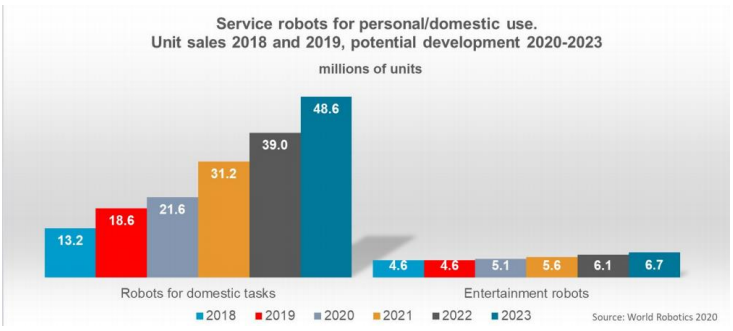
探秘 ROS 安全系列（一）

机器人操作系统 ROS 及其安全演进

1. 前言

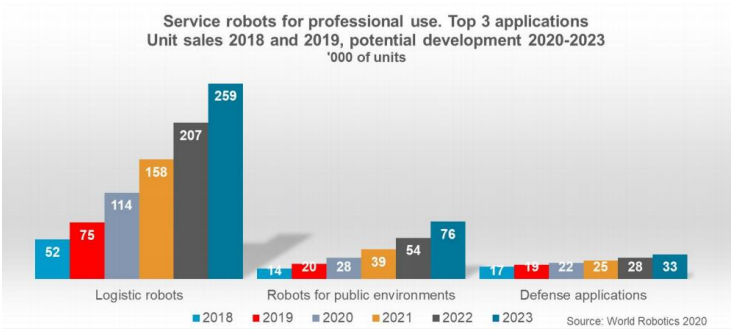
国际机器人联盟（IFR）将机器人划分成工业机器人 和服务机器人两类。工业机器人出现较早主要用于自动化制造领域，如焊接、装配等；服务机器人指用于非制造领域、以服务为核心的自主或半自主机器人，包括个人/家用服务机器人（扫地）、商用服务机器人（接待/巡检）、物流/仓储机器人（搬运/分拣）、医疗服务机器人（运送/辅助）等。IFR World Robotics 2020 预测服务机器人继续保持高速发展。



Personal/Domestic Service Robots

IFR International Federation of Robotics

Value of Sales:
2019: USD 5.7bn, +20%
2020: USD 6.5bn, +15%
2023: USD 12.1bn, +23% (CAGR)
Unit Sales:
2019: 23.2 million units, +34%
2020: 26.7 million units, +15%
2023: 55.3 million units, +27% (CAGR)



Professional Service Robots

IFR International Federation of Robotics

Value of Sales:
2019: USD 11.2bn, +32%
2020: USD 13.9bn, +24%
2023: USD 27.7bn, +26% (CAGR)
Unit Sales:
2019: 173,000 units, +32%
2020: 240,000 units, +38%
2023: 537,000 units, +31% (CAGR)

与传统工业机器人相比，服务机器人的工作环境更开放、网络连接更丰富、功能应用更智能，和用户、环境、数据的交互更深入，随着服务机器人在多领域推广应用，机器人的安全、数据和隐私保护等问题越来越受到关注。

当前服务机器人主流基于开源机器人操作系统 ROS 构建，故 ROS 系统安全性也成为研究热点。本文主要介绍机器人操作系统 ROS 及其安全演进，重点介绍机器人系统 ROS 安全风险和威胁、对应安全方案和演进趋势。

2. ROS 背景知识

2.1. ROS 发展简介

ROS（Robot Operating System）虽然名字叫操作系统，但并非传统意义的操作系统（如 Linux、Windows、Android 等），而是一种开源的机器人软件中间件（Robotics Middleware）。ROS 通过集成软件库、协议、工具等组件，构建适合多种机器人的通用软件框架，提高代码复用，降低开发难度，在机器人、无人机、自动驾驶等产品得到广泛应用。

ROS 项目最早可追溯到斯坦福大学的 STAIR（Stanford Artificial Intelligence Robot）和 PR（Personal Robotics） 研究项目。2007 年 Willow Garage 公司参与合作并基于 ROS 早期原型开发了 PR2 产品（Personal Robotics 2）。2010 年 1 月 ROS 1.0 (PR2 Milestone 3)第一个版本发布，2010 年 7 月 PR2 产品开始上线和销售。2012 年开源机器人基金会 Open Source Robotics Foundation（OSRF）成立，2013 年 ROS 项目移交给 OSRF（2017 年更名为 Open Robotics）并维护至今。

[图] ROS 1.0 logo

ROS 历史上有两个大版本，即 ROS 1.0 和 ROS2.0。为使 ROS 版本有相对稳定的开发环境，版本发布有节奏跟随 Ubuntu 发行版，详情可参考 ROS1 Release Schedule 或 ROS2 Release Schedule。

ROS 1.0 活跃版本信息如下左图所示，2020 年 Noetic 是 ROS 1.0 最后一个官方 LTS 版本。未来 ROS 社区主要发布和维护 ROS 2.0 版本。ROS 2.0 版本信息如下右图所示，最新 LTS 版本为 Foxy。

Distro	Release date	Poster	*Tuturtle*, turtle in tutorial	EOL date
ROS Noetic Ninjemys (Recommended)	May 23rd, 2020			May, 2025 (Focal EOL)
ROS Melodic Morenia	May 23rd, 2018			May, 2023 (Bionic EOL)
ROS Lunar Loggerhead	May 23rd, 2017			May, 2019
ROS Kinetic Kame	May 23rd, 2016			April, 2021 (Xenial EOL)

Distro	Release date	Logo	EOL Date
Foxy Fitzroy	June 5, 2020		May 2023
Eloquent Elusor	Nov 22nd, 2019		November 2020
Dashing Diademata	May 31st, 2019		May 2021

2.2. ROS 架构简介

2.2.1. ROS 1.0 架构

ROS 1.0 设计目标是解决：因缺乏通用软件组件，导致机器人应用或硬件有差异时，软件复用率低、开发量巨大的问题。应用场景主要聚焦在：专业用户（科研团队）、封闭环境（实验室等）、单机器人、无实时性要求等。**安全不在设计目标内。**

ROS 1.0 架构核心是基于 message 的松耦合、分布式架构。核心概念包括：

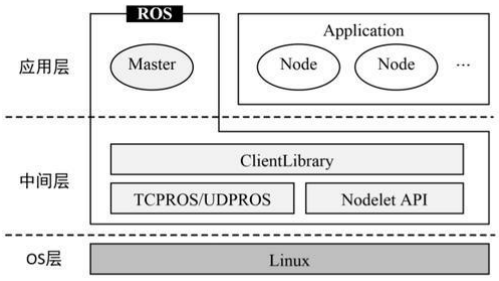
【Node】执行特定任务的进程。一个可执行程序可以创建一个或多个 node

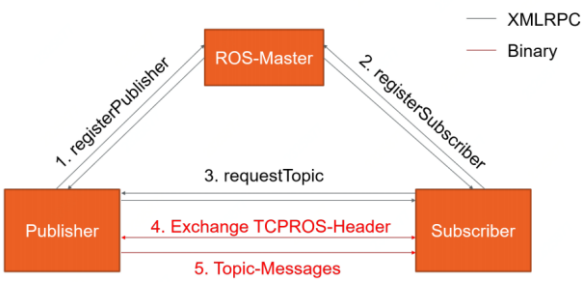
【Master】特殊 node，提供全局管理功能和服务，如参数服务、node 查找、消息注册等

【Message】node 之间的通信消息体，类似 OS 消息概念

【Topic】消息发布和接收的载体，publish-subscribe 机制，异步通信

【Services】另一种基于消息的通信机制，request-reply 机制，同步通信





2.2.2. ROS 2.0 架构

随着 ROS 1.0 和各种机器人产品应用推广，涌现了新的 ROS 需求，如多机器人支持、嵌入式平台支持、实时性需求、商用产品质量、开放环境等。同时开源社区也出现众多可借鉴的技术，如 **DDS（Data Distribution Service）数据分发服务**。在上述背景下，ROS 重新设计开发了 2.0 版本。

ROS 2.0 相比 ROS 1.0 的主要差异点可参考下图，主要在于 ：

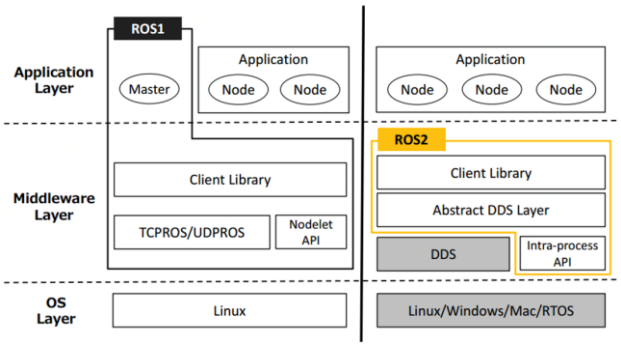
1）新特性：多机器人系统支持、良好的通信实时性、商用级代码质量、嵌入式平台支持

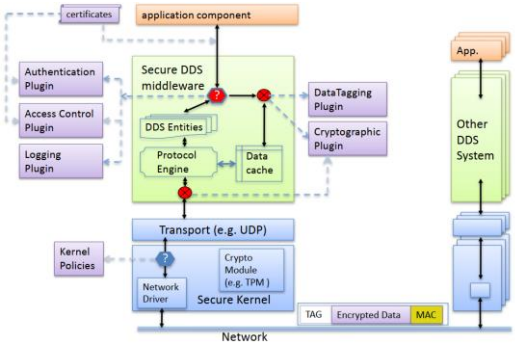
2）取消 master 节点，实现“去中心化”

3）引入 DDS 中间件，替换 ROS 1.0 自研消息通信机制

4）支持多种 Host OS 平台，如 Linux、Windows、Mac、RTOS

5）安全，DDS 协议有 5 大**安全标准**（下图 Plugin），ROS 2 利用 DDS 安全特性解决了身份认证、加密通信、访问控制等已知风险





2.3. ROS 系统搭建

ROS 作为中间件，需运行在 Host OS 之上。当前官方支持 Host 有 Ubuntu Linux、Windows、macOS。

以 Ubuntu 为例，ROS 支持 apt 安装和源码安装两种方式。读者可参考安装并运行 demo 体验 ROS 机制。

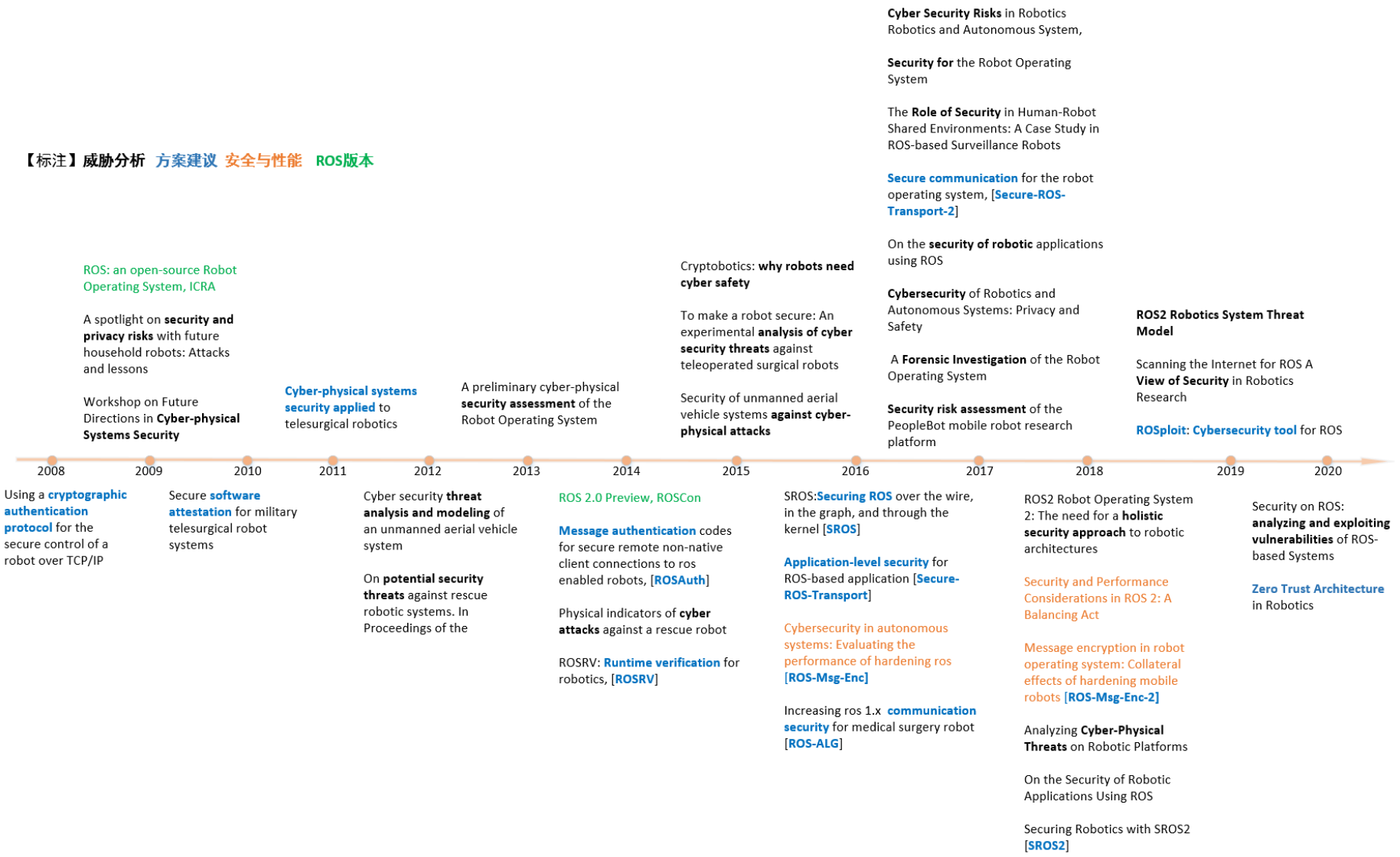
业界也有更丰富的机器人仿真环境，如 TurtleBot3 Simulation，感兴趣读者可自行参考。

3. 机器人安全分析

3.1. 安全研究

机器人系统是一种 Cyber-Physical System，特点是网络领域的威胁攻击最终可能影响到物理世界安全。我们回顾业界机器人安全研究文章（见下图），将其分为三个阶段：

第一阶段，2008-2012 年 ROS 发展初期，研究对象相对零散具体，表现在对特定机器人应用场景的威胁分析，比如救援机器人（Rescue Robot）、家用机器人（Household Robots）、远距医疗机器人（Telesurgical Robot）、无人机（Unmanned Aerial Vehicle）等。风险分析主要聚焦在远程通信和控制安全，如高效远程认证、远距医疗 ITP（Interoperable Telesurgery Protocol）协议等；另外也有相对综合性的分析，如对家用机器人和无人机产品的系统级安全和隐私分析。这些研究侧面反映了当时机器人缺乏统一底层框架、缺乏通用远程架构的情况。


【标注】威胁分析 方案建议 安全与性能 ROS版本
ROS: an open-source Robot Operating System, ICRA
A spotlight on security and privacy risks with future household robots: Attacks and lessons
Workshop on Future Directions in Cyber-physical Systems Security
Cyber-physical systems security applied to telesurgical robotics
A preliminary cyber-physical security assessment of the Robot Operating System
Cryptobotics: why robots need cyber safety
To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots
Security of unmanned aerial vehicle systems against cyber-physical attacks
Cyber Security Risks in Robotics Robotics and Autonomous System,
Security for the Robot Operating System
The Role of Security in Human-Robot Shared Environments: A Case Study in ROS-based Surveillance Robots
Secure communication for the robot operating system, [Secure-ROS-Transport-2]
On the security of robotic applications using ROS
Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety
A Forensic Investigation of the Robot Operating System
Security risk assessment of the PeopleBot mobile robot research platform
ROS2 Robotics System Threat Model
Scanning the Internet for ROS A View of Security in Robotics Research
ROSploit: Cybersecurity tool for ROS
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
Using a cryptographic authentication protocol for the secure control of a robot over TCP/IP
Secure software attestation for military telesurgical robot systems
Cyber security threat analysis and modeling of an unmanned aerial vehicle system
On potential security threats against rescue robotic systems. In Proceedings of the
ROS 2.0 Preview, ROSCon
Message authentication codes for secure remote non-native client connections to ros enabled robots, [ROSAuth]
Physical indicators of cyber attacks against a rescue robot
ROSRV: Runtime verification for robotics, [ROSRV]
SROS:Securing ROS over the wire, in the graph, and through the kernel [SROS]
Application-level security for ROS-based application [Secure-ROS-Transport]
Cybersecurity in autonomous systems: Evaluating the performance of hardening ros [ROS-Msg-Enc]
Increasing ros 1.x communication security for medical surgery robot [ROS-ALG]
ROS2 Robot Operating System 2: The need for a holistic security approach to robotic architectures
Security and Performance Considerations in ROS 2: A Balancing Act
Message encryption in robot operating system: Collateral effects of hardening mobile robots [ROS-Msg-Enc-2]
Analyzing Cyber-Physical Threats on Robotic Platforms
On the Security of Robotic Applications Using ROS
Securing Robotics with SROS2 [SROS2]
Security on ROS: analyzing and exploiting vulnerabilities of ROS-based Systems
Zero Trust Architecture in Robotics

第二阶段，2013-2017 年 ROS 1.0 发展成熟期，涌现了大量面向 ROS 机器人的安全分析和方案，相比第一阶段，研究对象更聚焦 ROS 框架，同时呈现许多新特征。具体如下：

2012 年 Defcon@20 会议现场，研究者举办了一个针对 ROS 小车的攻击测试，结果发表在 2013 年《A preliminary cyber-physical security assessment of the Robot Operating System (ROS)》论文中。测试显示，攻击者可成功发送指令控制小车，同时也出现了摄像头功能失效、本地控制主机硬盘错误等无法分辨是攻击还是软件异常的情况。一方面验证了 ROS 系统已知安全风险(如无身份认证、明文通信等)，一方面也反映了 Cyber-Physical 系统的复杂性。下图是该测试小车、软件架构、现场部署环境（图片引自上述论文）。

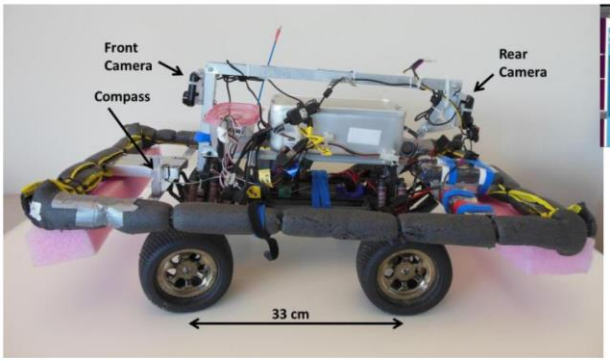


Figure 1. Cyber-physical security honeypot hardware.

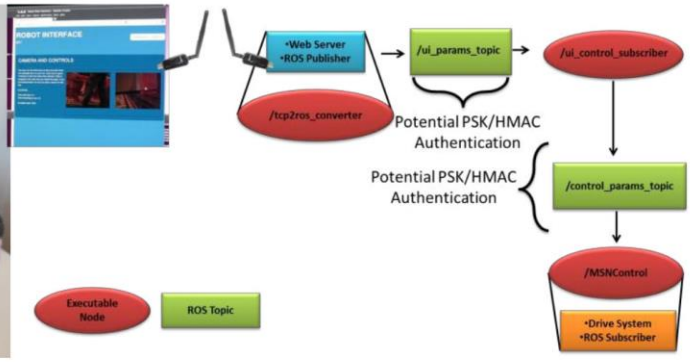


Figure 2. Honeypot software architecture.

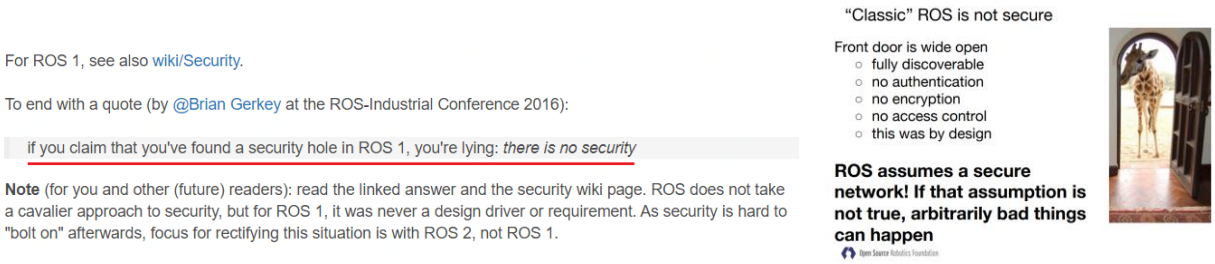
Figure 3. DEF CON 20 cyber-physical security honeypot contest/experiment setup.

Figure 4. Cyber-physical security honeypot located inside its cage.

该测试和论文成果开启了对 ROS 的安全研究热潮，并呈现出新趋势：从对单一机器人场景到共性安全问题分析、从对特定机器人架构到对通用 ROS 框架分析、从 ROS Application-level 应用层方案到 ROS 框架

通信层（Communication Channel）、从通信安全到系统访问控制、从安全特性到安全性能评估、从 ROS 框架安全到机器人全系统安全。

在这些分析过程中，ROS 1.0 框架主要安全风险充分暴露：匿名通信无身份认证、消息明文传输、缺少访问控制等。ROS 1.0 安全风险是有根源的，因为 ROS 1.0 设计之初就没有将安全作为目标和需求。关于这点，Open Robotics 的 CEO Brian Gerkey 在 2016 年 ROS-Industrial Conference 有过如下表述“**If you claim that you've found a security hole in ROS 1, you're lying; there is no security**”。



在此阶段，也涌现了多个针对 ROS 1.0 主要风险的安全方案，如 roauth、ROSRV、SROS 等。方案详情请参考 4.1 章节。

2017 年《The Role of Security in Human-Robot Shared Environments A Case Study in ROS-based Surveillance Robots》文章是一次综合考虑风险和消除方案、定制化安全（如多机器人通信协同）需求、全系统设计的尝试。下图是其 STOP R&D 项目综合安全分析和消除方案。

Security Level	Security Measurement
Wireless Network	• WPA2 + AES security • SSID hiding • MAC ID filtering • Static IP addressing
PHP GUI	• Binded to SSL/HTTPS • MVC AUTH and SSL websocket to cloud • SSL TCP/IP to low-level monitoring and control of robot
Cloud server	• SSL TCP/IP to robot-ARM • Firewall rules allowing traffic on specific ports • Disable SSH root login • Enable login with SSH keys • Strong (console) user password
roslibjs + *rosbridge* (human↔robot)	• Authentication (*rosauth*) • TLS/SSL encryption
ROS Multimaster (robot↔robot)	• Authentication and authorization levels • Encryption of ROS messages
ROS	• Running inside a VPN • Not using default ROS ports • Encryption of ROS messages
Operating System	• Firewall rules allowing traffic on specific ports from specific IPs • Disable SSH root login • Enable login only with SSH keys • Strong (console) user password
Disk	• Encryption of data storage • Logging connections and events
Hardware	• ARM controller connected to an independent battery sends keepalive packet and allows to receive low-level commands (*e.g.*, teleoperation) • Developer authentication (microprocessor bootloader)

第三阶段，2018 年后 ROS 2.0 发展期，随着 2.0 架构升级和 DDS 集成，安全研究呈现两个特点，一是研究对象从 ROS 1.0 过度到 ROS 2.0，二是对安全方案性能的分析。

首先，ROS 2.0 采用 DDS 替换了 ROS 1.0 自研的 publish-subscribe 通信机制。而 DDS 本身有 Security 安全协议规范，因此 ROS 2.0 安全主要基于 DDS-Security。ROS 2.0 中 DDS-Security 默认不使能，使能 DDS-Security 需打开配置并重新编译。

《Robot Operating System 2: The need for a holistic security approach to robotic architectures》综合分析了 ROS2 系统的安全风险，并针对 DDS-Security 使能和安全配置项（如 governance policy）对性能影响进行了定性分析。

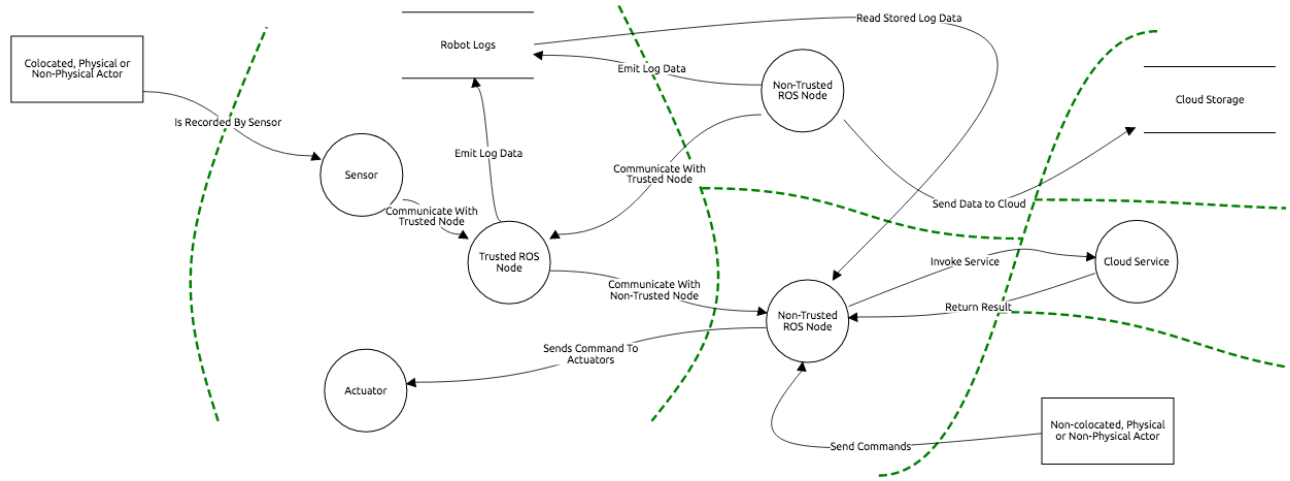
也有对具体性能的定量分析。如《Message encryption in robot operating system: Collateral effects of hardening mobile robots》继承 2016 年性能分析文章，评估 3 种算法（3DES、AES、Blowfish）对不同类型消息加密后的性能（时延、吞吐量）、系统（网络负载增量、CPU 占用率、电池损耗）的影响，提出了针对不同消息类型，有策略的选择加密算法的观点。《Security and Performance Considerations in ROS 2: A Balancing Act》针对 ROS2 使能 DDS-Security 进行了深度分析，对比了 ROS 2、ROS 2 + DDS Security Enable、ROS 2 + VPN 三种场景下通信性能指标，结果显示使能 DDS-Security 时性能均有不同程度劣化。

上述针对 ROS 2+DDS 的定性和定量分析，都显示使能 DDS-Security 安全后性能下降比较严重。但同时也应该注意到，ROS 2 +DDS-Security 实际是可以根据安全需求进行精细化配置的，性能调优有较大空间。

3.2. 威胁建模

在业界关于机器人系统安全研究基础上，ROS 社区创建了 ROS 2 Threat Model 威胁分析模型，对基于 ROS 2 的机器人系统，进行了全方位的威胁建模。采用业界标准的 STRIDE 和 DREAD 分析方法，定义系统元素并绘制数据流图，再对各元素进行威胁分析、制定风险消除方案。分析维度全面，可归纳概括有：内外部通信、远程控制/应用接口、主机系统和内核、端侧数据存储、云服务和云存储、云-端通信服务等。

下图是 ROS 2 系统通用 STRIDE 数据流图。实际上针对具体产品，由于通信方式、业务功能、云-端服务部署等差异，数据流图可能要复杂的多，需要具体分析。可参考 Turtlebot3 的威胁分析。



3.3. 安全设计

在上述安全研究和威胁建模分析过程中，业界对 ROS 安全方案设计主要有两种思路：

一种是网络隔离，即利用专网、VPN、防火墙等手段，构建 ROS 网络隔离区，缩小风险面。

另一种是基于 ROS 框架进行安全加固，代表有前文提到的 ROS 1.0 阶段的 rosauth、ROSRV、SROS 等、以及 ROS 2.0 阶段的 SROS2。