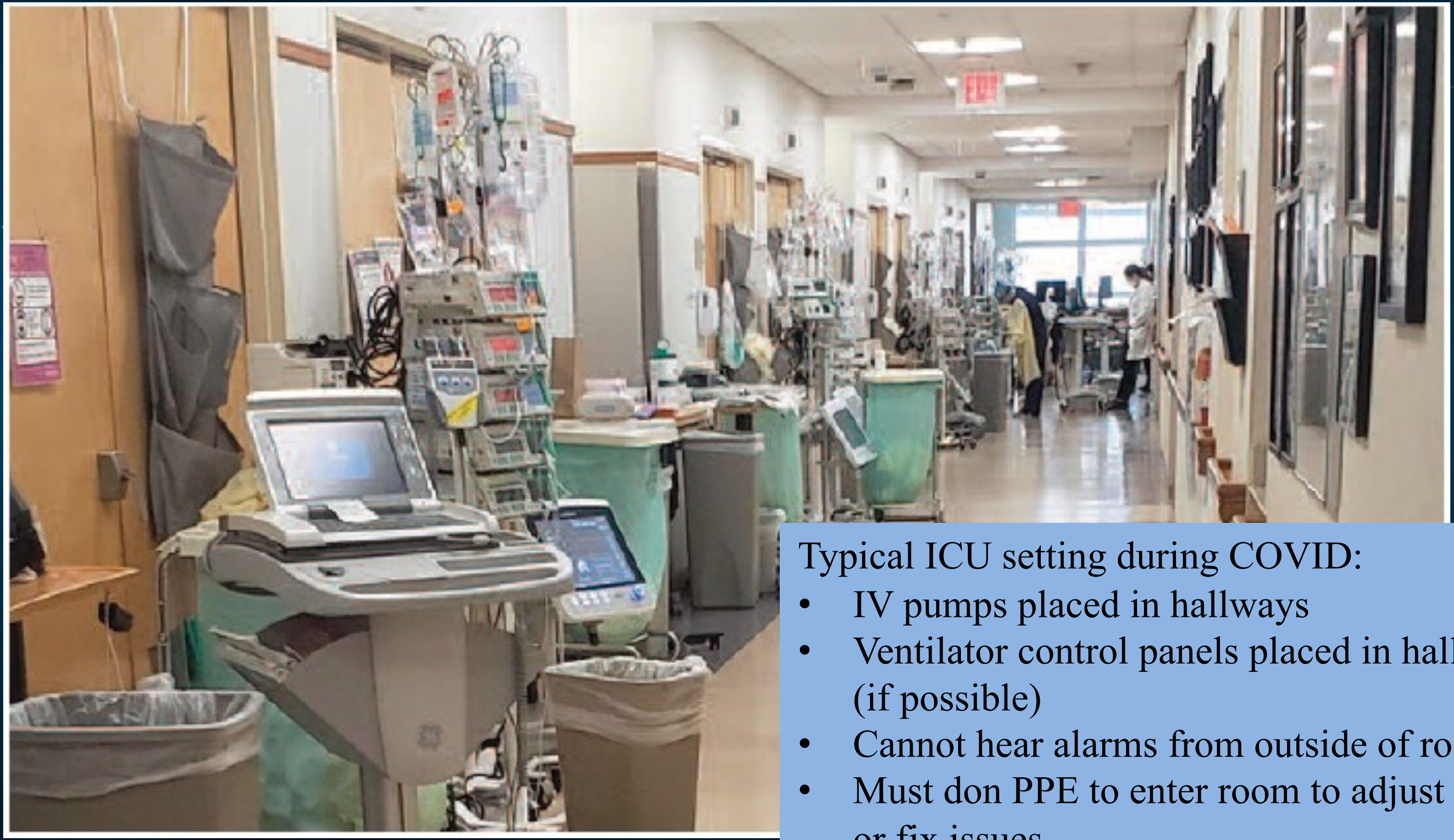
Remote Control of Medical Devices

- Definition: operation of the device is initiated or managed by transmission of signals from a location other than the device’s user interface [AAMI draft standard].

- Started with the concept of eICU about two decades ago[1].

- Technologies had not advanced much till the onset of COVID-19 [2]
    - Additional equipment and maintenance cost
    - High configuration complexity
    - Regulatory uncertainty

[1] Celi et al. The eICU: It’s not just telemedicine. Critical Care Medicine 29(8):p N183-N189, August 2001.
[2] Garzotto et al. Preventing infectious diseases in intensive care unit by medical devices remote control: lessons from COVID-19. J Crit Care. 2021;61:119-124.



Typical ICU setting during COVID:

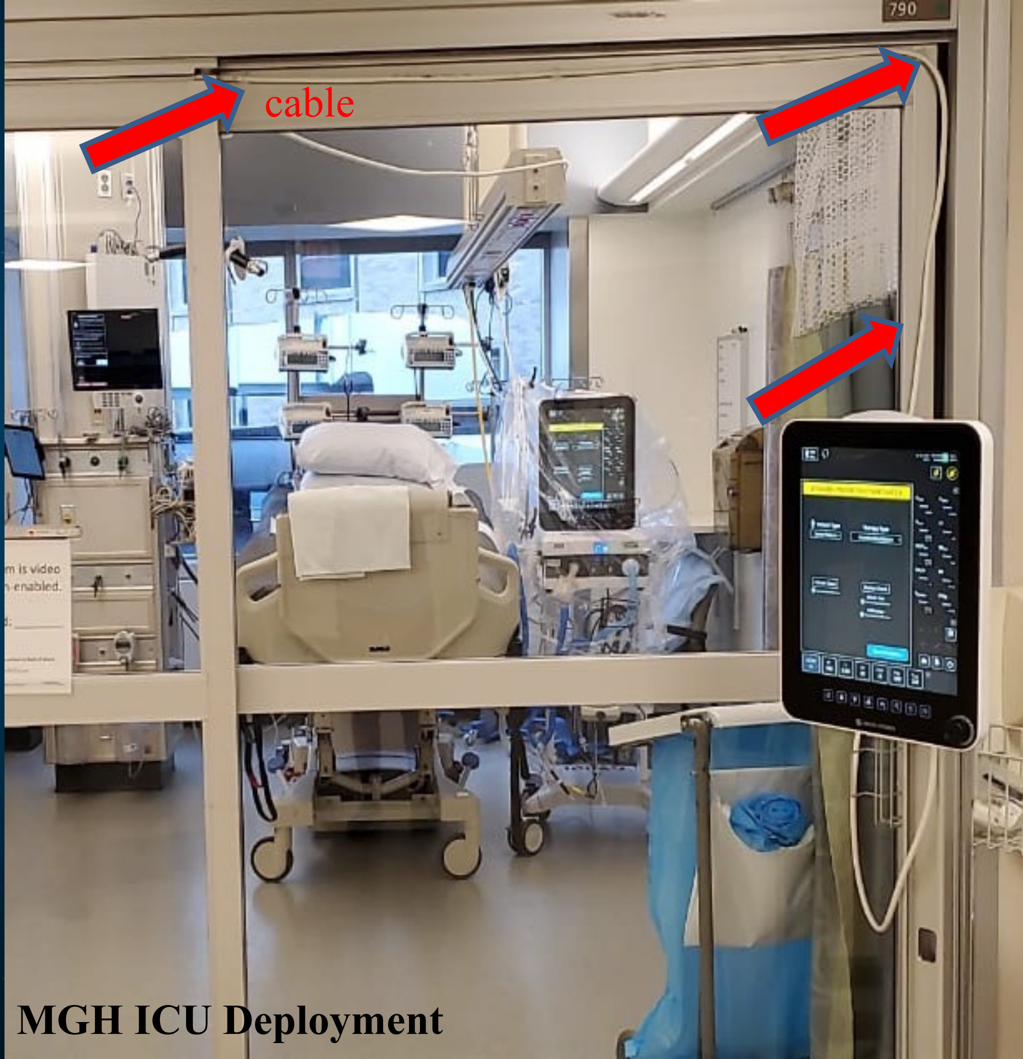
- IV pumps placed in hallways
- Ventilator control panels placed in hallways (if possible)
- Cannot hear alarms from outside of room
- Must don PPE to enter room to adjust settings or fix issues

https://www.ismp.org/resources/clinical-experiences-keeping-infusion-pumps-outside-room-covid-19-patients

Ventilator Remote Control (1) – Secondary GUI

Nihon Kohden (NK) OrangeMed NKV-550 Ventilator

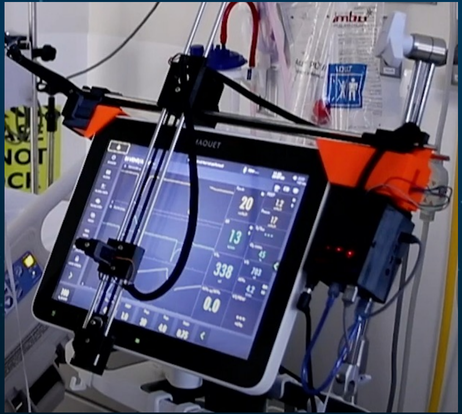
- FDA cleared in 2020 (K192307).
- A secondary GUI provides the same function as the primary (except for power on/off).
- Secondary GUI connected to the ventilator via a 10-meter cable.
- The primary and secondary GUIs enable and disable the other to avoid 'competing control'.



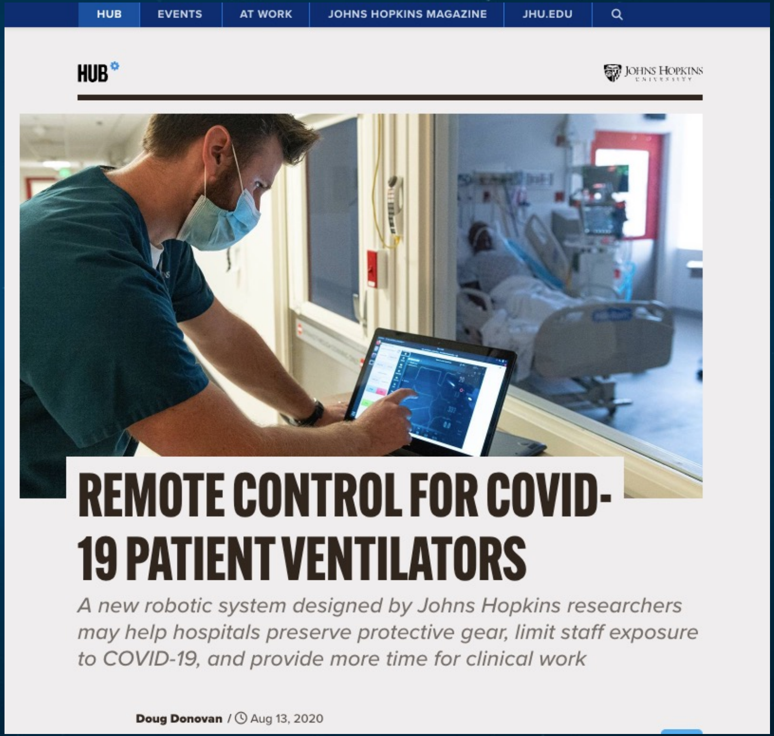
Ventilator Remote Control (2) - Robotic Finger

A robotic system is placed on the screen of a ventilator to mimic human operator's actions

Clinician outside the patient room controls the robotic system to operate on the ventilator screen.



From John Hopkins Medicine YouTube Channel https://youtu.be/ZG6RdPfghJs



REMOTE CONTROL FOR COVID-19 PATIENT VENTILATORS

A new robotic system designed by Johns Hopkins researchers may help hospitals preserve protective gear, limit staff exposure to COVID-19, and provide more time for clinical work

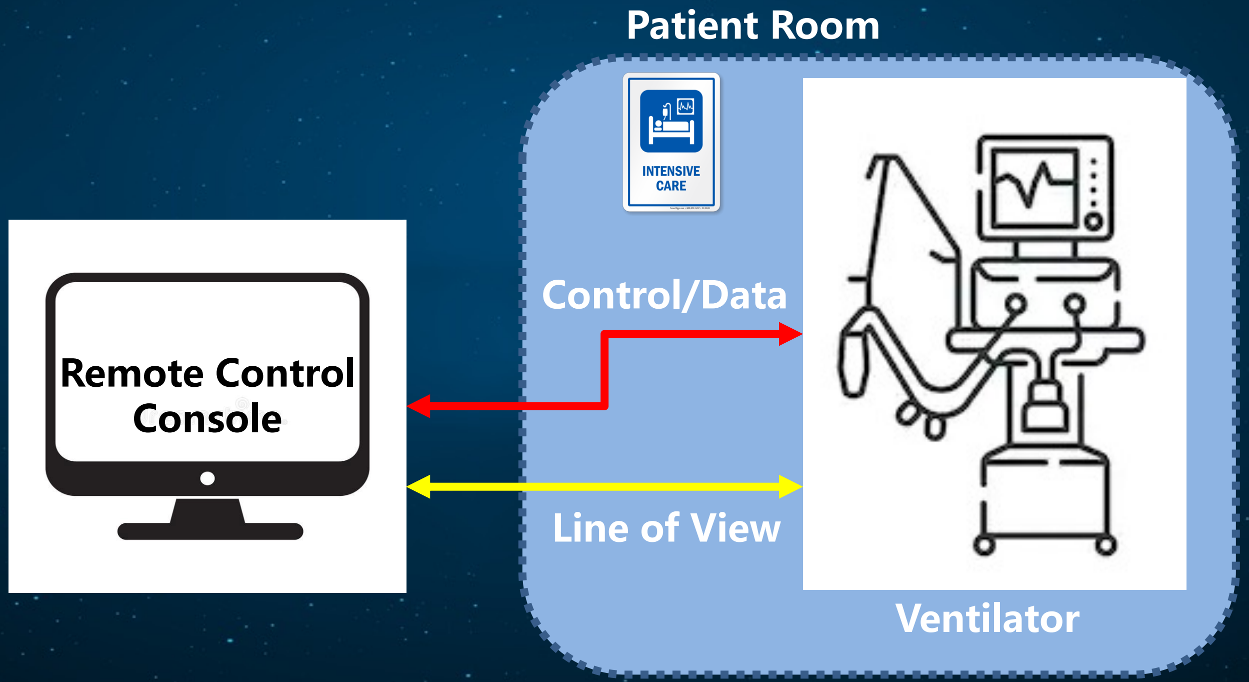
Doug Donovan / Aug 13, 2020

https://hub.jhu.edu/2020/08/13/remote-control-ventilators-covid-19-pandemic/

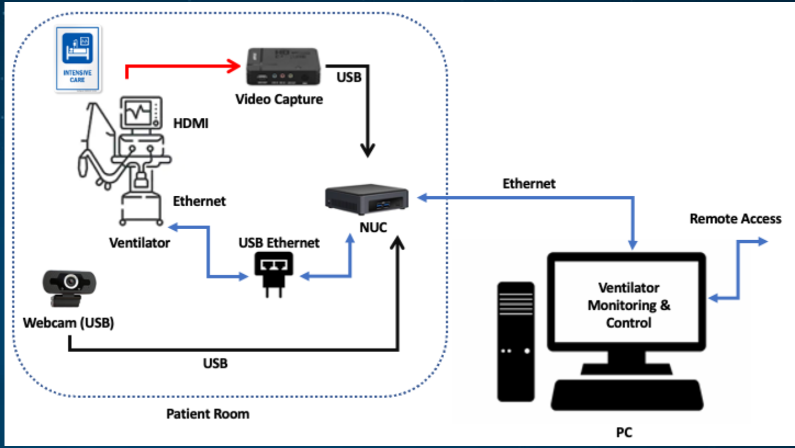
Near-Patient Remote Control

Operator can:

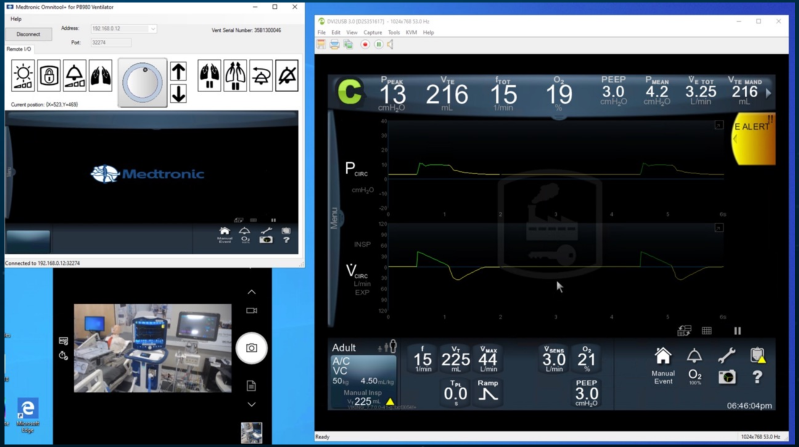
- Access to device and patient in a timely manner.
- View the patient directly.



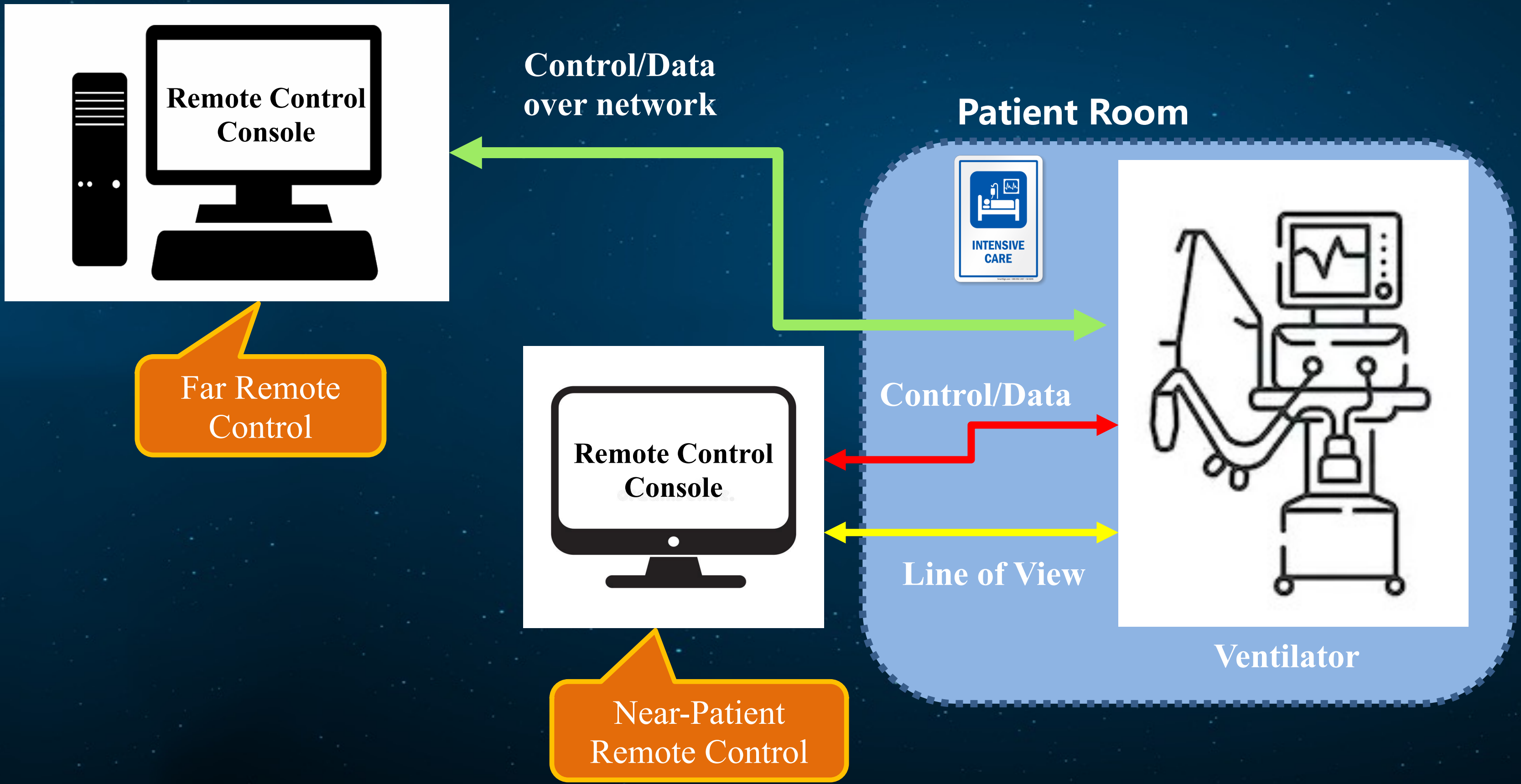
Ventilator Remote Control (3) – Remote Desktoping



- Medtronic PB980 Ventilator (FDA cleared)
- Omnitool software
  - View the user interface of the ventilator
  - User control operations are translated to UI coordinates + actions and sent back to vent.



Far Remote Control



Benefits & Limitations of Remote-Control Technologies

- Reduce ~50% of entries to the patient room [1]
  - save consumption of PPEs and the time delay to don/doff PPE upon emergencies
  - reduce healthcare staff's exposure to infection

- Extended reach of healthcare services

- Lack of communication protocols/APIs to allow third-parties to develop remote control applications

  - Real-time device data → continuously patient monitoring and timely intervention
  - Algorithmic control of devices → more frequent and personalized adjustments of therapies

1. Bruen et al. Rapid implementation of remote ventilator monitoring and control during the COVID-19 pandemic. Crit Care Med. 2021;49(1):7-7.

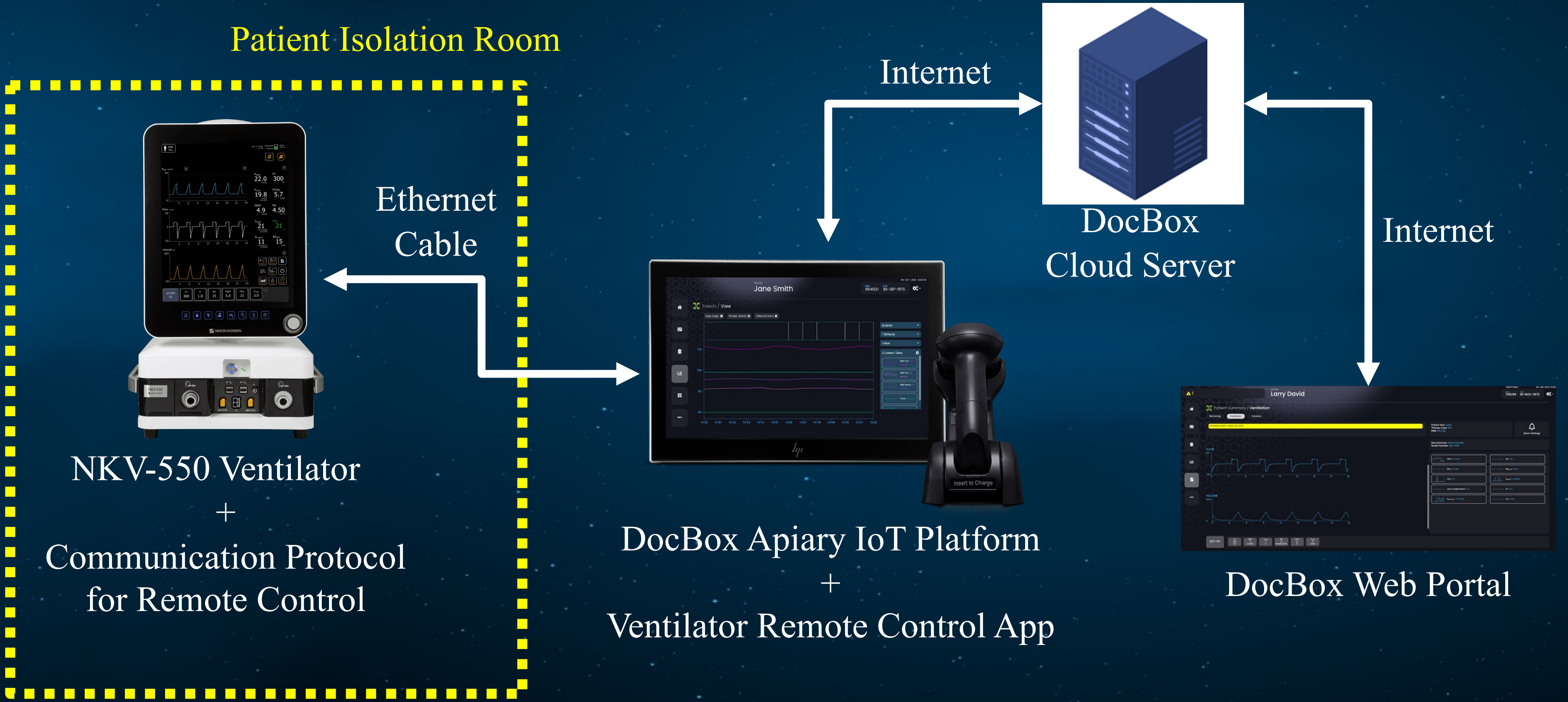
The NK-DocBox System

- Developed jointly by NK OrangeMed, DocBox Inc., and MD PnP, under U.S. Army Telemedicine and Advanced Research Center (TATRC)'s National Emergency Tele-Critical Care Network (NETCCN) and Technology in Disastrous Environment (TiDE) programs.

- Problem: locations without ICU beds do not have clinicians who know how to use critical care devices (ventilators, IV pumps, etc.), even when these devices are available.

- Solution:
    - Link remote critical care expertise to frontline clinicians using secure, HIPAA-compliant technologies → Virtual Hospital (NETCCN)
    - Provide a consistent, reliable means on top of NETCCN for remote clinicians to deliver mechanical ventilation (TiDE/NK-DocBox)

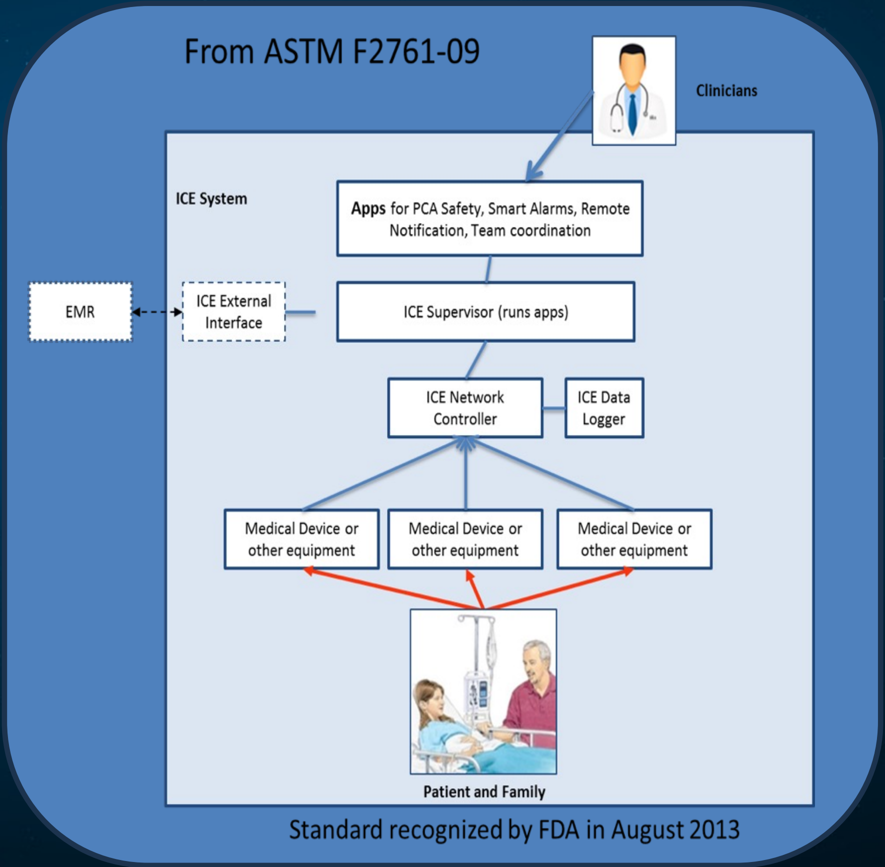
NK-DocBox System Architecture



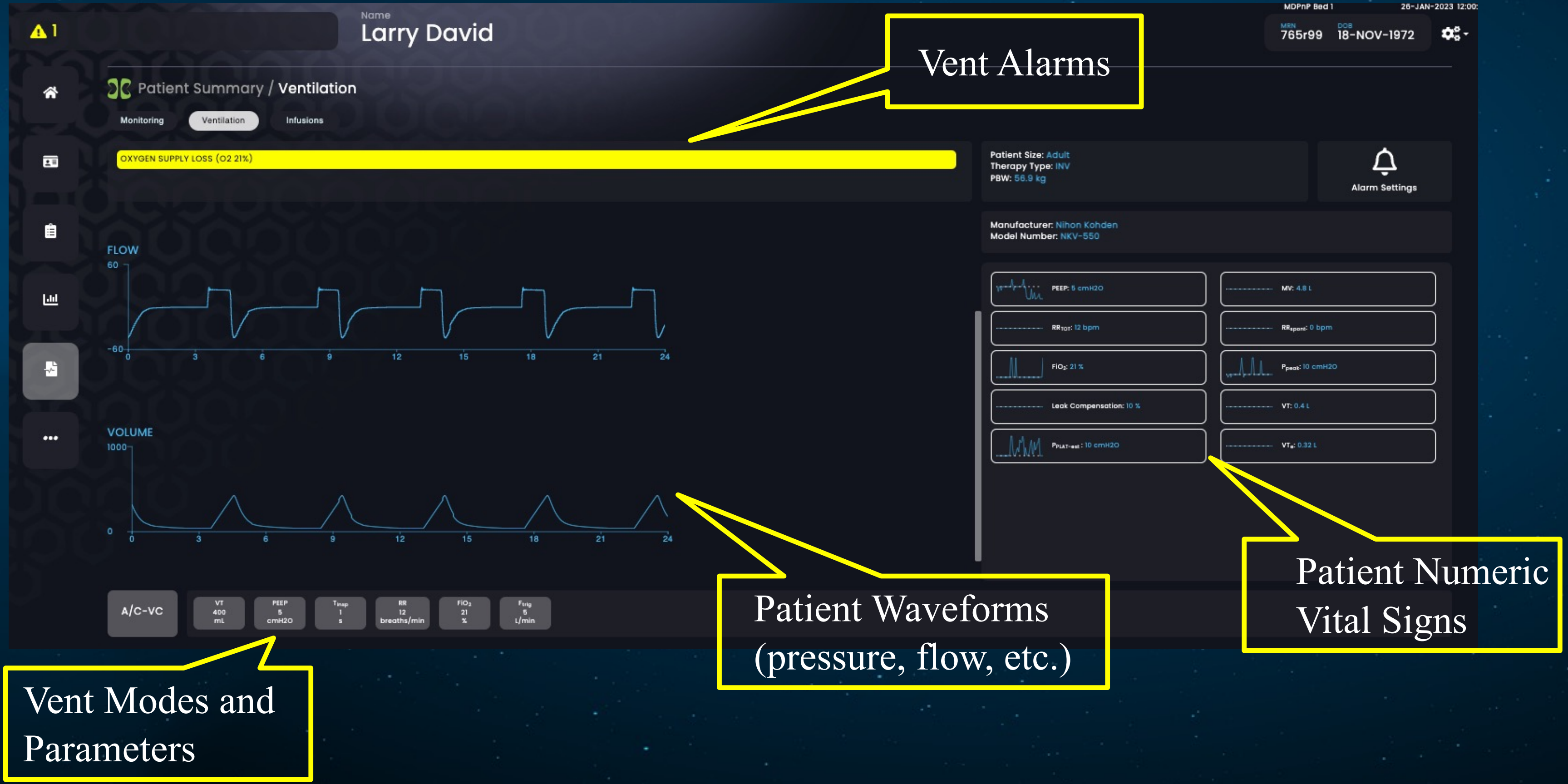
Interoperability Platform at the Patient's Bedside

DocBox Apiary platform implements the FDA-recognized Integrated Clinical Environment (ICE) interoperability architecture (ANSI/AAMI 2700-1)

- Medical devices, not just the ones under remote control, connect through device drivers.
- Clinical/safety algorithms, including the remote -control application, are deployed as apps on the platform.
- ICE Supervisor coordinates devices/apps and provides system-level services, e.g., time synchronization, forensic data logging, access control, etc.

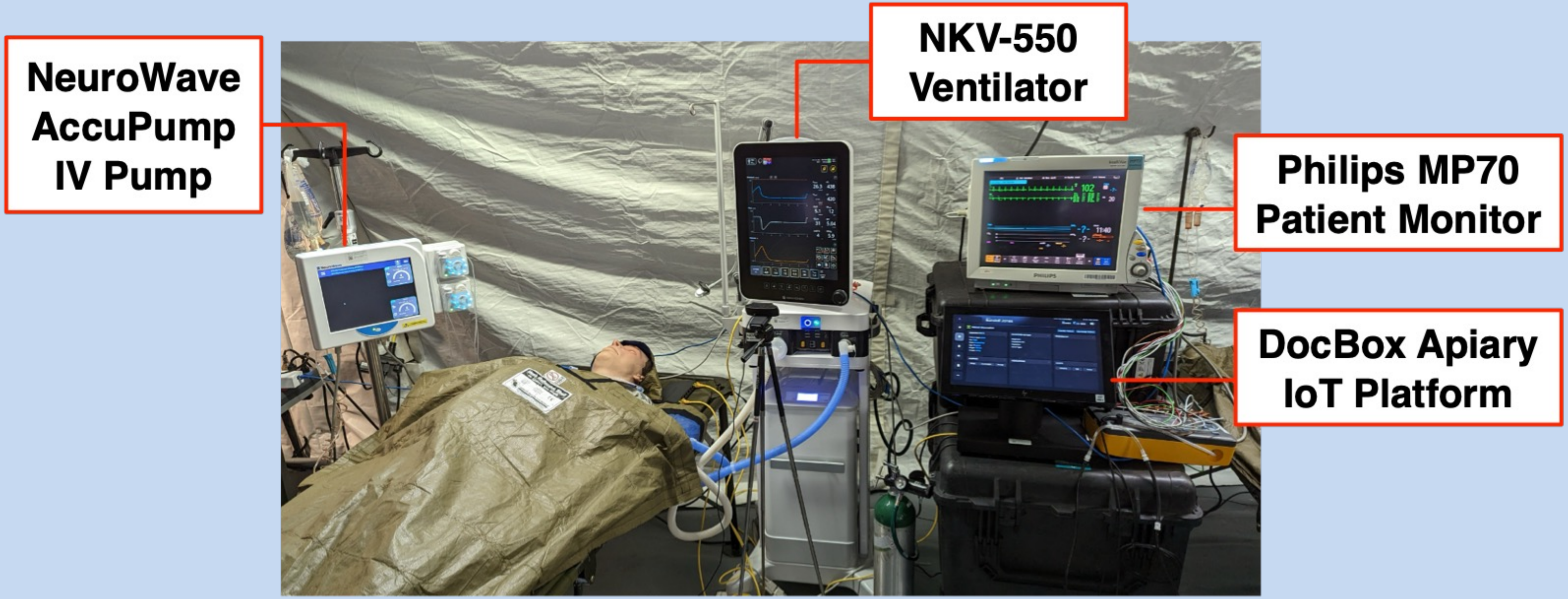


DocBox Ventilator Remote Control App



NK-DocBox System Demo

Demo in different simulated military mass casualty care scenarios : https://vimeo.com/784432343.



Simulated Medical Field Hospital Role II, Ft. Detrick, MD
Remote Control from Tacoma, WA

02. Case Study:

Safety Testing of the NK-DocBox System

Medical Device Remote Control: Recap

- Most technologies/solutions add remote control functions to existing devices → our research focus

The medical function, safety, and effectiveness of the original devices have been vetted

- Most technologies are still at the research prototype phase

Partly due to the lack of clear regulatory pathways, consensus safety requirements, and effective test methods

Testing Scope

Evaluate system safety and reliability in the MD PnP Cyber Range[1]

- Ventilator communication protocol robustness testing
- System end-to-end data flow testing
- System communication reliability testing
- Usability testing (preliminary)

1. Zhang et al. Reliability and Safety Testing of a Ventilator Remote Control System against Communication Failures and Network Disruptions. Military Medicine, accepted, Feb 2024. doi: 10.1093/milmed/usae067.

1. Ventilator Communication Robustness Testing

Goal: evaluate the behavior of NKV-550 and safety implications when facing erroneous remote-control commands

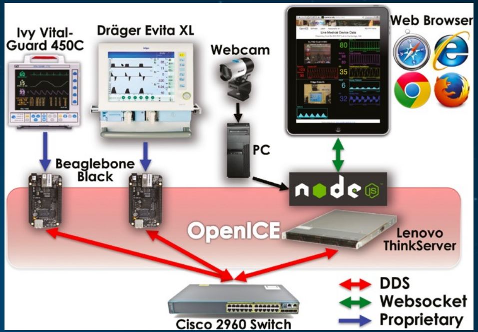
Method: develop driver and remote-control app for NKV-550 on the OpenICE interoperability platform (www.openice.info); alter the driver to inject a variety of erroneous commands.

- High frequency commands
- Set invalid ventilation modes
- Set invalid ventilation parameters
- Set out-of-range ventilation parameters

OpenICE-Based Remote Control for NKV-550

OpenICE: an open-source implementation of the ICE architecture developed by MDPnP.

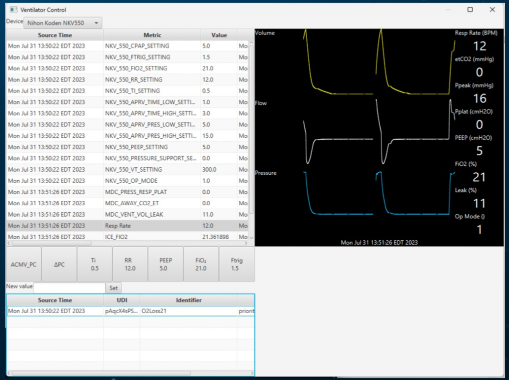
A wide array of device drivers, clinical/safety apps, and platform-level services to enable rapid prototyping and verification of innovative interoperable applications.



OpenICE Architecture

OpenICE Remote Control App for NKV-550

- Receive, interpret, and display ventilator data
  - numeric data: 2 Hz; waveform data: 40 data points/80ms
- Send control commands per the protocol → black-box protocol testing



OpenICE App for NKV-550 Remote Control

Test Results

- Ventilator responded as expected when commands arrived as fast as once per second.
- Ventilator ignored commands setting invalid ventilation parameters.
- Ventilator defaulted to the SPONT-APRV mode if the command requests to change to an invalid mode.
- When a command requests to change a parameter to an invalid value, ventilator set the parameter to the maximum or minimum value allowed.

(e.g., the command tries to set VT to 4000ml, ventilator set VT to the maximum 3000ml.)

Need further safety assessment

2. System Communication Reliability Testing

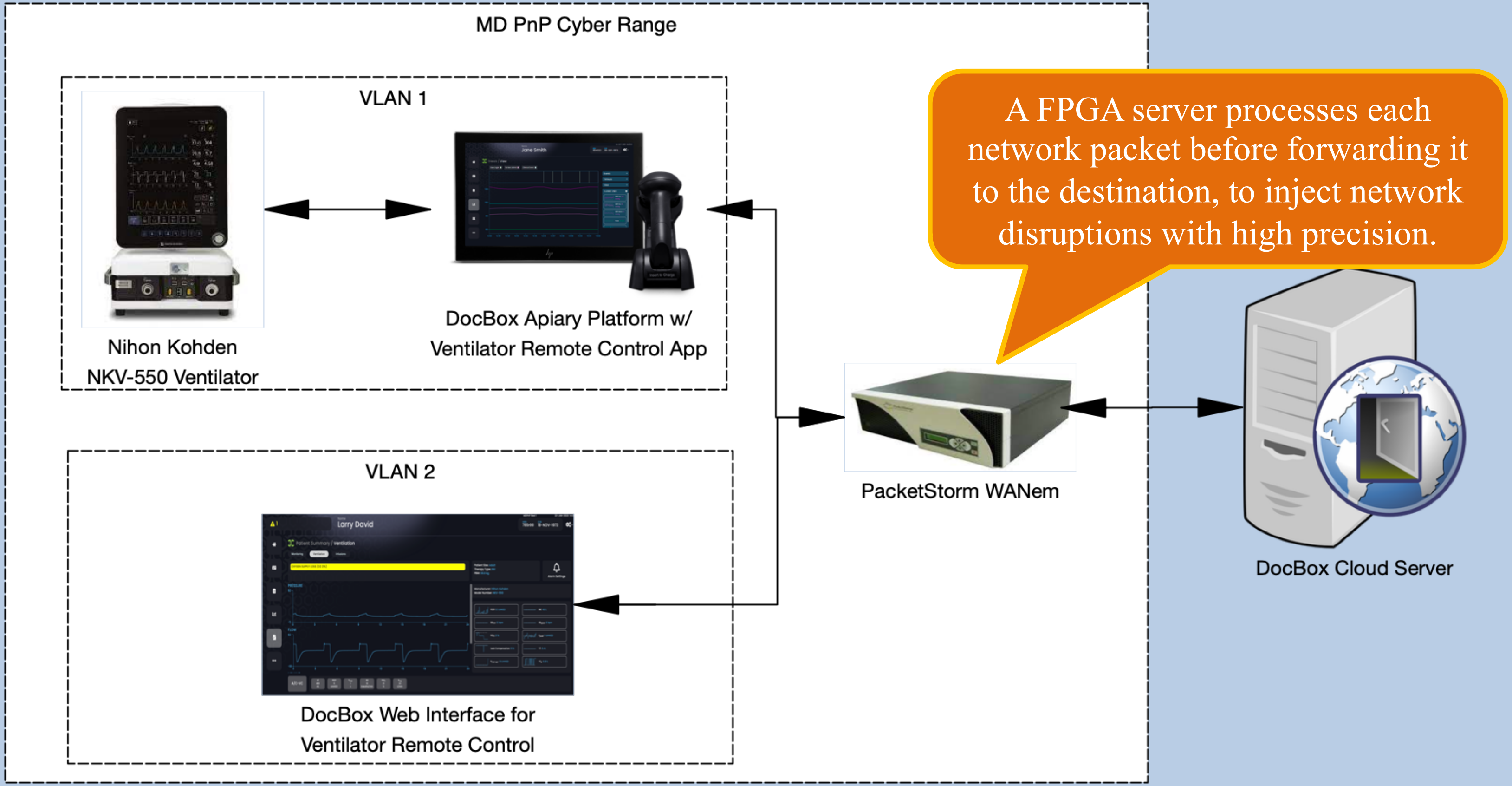
Goal: 1) evaluate the system's reliability, usability, and in turn safety when facing network disruptions commonly seen in tele-critical care;

2) quantify the minimal network quality for the system to operate safely.

Metrics:

- Connection stability (e.g., loss of connection, delay in reconnecting)
- Delay in sending commands to the ventilator
- Delay in the ventilator responding to commands
- Impact on vent data visualization at the web portal

Network Configuration for System Reliability Testing



Test Protocol and Results

Test Protocol: perform the same sequence of remote-control operations when a single network QoS attribute is adjusted to different levels (delay/jitter/packet drop/packet reordering/bandwidth/bit error)

Baseline: 1 Gb/s for both upload and download directions w/o QoS degradation.

Test Results:

- Minimal network QoS required: <500ms delay, <100ms jitter, <1% data drop, >12 Mb/s bandwidth, or $<1e^{-6}$ bit error rate. Packet reordering had no impact (up to 33% tested).
- System became unsafe to use when the minimal network QoS was not guaranteed.

connection unstable/lost; delay causing use errors; waveform skewed/frozen/moving backwards.

3. Preliminary Usability Testing

Setup

- Fifteen (15) respiratory therapists use the DocBox web portal from Irvine, CA to control the NKV-550 ventilator located in Boston, MA, or vice versa.
- Test protocol includes 19 use tasks of remote control (locate device data, recognize status change, recognize and respond to alarms, adjust settings, etc.).
- No network disruption

Results

- All use tasks (285) were successfully completed without use errors observed.
- Useful feedback was received from recruited RTs.

Before changing to the next ventilation mode, should be able to review and configure all associated parameter settings.

03. Safety Considerations

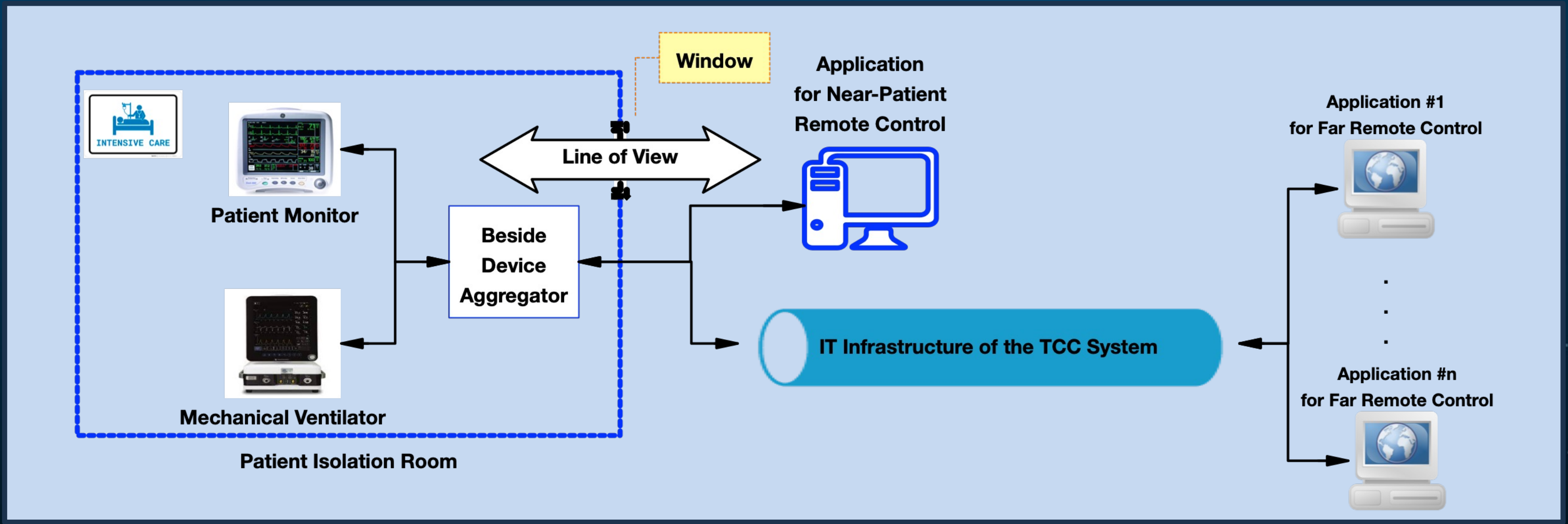
Factors to Consider for Remote Control Safety

- System Characteristics:
  - highly distributed, heterogeneous
  - ride on hospital IT networks and/or public networks
- Clinical scenarios:
  - Care models (e.g., how remote experts take on and hand off patients)
  - Clinical workflows implemented & resources allocated
- Use environments:
  - Devices may be deployed in unusual environments (e.g., field hospitals, hospitals-at-home)
  - Remote control applications may be used in non-clinical settings

Example Risks with Remote Control Functions (1)

<u>Contention of control</u>: device is operated from multiple locations at the same time

- Create nondeterministic device behavior and operator confusion
- Need mechanisms to eliminate competing/conflicting controls and clearly indicate the locus of control at all control locations



Example Risks with Remote Control Functions (2)

Non-Permissible Remote-Control Operations: unacceptable risks arise when certain device functions are being controlled remotely.

Example: changing ventilation to certain modes requires changing the vent circuit or even patient incubation.

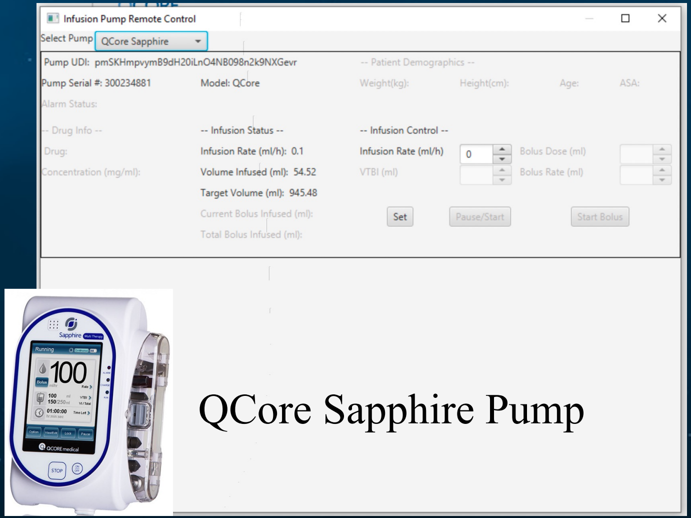
Use errors associated with the remote-control application

- The remote-control application UI may be different than the device's UI.
- Information presented at the remote-control application UI is incomplete, stale, in poor quality, or out of synchronization with the device.
- No line of view on the patient nor other means to monitor the patient's reaction to remote control.

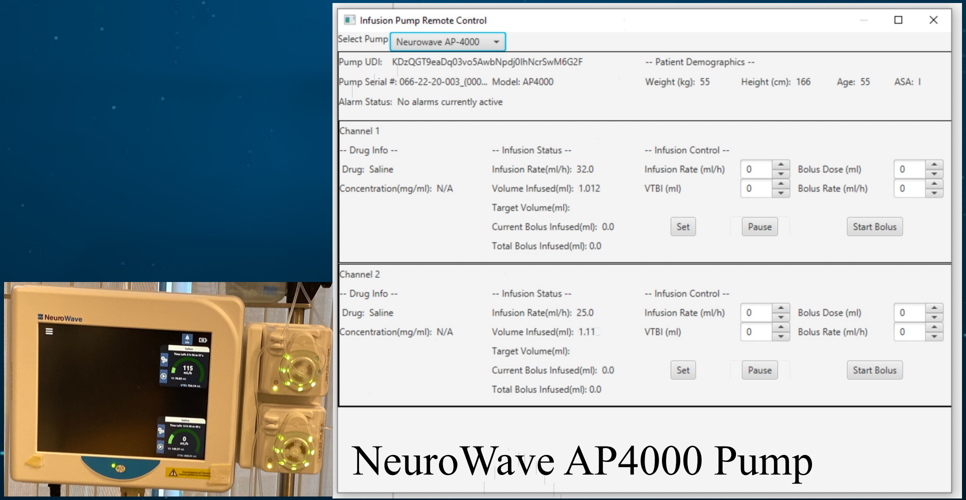
Example Risks with Remote Control Functions (3)

Data Interface/Interoperability Errors

- Lack of standardized terminology → syntactic or semantic interoperability errors
- Different devices have different levels of capability & adequacy in data interface



QCore Sapphire Pump



NeuroWave AP4000 Pump

Example Risks with Remote Control Functions (4)

Erroneous association among patient, device, and remote-control application

- Correct integration with the hospital's patient identity management system.
- Adaptive patient identity management for disasters or public health events.

Environmental conditions

- Lack of resources (e.g., frontline staff, patient monitoring, backup communication means)
- Patient transfer and handoff
- Degraded network resources (e.g., due to hospital IT infrastructure policies)

Adverse Impact on Device Safety and Performance

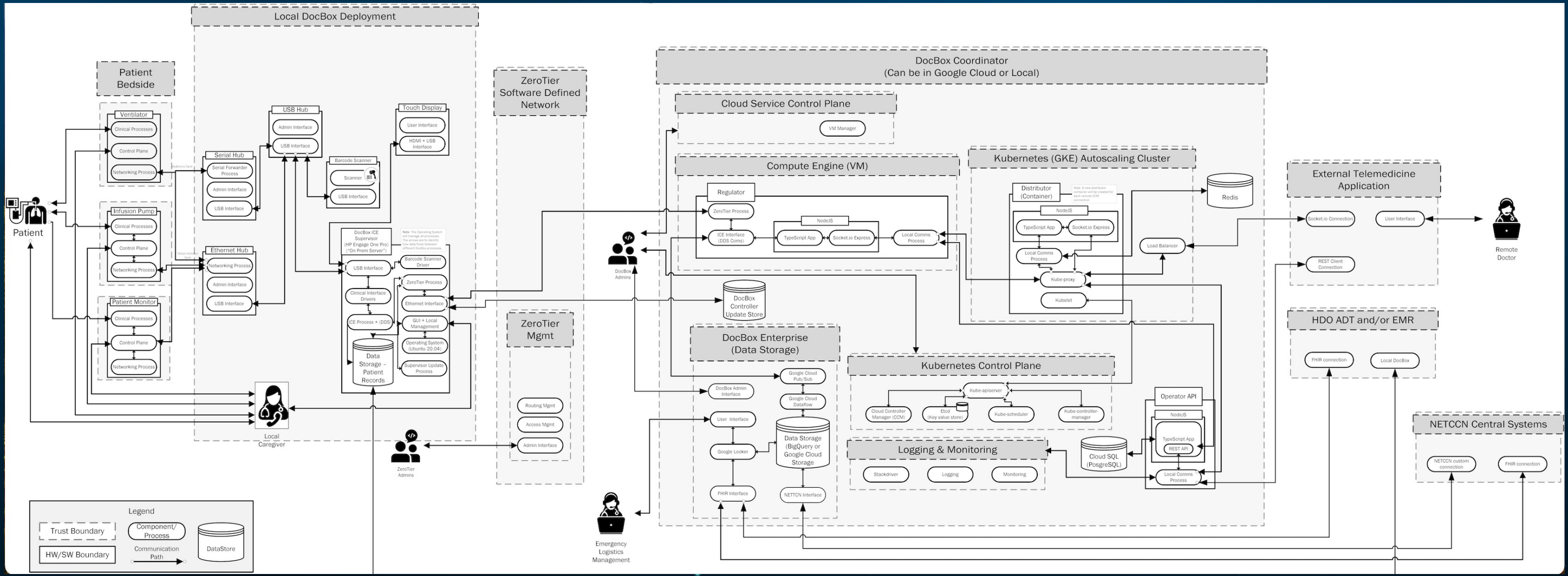
processing excessive remote-control related network traffic depletes computational resources in the device.

Example Risks with Remote Control Functions (5)

Cybersecurity

- Device access control
- User access control
- Authentication of the remote-control application
- PHI/PII privacy

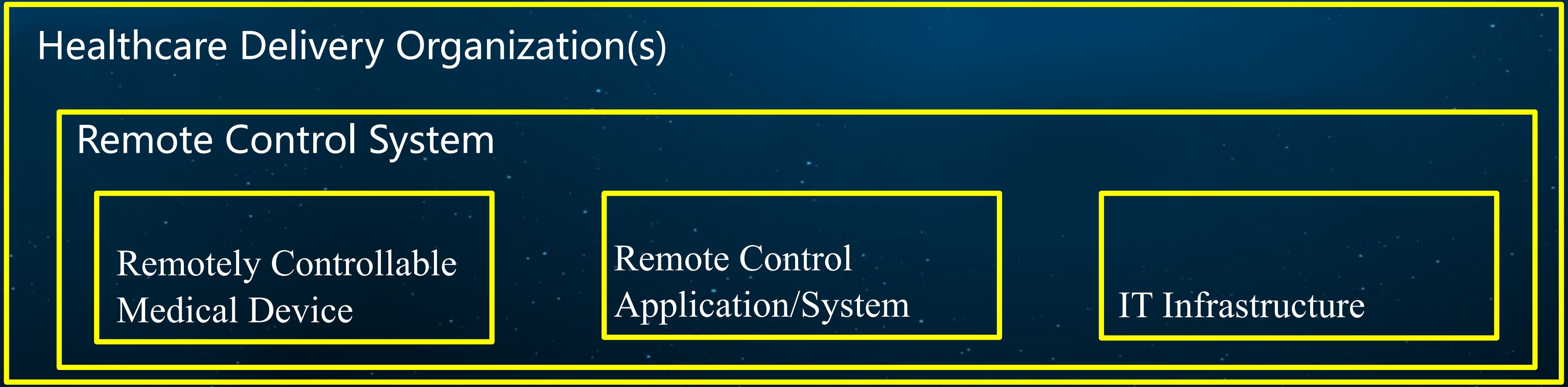
Complicated by the complex deployment environment & integration with the tele-critical system



System Architecture and Data Flow Diagram of NETCCN with NKV-550 Remote Control

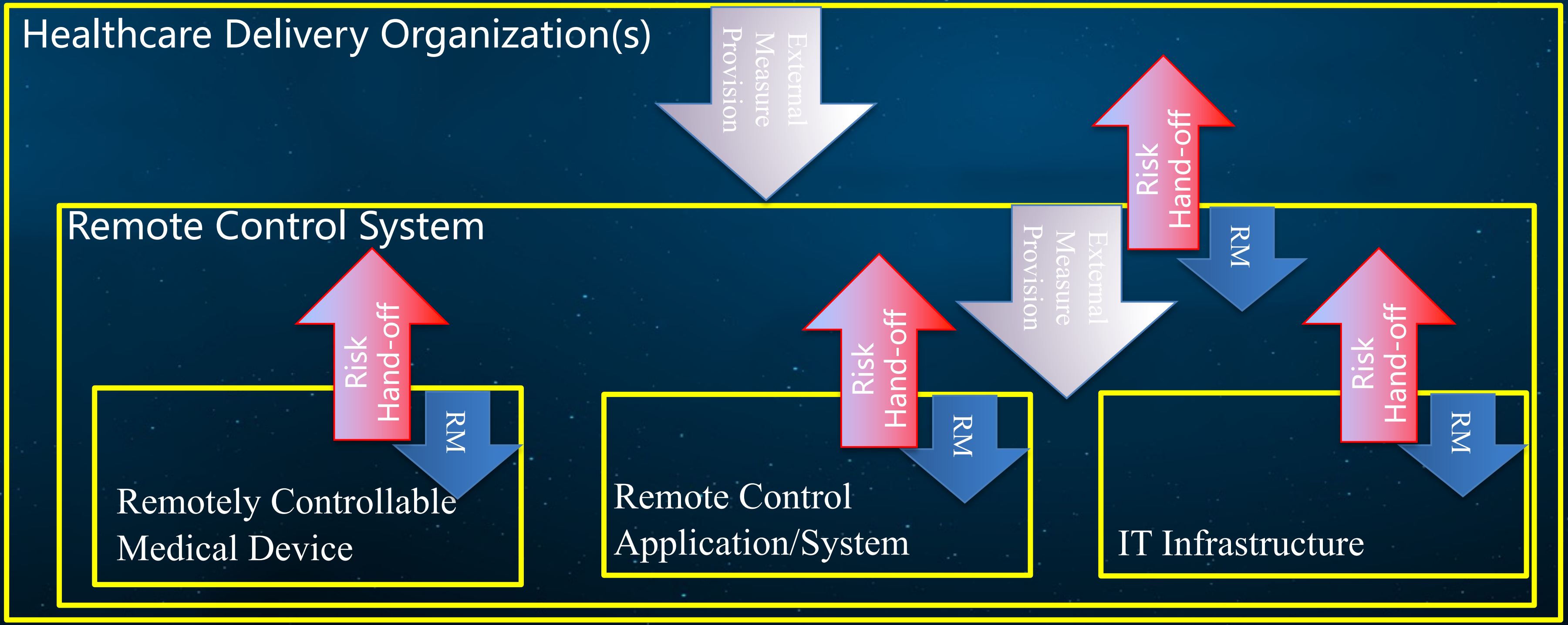
Challenges for Risk Management and Software Verification

- The heterogeneous nature of remote-control technologies
- Integration with tele-critical care systems across organizational boundaries
- Lack of standardized terminologies
- Clinical care models and processes are relatively new



Coordinated Risk Management

Need to expand current risk management practices (ISO 14971) and establish a coordinated risk management framework across the ecosystem, where each player's responsibility is clearly defined.



Assume-Guarantee Safety Verification

Verification at the component level:

- Assumptions on how the system will integrate and use the component are clearly defined and disclosed.
- Component safety goals are defined and verified based on the assumptions.

Verification at the system level:

- System safety is verified based on assumptions about component-level safety.
- Discharge assumptions about component-level safety.
- Provide measures that the components require for safety.

[1] J. Hatcliff, Y. Zhang and J. M. Goldman, Risk Management Objectives for Distributed Development of Interoperable Medical Products, *2019 IEEE Symposium on Product Compliance Engineering (SPCE Austin)*, Austin, TX, USA, 2019, pp. 1-6, doi: 10.1109/SPCE47297.2019.8950764.

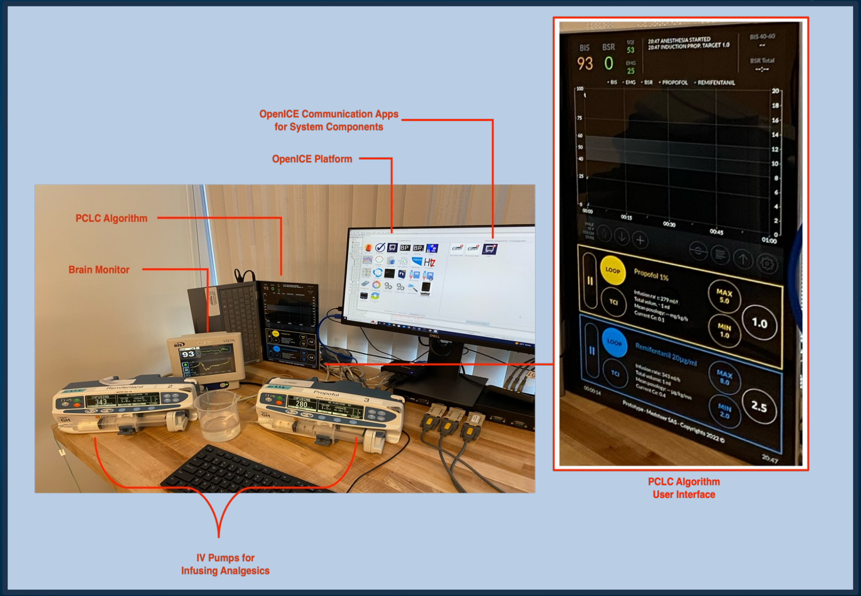
Another Use Context for Medical Device Remote Control

Use remotely/externally controllable devices in Physiological Closed-Loop Control Systems (e.g., autonomous anesthesia systems)

- The impact of device capability, performance, and errors on system performance:

  Measured by root mean square errors between the control algorithm's predicted values vs. the measured values[1]

- Safety fallback design to protect patient safety upon device failures.



OpenICE-based hardware-in-the-loop testbed for a PCLC anesthesia system

1. Varvel, J.R., et al. Measuring the predictive performance of computer-controlled infusion pumps. *Journal of Pharmacokinetics and Biopharmaceutics* **20**, 63–94 (1992). https://doi.org/10.1007/BF01143186

Smart and Autonomous Medical System (SaAMS) Collaborative Community

- In SaAMS, medical devices are controlled by (AI/ML-enabled) algorithms to transform healthcare.

  Autonomous anesthesia system, fluid resuscitation, blood pressure control, …

- SaAMS CC: partner with regulators, industry, and academia to solve key challenges (e.g., risks, safety requirements, and safety test/verification methods) for SaAMS that no single entity can solve.

  Endorsed by FDA and a number of professional associations

Scan to join

2024 SCC

Thank you!