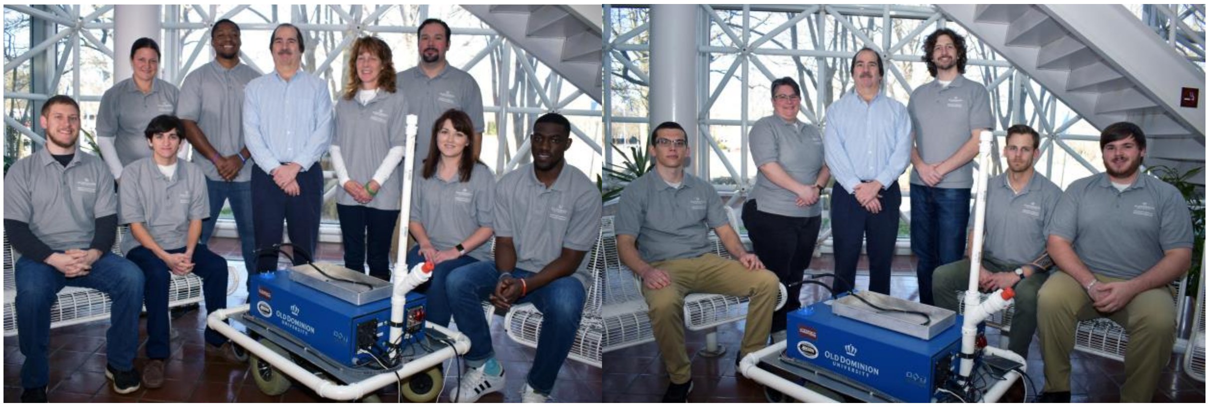
CYBER CHALLENGE

Old Dominion University

Batten College of Engineering & Technology



Date Submitted: May 17, 2019

Team Captains:

Bonnie Lee Miley (bmil001@odu.edu)

Dana Pelland (dpell001@odu.edu)

Team Members:

Mark Boyd (mboyd002@odu.edu)
Craig Earls (cearl001@odu.edu)
Jackie Edmiston (jedmi001@odu.edu)
Jason Felton (jfelt013@odu.edu)
Susana Long (slong001@odu.edu)
Carlos Martinez (cmart022@odu.edu)
David Osafo (dosaf001@odu.edu)

Preslav Ivanov (pivan001@odu.edu)
Ryan Miller (rmill001@odu.edu)
Taylor Roy (troyx001@odu.edu)
Justin Rush (jrush004@odu.edu)
Chase Vosler (cvosl001@odu.edu)

Graduate Adviser: Adam Seay (aseay001@odu.edu)

Intern: Ryan Redmon (rredm002@odu.edu)

We, the students of Old Dominion University, aspire to be honest and forthright in our academic endeavors. Therefore, we will practice honesty and integrity and be guided by the tenets of the Monarch Creed. We will meet the challenges to be beyond reproach in our actions and our words. We will conduct ourselves in a manner that commands the dignity and respect that we also give to others.

In addition, and as the faculty advisor, I hereby certify that the design and engineering of the vehicle (original or changes) by the current student team has been significant and equivalent to what might be awarded credit in a senior design course.

Faculty Adviser: Dr. Lee A. Belfore (lbelfore@odu.edu)

INTRODUCTION

This paper represents the conceptual design of our vehicle, IGOR, and its components. The design methodologies discussed in this paper covers all the processes we used to design the robot, but the focus will be on how we implemented the cyber controls needed to address the chosen cyber scenario.

Given the current implementation, the design methodology implemented is Continuous Process Improvement, specifically the DMAIC (Design, Measure, Analyze, Improve, and Control) principle. The DMAIC principle is considered a Lean Six Sigma (LSS) method looked upon favorably by government agencies because it focuses on the *reduction of waste* and *simplification* of processes. The letters within the principle itself are the abbreviations for the five phases of the Six Sigma Improvement [1]. By using this process, we started out by defining the existing project, developing a plan built around improving that project, defining the improvement process within the plan, and evaluating the existing project's progress [1]. From there, we needed to measure and collect all current data and analyze it [1]. Lastly, we need to move to improve the different items and systems on the project and organize ways to continuously measure and evaluate the progress accomplished within the project [1]. This methodology has allowed us to stay focused on the core design requirements of the competition. Once met, optimization of the vehicle's functionality related to the core design requirements will be addressed.

ORGANIZATION

This project is the culmination of predecessor teams, operating independently and often with complete redesigns. This year we have moved towards vertical integration by incorporating the preparatory design team into the current design team and creating a unique collaborative effort that utilizes a Lean Six Sigma (LSS) process of gap analysis and Continuous Process Improvement (CPI) to ensure the teams success. The competition team is interdisciplinary in nature and comprised of two distinct Electrical and Computer Engineering Senior Design II undergraduate engineering students and has primarily prepared not only to compete in the IGVC Design component, but also qualify for the Auto-Nav challenge.

Given the University's upward trend in the Auto-Nav challenge, Ms. Miley's teams' primary task is to ensure qualification for the 2019 IGVC. Ms. Pelland's team is focused on qualifying for the IOP and Cyber challenges, which is new for Old Dominion University this year.

The competition team has been split into four sub-teams, which are focused on documentation, safety, hardware, and software. Several team members share duties spanning several sub-teams, while some members have taken on more singular roles.

Name	Major	Primary	Secondary
Bonnie Lee Miley Dana Pelland	CpE[1] ECE[2]	Team Captain	Scheduling/Quality Control/Lab Tours/Fundraising
Susana Long Taylor Roy	CpE ECE	Project Lead	Documentation/Assignments
Craig Earls Ryan Miller	EE[3] EE	Hardware Lead	Safety Support
Jackie Edmiston Justin Rush	EE ECE	Hardware Support	Engineering Standards Finance
Carlos Martinez	CpE	Hardware Support	Requirements
Jason Felton Chase Vosler	ECE CpE	Software Lead	Finance
Mark Boyd Preslav Ivanov	CpE ECE	Software Support	Lab Tour Support
David Osafo	CpE	Safety Lead	Realistic Constraints

Table 1 – Tasks and Responsibilities

DEMONSTRATE UNDERSTANDING OF NIST RMF PROCESS

NIST RMF PROCESS OVERVIEW

The main purpose of Risk Management Framework (RMF) is to provide a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF process is divided into 7 steps. The first step of the process, the Prepare step, is simply an advance notice used by organizations to ensure that they are able to execute the other steps of the RMF process. The steps of the RMF are Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. Each of these steps are vital to the overall organizational RMF. Although the steps are generally performed in the order below, they can be done in a different order if the situation being addressed requires other steps to be done before others.

Prepare

[1] Computer Engineering

[2] Electrical Engineering and Computer Engineering (Dual Major)

[3] Electrical Engineering

This is the initial step for both organization and system level assessments. Organizations determine whether to update a current assessment or establish a new assessment. The Prepare step can essentially assist in previously implemented controls. Roles and responsibilities are assigned throughout the organization. A risk tolerance is established, and controls can be simplified by adopting common control profiles during the assessment. During the process a monitoring strategy is prepared to maintain implemented controls and determine controls effectiveness.

Categorize

The Categorize step is used by an organization to evaluate the system and the data being processed, stored and transmitted to determine what control needs to be implemented to reduce the impacts that could be felt by the organization if any loss of this data or system components occurs. This is performed by utilizing the following three tasks, System Description, Security Categorization, and Security Categorization Review and Approval, as the guideline for system evaluation.

The first task, System Description, allows the system owner to identify and document the characteristics of the system. To document the characteristics of the system, the system owner will utilize several different system documents available to them such as system design documents, processes that are controlled by system elements, information collected on system use, users and roles, and data maps for the information types used, stored, and transmitted by the system. All the data collected by the system owner is used to develop a documented description of the system being evaluated.

The second task, Security Categorization, allows the system owner to determine the security categories needed and to document the results collected from the system security categories. Several inputs, such as the system's security and privacy requirements and information about business processes supported by the system can be used by the system owner to develop the security categories needed. The inputs are utilized by the system owner to determine the impact of the information against each security category.

The third task, Security Categorization Review and Approval, allows the system authorizing official to review the security categories determined by the system owner and determine if they are valid for the system. The authorizing official will utilize inputs such as lists of organization assets, and the impact of the information from each security category collected during the second task. The desired outcome from this task is the overall approval of the security categories for the system.

Select

The controls selected in order to protect Nation, organizations and their external and internal assets are defined in the Select step. Ultimately, there are six tasks that establish guidance during the Select step. The tasks that complete the step are Control Selection, Tailoring, Allocation, Documentation, Monitoring, Reviewing and Approval.

Task one, Control Selection, defines two different methods of selection to select controls for the system and the environment of operation. The two methods defined are a baseline control selection or organization-generated control selection. Baseline control selections are predefined controls. They are targeted to provide consistency for multiple interests instead of just one. When customized controls are needed, organization-generated control selections method is used. This allows for an organization to define their own controls specific to their needs. Typically, controls for this method are for specialized or limited systems. Upon selection of method, both are subjected to the tailoring selections.

The second task, Control Tailoring, will take the broader selected controls combined risk assessments to tailor controls. An important factor that is taken into account, which informs and guides controls, are risk assessments. Controls can be categorized as common, system-specific, or hybrid controls and are defined in such a way that they support the level of protection and different systems of the organization.

The third task, Control Allocation, forms a working system that allocates common, hybrid, and system-specific controls with security and privacy requirements to the systems.

The fourth task, Documentation of Planned Control Implementations, is responsible for providing a detailed write-up to incorporate controls into the organization's security and privacy plans. Controls and their responsible systems are outlined in the plan are given sufficient information about their implementation and insure traceability of decision.

The fifth task, Continuous Monitoring Strategy, is designed to assist in monitoring post control implementation. The idea is to monitor the controls effectiveness to the systems and allow for changes during the development process.

The final task, Plan Review and Approval, allows the system owners or control providers to take all designated controls, their risk management levels and decide if the plan is complete and meet security and privacy components. Upon completion, either approval is given or further implementation and review is needed.

Implement

The Implement step is used to describe how the security controls identified by the system owner in the select step will be implemented into the system. The system owner will use the tasks, Control Implementation and Update Control Implementation Information, as guidelines to determine how to implement the controls.

The first task, Control Implementation, is used by the system owner to implement the security controls identified in the Select step. This is accomplished by using the approved security plans from the Categorize step, the system design documents, and a list of security and privacy requirements for the system. The desired outcome of this task is the successful implementation of the identified security controls.

The second task, Update Control Implementation Information, is used by the system owner document how the controls were implemented into the system. The system owner uses the security plans created to implement the controls to document the changes to the system. The outcome of this is that there is accurate and current documentation of the security stature of the system and the implemented security controls.

Assess

The Assess step is used by the Authorizing official, the Control Assessor, and the system owner to determine if the controls were properly implemented during the Implement step. The following six tasks, Assessor Selection, Assessment Plan, Control Assessments, Assessment Reports, Remediation Actions, and Plan of Action and Milestones, to assess the implementation of the controls.

The first task, Assessor Selection, allows the authorizing official to determine who will be selected to assess the implementation of the controls in the system. The outcome of this task is to have a team chosen to perform the assessment.

The second task, Assessment Plan, allows the authorizing official to develop and approve the plan that will be used by the assessment team to assess the implementation of the controls. The outcome of the task is that the authorizing official to have approved security assessment plans.

The third task, Control Assessments, allows the control assessor to assess the controls outlined in the assessment plan. The control assessor uses the security assessment plans developed and approved by the authorizing officer to assess the controls. After performing the assessment, the control assessor will use assessment evidence to provide completed control assessment reports.

The fourth task, Assessment Reports, allows the control assessor to document the results of the control assessment that was performed by the assessment team. The control assessor will use the findings of the assessment to develop the completed security assessment report. This report will detail all the findings the assessment team found during the control assessment as well as identify any recommendations made by the assessment team.

The fifth task, Remediation Actions, allows the System owner to correct any deficiencies identified in the assessment reports. The system owner will utilize the assessment reports generated by the assessment team to determine which of the implemented controls needs to be implemented better. The system owner will determine what actions need to be taken to perform remedial actions on any controls that did not pass the initial assessment.

The sixth task, Plan of Action and Milestone, allows the system owner to use the assessment report to develop the plan of action needed to implement any recommendations suggested by the assessment team. The system owner will utilize security assessment reports as well as security assessment results to develop the plan of action needed and identify the milestones that need to be remedied based on the reports.

Authorize

The Authorize step is used by the authorizing officer to determine if the security and privacy risks to the organization's assets are properly assessed and control implemented to authorize the system. The authorizing officer will utilize the following five tasks, Authorization Package, Risk Analysis and Determination, Risk Response, Authorization Decision, and Authorization Reporting, as guidelines to determine if the system can be authorized.

Task one, Authorization Package, is an initial package submitted with the most current information on security and privacy plans, their assessment reports, plans of actions and milestones, and executive summary for an authorizing official to make informed, risk-based decisions. Packages are reviewed by an appropriate official that meets all the levels of privacy and security requirements.

Task two, Risk Analysis and Determination, allows an authorized official to assess the authorization package and determine the current security and privacy exposure of the system.

Task three, Risk Response, is the process for an authorizing official to respond to risk exposures after risk analysis is completed and determined. Risks are either accepted or mitigated. Organization's decision also take in account acceptable residual risk.

Task four, Authorization Decision, will utilize the both organization's operations and risk responses from systems and controls to determine a decision whether a risk is acceptable or unacceptable. Decision are commonly submitted with feedback, authorization terms and conditions, and termination date or time-driven frequency.

Task five, Authorization Reporting, concludes that authorizing process by reporting decision and deficiencies made by the authorizing official to all included entities of the organization.

Monitor

The Monitor step ensures organizations are continuously informed of any changes to information systems and environment of operations along with their controls. The monitoring tasks are system and environment changes, ongoing assessments, ongoing risk response, authorization package updates, security and privacy reporting, ongoing authorization, system disposal.

The System and Environment Changes task is in charge of tracking the system and its environment of operations for unauthorized or authorized changes. The task is linked with any updated technology, plans, policies, and procedures. The expected result is to constantly keep systems and environment of operations at an authorized level of security and privacy.

The second task, Ongoing Assessments, is to perform ongoing assessments to controls after an initial system or common control authorization. This task monitors the controls effectiveness to the systems and establishes the monitoring frequency.

The third task, Ongoing Risk Response, is the action taken towards risk-based operations when risk response is acceptance or mitigation. Findings are documented and reported.

The fourth task, Authorization Package Updates, is an ongoing monitoring system that is capable of updating security and privacy plans, assessments, and plans of actions and milestones.

The fifth task, Security and Privacy Reporting, is reporting security and privacy posture of a system that is event-driven, time drive, or even and time-driven to authorizing officials.

The sixth task, Ongoing Authorization, is used to continuously review and determine whether risk to any system is acceptant or mitigation. Upon determination, authorization to continue or denial to continue of systems is enforced.

The seventh task, System Disposal, is responsible for properly disposing, updating inventory, and updating security and privacy plans of any systems removed from operation.

IDENTIFIED THREAT CONCEPT

For this competition, our team decided to use Scenario 1 from the provided scenarios. Below is the description of the scenario.

Scenario 1: Military Robotic Patrol

Your robot is part of a mission to protect a forward operating base (FOB) in Southwest Asia. It is a hot, empty desert environment surround by various sized sand dunes. The FOB is considered to be basic and temporary, and therefore consists of an arrangement of tents that serve various functions (including a hospital, a machine ship, and sleeping quarters) and a large open space to park ground vehicles and other similar systems. The FOB is under constant threat of attack by enemy forces and is therefore protected by a ring of barbed wire with a fortified entry control point, and sentries (mounted and dismounted) in key tactical locations. Your robot is part of a team of robots tasked with autonomously patrolling the FOB perimeter to detect intrusions. Your robots are not weaponized and only serve to provide early warning to sentries of an imminent attack. Your robots may also patrol areas around the perimeter that are out of the sentry line-of-sight, during daytime and nighttime, and be out of communication range for brief periods of time.

THOROUGH THREAT MODELING

Security category vs security impact level

All information and information systems are analyzed and sorted into one of the three categories representing the CIA triad. Any data that pertains to information access and protecting privacy and information will fall into the *confidentiality* category. Any data that is stored and require controls to prevent against modification or destruction will fall into the *integrity* category. Any requirements that require that the data be accessed in a timely manner will fall into the *availability* category. Each of these categories are then further categorized into security impact levels of low, moderate, and high. What impact level the data falls under is based on the effects that would be felt if the data experienced a loss of any of the categories occurred. So, while information and information systems will always be sorted into categories and impact levels, it cannot have impact levels without first being sorted into categories.

Information needed to categorize an information system

There is a variety of information needed to categorize an information system. The system owner will need to get any documents associated with network design, mission requirements, organizational specific information types, organization specific categorization policies and preliminary risk assessment result. Every information system is different however many of these documents are the same documents maintained by organizations.

Information system boundaries

The information system boundaries, also known as authorization boundaries, are used to establish the system consisting of the components contained within it. To define what components, make up the system many considerations are made. Some of those considerations are whether they support the same missions, how they process, store, and transmit information that is similar, and whether or not they are in the same environment of operation. Effective and meaningful authorization boundaries are essential for organizational mission success.

Types of information processed by information systems

Information processed by information systems is defined as any data that is provided as input or output of a system, data stored by a system, or data processed by a system. This information is divided into the following information types;

mission-based information types, management and support information, and any information not covered by the other two types and their sub types.

Mission-based information types are further divided into the business areas, services for citizens and mode of delivery. These business areas are then further divided into 26 direct services and delivery support lines of business with another 98 associated information types. Example of these mission areas are Homeland Security, Economic Development, Energy, and Intelligence Operations.

Management and support information types are further divided into the business areas, support delivery of services and management of resources. These are further divided into 13 lines of business with another 72 sub-functions. Examples of these are Revenue Collection, Planning & Budgeting, and General Government. All other information types not identified by the above two categories are assigned the general information type.

IDENTIFICATION AND MAPPING OF CYBER CONTROLS TO COUNTER IDENTIFIED THREATS

Defense-in-depth

Defense-in-depth is a construction of multilayer countermeasures that shields a cyber system from an attack. Defense-in-depth strategy utilizes the risk management framework to build its defense. This approach isn't 100 percent effective all the time. Risks are assessed and measures are built to deter and remove any single points of failures. Typically, this method only uses technology-based controls.

Technology based controls

Network and firewall security are important controls against cyber-attacks. These countermeasures are typically first line of defense in defense-in-depth strategy as they monitor network traffic and block or allow traffic through. Also, included are intrusion detection systems (IDS) and intrusion prevention systems (IPS) both these systems are responsible for assisting in alerting and protecting systems.

Management and operational controls

An important control that ensures coordination of all other controls is the inventory of all hardware and software. Once an inventory of all hardware and software is completed, continuous monitoring can be applied. This includes patch management and regular maintenance of a system. Since technology based controls are vulnerable to untrained users, another addressable control is employee cyber training. Finally, access controls are another form of management and operational implemented controls. These controls include user account and password management.

Security policies

Security policies are a control that aim to reflect organization policies, federal laws, Executive orders, directives, and other standards and guidelines in order to protect physical and information systems. Security policies cover physical security, personnel management, hardware and software, and operational vulnerabilities.

Holistic approach to information security

A holistic approach to information security is designing a defense-in-depth strategy to increase the adversary work factor. Information security remains exposed to many vulnerabilities such as human exposure, networks, software, and physical domains. First, protecting critical information resources requires an architecture that allocates security safeguards to defined locations and architectural layers. Second, requires systems and devices to be compatible and interoperable. Successful designs maximize the layers an adversary must penetrate before obtaining information resources.

NIST RMF PROCESS APPLIED TO COMPETITION ROBOT

DESCRIPTION OF IMPLEMENTED CYBER CONTROLS

Relation of chosen controls to mitigate risk

During the robot's patrols, threats to both network and information systems are vulnerable to attacks from outside and inside its environment. We want to only allow authorized users to be able to access the system at any time during patrols. The major risk we have identified is the need to prevent unauthorized access to the robot. The following three controls were chosen to mitigate the risk of unauthorized access to the robot; AC-3 Access Enforcement, AC-7 Unsuccessful Login Attempts, and AC-17 Remote Access.

Design and implementation details of controls

Information systems and active entities inside the robot are controlled by enforcing a password protected computer for the robot. When unauthorized attempts are made to access the computer system, the system denies the attempts.

To implement remote access controls on the robot, a Raspberry Pi with the Webmin software installed on it. This will be used to provide login access control as well as network security. Remote login to the system will be controlled with a few different controls. One control being used is to set up the authentication so that if a login attempt fails the user is blocked and eventually locked out. Another control being used is the enabling of a login timeout so that if the login isn't performed within a set time the user must attempt it again. Yet another control being used is the restriction of ports on the network so if a user attempts to connect to the robot from a port the robot is not listening for the robot will not allow it to be used. The final control that was implemented is that the robot is only usable on a private network. Any attempts to connect to the robot for an IP not on the private network will fail.

Description of appropriate but unimplemented controls

The following controls were identified as being applicable to support functions of the robot that support the scenario but were not implemented into the robot at this time; the SI-4 Information System Monitoring, PE-14 Temperature and Humidity Controls and SI-3 Malicious Code Protection.

DESCRIPTION OF CYBER CONTROLS DEMONSTRATION STRATEGY

Describe in detail how controls will be demonstrated

Controls implementation will be demonstrated three ways using simple audit options. The first way will be by demonstrating the restriction of access using port and IP access restrictions. This will be done through the setup of private network consisting of 3 nodes, the robot, and 2 computers, that will simulate the scenario setup. A third computer with a different IP address then the rest of the network will then attempt to access the robot. The outcome of this is that no connection to the robot is established.

The second way will be demonstrating access control through the use of a user account. A user account and password will be established for the evaluation team to log into the robot. The account will not have capabilities to change any settings in the robot. The evaluator will be able to connect to the robot using one of the computers on the network but will not be able to make any changes to the system.

The third way will be demonstrating incorrect login controls. This will be conducted by having the evaluator use a different password then the one set up for them. This should result in a failed login attempt. The evaluator will then make two more attempts, one of which be a login timeout attempt. The outcome of the fourth attempt will be a user lockout of the system.

RESOURCES

[1] “Continuous Process Improvement (CPI) and Lean Six Sigma (LSS).” Continuous Process Improvement (CPI) and Lean Six Sigma (LSS), www.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=3ac9f6c4-bede-4b63-9aac-7f4ba3c37162.

[2] National Institute of Standards and Technology Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008.

[3] National Institute of Standards and Technology Special Publication 800-37, Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, December 2010.

[4] National Institute of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.