# Tallinn University of Technology ISEAuto - Reference Architecture for Secure Remote Communication

Andrew Roberts, Pavel Tšikul, Olaf Maennel
TalTech Centre for Digital Forensics and Cyber Security

## Introduction

Remote control operations centres are an important facility for the safety and security of automated vehicular transportation management. A reference architecture for the security of the remote communication of the ISEAuto automated vehicle is vital to allow the ISEAuto to securely function on roads and test environments in accordance with EU and Estonian law requiring a driver to have control of the vehicle. The objectives of this document are to provide recommendations for security of remote communication function of ISE Auto.

## Background/Related Work

The ISEAuto uses a mixture of Wireless 802.11g and 4G data link for connectivity. The top speed of the ISEAuto is limited at 20 km/h. The ISEAuto is currently tested with a control operator inside the vehicle during operation. This is to ensure if there is any anomalous activity the emergency brake within the vehicle can be activated. The vehicle can be controlled via two methods:

> Method 1 - An operator can use the Control Computer with OpenVPN that uses SSL/TLS key exchange and driving commands can be sent to the vehicle using UDP.
>
> Method 2 - A local, wireless, remote control which uses Bluetooth connectivity connecting via usb dongle on the control computer.

ISEAuto has cameras installed within the vehicle to monitor passenger safety. In case of loss of connectivity the ISEAuto has a requirement for graceful degradation of services to shut down operations intelligently [1].

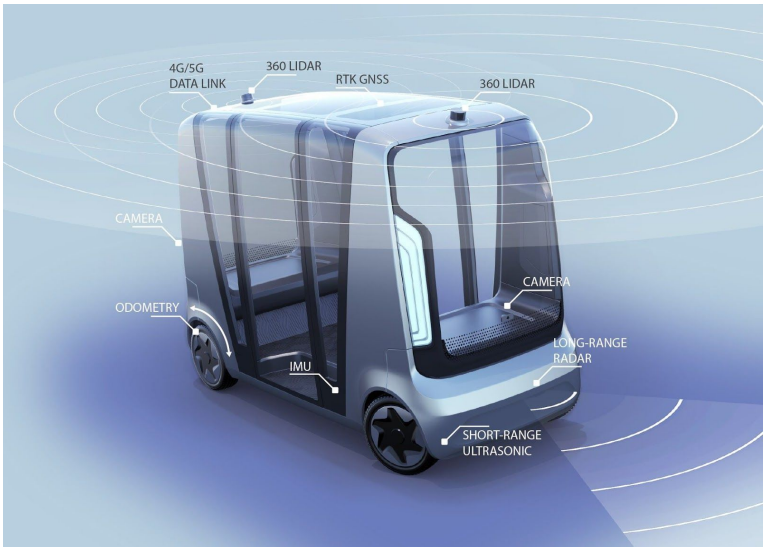


Figure 1: Sensonics and Connectivity of ISEAuto[2]

The Remote Operations Control Center is comprised of a remote facility for which an operator can login to the ROS application, view the environmental vision of the automated vehicle and make driving decisions as required. The experience of remote operations can be enhanced using real world simulation technologies such as virtual reality and steering wheels and brake pads. It is envisioned for the ISEAuto that the Remote Control Station will be located at the Tallinn University of Technology campus and be able to support the ISEAuto in varying traffic environments in and around the campus and at various locations in Tallinn[3].

Figure 2: Remote Operations Control Center for Automated Vehicular Support[4]

A State-Of-The-Art review of available standards of cyber security for automated self-driving vehicles found the most prominent are: The British Standards Institute Publication PAS:1885 - Fundamental Principles of Automotive Cyber Security and ENISA

Good Practices for security of Smart Cars. Applicable to the remote control facility of the ISEAuto, PAS:1885 lists the following cyber security requirements[5]:

> “5.1.3 The organization’s board-level management shall establish, document and operate policies, processes and procedures such that all new designs are conceived and implemented using a product and/or service lifecycle that embraces Secure-by-Design”[5, p.14].

> “7.5 The vehicle and equipment provide appropriate logging and audit functionality for connected devices, with non-repudiation built in to the logging process” [5, p.31-31]

The ENISA Good Practices for Security of Smart Cars section 4.2 also provides an extensive list of requirements for detection, protection of networks and protocols, software security, cloud security, cryptography, access control and cyber resiliency[6]. From the ENISA requirements definition the Remote Control facility should take these requirements into account in the solution:

> “TM-06: Protect remote monitoring and administration interfaces through mutual authentication and access control mechanisms to prevent illegitimate access to smart cars systems” [6. p.31].

> “TM-08: Protect the integrity and authenticity of all external communications between the smart cars and all the different entities it is interacting with” [6. p.31].

> “TM-14: Provide end-to-end protection of sensitive data in terms of confidentiality and integrity using secure protocols” [6, p.31].

> “TM-35: Segregate remote access by developing a set of rules for the control and monitoring of remote communications” [6, p.32].

The secure architecture of the remote control operations centre must support the following functional requirements specified by the ISEAuto engineering team:

> “FR 2.2 Safe stop in case of loss of communication. Ability for a remote driver person in the control room to oversee, select, take over and manually drive one selected vehicle at a time, remotely as the designated driver”[3].

These two functional requirements limit the impact of cyber attack:

> “FR 2.9 Capability of emergency stopping one or all of the buses quickly”[3].

> “FR 7.6 Electrically driven Emergency stop buttons inside the vehicle and Remote stop (that can be operated outside the vehicle)”[3].

The same system requirements will be used for secure remote connection as was used for monitoring and communications solution for video streaming[7].

> “SR1.0  Data extraction does not influence the Linux machine that controls the ISEAuto;”[7, p.2]
>
> “SR 1.1 Data must secured with encryption during the data transfer;” [7, p.2]
>
> “SR 1.2 ISEAuto’s visualization must present the basic parameters (such as alert indications, speed, weather conditions etc), live camera streams and LIDAR image streams.” [7, p.2]

The ISEAuto project including the design and conduct of experimental testing is governed by EU and Estonian legislation. Systems that process data gathered from autonomous vehicles must comply with the European General Data Protection Directive. The ISE Auto must comply with the basic traffic rules covered under the Vienna Convention on Road Traffic [8, p.23]. In 2016, amendments to the Vienna Road Traffic Convention that included conditions for research and development of autonomous vehicle technologies were adopted. These stipulate that autonomous self-driving vehicles can be used in traffic, however, on the condition that these technologies are in conformity with the United Nation's vehicle regulations and that the driver has the ability to take control over the driving. Estonian law, as covered in the Traffic Act, requires a vehicle to have  a driver and this definition assumes that the driver is in control of the vehicle and attentive to pedestrians and environmental surroundings[8, p.33-35]. In 2017, the Estonian Ministry of Economics Affairs and Communication announced that the test driving of autonomous vehicles (defined as SAE level 2 or 3) is allowed on the streets and roads of Estonia, however, the car must have a driver who is able to take control of the car at any time needed, additionally the driver can sit within the vehicle or act remotely, but is still responsible for the vehicle and must take control if necessary. It is for these reasons that the remote control function of the ISEAuto must be available and secure for use[9].

## Methodology

The methodological approach is as follows:

- Conduct a State-of-the-Art review of standards for automotive cyber security, legal environment and ISEAuto functional requirements.
- Model the existing ISEAuto communication security
- Provide recommendations for the Remote Control Station based on the State-of-the-Art review

## Results

*Communications Security*

### Existing Implementation

Latency and network signal analysis tests of Telia 5G and Elisa EE 4G have been conducted. The tests have shown the stability of 4G connectivity and concluded that further development of the 5G infrastructure is required for use of that technology [10]. Current expectations of 4G is; theoretical maximum of 150 Mbps, real life expectation 25 Mbps. In case of latency issues, the ISEAuto will graceful degrade the cellular services (4G - 3G - 2G - GSM). The signals coverage analysis has already identified areas of poor coverage in Tallinn and this is a factor in the selection of pre-programmed transportation routes.The ISEAuto have also experimented with the network requirements of video streaming. Their experimentation found that the optimal video bitrate is 560 kbps and that h265 (HEVC) compression should be used to further decrease bitrate and reduce latency[11].

The ISEAuto has used secure-by-design principles to build the communication channel for the monitoring and communication from the control computer in the vehicle to the monitoring server. OpenVPN is used on the control computer and data transfer is encrypted from the control computer to the monitoring server in the TalTech environment using TLS/SSL key exchange. RTSP is used for application layer for video streaming, MQTT for Data Transfer and UDP is used for transport layer communication[7, p.5-6].

### Recommendations

The Pylot Remote Control Station solution used by ISEAuto is a module on the Robotic Operating System. It utilises a VPN. Best practice to avoid man-in-the-middle attacks is to use certificate [7, p.16-18] pinning. Pylot opens these UDP ports 12-20.

ISEAuto should implement of h265 (HEVC) compression for reduction in bandwidth requirements of video streaming. This will ensure greater quality of service for remote communication traffic[11].

The bluetooth remote is vulnerable to jamming and override attacks such as BlueBorne. It would be optimal for a wired controller to be used, otherwise regular scanning of bluetooth vulnerabilities as part of security testing will be required[12].

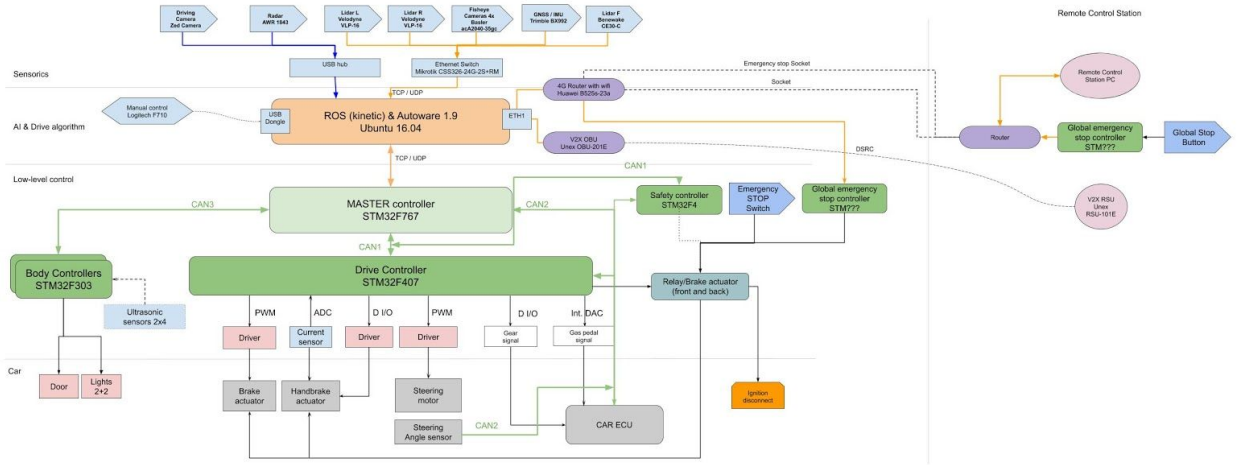


Figure 3: Connectivity Architecture of ISEAuto [13]

*Application Security*

Existing Implementation

As the robotic operating system (ROS) is an integral part of the Remote Communication Solution, the ISEAuto need to ensure that it is secure to cyber attacks. ROS is an open source platform built for research. It was built with no consideration for security.In the ROS architecture networked nodes act to facilitate actions and motions of physical systems enabling real-world actions of the ISEAuto. The ROS1, the version used by ISEAuto, the architecture has no security features for communication between nodes. The current security model for ROS in the ISEAuto is to provide security for system access using multi-factor authentication and network access using TLS/SSL VPN. In the current architecture, there is little available protection if an attacker is able to access the ROS, they will have full access to ISEAuto system functionality. There an exhaustive list of potential attacks on ROS (Appendix 3 [14]).

Recommendations

It is recommended that the ISEAuto team consider, for future planning, for the ROS1 to be updated to the latest version ROS2. This needs to be carefully considered as ROS2 is a different architecture to ROS1, it uses the Data Distribution Standard (DDS) to include authentication, encryption and process profile features. It uses a peer-to-peer connection to securely communicate between nodes. Each node has to be trusted through use of certificates [15]. ROS2 has a significant working community and ISEAuto engineers should actively engage with the it's working groups: embedded, navigation, safety, security, technical and tooling [16].

Other approaches include Secure ROS(SROS) which can be included in ROS1. SROS focuses security at the transport layer, using IPSec in transport mode and modified versions of the ROS master, rospy module and roscpp library to ensure secure communication [17].

*Access and Authentication Security*

Current Implementation
Access and authentication to the secure operations control center need to be considered for security, audit and logging purposes. The authentication system should support multi-factor authentication using a cryptographic hard token. Currently, ISEAuto meet this requirement by using YubiKeys which are unique to each authorised user. Physical access to the Remote Control Station at the TalTech campus is currently controlled through the use of TalTech access cards.

Recommendation
The ISEAuto team need to ensure proactive use of their multi-factor authentication solution. If usability is an issue then other solutions such as the Estonian ID Card for the hard cryptographic token should be explored. Entrance to the remote control facility should continue to be limited to authorised personnel only with use of TalTech staff ID card.

*Logging and Auditability*

Current Implementation
User access to the system and activity of the user needs to be logged in order to understand, for forensic and compliance purposes; who had access to the system, at what time and what actions did they perform. Logging and auditability should be expanded with ROS logs and other system logs. It is recommended that the log locations are more organized and/or documented.

Recommendation
For traceability, it is advised that access to the system needs to ensure that the individual accessing the system is uniquely identified. Video captures need to be stored. It is recommended for storage reasons these captures be compressed in an archive solution in order to preserve captures of a greater longevity. It is recommended that network monitoring of traffic associated with the ISEAuto is captured. Potentially, this could be a SPAN port on the in-car switch.

## Conclusion

The ISEAuto has been built with good manual security controls to limit the impact of cyber attack. These include the emergency stop button, internal and external to the car. The extension of control functionality to a remote control station introduces potentiality of attack using the communications channels of WiFi, 4G and 5G to infiltrate the control application to manipulate the ISEAuto. This report recommends that the ISEAuto validate that the Pylot Remote Control system uses VPN for encrypted communications with certificate pinning to reduce the potential for man-in-the-middle attacks. Other security controls recommended include hardening the vulnerable ROS system, using multi-factor authentication for user access, physical security and implementation of logging and

auditability of the car cameras and remote communication traffic. ISEAuto need to continue this proactive approach of designing systems to mitigate cyber security risks.

## References


1. Tallinn University of Technology ISEAuto Project Team, *TalTech Iseauto. 4/4: The overview of the bus*, 12. 20. 2018 Accessed on 20.11.2019.[Online]. Available: https://iot.ttu.ee/taltech-iseauto-4-4-testid-ja-tulemused/
2. Tallinn University of Technology ISEAuto Project Team, *TalTech Iseauto. 4/4: The overview of the bus*, 12. 20. 2018. Accessed on 11.20.2019.[Online]. Available:https://iot.ttu.ee/taltech-iseauto-3-4-bussi-ehitamine/
3. R.Sell, *Fabulos_demo_2019.10.03*. Tallinn, 2019.
4. Pylot, *Pylot teleoperation for autonomous vehicles*. Accessed on 11.20.2019 [Online]. Available: https://www.pylot.tech/
5. British Standards Institute, *PAS 1885:2018The fundamental principles of automotive cyber security – Specification*, London: The British Standards Institution. December 2018. Accessed on 10.11.2019.[Online]. Available: https://webstore.ansi.org/standards/bsi/pas18852018
6. European Union Agency for Cybersecurity, *ENISA Good Practices for Security of Smart Cars*, November 2019. Accessed on 11.27.2019. [Online]. Available: ISBN 978-92-9204-317-9, DOI 10.2824/17802: https://www.enisa.europa.eu/publications/enisa-good-practices-for-security-of-smart-cars
7. A. Koodi, *ISEAuto project: Data monitoring and communication*. Tallinn, 2017.
8. K. Lillemäe, *Bachelor Thesis: The legal issues regarding the regulation of autonomous vehicles in the european union.* Tallinn: Tallinn University of Technology, School of Business and Governance, Department of Law. , 2017. Accessed on 10.30.2019. [Online]. Available: https://digi.lib.ttu.ee/i/file.php?DLID=8382&t=1
9. Republic of Estonia Government, *Self-driving vehicles waiting for a new law*. Tallinn: Estonian Government Press Release, 10.15. 2019. Accessed on 10.30.2019. [Online]. Available: https://www.valitsus.ee/en/news/self-driving-vehicles-waiting-new-law
10. P.Ruberg, *4G/5G signaali mõõtmised*. Tallinn, 2019.
11. R. Sell, *Network Measurement Methodology*. Tallinn, 2019.
12. Armis, *The Attack Vector "BlueBorne" Exposes Almost Every Connected Device*. 2019. Accessed on 11.26.2019. [Online]. Available: https://www.armis.com/blueborne/
13. R.Sell, *Vehicle v2 hardware diagram*. Tallinn, 2019.

14. Open Source Robotics Foundation, *ROS 2 Robotic Systems Threat Model*, 2019. Accessed on 11.20.2019. [Online]. Available: https://design.ros2.org/articles/ros2_threat_model.html

15. ROS2 Index, *ROS2 Documentation.* 2019. Accessed on 11.20.2019. [Online]. Available: https://index.ros.org/doc/ros2/

16. Fkromer, *Github Repository: Awesome Robot Operating System 2 (ROS 2)*, 2019. Accessed on 11.20.2019. [Online]. Available: https://fkromer.github.io/awesome-ros2/

17. A. Sundaresan, Secure ROS 0.9.2 documentation, 2019. Accessed on 11.22.2019. [Online]. Available: https://sri-csl.github.io/secure_ros/

# Appendix 1 - Robotic System Threat Model (Example Threats) [14]

| Threat Description | Threat Category (STRIDE) | | | | | | Threat Risk Assessment (DREAD) | | | | | | Impacted Assets | | | | | | | Impacted Entry Points | | | | Mitigation Strategies | Similar Attacks in the Litterature |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Spoofing | Tampering | Repudiation | Info. Disclosure | Denial of Service | Elev. of Privileges | Damage | Reproducibility | Exploitability | Affected Users | Discoverability | DREAD Score | Robot Compute Rsc. | Physical Safety | Robot Avail. | Robot Integrity | Data Integrity | Data Avail. | Data Privacy | Embedded HW | Robot Comm. Channels | Robot Admin. Tools | Remote App. Interface | Deployment Infra. | | |
| **Embedded / Software / Communication / Inter-Component Communication** | | | | | | | | | | | | | | | | | | | | | | | | | |
| An attacker spoofs a component identity. | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | 3 | 1 | 1 | 2 | 3 | 10 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | • Components should authenticate themselves.<br>• Components should not be attributed similar identifiers.<br>• Component identifiers should be chosen carefully. | Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots." ArXiv:1504.04339 [Cs], April 16, 2015. |
| An attacker intercepts and alters a message. | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | 3 | 3 | 3 | 3 | 3 | 15 | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ▲ | ✗ | ✓ | ✗ | ✗ | ✗ | • Messages should be signed and/or encrypted. | Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots." ArXiv:1504.04339 [Cs], April 16, 2015. |
| An attacker writes to a communication channel without authorization. | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | 3 | 3 | 3 | 3 | 3 | 15 | ✗ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | • Components should only communicate on encrypted channels.<br>• Sensitive inter-process communication should be done through shared memory whenever possible. | Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots." ArXiv:1504.04339 [Cs], April 16, 2015. |
| An attacker listens to a communication channel without authorization. | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | 2 | 3 | 3 | 3 | 3 | 14 | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | • Components should only communicate on encrypted channels.<br>• Sensitive inter-process communication should be done through shared memory whenever possible. | Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots." ArXiv:1504.04339 [Cs], April 16, 2015. |
| An attacker prevents a communication channel from being usable. | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | 3 | 3 | 3 | 3 | 3 | 15 | ✓ | ▲ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | • Components should only be allowed to access channels they require.<br>• Internet-facing channels and robot-only channels should be isolated.<br>• Components behaviors should be tolerant of a loss of communication (e.g. go to x,y vs set velocity to vx, vy). | Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots." ArXiv:1504.04339 [Cs], April 16, 2015. |
| **Embedded / Software / Communication / Long-Range Communication (e.g. WiFi, Cellular Connection)** | | | | | | | | | | | | | | | | | | | | | | | | | |
| An attacker hijacks robot long-range communication | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | 3 | 2 | 1 | 3 | 1 | 10 | ✗ | ✓ | ▲ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | • Long-range communication should always use a secure transport layer (WPA2 for WiFi for instance) | Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots." ArXiv:1504.04339 [Cs], April 16, 2015. |
| An attacker intercepts robot long-range communications (e.g. MitM) | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | 1 | 2 | 1 | 3 | 1 | 8 | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | • Long-range communication should always use a secure transport layer (WPA2 for WiFi for instance) | Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots." ArXiv:1504.04339 [Cs], April 16, 2015. |
| An attacker disrupts (e.g. jams) robot long-range communication channels. | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | 2 | 2 | 1 | 1 | 3 | 9 | ✗ | ▲ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ | • Multiple long-range communication transport layers should be used when possible (e.g. cellular and WiFi) | Bonaci, Tamara, Jeffrey Herron, Tariq Yusuf, Junjie Yan, Tadayoshi Kohno, and Howard Jay Chizeck. "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots." ArXiv:1504.04339 [Cs], April 16, 2015. |
| **Embedded / Software / Communication / Short-Range Communication (e.g. Bluetooth)** | | | | | | | | | | | | | | | | | | | | | | | | | |
| An attacker executes arbitrary code using a short-range communication protocol vulnerability. | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | 3 | 2 | 1 | 1 | 3 | 10 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | • Communications protocols should be disabled if unused (by using e.g. rfkill).<br>• Binaries and libraries required to support short-range communications should be kept up-to-date. | Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." In Proceedings of the 20th USENIX Conference on Security, 6–6. SEC'11. Berkeley, CA, USA: USENIX Association, 2011. |

| | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Embedded / Software / Communication / Remote Application Interface** | | | | | | | | | | | | | | | | | | | | | | | |
| An attacker gains unauthenticated access to the remote application interface. | ✓ | ✓ | ✗ | ✓ | ✓ | ▲ | 3 | 3 | 1 | 1 | 3 | 11 | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | • Implement authentication and authorization methods.<br>• Enable RBAC to limit permissions for the users. | |
| An attacker could eavesdrop communications to the Robot's remote application interface. | ✗ | ✗ | ✗ | ✓ | ✗ | ✗ | 1 | 1 | 1 | 1 | 3 | 7 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | • Communications with the remote application interface should be done over a secure channel. | |
| An attacker could alter data sent to the Robot's remote application interface. | ✓ | ✓ | ✗ | ✓ | ✓ | ▲ | 3 | 3 | 1 | 1 | 3 | 11 | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ | • Communications with the remote application interface should be done over a secure channel. | |
| **Embedded / Software / OS & Kernel** | | | | | | | | | | | | | | | | | | | | | | | | | | |
| An attacker compromises the real-time clock to disrupt the kernel RT scheduling guarantees. | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | 3 | 2 | 1 | 3 | 2 | 11 | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | • Hardened kernel (prevent dynamic loading of kernel modules)<br>• Ensure only trustable kernels are used (e.g. Secure Boot)<br>• /boot should not be accessible by robot processes<br>• NTP security best practices should be enforced to ensure no attacker can manipulate the robot computer clock. See also RFC 7384, NTPsec and Emerging Solutions in Time Synchronization Security. Additionally, PTP protocol can be considered instead of NTP. | Dessiatnikoff, Anthony, Yves Deswarte, Eric Alata, and Vincent Nicomette. "Potential Attacks on Onboard Aerospace Systems." IEEE Security & Privacy 10, no. 4 (July 2012): 71–74. |
| An attacker compromises the OS or kernel to alter robot data. | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | 3 | 2 | 1 | 3 | 2 | 11 | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | • OS user accounts should be properly secured (randomized password or e.g. SSH keys)<br>• Hardened kernel (prevent dynamic loading of kernel modules)<br>• Ensure only trustable kernels are used (e.g. Secure Boot)<br>• /boot should not be accessible by robot processes | Clark, George W., Michael V. Doran, and Todd R. Andel. "Cybersecurity Issues in Robotics." In 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), 1–5. Savannah, GA, USA: IEEE, 2017. |
| An attacker compromises the OS or kernel to eavesdrop on robot data. | ✗ | ✗ | ✓ | ✗ | ✗ | ✗ | 1 | 2 | 1 | 3 | 2 | 9 | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | • OS user accounts should be properly secured (randomized password or e.g. SSH keys)<br>• Hardened kernel (prevent dynamic loading of kernel modules)<br>• Ensure only trustable kernels are used (e.g. Secure Boot)<br>• /boot should not be accessible by robot processes | Clark, George W., Michael V. Doran, and Todd R. Andel. "Cybersecurity Issues in Robotics." In 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), 1–5. Savannah, GA, USA: IEEE, 2017. |