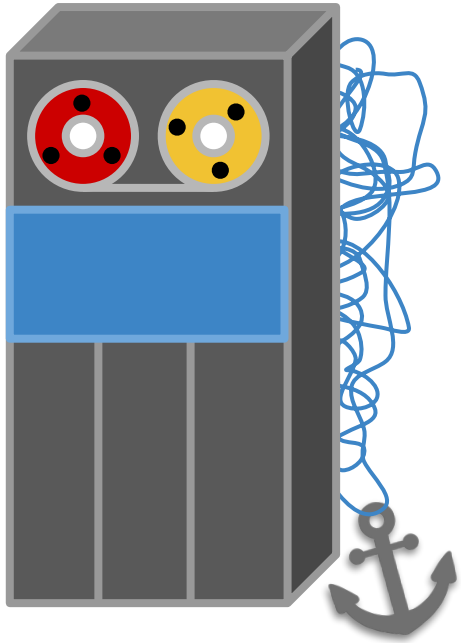
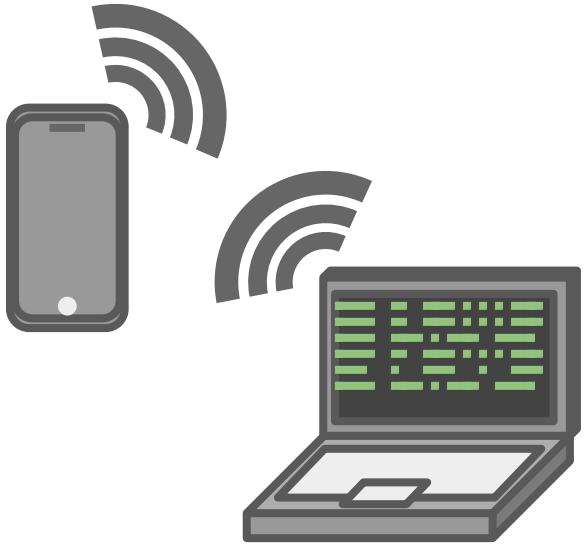
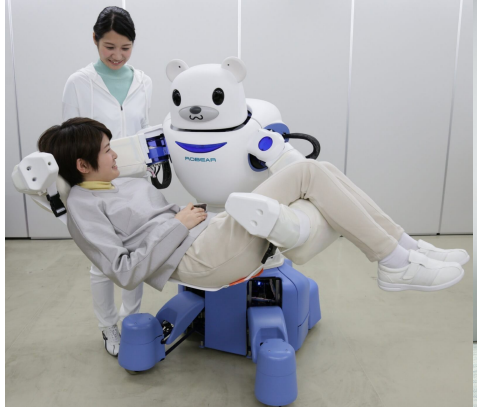
Securing Robotics with SROS2

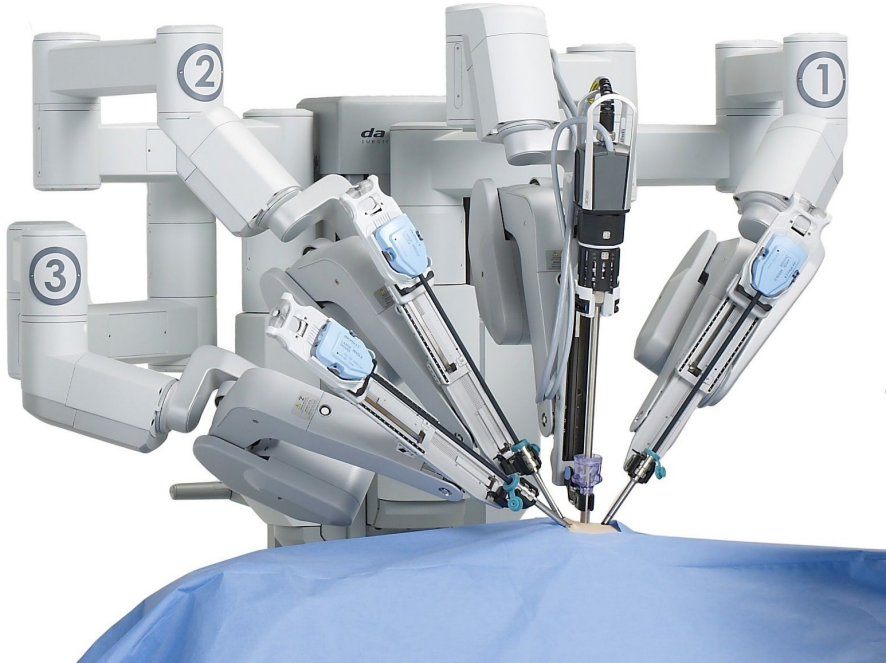




Motivation | Medical

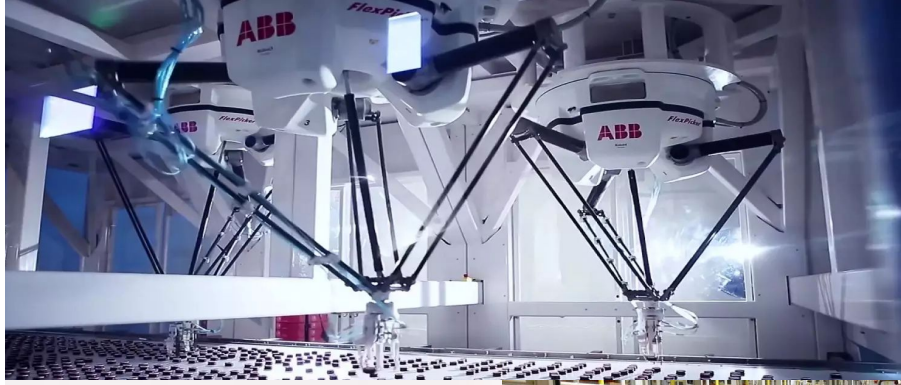
- Patient Mobility
  - Safely transferring immobilised patients
  - Offloading strenuous lifting from nurse
- Indoor logistics
  - Routine deliveries of supplies, food, medicine
  - Abolish tedious tasks for high trained staff
- Telesurgery
  - Minimally Invasive Surgery for faster recovery
  - Remote operations when surgeons are offsite
- Examples
  - **RoBear** developed by *RIKEN-SRK*
  - **TUG** Robot Flexible Carts from *Aethon*
  - **Da Vinci Surgical System** from *Intuitive Surgical*

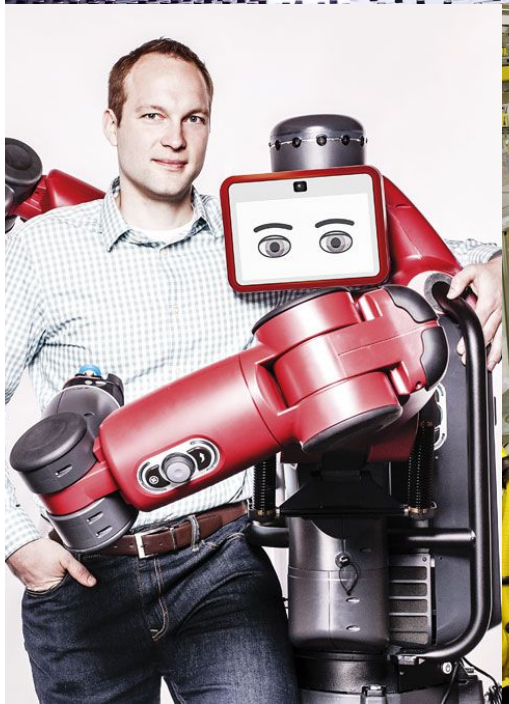


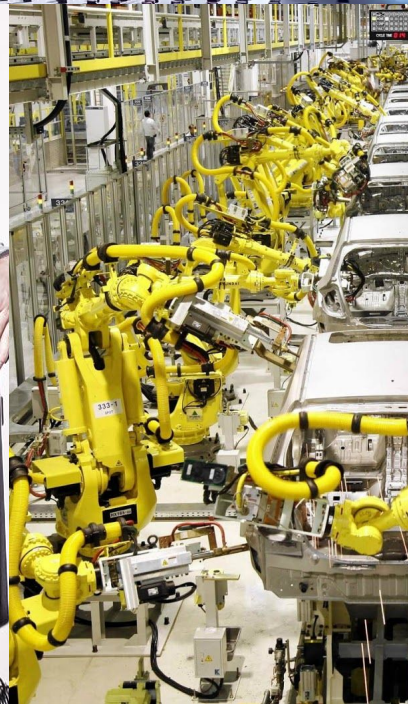


Motivation | Industrial

- Food Processing
  - Maintain a sanitary and sterile environments
  - Enable meticulous and adaptive quality control
- Manufacturing
  - Minimize assembly costs and maximizing efficiency
  - Remove humans from toxic or dangerous stages
- Packaging
  - Cooperative human shared workspaces
  - Flexible and dynamic multipurpose work cells
- Examples
  - **Flexpicker** from *ABB*
  - **Robotic Arms** from *Kuka, Bosch, Fanuc, Yaskawa*
  - **Sawyer, Baxter** from *Rethink Robotics*







Motivation | Transport

- Warehouse
  - Efficient and compact storage of assets
  - Meeting fulfilment demand during worker shortage
- Personal Transit
  - Avoid driving while distracted or fatigued
  - Mobility and independence for the impaired
- Freight Shipping
  - Safer operation with less on ground personal
  - Synchronized orchestration of equipment
- Examples
  - **Warehouse robots** from *Amazon, Fetch*
  - **Autonomous cars** from *Wamo, Uber*
  - **Autonomous freight yard** from *VDL*

Motivation | Service

- Logistics
  - Round the clock last mile mail delivery
  - Rapid online grocery fulfilment to doorstep
- Surveillance
  - Unmanned public/private security monitoring
  - Unwavering vigilance in monotonous patrols
- Cleaning
  - Continuous or scheduled cleaning
  - Reduction of menial household chores
- Examples
  - **Delivery robot** from *Starship Technologies*
  - **K3, K5** patrols robots from *Knightscope*
  - **Roomba** robot vacuum from *iRobot*

Exposure

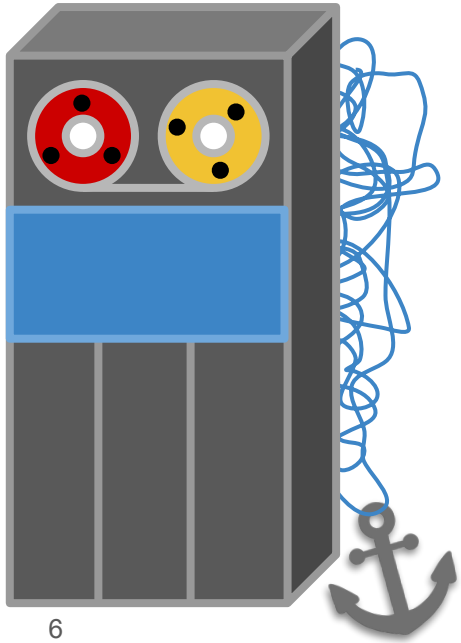
Connectivity, Mobility, Autonomy

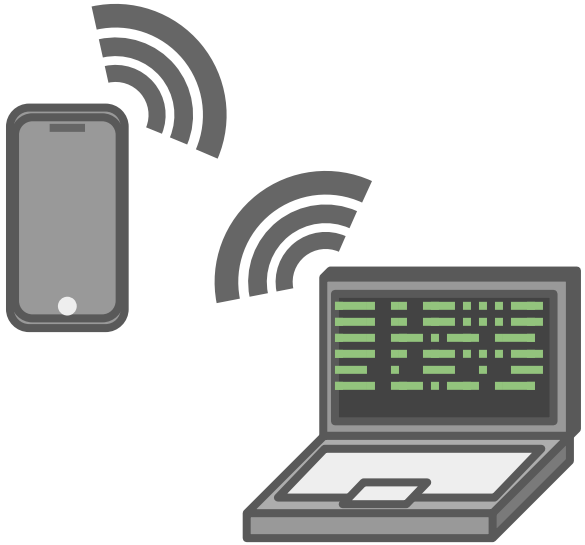
Risk

Mainframe Networks

Wireless Personal Computing

Autonomous Robotic Systems



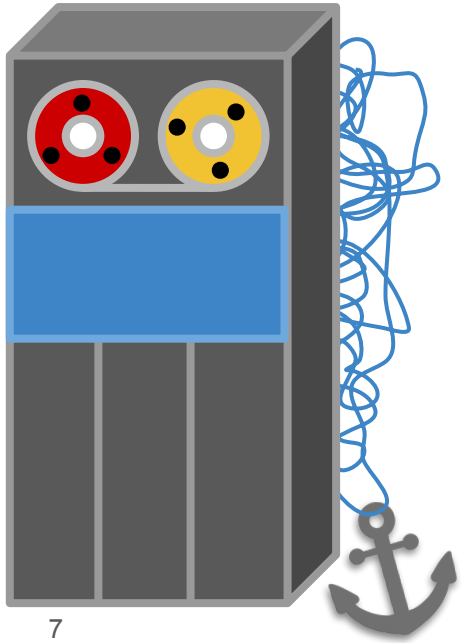


Exposure

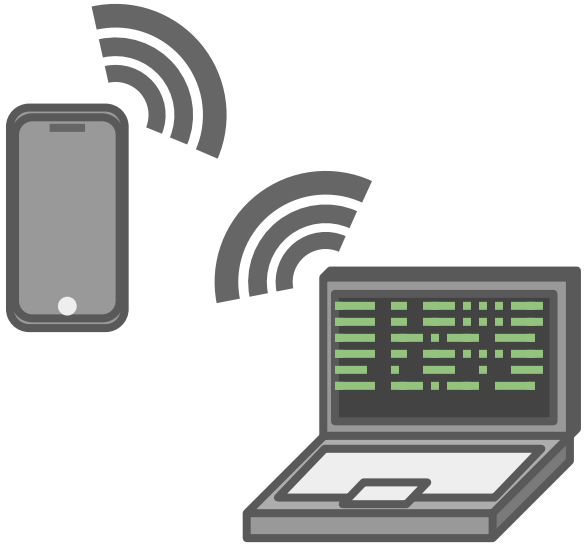
Connectivity, Mobility, Autonomy

Risk

Mainframe
Networks



Wireless
Personal Computing



Virtual:

- **Computation**
  - Correct and intended operation
  - Continuous monitoring
- **Networking**
  - Private communication
  - Controlled connections
- **Memory**
  - Confidentiality of data
  - Contained ownership

Exposure

Connectivity, Mobility, Autonomy

Risk

Autonomous Robotic Systems

Physical:

- **Environment**
  - Dynamic unchecked hazards
  - Limited uncontrolled connectivity
- **Sensing**
  - Imperfect onboard perception
  - Entrusted selfreliance
- **Safety**
  - Physical real-world interactions
  - Avoid risking human life & property
- **Privacy**
  - Active and passive data collection
  - Involuntary participation by proximity

Exposure

Connectivity, Mobility, Autonomy

Risk

Autonomous Robotic Systems

Cryptobotics

> *"A unifying term for research and applications of computer and microcontrollers' security measures in robotics."*

S. Morante, J. G. Victores, and C. Balaguer, "Cryptobotics: Why Robots Need Cyber Safety," Frontiers in Robotics and AI, vol. 2, no. Sep 2015.

Exposure | Environment

- Malicious physical access
  - Hardware tampering
  - Platform Theft
- Adversarial Interference
  - Compromised wireless network
  - Forceful termination or power loss
- Examples
  - Mobile public service robots

S. Morante, J. G. Victores, and C. Balaguer, “Cryptobotics: Why Robots Need Cyber Safety,” Frontiers in Robotics and AI, vol. 2, no. Sep 2015.

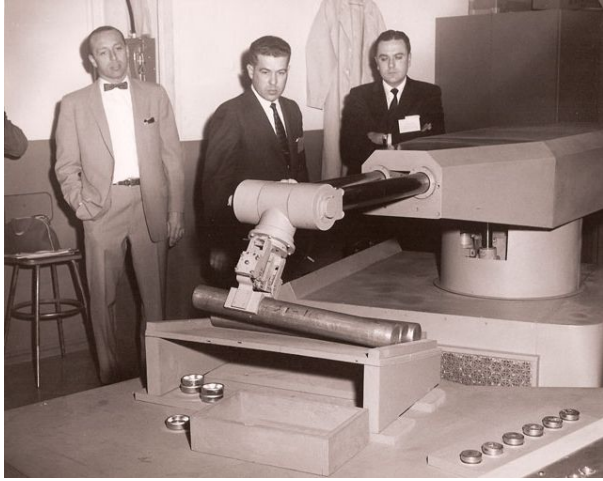
Exposure | Perception

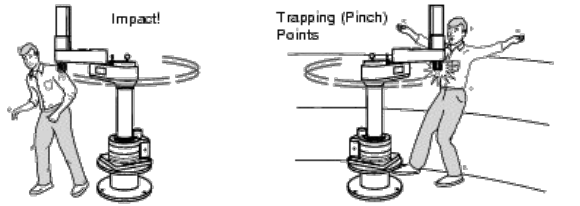
- Jamming
  - Degrading Signal to Noise Ratio
  - Damaging sensor from over exposure
- Spoofing
  - Synthesizing Falsified return signals
  - Truncating or silencing range measurements
- Examples
  - Ultrasonic, Cameras, LIDAR, Radar, GPS

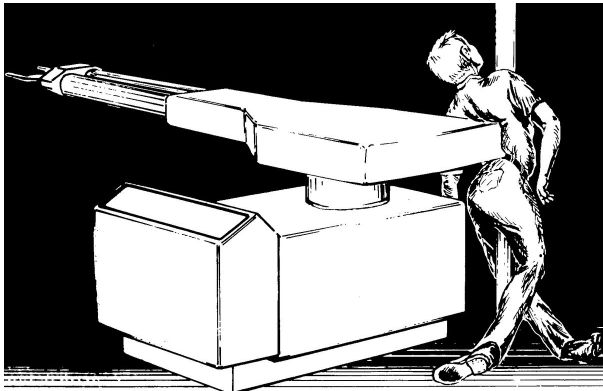
C. Yan, W. Xu, and J. Liu, “Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle,” DEF CON, vol. 24, 2016.

Exposure | Safety

- Reliability
  - Mission critical applications
  - Hazardous environments and materials
- Emergency procedures
  - Redundant failsafes
  - Graceful failure methods
- Examples
  - DDoSing E-stop channels
  - First recorded human death by robot occurred January 25, 1979, Ford factory in Flat Rock, Michigan







D. Portugal, S. Pereira, and M. S. Couceiro, “The role of security in human-robot shared environments: A case study in ros-based surveillance robots,” in 2017 IEEE International Symposium on Robot and Human Interactive Communication Aug 2017

T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, and H. J. Chizeck, “To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots,” arXiv preprint arXiv:1504.04339, 2015.

Exposure | Privacy

- Active and passive data collection
  - Audible and visual recording in the home
  - Meta information, e.g. floor plans, usage activity
- Data retention, ownership, and locality
  - Where, when, and what information can be logged
  - Where should data reside and for how long
- Social concerns
  - Mental health effects from continuously monitoring

W. K. Edwards and R. E. Grinter, “At home with ubiquitous computing: Seven challenges,” in Ubiquitous Computing, ser. UbiComp ’01, 2001

T. Denning, et. al, “A spotlight on security and privacy risks with future household robots: Attacks and lessons,” in International Conference on Ubiquitous Computing, ser. UbiComp ’09, 2009

Tutorial Overview

- Motivation
  - Cyber threats in Robotics
  - Existing attacks on ROS
  - Available pentesting tools
- Background
  - Secure DDS spec from OMG
  - Feature and performance analysis
  - Hands on classic Shapes Demo
- SROS2 Basics
  - Implementation details
  - Installation setup and runtime
- SROS2 Demos
  - Hands on examples
  - Using Comarmor and Keymint

Tutorial Logistics

Check the tutorial website for accompanying materials, references and additional documentation

Follow up discussion and notices will be posted to the original announcement on discourse.ros.org

- Tutorial Website
  - ruffsl.github.io/IROS2018_SROS2_Tutorial
- Discourse Announcement
  - discourse.ros.org/t/sros2-tutorial-iros-2018/5841