Document Title: Requirements Specifications		
Document #: RS 01	Revision #: 05	Previous Doc/Rev #: RS01-05

CHANGE HISTORY

Rev.	Date	Detailed change description (include rationale for change)	Affected Documents	Supporting Documents
01	09/21/2023	Initial Release	N/A	<Top-level System diagram.>
02	9/29/2023	Updated the document with insights gained from the initial meeting with VSA. Added a verification approach.	N/A	<Poc_com_protocols_dtaft_V1_0>
03	10/13/2023	Updated the document based on customer's feedback	PoC, top-level system diagram	
04	10/18/2023	Added more target specifications and measurement devices for verification of the specifications.	Verification Test Plan	
05	11/12/2023	Revise target specifications table to better suit our verification test plan	Verification Test Plan	<Verification Test Plan>

DOCUMENT REVIEW AND APPROVAL

Name	Title	Contributed Sections	Signature/Date
Thomas Langley	Technical Lead	Definitions, Stakeholders, Project Requirements, Target Specifications, verification approach	TL 09/29/2023
Ryan Clarke	Security Lead	External Factors, Standards and Statutory Requirements	RC 09/21/2023
Patrick Aguda	Data Lead	Customer Needs, Product Requirements, Target Specs.	PA 09/21/2023
Sagar Ranga	Research Lead	Ethical factors, Definitions	SR 09/22/2023

Nithin Kumar	Project Manager	Social Factors, Definitions, Project Requirements	NK 09/21/2023
Sidnee McGee	Customer		
Joe Adams, Dr.	Mentor/ SME		
Walter Taraila	VSA Engineer		

TABLE OF CONTENTS

Purpose

To establish a clear and standardized set of requirements for the development of an overarching SCADA system designed to provide a unified interface across all MARS facilities, ensuring data visibility, logging, and manipulation with a focus on scalability, reliability, and security.

Definitions

Document Definitions

Table 01-1 Document Definitions

Term	Definition
Design History File	A compilation of records containing the complete design history of a finished device or service
Verification	Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled
Validation	Establishing objective evidence that system specifications conform to user needs and intended uses
Component	One of the parts that make up a system. A component may be hardware or software and may be subdivided into components
Functional Testing	Testing that ignores the internal mechanism of a system or component and focuses on the outputs generated in response to selected inputs

Document Acronyms

Table 01-2 Document Acronyms

Acronym	Description
DHF	Design History File
IEEE	Institute of Electrical and Electronics Engineers

CR	Customer Requirement
SR	System Requirement
VPN	Virtual Private Network
DAS	Data Acquisition Systems
IDS	Intrusion Detection Systems
VSA	Virginia Spaceport Authority
SCADA	Supervisory Control and Data Acquisition
PLC	Programmable Logic Controller
HMI	Human-Machine Interface
GUI	Graphical User Interface
MARS	Mid-Atlantic Regional Spaceport

Customer Needs

Problem Statement

Design and implement a SCADA system to integrate all MARS launch pad facilities, providing a unified, secured, reliable, and scalable interface that efficiently collects sensor and relay device data to the central server's database and GUI.

Customer Needs Description

Based on the high-level system development description provided by our customer our SCADA system would require four main parts, (1) scalable network technology, (2) server configuration development, (3) site control interfacing, and (4) security measures.

(1) Scalable Network Technology
Based on the project description provided by the customer, our SCADA system would require implementation of the overall design architecture using either a star or ring design. We have decided to utilize the star design due to its cost effective and less complex design compared to the ring design [1]. As displayed in the figure below each facility node represents the launchpad site systems that have their own local HMI. The central server would interconnect each of these systems and can be interfaced through a main UI. This design is also highly scalable, as more

facility nodes can be easily added to the system as long as the central server is capable of handling a large capacity of connected nodes. On the contrary, the ring design may have trouble incorporating additional nodes as it would have to be reconfigured each time a new node is added.

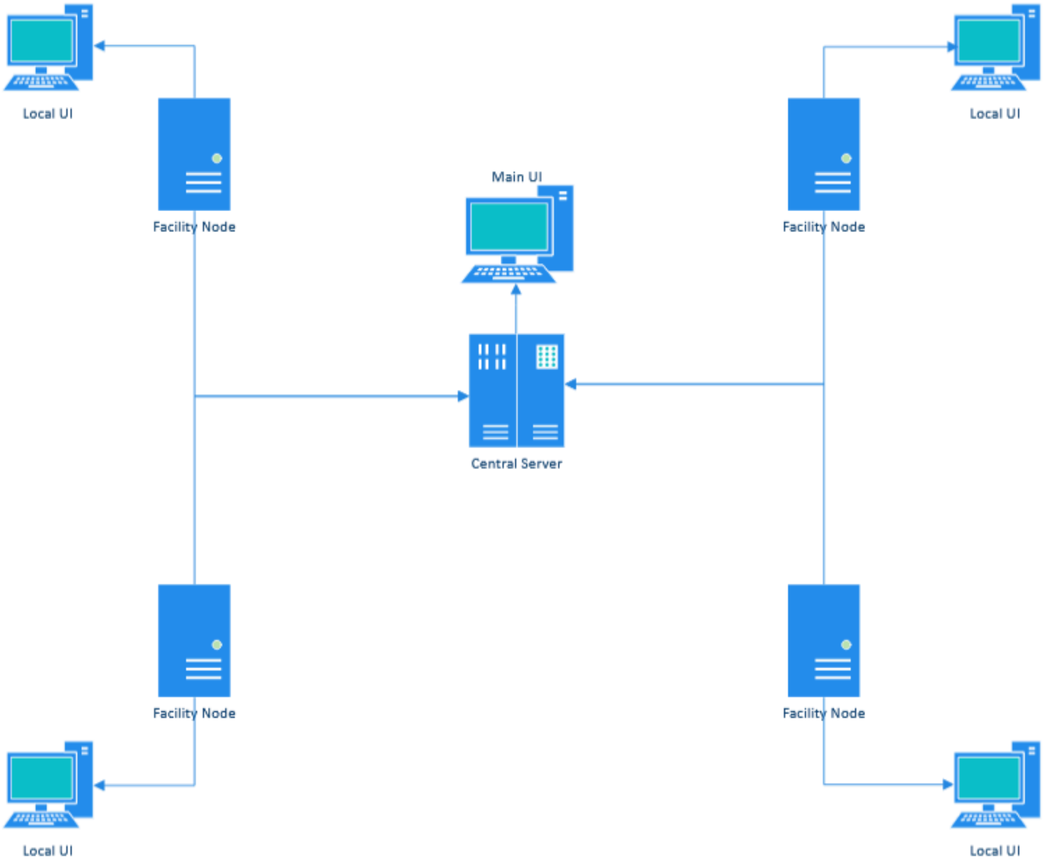

Figure 01-1 Top-level System Diagram

The customer would also require us to coordinate with the IT department to develop network diagrams and associated hardware. Eventually, once we have determined what materials are necessary to produce a prototype of our system, the customer would require a bill of materials, cable routing map, and any other related information records.

(2) Server Configuration Development
Our customer requires us to use redundant virtual machines in order to preserve data in the event of a server shutdown. We are expected to outline our development of the virtual machine. Additionally, the virtual machine must be divided into primary and secondary operations each having a historian to monitor the VMs. Lastly, all of these virtual machines will run through a hypervisor and are to be located on the central server.
Every server in our system must have a dedicated I/O port to deliver network communications that can be accessed through a client station interface.

(3) Site Control System Interfacing
This customer need may require us to stay in contact with the Virginia Spaceport Authority faculty to consult with their specific site control system experts. This requirement is needed to ensure that the Virginia Spaceport Authority is satisfied with our prototype and that it is compatible with their current and future hardware systems.

(4) Security Measures
This customer need was discussed during our first meeting with them on 09/28/2023. The customer emphasized that SCADA systems are infamous for cybersecurity vulnerabilities. Thus, it is paramount that our system is secured both by software and hardware means. In terms of software, this includes maintaining secure internet protocols. For hardware, this entails “air gapping” our system. Also important to note, is that our system must satisfy proprietary use. I.e. there should not be any interference with our system and any other connected systems from NASA or foreign spaceport related organizations.

Table 01-3 Current Customer Needs Table

Specific Needs	**Description**
Existing Systems and Software	-Current SCADA software (Aviva) is expensive -Encouraged to research open-source alternatives
PLCs	-Potential to use Allen-Bradley PLCs -Mentor suggested use of virtual PLC software
Communication Protocols	-Existing protocols include ethernet IP, profenet, and ethercat with Bekoff
Security and Networking	-Future infrastructure must be “air-gapped” -System must not “shell onto other sites” -Must integrate launch pads while maintaining robust security
Systems Engineering Approach	-Referral to NASA Systems Engineering Handbook -Preferred to use tiered organization requirements
Proof of Concept	-Demonstrate a working concept using an Arduino or PLC to emulate digital/analog signals as well as collect sensor data (e.g. thermostat)
Virtual Machine Configurations	-VM is to serve as the central server for the SCADA system (VirtualBox or Docker)

Key Stakeholders

1. Virginia Spaceport Authority (VSA):
   - As the governing body for spaceport activities in the state, the VSA will be directly impacted by the efficiency, reliability, and security of the SCADA system. Their operational success depends on the comprehensive visibility and control offered by this system.
2. MARS Facility Management Teams:
   - They manage the day-to-day operations of the individual facilities. The SCADA system will be their primary tool to oversee, coordinate, and troubleshoot processes across the MARS sites.
3. IT and Network Department:
   - This team will be responsible for the actual implementation, maintenance, and troubleshooting of the SCADA system. They would ensure the system's integration with existing IT infrastructure, maintain cybersecurity standards, and ensure the system's uptime.
4. Local and State Regulatory Bodies:
   - These entities have set guidelines and standards that the SCADA system and its operations must comply with. The compliance, safety, and environmental impact of the SCADA system directly concern them.
5. Launch Service Providers and Customers:
   - Companies or organizations that utilize the MARS facilities for their launch activities are directly impacted by the efficiency and effectiveness of the SCADA system. They rely on the facilities to ensure timely, safe, and coordinated launch processes. The SCADA system's data visibility, logging, and manipulation capabilities will have direct implications on their missions' success, scheduling, and cost-efficiency.

General Constraints

External Factors - Global, Cultural, and Environmental

The evaluation of external factors, including global, cultural, and environmental considerations, is essential for the success of the SCADA system. A critical component of the SCADA system is the security of the system. When considering security solutions, we must keep in mind that the system may need to adhere to global standards and regulations related to industrial control systems and data security, like the NIST Cybersecurity Framework [2] and the IEC 62443 series [3]. Non-compliance with these regulations can potentially lead to legal issues and financial penalties later down the road. Outside of standards, other global factors that could potentially impact the development of the SCADA system include geopolitical stability and global economic conditions. These factors are less directly related to the SCADA system, but can still impact the project timeline, budget, and resource availability if there were to be a disruption in the supply chain, rise in inflation, etc.

The cultural factors of this project deal a lot less with the technical aspect and focus more on the interpersonal communication between team members and stakeholders. With members and stakeholders coming from different backgrounds and cultures, it is crucial to understand and respect these cultural differences in order to prevent misunderstandings. Along with this, language barriers and differences in communication styles may arise as well. Proper cross-cultural communication methods are essential for team cohesion.

The environmental factors of this project focus mostly on climate variability. In order to keep the system intact, we must plan for extreme weather conditions, such as extreme temperatures, humidity, or natural disasters, as they can have a significant impact on the performance of the system. Due to the nature of the networking reliability in the system, it is a best practice to build a robust infrastructure with redundant servers. If one server goes down, a backup must be in place to prevent the entire system from failing. Environmental regulations must also be considered in the development of this system, as it is essential to avoid potential legal issues and further financial penalties.

Social Factors - Public Health, Safety, and Welfare

Due to the complexity of the SCADA system, public health, safety, and welfare will be a key standard that must be upheld throughout the project. As stated in the project specification, the purpose of the SCADA system is “to create overarching architecture for all MARS facilities to tie back into one common interface for data visibility, logging, and manipulation. [4]” Maintaining the standards for public health is demanded for the survival of this project. This requires every member of the project to be mindful of the environment and expectations set by the customer, subject matter expert, and mentor.

To increase the welfare of the Virginia Spaceport Authority, it is imperative that the SCADA system is created to reduce mistakes, miscommunication, and misunderstandings by having one common interface to handle all MARS facilities. Furthermore, having one interface to store information on launch pads and processing facilities online will be more efficient in data manipulation and visibility. The development of the graphical user interface will be useful in terms of the system architecture and networking. Having a user interface that will be able to “provide the full visibility into all systems at all sites [4]” is necessary for the success of the system.

The safety of the SCADA system is one of, if not the most important, aspect of this project. Also, safety precautions must be upheld throughout the creation of the system. Adhering to all lab safety practices such as no open shoes, untied long hair, safety goggles, construction hat, etc. Ensuring that these practices are always maintained is essential in the overall success of the SCADA system. The safety standards in engineering design must be accounted for as well. These safety standards include, but are not limited to: performance test codes, work safety designs, hazard controls, and documentation.

Ethical Factors - Global, Societal, Economic, and Environmental

Key aspects of the IEEE code of ethics [5] that relate to this include:

- To hold paramount the safety, health, and welfare of the public: The SCADA system will play a pivotal role in the operation of the MARS and we must ensure that it does not pose risk to human life or property.
- To strive to comply with ethical design and sustainable development practices: The SCADA system will be designed to meet industry standards to the best of our ability.
- To promptly disclose factors that might endanger the public or the environment: The SCADA system is energy intensive in nature and we will do our best to design it with energy efficiency and sustainability in mind.

The ethical dimensions involving the SCADA system for MARS include:

- The SCADA system is essential for space launches and any malfunction or security error could cause global implications which could affect the safety of the launches as well as other operations.
- The SCADA system will have many economic factors to be taken into consideration and there is an ethical responsibility to balance cost effectiveness and efficiency with prioritizing safety and security.
- The SCADA system will have significant environmental impacts from energy consumption alone. We need to design it with energy efficiency and minimal carbon footprint.

The SCADA system design will require many considerations to be made to fulfill our ethical obligations. We need to conduct thorough risk analysis to identify potential hazards in the system to prioritize safety and security. We need to ensure regular communication and transparency in handling sensitive data and critical infrastructure. Clear documentation is essential to ensure we are making correct efforts and adhering to ethical design principles. Comprehensive research needs to be carried out to identify opportunities for sustainable design like energy-efficient components. Additionally we will regularly consult the SME to facilitate ethical and sustainable design.

Product Requirements

Target Specifications

Target specifications are prioritized 1 to 5, 5 being the highest priority.

Table 01-5 Target Specifications

Req. #	Metric	Priority	Units	Marginal Value	Ideal or Target Value	Measurement Device(s)
SR-1	System operating temperature	5	°C	10 - 35°C	20-30°C	Thermocouples
SR-2	System Response Time	4	Seconds	<=3	<=1	Google Public NTP
SR-3	Network Bandwidth	5	Mbps	>=500	>=1000	Network Cable Tester
CR-1	System Operating Voltage	5	V	10-500V	110-240V	Oscilloscope
SR-4	System Data Logging Frequency	5	Seconds per log	Every 5	Every 1	Frequency Counter
SR-5	VM Boot-up Time	2	seconds	<=60	<=30	Central Time Source (CTS)
SR-6	System Monitoring Frequency (Health/Alerts)	5	seconds	Every 10	Every 2	Google Public NTP
CR-2	External Vibration Tolerance	3	g-force	Up to 1g without data loss	Up to 2g	Accelerometer
CR-3	Virtual Machine Configuration	4	NIST Standard	At least 1 VM per operation	2 VMs per operation	Hypervisor
CR-4	Communication Redundancy	5	# of Comm. lines	At least 1 Comm. line per node	2 Comm. Lines per node	Network Cable Tester

Table 01-6 Standards and Statutory Requirements

Req. #	Requirement	Source Document (e.g., standard,	Details

		regulatory requirements)	
SR-1	Server Configuration Development part 1: Configure redundant virtual machines	NIST CSF 2.0	Section 3.1: Creating and using framework profiles to understand, assess, prioritize, and communicate
SR-2	Scalable Network Topology, Server Configuration Development	IEC 62443	Standards for securing industrial controls systems against cyber threats and vulnerabilities
SR-3	Human-Machine Interfaces	ISO 92-41-410 [6]	Standards related to the ergonomic design of human-system interfaces, particularly displays and control software.
SR-4	Interoperability in Power Utilities	IEC 61850 [7]	Standards focused on data and communication exchange in power utility automation systems
SR-5	Quality Management System Requirements	ISO 9001:2015 [8]	Standards that specify requirements for establishing, implementing, and maintaining a quality management system within an organization. Emphasizes customer satisfaction.
SR-6	Security and Privacy Controls for Information Systems	NIST SP 800-53 [9]	Standards for protecting organizational operations and assets from a diverse set of threats and risks.
SR-7	Manufacture, Export and temporary Import of Defense Articles	ITAR Part 121 [10]	Standards for International Traffic in Arms Regulations, specifically the US Munitions List.

Verification Approach

The verification approach for this project is designed to ensure that all specified requirements are met and validated through practical tests and observations. Given the importance of communication protocols in this project, the initial verification will be done through the implementation of a proof of concept (POC) using an Arduino.

Proof of Concept

Objective: To demonstrate the feasibility of communication between PLCs and sensors using different communication protocols.

Tools and Equipment:
- Arduino board.
- Digital and analog sensors.
- RS485, RS232, and Modbus communication modules.
- Breadboard and necessary connection cables.

Steps for Verification:
1. Setup and Initial Test:
    a. Configure hardware and software.
    b. Conduct initial tests to ensure proper operation and data transmission.
2. Communication Test:
    a. Using RS485, RS232, and Modbus, set up communication links.
    b. Monitor data flow between sensors and the Arduino, ensuring consistency and accuracy of data collection.
3. Protocol Integration Test:
    a. Test data transmission using each protocol individually.
    b. Monitor and document latency, data loss, or other potentially problematic issues.
    c. Validate data received against expected values.
4. Failure and Recovery Test:
    a. Intentionally disrupt the communication, simulating different failure scenarios.
    b. Monitor and document the system’s ability to recover and re-establish communication post-failure.
5. Documentation:
    a. Document all observations, anomalies, and results during each test.
    b. Compare results with expected outcomes.

Expected Outcomes:
- Seamless communication between the Arduino and sensors using RS485, RS232, and Modbus protocols.
- Minimal to no data loss during data transmissions.
- Timely recovery during failure and recovery tests.

Future Extensions:

Once the initial POC is successful, the following extensions will be considered:

- Integration of additional communication protocols, as discussed during customer meetings.
- Introduction of cybersecurity measures to ensure data integrity and protection.
- Exploration of software solutions for centralized monitoring and control.

Benchmarking Information

Competitive benchmarking based on engineering metrics. This analysis can also be performed based on perceived satisfaction of customer requirements (i.e., user needs).

Table 01-7 Benchmarking Information (Will be expanded upon in future customer meetings)

Spec. #	Req. #	Metric	Priority	Units	<existing alternative #1>	<existing alternative #2>	<existing alternative #3>

References

[1] “Difference between Star and Ring Topology,” *www.tutorialspoint.com*. https://www.tutorialspoint.com/difference-between-star-and-ring-topology 9/21/2023

[2] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," NIST Technical Series Publications, NIST.CSWP.29.ipd.pdf, April 16, 2018. 9/21/2023

[3] IEC 62443, "Security for industrial automation and control systems (IACS)," International Electrotechnical Commission, Geneva, Switzerland, 2013. 9/21/2023

[4] MDE, “MDE ProjectList S24Projects v2.1 PDF” 9/21/2023

[5] IEEE, “IEEE Code of Ethics,” *ieee.org*, 2020. https://www.ieee.org/about/corporate/governance/p7-8.html 9/22/2023

[6] ISO, "ISO 9241-410:2008 Ergonomics of human-system interaction — Part 410: Design criteria for physical input devices," International Organization for Standardization, [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:9241:-410:ed-1:v1:en. 9/21/2023

[7] “IEC 61850 – Home.” https://iec61850.dvl.iec.ch/ 9/22/2023

[8] International Organization for Standardization, “ISO 9001:2015,” *ISO*, Mar. 26, 2015. https://www.iso.org/standard/62085.html 9/22/2023

[9] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," NIST Special Publication 800-53, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. [Accessed: September 29, 2023].

[10] ITAR Part 121 - The International Traffic in Arms Regulations, Title 22, Code of Federal Regulations, Section 121.