DELHI
TECHNOLOGICAL
UNIVERSITY

KURM

Date - 15 May, 2023

Lakshay (**Captain**)	lakshay_co21a4_72@dtu.ac.in
Abdul Basit	abdulbasit_se21b1_047@dtu.ac.in
Daksh Gupta	dakshgupta_it21a9_14@dtu.ac.in
Rajat Chandra	rajatchandra_me21b15_50@dtu.ac.in
Kaushal Kumar	kaushalkumar_co21a4_58@dtu.ac.in
Lakshya Kumar Sinha	lakshyakumarsinha_pe21b2_39@dtu.ac.in
Harsh Saini	harshsaini_ep22b4_51@dtu.ac.in
Aditya Kumar	adityakumar_co22a1_19@dtu.ac.in
Utkarsh Diwakar	utkarshdiwakar_co22a1_09@dtu.ac.in

I hereby certify that the design and development of the vehicle **KURM**, described in this report is significant and equivalent to what might be awarded credit in a senior design course. This is prepared by the student team under my guidance.

Prof. S Indu
Faculty Advisor
Dean Student Welfare
Delhi Technological University

Prof. S. Indu
Dean (Student Welfare)
Delhi Technological University
Shahbad Daulatpur, Bawana Road,
Delhi-110042

First Section: Team Intro and Overview

1.1. Introduction

UGV (Unmanned Ground Vehicle) is a group of highly motivated and enthusiastic students at Delhi Technological University, India whose sole purpose is to develop autonomous ground vehicles for industrial applications like delivery bot, autonomous self driving car. We devote our time to doing research on autonomous technology and passing the knowledge and technical know-how to our juniors so that they can take it forward and make some useful implementation out of it. For the purpose of IGVC 2023, we have developed an autonomous ground vehicle for the Autonav Challenge. The vehicle is named ‘**KURM**’ which is the sanskrit translation of the english word ‘**Tortoise**’ as due to the shape and structure the robot displays.

1.2. Organization

We believe that teamwork is at the heart of any great achievement. Our goal was not just to develop an autonomous vehicle but to build an environment that nurtures team and individual’s growth simultaneously.

Name	Major/Year	Software	Mechanical	Electrical	Hours
Lakshay	CSE/2nd	✔			500+
Abdul Basit	SE/2nd	✔			600+
Daksh Gupta	IT/2nd			✔	550+
Rajat Chandra	ME/2nd		✔		650+
Kaushal Kumar	CSE/2nd			✔	500+
Lakshya Sinha	ME/2nd		✔		700+
Harsh Saini	EP/1st.			✔	550+
Aditya Kumar	CSE/1st.	✔			700+
Utkarsh Diwakar	CSE/1st	✔			650+

Second Section: Demonstrate Understanding of NIST RMF Process

The NIST Risk Management Framework (RMF) is a crucial cybersecurity process that helps organizations develop and maintain secure information systems. The RMF provides a structured, standardized methodology for organizations to identify, assess, and manage risks associated with their IT infrastructure. This process aids in the development of secure and resilient systems by implementing essential security controls and promoting continuous monitoring. This process encompasses six primary steps: categorizing systems, selecting security controls, implementing controls, assessing control effectiveness, authorizing operation, and monitoring system security. By applying this holistic and iterative approach, organizations can maintain robust and resilient systems capable of defending against the constantly evolving cyber threat landscape. Hence we as a team, to ensure a comprehensive approach to securing our vehicle, adopted the NIST RMF process as the foundation for our cybersecurity evaluation and implementation.

Categorize

- ➔ Categorization is a key part of risk management, helping organizations understand their system's characteristics and potential security impact.
- ➔ This process allows organizations to make informed decisions about resource allocation and the implementation of security controls.

1. **System Description:**
    - ◆ Creating a comprehensive inventory of the system's components and their interconnections.
    - ◆ All hardware, software, and firmware should be identified, along with the system's boundary, operational environment, and information flows.

2. **Security Categorization:**
    - ◆ This task involves applying the Federal Information Processing Standards (FIPS) Publication 199 to identify the system's impact level for Confidentiality, Integrity, and Availability (CIA).
    - ◆ The information type of the system is identified and then categorized based on the potential impact on the organization.

3. **Security Categorization Review and Approval:**
    - ◆ Involves validation and approval of the previous tasks by a senior organizational official.
    - ◆ The security categorization and supporting rationale should be reviewed to ensure their accuracy and completeness.
    - ◆ Ensures that the system's categorization aligns with the organization's risk tolerance, strategy, and budget.

Select

- ➔ The 'Select' step provides a comprehensive, structured, and risk-based approach to establishing robust cybersecurity measures.
- ➔ Involves careful control selection, tailoring, allocation, documentation, continuous monitoring, and approval to protect organizational assets, ensure operational continuity, and contribute to national cybersecurity.

1. **Control Selection:**
    - ◆ The first task involves identifying appropriate security controls based on the system's security categorization, federal legislation, directives, regulations, standards, and guidelines.
    - ◆ NIST SP 800-53 guides the selection process, which contains security and privacy controls. Organization chooses these controls considering the potential impact on their systems.

2. **Tailoring:**
    - ◆ This task allows organizations to modify the initial control set to suit their specific operational environment and risk tolerance.
    - ◆ Tailoring considers factors like legal requirements, mission criticality, and available resources.

3. **Allocation:**
    - ◆ This task involves assigning the selected and tailored controls to organizational systems.
    - ◆ Ensures efficient and effective distribution of controls across the IT infrastructure, eliminating defense gaps.

4. **Documentation:**
    - ◆ Documentation serves as an important reference point, facilitating communication, consistency, and compliance throughout the security implementation process.
    - ◆ It helps in maintaining an official record of the selected controls.

5. **Monitoring:**
    - ◆ This task involves establishing processes to continuously track the effectiveness of the selected controls.
    - ◆ Ongoing assessment allows for adjustments as threats evolve or new vulnerabilities are identified.

6. **Reviewing and Approval:**
    - ◆ The final task involves evaluation and approval of the selected controls and their implementation by a senior official.
    - ◆ This provides assurance that the organization's risk has been properly managed.

Implement

- ➔ The 'Implement' step of the NIST-RMF is critical in operationalizing the controls selected in the previous phase.
- ➔ This phase involves turning the chosen controls into workable procedures and incorporating them into the system's design, development, and operation.
- ➔ Proper documentation is a crucial component of this step.
    - ◆ It includes in-depth explanations of how the security controls are applied within the system.
    - ◆ This documentation serves as a crucial reference point, promoting system understanding, compliance, and accountability among users and stakeholders.
- ➔ The 'Implement' step is a continuous process, not a one-time event.
    - ◆ As systems and threats evolve, controls may need to be adjusted or supplemented.

Assess

- ➔ The 'Assess' step in the NIST-RMF is a crucial stage where organizations evaluate the effectiveness of their implemented security controls.
- ➔ This step provides a clear understanding of the current security posture and helps identify and address any gaps or weaknesses in cybersecurity defenses.

1. **Developing and Approving an Assessment Plan:**
    - ◆ This task involves creating a plan outlining the procedures, methods, and timing of assessments.
    - ◆ The plan ensures the process is coordinated and aligns with the organization's risk strategy.
    - ◆ It should be developed with stakeholder input and approved by the appropriate authority to align with operational needs.

2. **Assessing the Security Controls:**
    - ◆ This task involves examining and testing each security control to ensure they're correctly implemented, functioning as intended, and effectively mitigating risks.

3. **Producing an Assessment Report:**
    - ◆ After the assessments, organizations produce a report summarizing the results, including identified vulnerabilities, their potential impacts, and recommended corrective actions.
    - ◆ The report serves as a critical tool for informed decision-making about the system's security state.

4. **Remediation of Identified Vulnerabilities:**

    - ◆ Based on the assessment report, organizations may need to adjust existing controls, implement new ones, or modify system processes or configurations.
    - ◆ This continuous improvement is integral to maintaining an effective cybersecurity posture.

➔ In summary, the 'Assess' step provides a comprehensive diagnostic check, highlighting areas for improvement and ensuring system resilience, thereby contributing to robust cybersecurity development.

Authorize

➔ The 'Authorize' step in the NIST-RMF is a critical point where the organization's senior leadership makes a risk-based decision about the system's risk to organizational operations, assets, or individuals.

➔ This step involves understanding the system's risk posture and authorizing its operation based on that understanding.

1. **Preparation of the Security Authorization Package:**
    - ◆ The process begins with preparing the security authorization package, which includes the system security plan, security assessment report, and plan of action and milestones (POA&M).
    - ◆ It provides a comprehensive view of the system's security posture, including its vulnerabilities, the effectiveness of controls, and the plan for addressing any remaining weaknesses.

2. **Review by the Authorizing Official (AO):**
    - ◆ The package is then reviewed by the AO, usually a senior executive, who is responsible for the risk associated with system operation.
    - ◆ Based on the authorization package, the AO makes a risk-based decision whether to authorize system operation, deny authorization if the risk is deemed too high, or request additional information or actions.

3. **Documentation in an Authorization Decision Document:**
    - ◆ The AO's decision is documented in an Authorization Decision Document.
    - ◆ If system operation is authorized, an Authorization to Operate (ATO) is issued, which might come with certain conditions or terms of acceptance.

➔ In conclusion, the 'Authorize' step that the system's security risks are understood and accepted by the organization's leadership before the system is allowed to operate.

Monitor

➔ The 'Monitor' step in the NIST-RMF is a continuous and crucial process that ensures the ongoing effectiveness of an organization's security controls.

➔ It recognizes that the security posture of a system isn't static, and regular monitoring is key to maintaining a robust cybersecurity stance.

1. **Establishing a System and Security Controls Monitoring Strategy:**
    - Organizations must define a strategy for monitoring systems and security controls.
    - This includes defining the frequency and methods of monitoring, which can involve automated tools, regular audits, or manual reviews.

2. **Conducting Ongoing Security Control Assessments:**
    - Next, organizations carry out continuous security control assessments to ensure the controls continue to function as intended.
    - These assessments identify changes that could impact the system's security state, such as new vulnerabilities or shifts in the threat landscape.

3. **Updating Key RMF Documentation Regularly:**
    - Organizations need to regularly update key RMF documents, including the system security plan, security assessment report, and the POA&M.
    - These documents provide a running record of the system's security status and planned actions to address identified weaknesses.

4. **Reporting the Security State to the AO:**
    - Finally, organizations report the security state of the system to the AO.
    - The AO reviews these updates to maintain awareness of the system's security posture and make informed, risk-based decisions.

Identified Threat Concept

We have chosen a threat concept for ourselves as given in the third option.

India, with its rich agricultural heritage, is ripe for the integration of our Unmanned Ground Vehicles. The increasing pressure to feed the most populous country, coupled with the labor shortage in agriculture necessitates advanced technological solutions. The nation is progressively open to automation trends, evident from the rising adoption of smart farming techniques. Our chosen scenario focuses on this transition.

Case:

A farmer in Maharashtra is having trouble. He can't grow enough crops because there's not enough help and his tools are old. Bad weather and disasters like floods make things worse. Also, he's using too much water and fertilizer, which is not good for the environment. He can make use of a UGV for the following:

1. **Automated Farming:** UGVs can automate farming tasks, beneficial for Maharashtra's diverse crop cultivation.

2. **Flood Prediction:** UGVs can assist in managing monsoon rains by predicting floods, crucial for protecting Maharashtra's agricultural lands.
3. **Disaster Response:** During natural disasters such as droughts and cyclones, UGVs can assess damage and aid recovery efforts.
4. **Resource Optimization:** UGVs' ability to optimize resource usage can contribute to water conservation, essential in Maharashtra's drought-prone regions.
5. **Data-Driven Agriculture:** UGVs can collect and analyze extensive data, thereby informing and improving farming decisions, and promoting sustainable agriculture in Maharashtra.

The information systems at risk include the onboard computers, the sensors related to it, the weather changes, and the back-end management system. Presented here is a list of possible threats:

1. **Physical Security Threats:** UGVs can be subject to theft or vandalism, given their valuable components and the open nature of farmlands. Moreover, they could be misused if they fall into the wrong hands.
2. **Data Security Threats:** UGVs collect and process vast amounts of sensitive data, including crop information, land details, and potentially personal information. Unauthorized access to this data could lead to misuse or manipulation.
3. **Network Security Threats:** UGVs often rely on wireless communication for operation and control, making them susceptible to network attacks. Hackers could intercept and alter the data being transmitted, leading to incorrect actions by the UGV.
    a. To take revenge on owner over a personal feud
    b. To use it as a weapon
4. **Software Security Threats:** The software running the UGV could be vulnerable to malware, ransomware, or other types of attacks. An attacker could exploit these vulnerabilities to gain control of the UGV or disrupt its operations.
5. **Operational Security Threats:** If the UGV is remotely controlled, there's a risk of the control being hijacked, leading to potential misuse of the vehicle or damage to the crops
6. **GPS Spoofing:** UGVs often rely on GPS for navigation. Hackers could deceive the GPS system to mislead the UGV, disrupting its operation or even leading to accidents.

NOTE: *Since this is a situation of a farm, the objectives of the manipulators are usually the same. Hence, the objective has been generalized.*

Security Category	Confidentiality	Integrity	Availability
Physical Security Threats, Vandalism, etc.	Low	High	High

Data Manipulation		Low	Moderate	High
Network Security Hacking	(a) Personal Feud	Low	High	High
	(b) Use it as a weapon	Moderate	High	High
Ransomware, Malware Attacks		High	Moderate	High
Controls being hijacked to disrupt and damage crops		Low	Moderate	High
GPS Spoofing by hackers		High	Moderate	Low

Security Control	**Tailoring**
AC-1	Access Control & Policy: Only the core team members that will have signed the NDA will be allowed admin logins.
AC-2	Account Management: The use of Biometric Login for the admins for accessing superuser commands
AC-3	Access Enforcement: The password will be changed every 3 months and will be given again to the members. Integrity questionnaires will be handed.
AC-7	Least Privilege - This control will ensure the principle of least privilege, allowing only authorized accesses necessary for users to accomplish assigned tasks.
AC-8	System Use Notification: The information system will display an approved system a notification message before granting access to superuser.
AC-11	Session Lock: The session will be locked if suspicious activity is detected.
AC-12	Session Termination: Several session locks over a specified period of time will lead to session termination and deletion of the admin privileges.
IA-2, IA-3, PE-8	Access Control for Mobile and Device Authentication: The farmer mentioned, shall use his mobile application to interact with the robot. He will be educated on how to be safe himself and be provided with 2FA from his mobile/E-Mail.
PE-5	Access Control for Output Devices: Only devices which are a part of the robot can be used in the ports provided and all other ports

	shall be blocked off.
SA-5	Information System Documentation: Security protocols will be documented appropriately along with a log file.
SC-7	Boundary Protection: Geo Fencing the farm area of every owner by one time survey.
SI-7	Software, Firmware, and Information Integrity: Monthly checks shall be done to maintain highest security firmware updates on all the sensors and modules while protecting against unauthorized changes

Third Section: NIST RMF Process Applied to Competition Robot

1. Categorize

Security Category	Confidentiality	Integrity	Availability
A student hacker might try to take control of the vehicle to tamper the functionality of the robot	Low	Moderate	High
A student hacker might try to inject viruses and malware	Low	Moderate	High
A student hacker might try to tamper with the GPS Base Receiver	Low	High	Moderate
Competing teams might try to steal the workspace	High	Low	Low
Someone could try to spoof the GPS data received	Low	High	Moderate

2. Select

Security Category	AC-1	AC-3	AC-7	PE-5	SC-7	CM-6	PE-13	PE-8	SA-6
A student hacker might try to take control of the vehicle to tamper	✔	✔		✔		✔	✔	✔	✔

the functionality of the robot									
A student hacker might try to inject viruses and malware	✔	✔		✔		✔		✔	
A student hacker might try to tamper with the GPS Base Receiver	✔		✔	✔	✔	✔	✔	✔	✔
Competing teams might try to steal the workspace	✔		✔	✔				✔	✔
Someone could try to spoof the GPS data received	✔			✔	✔		✔		✔

3. Implement

Security Control	Tailoring
AC-1	Access Control & Policy: Only the core team members that will have signed the NDA will be allowed admin logins.
AC-3	Access Enforcement: The password will be changed every 3 months and will be given again to the members. Integrity questionnaires will be handed.
AC-7	Least Privilege - This control will ensure the principle of least privilege, allowing only authorized accesses necessary for users to accomplish assigned tasks.
PE-5	Access Control for Output Devices: Only devices that are a part of the robot can be used in the ports provided and all other ports shall be blocked off.
SC-7	Boundary Protection: Geo Fencing of the nav course, moving out of the area will cause an error and the robot will stop.
CM-6	Configuration Settings: Helps to establish and maintain baseline configurations and inventories of organizational information systems. Ensures that the settings of the LIDAR sensor, ZED cam, and GPS are configured correctly and securely.

PE-13	Protection from Electromagnetic Interference: This control requires the organization to protect the information system from damage resulting from electromagnetic radiation/interference or other physical environmental factors.
PE-2, PE-3, PE-8	Physical Access to Device: Secures physical access devices, list of personnel authorized for physical access, maintaining a record of visitor access.
SA-5, SA-6	System Documentation and Usage Restrictions: The RTK configuration file is not stored in the competition computer. It is stored somewhere else.

4. **Assess**

Assess step provided the KURM team with a comprehensive diagnostic check that highlighted areas for improvement, and ensured system resilience, thereby contributing to robust cybersecurity development.

5. **Authorize**

Being a small group rather than an entire organization. We don’t have a separate authorizing officer in our team, however, we have consulted our professors and seniors. Their feedback and assessment have been an invaluable assets.

6. **Monitor**

The 'Monitor' step in the NIST-RMF process is a critical component of a proactive and adaptive cybersecurity program in organizations. KURM however, being a small-scale project, has a lack of dedicated automated auditing programs. However, it is manually audited before every run and the assessment is done by us students. This is something we plan to improve on in the coming future.

Description of Implemented Cyber Controls

AC-1: Establishes and disseminates access control policies and procedures.

- The members with the admin ID and Password have signed an NDA.
- Anyone who is found to have shared their Password with another person will be immediately stripped of their admin privileges.

AC-3: Enforces approved authorizations for information system access.

- The password changes whenever someone in the core functioning group leaves.
- They lose access to the team’s GitHub and the team’s Notion Workspace and Google Drive. This happens yearly when our seniors leave.

AC-7: Implements least privilege principle for system access

- ➔ All members do not have access to all domains. Apart from the captain and vice captains, the other members only have restricted access to departments other than their own domain.

PE-5: Prevents unauthorized access to system output devices.

- ➔ The USB ports have been blocked and inserting any drive would not show up, hence strengthening the security.

SC-7: Provides geo-fencing.

- ➔ If the GPS is found to be out of the track dimensions due to any reason it will automatically stop sending the move base values, raising errors that'll stop the bot.

CM-6: Ensures correct and secure configuration of system settings.

- ➔ An extensive audit of all working sensors, drivers, and motors is done. The robot is not run until all the default configurations have been loaded.

PE-13: Shields system from harmful electromagnetic interference.

- ➔ A strong external electromagnetic radiation could severely alter the performance of our bot if we hadn't taken extra steps, such as but not limited to:
  - ◆ Using Shielded Cables
  - ◆ Installing Ferrite Chokes and Beads
  - ◆ Proper Grounding
  - ◆ Physical Separation

PE-8: Maintains record of visitor access

- ➔ We strongly avoid users outside the team access to the computers controlling the robot and hence the Guest Login has been blocked off.
- ➔ In case someone uses our system in an extraordinary condition, we plan to observe them carefully and note down their contact details.

SA-6: Places restrictions and controls on software usage.

- ➔ The RTK configuration files have been stored outside the computer as it contains crucial information.
- ➔ The radios have also been configured with matching NetID's which have also been configured outside the device used to run the bot.

Description of Appropriate but Unimplemented Controls

PE-8: Maintains record of visitor access

By implementing RFID technology in, we can ensure that all the members can be logged in seamlessly. Moreover, they can be identified and their activities can be logged in. This can be further improved by biometrics. Another alternative could be to add 2FA.

AC-7: Unsuccessful Login Attempts
This control requires the information system to enforce a limit of consecutive invalid login attempts by a user during a specific time period. After reaching this limit, the system must automatically lock the account or delay further login attempts.

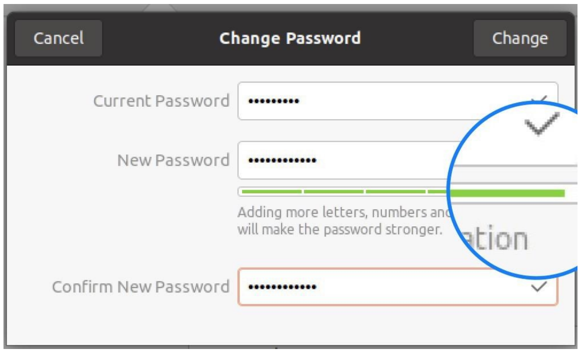
AC-11: Session Lock
Requires the system to prevent further access or initiate a session termination after a predetermined period of inactivity, enhancing the security of unattended user sessions. More importantly, it involves loss of access upon detection of suspicious activity.

AC-8: System Use Notification
The information system will display an approved system notification message before granting access to the superuser.

Demonstration Strategies for Audit

1. The password set for the robot is extremely strong. This can be verified by the judges when the password is given to them as well as by Ubuntu's inbuilt password strength measure.

2. When students leave the team, the password changes and a strong password is set, which can be confirmed.



Current Password ••••••••••

New Password •••••••••••••

Adding more letters, numbers and
will make the password stronger.

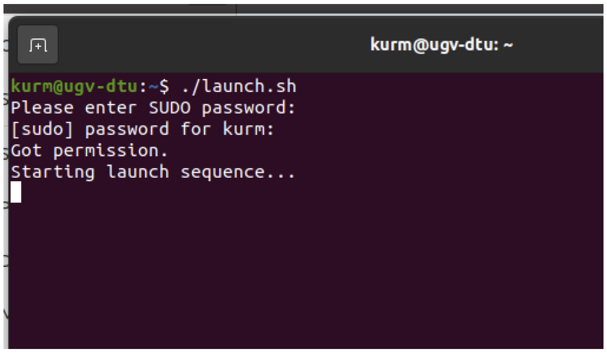
Confirm New Password •••••••••••••

Fig: We necessarily require very strong passwords

3. Guest login has been disabled. The bot's code can only be run through superuser commands. Moreover, we have disabled the WiFi and Bluetooth from our on-board computer.

4. The geofencing can be tested by putting foil near the antenna to get garbage data that will stop the bot instantly. This can also be done by disconnecting/causing interference near the radio.

5. The GitHub, notion, and google drive access can be previewed. A copy of the NDA can also be shown.



```
kurm@ugv-dtu:~$ ./launch.sh
Please enter SUDO password:
[sudo] password for kurm:
Got permission.
Starting launch sequence...
```

Fig. Launching robot requires superuser commands