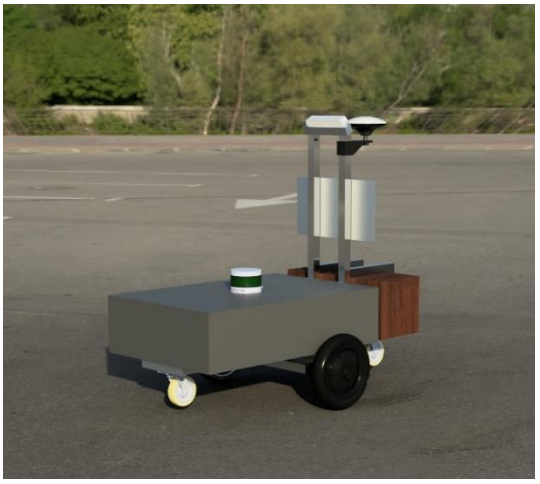
MUKESH PATEL SCHOOL OF TECHNOLOGY MANAGEMENT & ENGINEERING™

TEAM DARVIN

Cyber Report



Vehicle Name: SOCRATES 2.0

Prof. Kashyap Joshi - Faculty Mentor - kashyap.joshi@nmims.edu

Sarthak Mishra - Team Captain - sarthak.mishra25@nmims.edu.in

Date Submitted: 13th May 2023

Team Members

Vaibhav Raheja – Co-Captain - vaibhav.raheja34@nmims.edu.in

Parthak Mehta - Vice Captain - parthak.mehta23@nmims.edu.in

Rudra Makwana - Core Member -rudra.makwana19@nmims.edu.in

Harshil Shah - Core Member - harshil.shah22@nmims.edu.in

Pranav Lavande - Core Member - pranav.lavande029@nmims.edu.in

Saksham Gupta - Team Mentor - saksham.gupta82@nmims.edu.in

I, Professor Kashyap Joshi, hereby declare that the work done by Team D.A.R.V.I.N under my guidance for the IGVC competition 2022 has been significant and equivalent to what might be awarded credit in a senior design course.

Prof. Kashyap Joshi

EXTC Department

NMIMS MPSTME

(kashyap.joshi@nmims.edu)

Table of Contents

Team Organization

After many hours of tedious hard work, Team Darvin achieved 3rd place in IGVC 2022 - Autonav. For IGVC 2023, Team Darvin embarked on an ambitious project to enhance the capabilities of the autonomous robot, SOCRATES 2.0. Through collaborative efforts and a multidisciplinary approach, our team worked tirelessly to push the boundaries of autonomous vehicle technology. In this report, we present our progress, design considerations, and solutions implemented to enhance SOCRATES 2.0's performance and autonomy. Our dedication, expertise, and teamwork have been instrumental in overcoming challenges and achieving remarkable results. As we continue our pursuit of innovation, we are excited for the future advancements that lie ahead. The work for this project was divided into mainly four sections: Mechanical, Electronics, Software, and Administrative.

Name	Position	Major work
Sarthak Mishra	Team Captain	Software, Electronics, Administrative
Vaibhav Raheja	Co-Captain	Software, Mechanical, Administrative
Parthak Mehta	Vice-Captain	Cyber Challenge, Administrative
Rudra Makwana	Core Member	Mechanical, Software
Harshil Shah	Core Member	Mechanical
Pranav Lavandhe	Core Member	Electronics

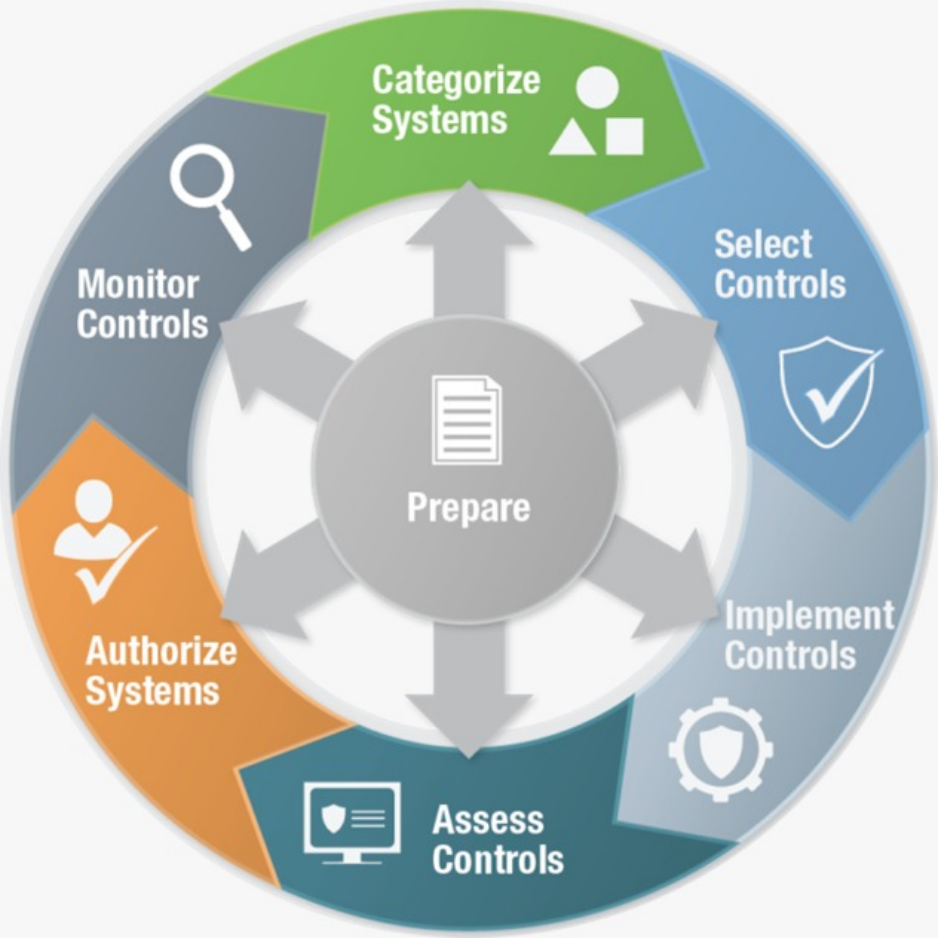
Demonstrate Understanding of the NIST RMF Process

Detailed Overview of the NIST RMF Process

The NIST RMF (Risk Management Framework) is a comprehensive and structured process designed to manage cybersecurity risks effectively. The process is organized into six distinct steps:

1. **Categorize:** In this first step, the information system, and the information it processes, stores, and transmits are categorized based on the potential impact on the organization if a security breach occurs. The categorization process considers the confidentiality, integrity, and availability (CIA) of the information, and it is aligned with the Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems."
2. **Select:** Once the information system is categorized, appropriate security controls are selected to mitigate identified risks. The selection of security controls is guided by NIST Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," which offers a catalog of controls organized by families. The organization's risk tolerance, mission, and operational environment must also be considered when selecting controls.
3. **Implement:** The selected security controls are then applied and integrated into the information system. The implementation process involves configuring hardware, software, and network components and documenting the details of the applied controls in a System Security Plan (SSP). Proper documentation is essential for understanding the system's security posture and ensuring the controls are implemented correctly.

4. **Assess:** The implemented security controls are evaluated for their effectiveness in mitigating risks. NIST SP 800-53A, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," provides guidance on assessment methods and procedures. The assessment process identifies any weaknesses or deficiencies in the security controls and generates a Plan of Action and Milestones (POA&M) to address them.
5. **Authorize:** Based on the assessment results, the Authorizing Official (AO) or a designated representative determines if the residual risk is acceptable and grants the information system authorization to operate (ATO). The Authorization Package, which includes the SSP, assessment results, and POA&M, is reviewed to make this decision.
6. **Monitor:** Continuous monitoring of the information system's security controls and risk posture is crucial to maintaining a robust security stance. The monitoring process involves tracking changes to the system, re-assessing the effectiveness of security controls, updating the risk assessment, and reporting the security status to relevant stakeholders.



Source: https://www.telos.com/offerings/xacta-risk-management-framework-rmf/

Threat Concept

Military Robotic Patrol

The mission of your robot is to protect a forward operating base (FOB) located in Southwest Asia. The FOB is situated in a hot and empty desert environment, surrounded by various-sized sand dunes. It is a temporary facility composed of tents serving different functions, such as a hospital, a machine shop, and sleeping quarters. There is also a large open space designated for parking ground vehicles and similar systems. To safeguard the FOB, a ring of barbed wire is in place, along with a fortified entry control point and sentries positioned strategically, both mounted and dismounted, at key tactical locations. Your robot is part of a team responsible for autonomously patrolling the FOB perimeter to detect any intrusions. These robots are not equipped with weapons and are solely intended to provide early warning to the sentries about potential attacks. They may patrol areas beyond the sentry line-of-sight, both during the day and at night, and could experience brief periods without communication range.

Possible threats to the FOB perimeter:

1. **Unauthorized Access:** Potential threats could include attempts by hostile forces to gain unauthorized access to the FOB perimeter or breach the entry control point. This could involve physical intrusion or attempts to disable or bypass security measures.
2. **Communication Interference:** Hostile actors may attempt to disrupt or jam the communication systems used by the robots and the sentries. This could hinder the robots' ability to relay real-time information or receive commands from the control center.
3. **Cyber Attacks:** The control systems and software powering the robots could be vulnerable to cyber-attacks. Threats such as malware, ransomware, or unauthorized access to the robot's operating system could compromise their functionality or allow an attacker to gain control over the robots.
4. **Sensor Spoofing or Tampering:** Adversaries may try to manipulate or tamper with the sensors on robots, such as cameras or proximity sensors. This could lead to false detections or blind spots, compromising the accuracy and effectiveness of the robots' intrusion detection capabilities.
5. **Physical Attacks:** The robots themselves could be subject to physical attacks, such as vandalism or destruction by hostile forces. Sabotage or tampering with the robot's components or power supply could render them inoperable.
6. **Data Breach:** If the robots store or transmit any sensitive or classified information, there is a risk of data breaches. Hostile actors may attempt to intercept or steal data captured by the robots, compromising the security of the FOB.
7. **Insider Threats:** It is crucial to consider the possibility of insider threats within the FOB. Unauthorized personnel or individuals with malicious intent who have gained

access to the FOB may pose a risk to the robots' operations or compromise sensitive information.

Thorough Threat Modelling

Security category vs security impact level

The security category is the classification assigned to the information system based on the sensitivity of the information processed (confidentiality, integrity, and availability). In contrast, the security impact level represents the degree of potential harm that could be caused by a security breach (low, moderate, or high).

Threat	Confidentiality	Integrity	Availability
Unauthorized Access	Medium	Medium	Medium
Communication Interference	Low	Medium	High
Cyber Attacks	High	High	High
Sensor Spoofing/Tampering	Low	Medium	Medium
Physical Attacks	Low	High	High
Data Breach	High	High	Medium
Insider Threats	Medium	Medium	Medium

Identification and Mapping of Cyber Controls to Counter Identified Threats

Technology based controls

Categorizing an information system requires information such as the types of data processed, the system's purpose and mission, the organization's risk tolerance, any applicable laws and regulations, and the potential impact of security breaches on the organization.

Threat	NIST Cyber Control Codes
Unauthorized Access	AC-2, AC-3, AC-6
Communication Interference	SC-7, SC-8, SC-13
Cyber Attacks	AC-17, AC-19, SI-4
Sensor Spoofing/Tampering	IA-5, IA-8, IA-9
Physical Attacks	PE-3, PE-6, PE-9
Data Breach	AC-16, AC-19, IR-4
Insider Threats	IA-2, IA-3, IA-4
Unauthorized Access	AC-2, AC-3, AC-6

Security policies

Threat	Security Policies
Unauthorized Access	Access Control Policy: Specifies rules and procedures for granting and revoking access to the FOB perimeter. Physical Security Policy: Defines measures for securing the entry control point and preventing intrusion.
Communication Interference	Communication Security Policy: Outlines protocols and encryption methods to protect against interference.
Cyber Attacks	Incident Response Policy: Establishes procedures for detecting, responding to, and recovering from cyber-attacks. System Hardening Policy: Defines configurations and measures to reduce vulnerabilities and strengthen security.
Sensor Spoofing/Tampering	Security Configuration Policy: Specifies secure configurations for sensors and devices used by the robots.
Physical Attacks	Physical Security Policy: Outlines measures to protect the robots from vandalism, theft, or physical tampering.
Data Breach	Data Protection Policy: Defines rules for safeguarding sensitive information captured by the robots. Data Encryption Policy: Specifies encryption methods for data at rest and in transit to prevent unauthorized access.

NIST RMF Process Applied to Competition Robot

Categorize:

1. Unauthorized Access
2. Communication Interference

3. Cyber Attacks
4. Sensor Spoofing/Tampering
5. Physical Attacks
6. Data Breach
7. Insider Threats

Threat Modelling

Threat	Confidentiality	Integrity	Availability
Unauthorized Access	High	High	High
Sensor Spoofing/Tampering	High	High	High
Physical Attacks	High	High	High
Insider Threats	High	High	High

Select and Implement

Threat	Security Policies	Explanation
Unauthorized Access	Access Control (AC-3)	Implements access controls to ensure that only authorized individuals have access to Team DARVIN's systems and resources. This policy includes defining user roles, permissions, and authentication mechanisms.
	Authentication (AC-2)	Implements strong authentication mechanisms to verify the identity of users accessing Team DARVIN's systems. This policy may involve the use of multi-factor authentication, passwords, biometrics, or other authentication factors.
	Security Awareness Training (AT-2)	Conducts regular security awareness training sessions for Team DARVIN members to educate them about potential threats, safe computing practices, and the importance of maintaining the security of their access credentials.
Sensor Spoofing/Tampering	Tamper-Evident Seals (SI-10)	Applies tamper-evident seals on critical components and sensors of the robots to detect and deter any unauthorized manipulation or tampering attempts.
	Physical Access Controls (PE-3)	Implements physical access controls to restrict and monitor access to Team DARVIN's robots and their sensitive components. This policy includes secure storage, controlled entry points, and surveillance measures.

	Configuration Management (CM-8)	Follows proper configuration management practices to ensure that the robots' software and hardware configurations remain secure and unchanged. This policy includes version control, change management, and integrity checks.
Physical Attacks	Physical Access Controls (PE-3)	Implements physical access controls to prevent unauthorized physical access to Team DARVIN's robots and their critical components. This policy includes secure storage, controlled entry points, and surveillance measures.
	Intrusion Detection System (SI-4)	Deploys intrusion detection systems to monitor Team DARVIN's robotic systems for any unauthorized physical access attempts or tampering.
	Security Monitoring (SI-4)	Implements security monitoring mechanisms to continuously monitor the status and activities of Team DARVIN's robots, sensors, and critical components. This policy includes log analysis, anomaly detection, and incident response.
Insider Threats	User Access Monitoring (AC-6)	Monitors and logs the activities of authorized users within Team DARVIN's systems to detect any suspicious or unauthorized actions. This policy helps identify and respond to potential insider threats promptly.
	Separation of Duties (AC-5)	Implements separation of duties to ensure that no single individual has excessive privileges or control over critical systems. This policy helps minimize the risk of insider threats and unauthorized actions.
	Security Awareness Training (AT-2)	Provides security awareness training to Team DARVIN members to educate them about the risks and consequences of insider threats and to promote a culture of security within the team.

Assess

For SOCRATES 2.0 in the IGVC competition, the assessment of cyber controls will be based on the demonstration strategies outlined in the report. These strategies will serve as a means to evaluate the effectiveness and functionality of the implemented controls in mitigating the identified risks. The assessment will focus on verifying whether the controls perform as intended and provide the desired level of security for the robot.

Authorize

The authorization of security controls for SOCRATES 2.0 rests with the Robot Team coach. The coach will review the security plan, assess the chosen controls, and evaluate their adequacy in addressing the identified risks. Based on this evaluation, the coach will either approve the implementation of the controls or request additional study to identify any potential gaps in security coverage. The authorization process ensures that the implemented controls align with the overall security objectives and requirements for the competition.

Monitor

Throughout the competition, regular monitoring of the security controls will be conducted. At the start of the competition, a comprehensive security audit will be performed to verify that all the intended controls are in place and functioning effectively. This audit will help ensure that the security posture of SOCRATES 2.0 remains intact and that no unauthorized changes or vulnerabilities have been introduced. Ongoing monitoring activities will be carried out to detect any deviations or anomalies that may require immediate attention.

Description of Implemented Cyber Controls

Relation of Chosen Controls to Mitigated Risk

1. AC-3: Access Control
    - Ensures that only authorized members have access to Team DARVIN's systems and resources.
    - Implements access controls, user authentication, and user role management to enforce proper access privileges.
    - Regularly reviews and updates access controls to align with changes in team membership and system requirements.
2. AC-2: Authentication
    - Implements strong authentication mechanisms to verify the identity of users accessing Team DARVIN's systems.
    - Utilizes multi-factor authentication, such as passwords, biometrics, or smart cards, to enhance the security of user authentication.
    - Establishes password policies and enforces regular password changes to mitigate the risk of unauthorized access.
3. AT-2: Security Awareness Training
    - Conducts regular security awareness training sessions for Team DARVIN members.
    - Educates team members about potential threats, safe computing practices, and their responsibilities in maintaining the security of access credentials.

- Raises awareness of social engineering attacks, insider threats, and the importance of reporting any suspicious activities.

4. SI-10: Tamper-Evident Seals
    - Applies tamper-evident seals on critical components and sensors of the robots to detect and deter unauthorized manipulation or tampering attempts.
    - Regularly inspects the seals to ensure their integrity and identifies any signs of tampering promptly.
    - Maintains records of seal inspections and actions taken in response to any tampering incidents.
5. PE-3: Physical Access Controls
    - Implements physical access controls to restrict and monitor access to Team DARVIN's robots and their sensitive components.
    - Establishes controlled entry points, secure storage facilities, and surveillance measures to prevent unauthorized physical access.
    - Maintains visitor logs, access control records, and conducts periodic reviews of physical access controls for effectiveness.
6. CM-8: Configuration Management
    - Follows proper configuration management practices to ensure the secure and controlled configuration of Team DARVIN's robots.
    - Establishes a configuration baseline and controls changes to software and hardware configurations.
    - Utilizes version control, change management, and integrity checks to maintain the integrity and security of robot configurations.
7. SI-4: Information System Monitoring
    - Implements security monitoring mechanisms to continuously monitor the status and activities of Team DARVIN's robots and critical components.
    - Deploys intrusion detection systems to detect any unauthorized physical access attempts or tampering incidents.
    - Conducts log analysis, anomaly detection, and incident response to identify and respond to security events promptly.

Design and Implementation Details of Controls:

1. Access Control Policy:
   Requires strong authentication for system access, role-based access controls, and regular access reviews.
2. Communication Security Policy:
   Enforces encryption and authentication protocols for secure data transmission.
3. Incident Response Policy:
   Defines incident detection mechanisms, reporting procedures, and incident handling and recovery processes.

4. Security Configuration Policy:
   Implements secure software and firmware configurations, regular updates, and integrity checks.
5. Physical Security Policy:
   Implements physical barriers, locks, and surveillance measures to protect the robot's physical integrity.
6. Data Protection Policy:
   Implements encryption for data at rest and in transit, access controls, and regular backups.

Description of Appropriate but Unimplemented Controls:

1. Network Security Policy (SC-7):
   Specifies additional measures to protect network infrastructure and detect network-based attacks.
2. Security Assessment and Authorization Policy (CA-2):
   Establishes a systematic approach to assess and authorize SOCRATES 2.0's security controls.

Demonstration Strategy:

1. Access Control (AC-3) and Authentication (AC-2):
   - Demonstration: Conduct a scenario where unauthorized access attempts are made to Team DARVIN's systems or resources.
   - Show how access control measures and authentication mechanisms prevent unauthorized individuals from gaining access.
   - Highlight the use of strong passwords, multi-factor authentication, and user role management in the demonstration.
2. Security Awareness Training (AT-2):
   - Demonstration: Organize security awareness training sessions for Team DARVIN members.
   - Include interactive activities, presentations, and discussions to educate team members about potential threats and safe computing practices.
   - Emphasize the importance of maintaining the security of access credentials and reporting any suspicious activities.
3. Tamper-Evident Seals (SI-10) and Physical Access Controls (PE-3):
   - Demonstration: Display the tamper-evident seals placed on critical components of Team DARVIN's robots.
   - Explain how the seals are designed to detect and deter unauthorized tampering attempts.

- Showcase the physical access controls, such as controlled entry points and secure storage facilities, to restrict unauthorized physical access to the robots.

4. Configuration Management (CM-8):
    - Demonstration: Showcase the configuration management process for Team DARVIN's robots.
    - Highlight the version control, change management, and integrity checks implemented to ensure secure and controlled configurations.
    - Demonstrate how changes to software and hardware configurations are properly documented, reviewed, and validated.
    - Intrusion Detection System (SI-4) and Security Monitoring (SI-4):
    - Demonstration: Simulate security events and intrusion attempts on Team DARVIN's systems.
    - Showcase how the intrusion detection system alerts and triggers appropriate responses to mitigate potential threats.
    - Highlight the security monitoring practices, such as log analysis, anomaly detection, and incident response, to detect and respond to security incidents promptly.