

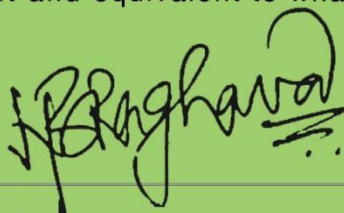
CAPELLA CYBER SECURITY REPORT

17th May 2019

TEAM MEMBER	EMAIL ID
Divye Bhutani (Captain)	bhutanidivye@yahoo.com
Adhiraj Singh	adhirajsingh1206@gmail.com
Sahil Singh Bhatia	sahil.singh.bhatia@gmail.com
Yusuf Ali	thephysicist2025@gmail.com



I hereby certify, as the faculty advisor, that the design and engineering of the vehicle outlines in this report to be entered in the 2019 Intelligent Ground Vehicle Competition has been significant and equivalent to what might be awarded credit in a senior design course.



Dr. N.S Raghava

Faculty Advisor
Department of ECE
Email - nsraghava@dce.ac.in

Contents

1	Introduction	3
2	Team Organization	3
3	Overview of NIST RMF Process.....	3
3.1	Prepare	4
3.2	Categorize	4
3.3	Select.....	4
3.4	Implement.....	4
3.5	Assess.....	4
3.6	Authorize	4
3.7	Monitor.....	4
4	Threat Concept.....	5
5	Threat Modelling.....	5
5.1	Security category vs Security impact level.....	5
5.2	Information needed to categorize an information system.....	6
5.3	Information system boundaries	6
5.4	7
5.5	Types of information process by information systems.....	7
6	Identification and Mapping of Cyber Controls.....	7
6.1	Defense-in-Depth.....	7
6.2	Technology based controls.....	7
6.3	Management and Operational Controls	9
6.4	Security policy	10
6.5	Holistic approach to information security.....	12
7	Description of implemented cyber controls.....	13
7.1	Relation of chosen controls to mitigated risks.....	13
7.2	Design and implementation details of controls.....	13
7.3	Appropriate but unimplemented controls	14
7.3.1	Biometric authentication	14
7.3.2	Physical locks	14
8	Cyber Controls Demonstration Strategy.....	14

1 Introduction

Zephyr is the autonomous ground vehicle team of Delhi Technological University, India. We are a group of highly driven and motivated polymaths who develop, envision and engineer cutting-edge technology in the field of autonomous mobility. With the inception of Cyber Security Challenge in IGVC 2019, we got an opportunity to explore the domain of vehicle security and familiar ourselves with the best practices adopted to mitigate the risks induced by cyber threats. We believe this is a great initiative from the organizers pertaining to the fact that cyber security has now become a serious issue that must be addressed by every organization which makes it an integral part of any product development. It is with great pleasure that we introduce our cyber security system for our vehicle *CAPELLA* in Intelligent Ground Vehicle Competition 2019.

2 Team Organization

We believe that team work is at the heart of any great achievement. Our goal was not just to develop an autonomous vehicle security system but to build an environment which nurtures team and individual's growth simultaneously. To ensure that the team functions as a well-oiled machine, we ascertained that there exists good communication and effective knowledge transfer among team members so that every member shares a common vision.

Cyber security challenge compelled us to delve into the domain in which we possessed no prior knowledge or experience. In order to get started we adhered to the guidelines mentioned in the competition rule book and also consulted with professionals working in this field to attain an insight of the problem statement. To begin with task of acquiring the knowledge, we assigned few team members which were held responsible for this challenge and then we initiated our learning of this subject from massive open online courses. Once we attained understanding in this subject, we bridged the gap between theory and practical through our pre-acquired computing skills and experience in working with several software languages and frameworks. The implementation task was undertaken by the whole team and was led by the think tank initially designated for this challenge. This ensured holistic development of individuals and the Capella project as a whole.

TEAM MEMBER	MAJOR	ROLE
Adhiraj Singh	Computer Science	Common Control Provider
Divye Bhutani	Software Engineering	System Owner/ Team Leader
Sahil Bhatia	Engineering Physics	Chief Information Officer
Yusuf Ali	Mechanical Engineering	Control Assessor

3 Overview of NIST RMF Process

With latest developments in interconnected world (information system and devices), security and privacy risks have been increased in recent years due to complexity in hardware, software and firmware; this increases the attack surface that can be exploited by adversaries by various attack vectors to compromise integrity of systems.

The National Institute of Standards and Technology is a physical sciences laboratory which worked in partnership with Department of Defense, to develop a Risk Management Framework (RMF) to improve information security, strengthen risk management processes, and encourage reciprocity among organizations.

We developed our comprehension of the RMF processes by referring to the latest publication **NIST SP 800-37 REV 2** released in December 2018.

There are seven steps in the RMF; a preparatory step addition is to ensure that organizations are ready to execute the process and six main steps. All seven steps are essential for the successful execution of the RMF, as discussed below.

3.1 Prepare

The purpose of the Prepare step is to carry out essential activities at the organization, mission and business process, and information system levels of the organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework. Individuals are identified and assigned key roles, a risk management strategy for the organization that includes a determination and expression of organizational risk tolerance is established.

3.2 Categorize

The purpose of the Categorize step is to inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability (CIA) of organizational systems and the information processed, stored, and transmitted by those systems.



3.3 Select

The purpose of the Select step is to select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation. Control baselines necessary to protect the system commensurate with risk are selected and tailored according to organization’s control baselines.

3.4 Implement

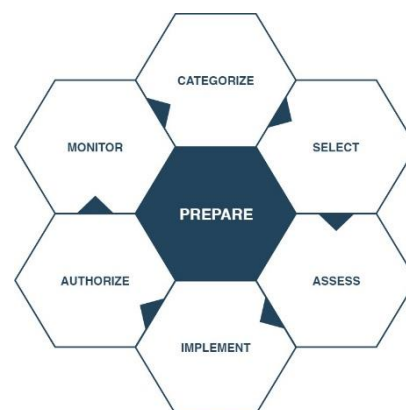
The purpose of the Implement step is to implement the controls in the security and privacy plans for the system and for the organization and to document in a baseline configuration, the specific details of the control implementation.

The controls specified in the security and privacy plans are implemented. Systems security and privacy engineering methodologies are used to implement the controls in the system security and privacy plans. Changes to the planned implementation of controls are documented. The security and privacy plans are updated based on information obtained during the implementation of the controls.

3.5 Assess

The purpose of the Assess step is to determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization.

An assessor or assessment team is selected to conduct the control assessments. The appropriate level of independence is achieved for the assessor or assessment team selected. Documentation needed to conduct the assessments is provided to the assessor or assessment team. Security and privacy assessment plans are developed and documented.



3.6 Authorize

The purpose of the Authorize step is to provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable.

3.7 Monitor

The purpose of the Monitor step is to maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions. The information system and environment of operation are monitored in accordance with the continuous monitoring strategy.

4 Threat Concept

We envision Capella as part of swarm of autonomous robots facilitating the agricultural cycle liberating farmers from slow, repetitive and dull tasks and allowing them to focus more on improving overall production yields. The swarm of robots comprises of autonomous land mower, harvester, sorting and pest control robots operating on 5 hectares of farm. The swarm communicates wirelessly with each other through a centralized database stationed in the computer centre established on the farm.

Our vehicle Capella is the pest control robot whose responsibilities are as follows:

- **Patrols the farm for pest attack**

On the command from the farmer (end-user) Capella navigates in the farm by localizing itself on an established map, watching for pest attack on the plantation using its start-of-art computer vision algorithm. The information gathered in every session is wirelessly updated on the centralized database which can be fetched by the client.

- **Spray pesticides in the affected region**

Capella sprays the pesticides in the affected region as a preventive measure. It updates the amount of spray used over a region of farm and also the amount remaining in its payload (original capacity of 10kg).

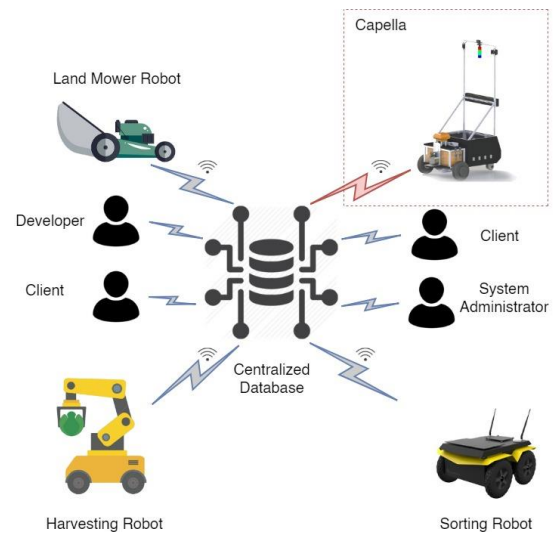
- **Pesticide inventory management**

Capella keeps an account of daily usage of pesticides and ensures that the farm is never out of stock by autonomously placing the order for new stock of pesticides timely, considering the lane time of 3 days.

- **Self-diagnostic and maintenance system**

Owing to the on-board health monitoring system, Capella can diagnose its condition such as battery level, sensor input or actuator control. In case of any fault it can notify the technical team and the end-user.

Capella heavily relies on its perception system for localization, navigation and monitoring therefore it is necessary that it operates during the day in ambient light and does its maintenance work during the night in the base station assigned for it.



5 Threat Modelling

5.1 Security category vs Security impact level

Security categorization provides a structured way to determine the criticality and sensitivity of the information being processed, stored, and transmitted by an information system.

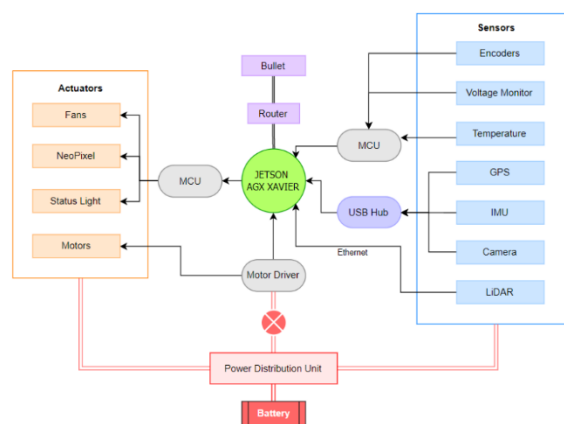
The system owner identifies the types of information associated with the information system and assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability to each information type.

The generalized format for expressing the security category, SC, of an information type is:
 $SC \text{ information type} = \{(confidentiality, impact), (integrity, impact), (availability, impact)\}$
The system components are shown in diagram.

Referring to above diagram, sensors and actors which are critical to achieving mission are identified and are as follows:

- Jetson AGX Xavier
- Motor driver
- LiDAR
- GPS
- IMU
- Camera
- Bullet transmitter

These are further categorized according to confidentiality, integrity and availability. Also, impact values are considered as high, medium and low accordingly.



5.2 Information needed to categorize an information system

The vehicle is fitted with an Inertial Measurement Unit, RTK GPS, a LiDAR, cameras. Furthermore, individual wheel speeds are determined by reading out each wheel encoder. Perception system that governs the admissible navigation area for the autonomous vehicle are detected by both camera and LiDAR to create redundancy in the perception pipelines.

The chosen computing system is NVIDIA Jetson AGX Xavier – an embedded system-on-module (SoM), to deploy the software of our autonomous ground vehicle.

The designed software system runs on Ubuntu 18.04 LTS within the ROS Melodic framework which provided collaborative environment during software development life cycle which enabled us to concurrently design several components of the software and test in isolation because of its highly modular and distributed computing nature.

This year we implemented a Telemetry Unit in our system which enabled the control system of the vehicle to be supervised as well as it can be modified and tweaked during the development and calibration phase. It also provides insight into sensor data like the GPS Co-ordinates as well as system parameters like the battery percentage. Additional data collected in the car, such as video data, can also increase the understanding of the observed processes.

5.3 Information system boundaries

At the simplest level, the system boundary covers all the components of an information system. Defining the boundary is the process of uniquely assigning information resources to an information system.

5.3.1 Hardware System Boundary

As discussed from the previous section's hardware boundaries are governed by the sensors and actuators distinguished clearly from the diagram.

5.3.2 Software Boundary and Interfaces

Software boundaries are determined by the key processes running to ensure the functional and non-functional aspects of the system. It can be accessed only using the custom application developed for the purpose.

5.3.3 Network Boundaries

Capella can only be accessed by connecting to its local network generated by the on-board router. One exception to this can be by the physical access to processing unit and connecting to local network using the ethernet port installed on the Jetson.

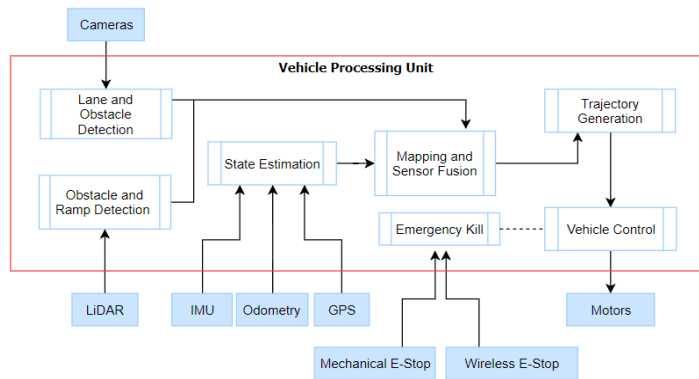
5.3.4 Authorization Boundary

The authorization boundary is the boundary where the authorizing official (AO) has management control which involves budgetary, programmatic, or operational authority and associated responsibility. Information resources identified as within the information system boundary should be under the same management control.

5.4

5.5 Types of information process by information systems

Information processes are identified which are at the heart of successful localization, navigation and perception in an outdoor environment such as a farm in our case, by the virtue of which Capella smoothly operates. The underlying diagram clearly distinguishes the information processes.



6 Identification and Mapping of Cyber Controls

6.1 Defense-in-Depth

Defense-in-depth is an information assurance strategy that provides multiple, redundant defensive measures in case a security control fails or a vulnerability is exploited. It originates from a military strategy by the same name, which seeks to delay the advance of an attack, rather than defeating it with one strong line of defense.

Defense-in-depth cybersecurity use cases include end-user security, product design and network security.

Defense-in-depth security architecture is based on controls that are designed to protect the physical, technical and administrative aspects of your network.

Physical controls

These controls include security measures that prevent physical access to IT systems, RFID cards are used to restrict physical access.

Technical controls

Technical controls include security measures that protect network systems or resources using specialized hardware or software, uncomplicated firewall (UFW) and custom application is developed for same case.

Administrative controls

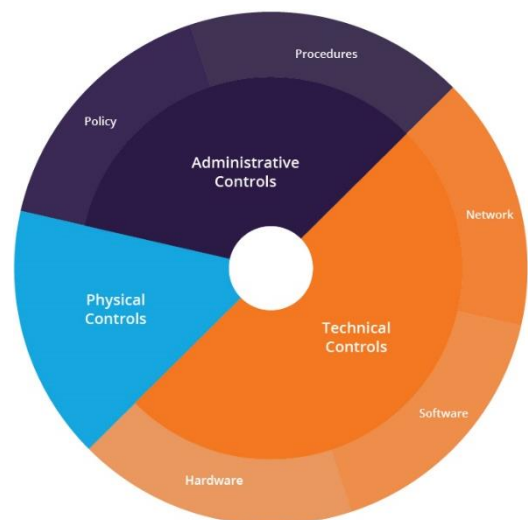
Administrative controls are security measures consisting of policies or procedures directed at an organization's employees, includes organization's security and privacy policies

Additionally, the following security layers help protect individual facets of Capella's network:

Data protection: Include data at rest encryption, hashing, secure data transmission and encrypted backups.

Perimeter defenses: Network perimeter defenses include firewalls, intrusion detection and prevention systems

Monitoring and prevention: The monitoring and prevention of network attacks involves logging and auditing network activity, vulnerability scanning, sandboxing and security awareness training.



6.2 Technology based controls

Technology based controls are the specific activities performed by persons or systems designed to ensure the confidentiality, integrity and availability of the data and overall management of the information system and organization.

6.2.1 Firewall

It is a network security device, either hardware or software based, which monitors all incoming and outgoing traffic and based on defined set of security rules it accepts, reject or drop that specific traffic.

- Accept: allow the traffic
- Reject: block the traffic but reply with an “Unreachable Error”
- Drop: block the traffic with no reply

Example: UFW (Uncomplicated Firewall), an open source software is used for monitoring traffic based on organization’s policy

6.2.2 Wireless Encryption

In wireless security, passwords are only half the battle. Choosing the proper level of encryption is just as vital. Choosing the wrong protocol can leave the system vulnerable to attack.

The most common types of wireless security algorithms are:

- Wired Equivalent Privacy (WEP): It is the oldest and has proven to be vulnerable as more and more security flaws have been discovered.
- Wi-Fi Protected Access (WPA): It had improved security, but is now also considered vulnerable to intrusion.
- Wi-Fi Protected Access II (WPA2): While not perfect, it is currently the most secure choice

Example: WPA2-AES encryption is being used for wireless communication between robot server and client

6.2.3 IDS/IPS

An Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.

It works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

There are three primary components of an IDS:

- Network Intrusion Detection System (NIDS): This does analysis for traffic on a whole subnet and will make a match to the traffic passing by to the attacks already known in a library of known attacks.
- Network Node Intrusion Detection System (NNIDS): This is similar to NIDS, but the traffic is only monitored on a single host, not a whole subnet.
- Host Intrusion Detection System (HIDS): This takes a “picture” of an entire system’s file set and compares it to a previous picture. If there are significant differences, such as missing files, it alerts the administrator.

Example: The system continuously monitors the traffic taking note of robot good and bad commands with respect to robot integrity.

6.2.4 Data backup

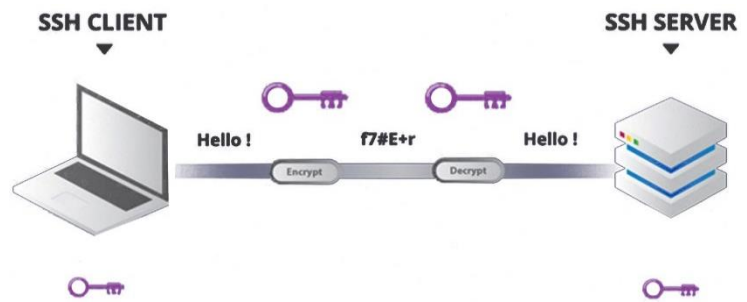
A data backup is the result of copying or archiving files and folders for the purpose of being able to restore them in case of data loss.

As part of a data backup plan, following considerations are taken:

- Criticality of files and folders
- Compression method
- Frequency of backup
- On-site/Cloud backup for safekeeping

6.2.5 SSH

The SSH protocol (also referred to as Secure Shell) is a method for secure remote login from one computer to another. It provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption. It is a secure alternative to the non-protected login protocols (such as telnet, rlogin) and insecure file transfer methods (such as FTP).



The protocol is used in autonomous vehicle network for:

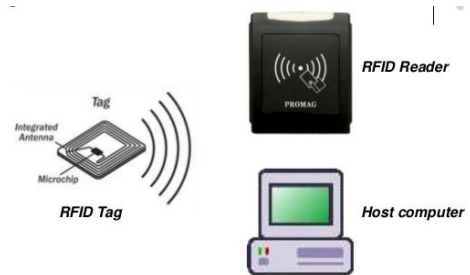
- Providing secure access for users and automated processes
- Interactive and automated file transfers
- Issuing remote commands
- Managing network infrastructure and other mission-critical system components.

Integrity Protection

Once a connection has been established between the SSH client and server, the data that is transmitted is encrypted according to the parameters negotiated in the setup (sshd_config) file.

6.2.6 RFID

The Radio Frequency Identification technology makes use of electromagnetic waves to capture and read data. The information is electronically stored on a tag that is attached to an object or the carrier. The tags can be detected from several feet away by the receiver.



RFID system is composed of the following main components:

- The RFID Card or Tag
- The RFID Reader
- Card Access Management Software
- Access Control Panel

The software system reads the signal received from RFID reader and grants or rejects the access of system to the person.

Example: It is used to allow access to physical components of intelligent ground vehicle

6.3 Management and Operational Controls

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

6.3.1 Risk Assessment and Management

- Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. Include the date the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.
- Identify and assign individuals to specific roles associated with security and privacy risk management.
- Establish a risk management strategy for the organization that includes a determination of risk tolerance.

6.3.2 Review of Security Controls

- List any independent security reviews conducted on the system in the last few years.
- Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

6.3.3 Operational controls

The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes:

- Conduct of a risk assessment;
- Implementation of a risk mitigation strategy
- Employment of techniques and procedures for the continuous monitoring of the security state of the information system.
- Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis.

6.4 Security policy

6.4.1 Purpose

It is a set of rules and practices that specify or regulate how a system or an organization provides security services to protect sensitive and critical system resources.

6.4.2 Scope

This policy applies to:

- Information System
- Physical Systems
- Network
- Application
- Location
- Users of Organization
- Developers of Organization
- Any third-party entity or operators providing services under contract

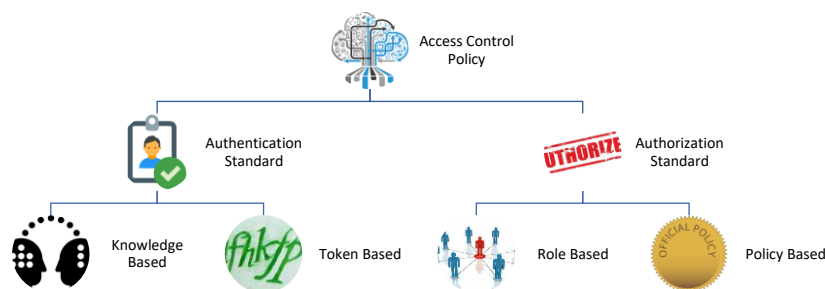
All information systems or applications managed by CAPELLA that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

6.4.3 Objective

The preservation of confidentiality, integrity, and availability of systems and information used by an organization's members.

6.4.4 Access Control Policy

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.



6.4.4.1.1 Access Control Authentication

Remote Authentication

Access to remote user shall be subject to authorization in accordance with remote access and information security policy. No external access shall be permitted to any network device or networked system.

User accounts

Access to autonomous system resources and services will be given through the provision of a unique user account and complex password.

Password

Password issuing, strength requirements, changing and control will be managed through formal processes.

Authentication Standard:

- Username/ Passwords are case sensitive
- Minimum length of password is 8

- Password must meet at least 3 out of the following complexity rules
 - at least 1 uppercase character(A-Z)
 - at least 1 lowercase character(a-z)
 - at least 1 digit (0-9)
 - at least 1 special character (punctuation)
- Account is blocked for an hour after 6 unsuccessful attempts to avoid brute force attempts

Physical Authentication

Physical access of the autonomous system where restricted, is controlled primarily via RFID cards

RFID

Authorized personnel are given RFID cards which allows them to perform their respective role.

Lost cards must immediately be reported at higher authorities which will cancel the card through the physical access control system and an application for reissuance of the replacement card can be submitted.

6.4.4.1.2 Classification of Data

An information classification system therefore may succeed to pay attention to protection of data that has significant importance for the organization, and leave out insignificant information that would otherwise overburden organization’s resources.

1. **High Risk Class:** Information of data ports responsible for physical actuation of autonomous ground vehicle and critical information regarding different layers of architecture of the system
2. **Confidential Class:** Data owner judges that it should be protected against unauthorized disclosure. For instance, it should cover the financial and contractual records
3. **Class Public:** This information can be freely distributed

Access to ‘Confidential’, ‘Restricted’ and ‘Internal Use’ information will be limited to authorized persons whose job or study responsibilities require it, as determined by law, contractual agreement with stakeholders or the *Information Security Policy*.

6.4.4.1.3 Access Control Authorization

Purpose of the Access Control Policy to ensure that all access to information assets is properly authorized, maintained and reviewed.

Principle

It is to facilitate all developers, operators, users and third-party contractors with on-site access to information they need to carry out responsibilities in as effective and efficient manner as possible.

Generic Identities

Generic or group IDs shall not normally be permitted as means of access to vehicle data, but may be granted under exceptional circumstances if sufficient other controls on access are in place.

Privileged Accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default. Technical teams shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity.

Least privilege and need to know : Access rights to robot physical and logical assets will be accorded following the principles of least privilege *and* need to know.

6.4.5 Data Support and Operations

The objective of this policy is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all data assets that exist, in any of our processing environments. The processing environment is considered to be, collectively, all applications, systems, and networks that are owned by Capella.

6 6.4.6.1.1 Data Generation

All users that access Capella Application must use the data generated by Capella's on-board sensors only including the use of confidentiality, integrity and availability mechanisms.

6.4.6.1.2 Data Usage

All users that access Capella Application data must do so only in conformance to this policy. Uniquely identified, authenticated and authorized users must only access data. Each user must ensure that Capella Application data assets under their direction or control are properly labelled and safeguarded according to their sensitivity, proprietary nature, and criticality.

6.4.6.1.3 Data Storage

Where necessary, data stored must be secured via cryptographic mechanisms. Including the use of confidentiality and/or integrity mechanisms.

6.4.6.1.4 Data Disposal

Access control mechanisms must also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights during the disposal process.

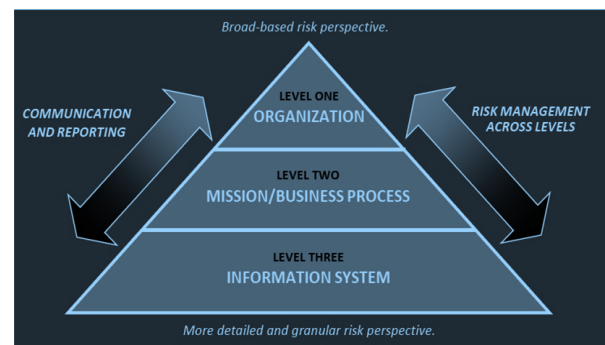
6.4.7 Roles and Responsibilities

6 6.4.9 Stakeholder	6.4.10 Responsibilities
Enterprise Architect	The enterprise architect is an individual or group responsible for working with the leadership and subject matter experts in an organization to build a holistic view of the organizations.
Chief Information Officer	The chief information officer is an organizational official responsible for designating a senior agency information security officer; developing and maintaining security policies, procedures, and control techniques to address security requirements.
Authorizing Official	The authorizing official is a senior official or executive with the authority to formally assume responsibility and accountability for operating a system;
Common Control Provider	The authorizing official is a senior official or executive with the authority to formally assume responsibility and accountability for operating a system; providing common controls inherited by organizational systems.
Control Assessor	The control assessor is an individual, group, or organization responsible for conducting a comprehensive assessment of implemented controls and control enhancements to determine the effectiveness of the controls
System Administrator	The system administrator is an individual, group, or organization responsible for setting up and maintaining a system or specific system elements. System administrator responsibilities include, for example, installing, configuring, and updating hardware and software; establishing and managing user accounts.
System Owner	The system owner is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a system.

6.5 Holistic approach to information security

A holistic approach is an integrated, cybersecurity approach that considers the human, cultural, and social factors together in an organization. Cybersecurity is a human-centric field. After all, cyberattacks are planned and executed by a person and most attacks target a person for access.

It affects every aspect of the organization including the mission and business planning activities, the enterprise architecture, the SDLC processes.



Traceability of controls to the security and privacy requirements that the controls are intended to satisfy. Establishing such traceability ensures that all requirements are addressed during system design, development, implementation, operations, maintenance, and disposition.

Technology needed to be integrated, and multiple technology solutions were provided end-to-end cybersecurity to help improve incident detection, prevention, and response, and to streamline security operations to stop threats before they reach clients.

An important aspect of risk management is the ability to monitor the security and privacy posture across the organization and the effectiveness of controls implemented within or inherited by organizational systems on an ongoing basis. This was well considered in our SDLC.

7 Description of implemented cyber controls

7.1 Relation of chosen controls to mitigated risks

Based on the identified threats and risks (mentioned in the previous sections), we implemented the following technical controls to mitigate risks. Along with the implemented control, control family has also been identified from the NIST RMF guidelines on cyber controls.

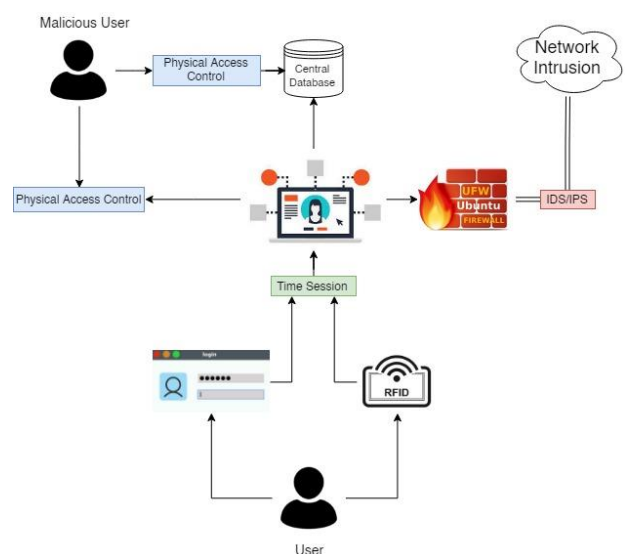
S.no	Implemented Control	Control Family	Mitigated Risk
1.	Custom application developed to configure and monitor system parameters	AC-1/ AC-2/ AC-3/AC-4/AC-8/AU-2/AU-5/CA-1/CA-2/CA-3/SC-2/MA-1/CM-11	Multiple ways of accessing the system, Unauthorised access, Setting higher privileges
2.	Wireless encryption	AC-18/AC-19	Password can often be cracked in a few minutes
3.	Firewall	CA-7/SI-4/SC-7/RA-4	Malicious packet flow and port connection activities
4.	Intrusion Detection and Prevention System	SI-4	Malicious commands and node creation
5.	Data port blocking	CA-7/SI-3	Individual system element attacks
6.	Time bound access	IA-5	Unauthorized person accessing the system when proper logout procedures not followed
7.	RFID authorization	SC-7	Physical access, uploading malicious codes

7.2 Design and implementation details of controls

7.2.1 Application developed to configure and monitor system parameters:

A cross platform; front-end application has been developed for access/monitoring the robot which adheres to organization policy and procedures. It prevents unauthorized access to system using access control policy. An open source framework Electron is used in developing same. It is an open source library developed for building cross-platform desktop applications. HTML, CSS are responsible for front end GUI elements. Python and JavaScript are working in back-end to handle all logic. An open source software MongoDB is used as Database Management System (DBMS).

The connection is established using SSH.



All this is taken care in back-end using Paramiko, an open source python library is used for enabling SSH connection and to run python scripts remotely. Code takes username and password from Capella Application and feeds it to python script which authenticates and enables connection in backend. On server side, another script enabling firewall rules specific to user is run adhering to organization policies.

7.2.2 Wireless encryption

WPA2-AES encryption standard is used for wireless connection with robot. After connecting to same network as robot. User can only access system via Capella Application with their credentials provided by system administrator.

7.2.3 Firewall

Firewall in use on server side is Uncomplicated Firewall (UFW), which is an open source software in Linux environment.

Rules are defined in here particular to each user.

It helps in Intrusion Avoidance as after a predefined unsuccessful login attempts it blocks the Port 24 of SSH with a timer set by python script further denying access to system.

7.2.4 Intrusion Detection and Prevention System

System architecture is based on ROS2 which uses TCPROS which is a transport layer for ROS Messages and Services. It uses standard TCP/IP sockets for transporting message data. Inbound connections are received via a TCP Server Socket with a header containing message data type and routing information. Communication node and its data are monitored via python script.

If an intruder somehow manages to access the system then again, he won't be able to perform any unauthorized commands as an Intrusion Detection and Prevention System is in place which continuously monitors for commands and updates it with database.

According to robot dynamics, a dataset has been collected with past experiences and any new entry/commands are verified.

The system takes in account of current user and verifies its activity along with commands according to security policies.

7.2.5 Data Port Blocking

USB and TCP/IP ports being used by the system are recognized and based on the privileges assigned to the user, administrator can enforce the access to only certain ports to the user using a slider control provided on his interface in the application. It is implemented by changing the permission status of the ports through a python script running in the kernel mode of the operating system.

7.2.6 Time bound access

When a particular user logs into the system, a time bound session is initiated which can only last up to 6 hrs. at a stretch after which the user is required to re-login in to the system. This has been implemented by maintaining the entry and exit time of each user in the central database.

7.2.7 RFID Authorization

RFID readers are installed on the robot compartment housing the processing unit, and it would also be installed on the computer center as mentioned in the threat concept. On the basis of RFID card brought near by the user, the MCU connected to it authorizes the privileges for the user by referring to the central database.

7.3 Appropriate but unimplemented controls

7.3.1 Biometric authentication

Biometrics is the technical term for body measurements and calculations. It refers to the metrics related to human characteristics. It is widely used in access control.

7.3.2 Physical locks

Locks are effective in restricting access to physical systems. A smart lock is an electronic lock that gets instructions to lock and unlock the door from an authorized device using a cryptographic key.

8 Cyber Controls Demonstration Strategy

1. Judges will be made acquainted with information system and its associated security impact level during the oral presentation.
2. Emphasize will be laid on the identified cyber threats and chosen cyber controls to mitigate the associated the risks.
3. Test plan and test cases will be conveyed to the judges along with its hardcopy.

4. Based on the test plan we will implement the developed test cases serially to effectively demonstrate the efficacy of the system.

TEST PLAN	
Test Scope	To verify and validate the baseline set for the implemented cyber controls and to prove the efficacy of the cyber security system developed.
Test Approach	Testing will be done at the competition site and will be the test cases will be implemented to demonstrate the test plan to the judges in-person.
Test Environment	Physical environment will be the competition site where the Capella will be jacked to avoid any undesirable actuation of the motors during test sequences. The software environment required for testing will be on Ubuntu and Windows machine.
Features to be tested	<ol style="list-style-type: none"> 1. Access to network – wireless and physical 2. Role-based authentication and authorization to system 3. Role-targeted graphical user interface of the application developed 4. Monitoring/ Calibrating system elements 5. Malicious commands for emulating intrusion 6. Intrusion detection and prevention of the system 7. Identification of communication ports 8. Firewall system 9. Data port blocking slider and algorithm 10. User have a time bound access to the system

In reference to the aforementioned test plan, we have devised a test suite to effectively demonstrate the efficacy of the identified threats and the chosen cyber controls in action.

TEST SUITE			
S. No	Test Case No.	Input	Expected Output
1	Wireless access to Capella network (assuming SSID is hidden)	Scanning for Wi-Fi networks	Network is not visible
2	Wireless access to Capella network (SSID and Password are provided)	Connecting laptop to hidden network with provided SSID and password	Both Laptop and Capella are in same network
3	Physical Access (RFID cards with known secret provided to judges)	Touching the card and entering correct password	Access to physical system is granted.
		Touching right card with wrong password	Data ports are blocked
4	Testing Capella Application	Opening Capella application	Application is opened, prompting user to select role
5	Role-based access (Guest)	Selecting role as Guest	UI prompting username & password is opened
6	Access to network (assuming incorrect credentials, and checking privacy policy)	Username: "guest"	Error: "Incorrect username/password combination"
		Password: "testingpassword"	
		Security and Privacy policy: "Checked"	
7	Access to network (assuming correct credentials, without checking privacy policy)	Username: "guest"	Error: "Please check privacy and security policy"
		Password: "Capella_guest2k19"	
		Security and Privacy policy: "Unchecked"	
8	Access to network (assuming correct credentials, and checking	Username: "guest"	Access to system is granted, System-use-notification is sent to system administrator.
		Password: "Capella_guest2k19"	

	privacy policy)	Security and Privacy policy: "Checked"	Guest UI is opened with limited read-only controls
9	Guest - Monitoring	"Monitor" button is pressed after multiple sensors are selected from list view	A new page is opened with raw input of selected controls data
10	Guest – Logout	Logout button is pressed	Role selection screen is opened
11	Token based access	Selecting role as "Guest Token Test" no credentials needed as only timer is tested	System is logged out automatically after one-minute
12	User – Maintainer	Username: "maintainer" Password: "Capella_maintainer2k19" Security and Privacy policy: "Checked"	Access to system is granted, System-use-notification is sent to system administrator. Maintainer UI is opened with limited read-only controls
13	Maintainer – Calibration	Selecting IMU from calibration tab Setting initial position as zero "Calibrate" button is pressed	Resting orientation is set to zero as seen in monitoring tab
14	Maintainer – Control Testing (Safe Input)	Target velocity for wheels is set (Safe Zone: 0.5 to 1.2 m/s)	Wheels reach the target velocity
15	Maintainer – Control Testing (Unsafe Input) / Intrusion Detection	Target velocity for wheels is set as: vtarget=2m/s	Warning is displayed for exceeding safe limits.
16	Maintainer – Control Testing (Unsafe Input) / Intrusion Prevention	Warning is ignored	Intrusion Detection and Prevention system takes action; user is logged out and notification is sent to system administrator
17	User – System Administrator	Username: "admin" Password: "Capella_admin2k19" Security and Privacy policy: "Checked"	Access to system is granted, System Administrator UI is opened without any time-based token
18	Admin – Uploading Codes (sample code is provided)	Code is uploaded	Status LED starts blinking
19	Admin – Data Ports Turn Off	Particular sensors are turned off	Data gathering from sensors is stopped
20	Admin – Terminal Access	Terminal Access button is pressed, password is entered in the prompt	Robot's terminal is accessed wirelessly
21	Admin – Remote Kill	Kill button is pressed, admin password is entered	Power Supply to actors is cut
22	Intrusion Detection and Prevention	Original camera feed is replaced with tampered one (sample feed provided)	Robot goes haywire for a while and then stops
23	Unauthorized commands	New malicious node is created (sample code provided)	Automatic deletion of node
24	Multiple unsuccessful login attempts	Wrong password is entered for Guest User > 6 times	Account is blocked for an hour, notification sent to the system administrator