Upgrading Saint Louis University, Maryheights Campus' Turnstile System

9494 - IT 412 - TThS 1:30-2:30 PM

LAO-E, Adlei Vic

ABAYA, Jieben Kayla
ALIBA, John Rex
ANGWAY, Timothy
GARAS, Trisha Denise
LABAN, Paula Brittany
LUMBAS, Andrei Gail
ODCHEO, Jermin

NOVEMBER , 2024

I. INTEGRATION: BUSINESS CASE

II. INTEGRATION: STAKEHOLDER REGISTRY AND ANALYSIS

A. STAKEHOLDER REGISTRY

Stakeholder Name/Group	Role	Category	Interest Level	Influence Level	Key Concerns/Expectations
University Administration	Decision-makers and project sponsors	Internal	High	High	Budget approval, successful implementation, adherence to timeline and compliance.
IT Department	Technical support and system integrators	Internal	High	High	Compatibility with existing systems, smooth integration, and data security.
Maintenance Team	Responsible for system upkeep	Internal	Medium	Medium	Easy maintenance, availability of diagnostics, and durable hardware.
Office of Student Affairs	Manages student access and IDs	Internal	Medium	Medium	Efficient handling of temporary access for students.
Security Department	Manages physical security	Internal	High	High	Enhanced access control, anti-sneak features, and emergency response protocols.
Faculty and Staff	Daily users of the system	Internal	High	Low	Efficient and reliable access with minimal disruption.

Students	Primary users of the turnstile system	Internal	High	Low	Convenient and fast entry, provision for forgotten IDs, and smooth functionality.
Visitors	Occasional users of the system	External	Medium	Low	Easy visitor registration and seamless access during events.
Vendors and Suppliers	Provide turnstile hardware and software	External	Medium	Medium	Timely payment, clear requirements, and successful delivery of components.
Regulatory Authorities	Ensure legal and regulatory compliance	External	Low	High	Adherence to data protection laws and safety standards.

B. STAKEHOLDER ANALYSIS

Stakeholder Name	**Power**	**Interest**	**Current Engagement**	**Potential Management Strategies**
University Administration	High	High	Responsible for funding decisions and general project approval.	Frequent reference to and synchronization with their strategic plans.
IT Department	High	High	Oversees technical adoption, existing system integration,	Provide extensive technical documentation and collaborate on system integration with vendors.

			and resolving technical issues.	
Security Department	High	High	Aligns operational goals with project objectives.	Provide clear and comprehensive reports on security standard upgrades.
Students	Low	High	Primary users require updates on new features or system changes.	Conduct user surveys to assess satisfaction and ensure the system meets their needs.
Faculty and Staff	Low	High	Require updates on progress and system changes, as well as training for the new system.	Inform them of progress, timelines, and offer training sessions on system usage.
Regulatory Authorities	High	Low	Ensure compliance with data protection and safety regulations.	Engage early, conduct routine assessments, and provide records to ensure adherence to regulations.
Office of Student Affairs	Mediu m	Medium	Handles issuing of temporary passes and processing access exemptions.	Foster collaboration to align their processes with the upgraded system.

Vendors and Suppliers	Mediu m	Medium	Supply hardware and software, and require timely payments.	Maintain effective communication and ensure timely payments to avoid delays.
Visitors	Low	Low	Infrequent users require simple and user-friendly access.	Ensure the visitor pass system is easy to use and intuitive.

III. SCOPE: SCOPE STATEMENT

Project Title: Upgrading Saint Louis University, Maryheights Campus' Turnstile System	
Product Scope Description	Students, employees, and guests will have safe, automated access using Saint Louis University's improved turnstile system. It will provide self-diagnostic monitoring, online visitor pass registration, QR code-based temporary passes, and anti-trailing and anti-sneak features. The system will be equipped with waterproof, long-lasting hardware to endure the climate of Baguio City. In order to ensure smooth and effective access management, the project intends to improve campus security, maximize pedestrian traffic flow, and reduce manual interventions.
Project Objectives	1. Enhance security and operational efficiency at the campus gates. 2. Implement modern access control features such as QR code-based temporary passes, visitor pass integration, and anti-trailing technology.

	3. Ensure the system can manage large pedestrian traffic effectively. 4. Provide a durable, weatherproof turnstile solution suitable for Baguio's humid climate. 5. Reduce manual interventions with automated features such as self-diagnostic systems and emergency response.
Acceptance Criteria	***Functional Requirements:*** ● Students can successfully request and use temporary QR code passes via the student portal, valid for one day. ● Visitors can register online and use time-restricted digital passes for access. ● Anti-sneak and anti-trailing features are functional and detect unauthorized entry effectively. ● Emergency response features enable automatic unlocking of turnstiles during emergencies. ***Performance Requirements:*** ● Turnstiles can handle large volumes of pedestrian traffic without delays or failures. ● Self-diagnostic systems can monitor hardware/software and notify maintenance teams promptly. ***Technical Requirements:*** ● Hardware (turnstiles, QR code scanners, sensors) integrates seamlessly with existing IT systems. ● Software functions reliably with existing student portals and visitor management

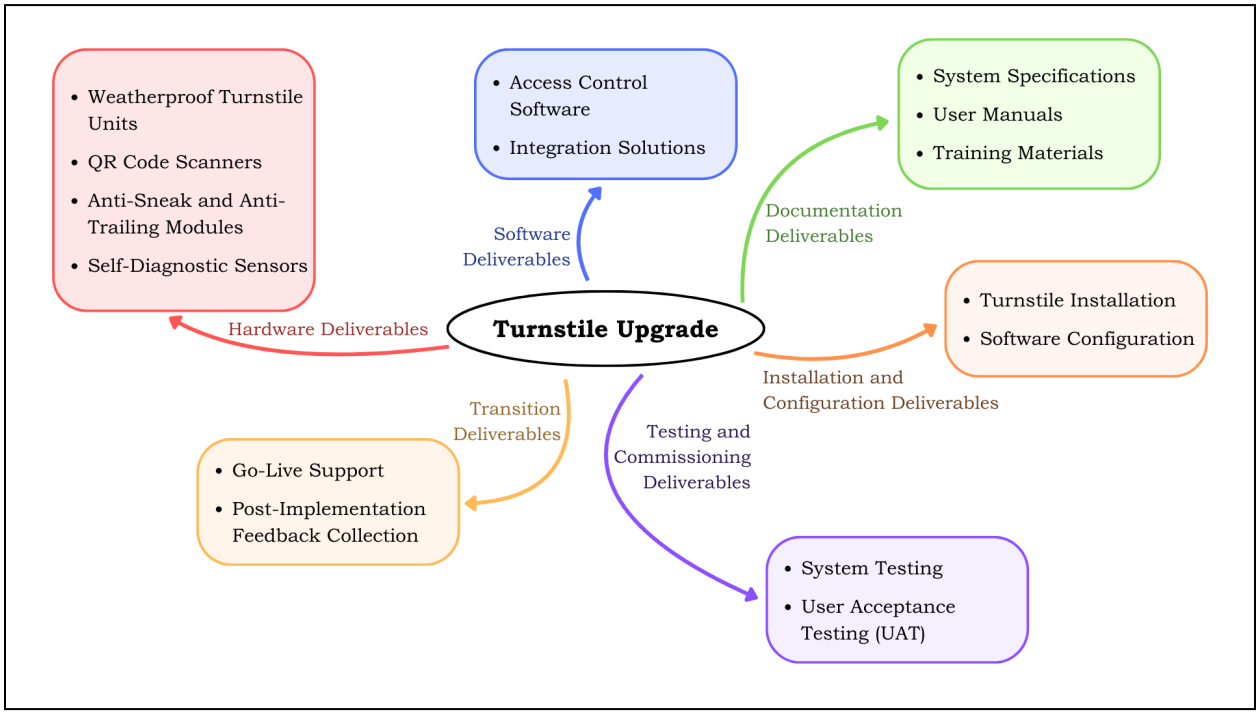
	systems. ***Durability Requirements:*** ● Weatherproof hardware resists rust and corrosion for at least 5 years under Baguio's humid conditions. ***Stakeholder Satisfaction:*** ● Positive feedback from students, staff, visitors, and campus security during post-implementation review.
Project Deliverables	***Hardware Deliverables:*** ● *Weatherproof Turnstile Units:* ○ Features: High durability, corrosion resistance, automated locking mechanisms. ○ Quantity: As per campus requirements. ● *QR Code Scanners:* ○ Integration with student portal and visitor management system. ● *Anti-Sneak and Anti-Trailing Modules:* ○ Sensors to detect unauthorized multiple entries and trailing individuals. ● *Self-Diagnostic Sensors:* ○ Real-time monitoring of hardware/software status. ○ Automated error detection and reporting features. ***Software Deliverables:*** ● *Access Control Software:* ○ Temporary QR code generation for students. ○ Online visitor registration and

	management. ● *Integration Solutions:* ○ API and backend integration with existing student and visitor management systems. ***Documentation Deliverables:*** ● *System Specifications:* ○ Detailed technical documentation for hardware and software. ● *User Manuals:* ○ Step-by-step guides for system users (students, visitors, staff, and security). ● *Training Materials:* ○ Resources for IT personnel and campus security staff. ***Installation and Configuration Deliverables:*** ● *Turnstile Installation:* ○ Proper placement and network connection setup. ● *Software Configuration:* ○ Tailoring features for SLU-specific requirements. ***Testing and Commissioning Deliverables:*** ● *System Testing:* ○ Functional, performance, and security testing to ensure reliability. ● *User Acceptance Testing (UAT):* ○ Testing by stakeholders to validate features and usability. ***Transition Deliverables:*** ● *Go-Live Support:*

	○ On-site technical assistance during the first week of implementation. ● *Post-Implementation Feedback Collection:* ○ Feedback from students, staff, and visitors to refine the system.
Project Scope	
Inclusions	● Installation of weatherproof turnstile units. ● Integration of QR code readers and sensors for real-time monitoring and access control. ● Development of software for temporary student passes and visitor pass management. ● Anti-sneak and anti-trailing security modules. ● Implementation of a self-diagnostic system to monitor hardware and software status. ● Automated emergency response mechanisms.
Exclusions	● External perimeter security systems beyond the turnstile areas. ● Advanced biometric authentication systems not related to QR codes.
Constraints	● The project must be completed during a semester break to avoid disruptions. ● The budget is fixed and must accommodate both hardware and software integration.
Assumptions	The existing IT infrastructure and student portal are compatible with the upgraded system.

	Skilled technicians and IT personnel will be available for installation and maintenance. Vendors will provide adequate training for the university staff.

IV. SCOPE: MINDMAP



V. SCOPE: WBS AND WBS DICTIONARY

VI. SCOPE: SWOT

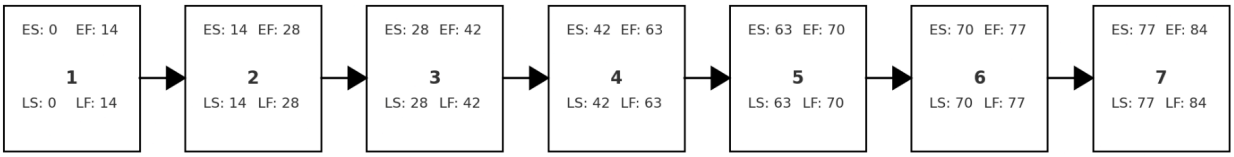
VII. TIME: GANTT CHART

VIII. TIME: MILESTONE LIST

IX. TIME: ACTIVITY LIST (CONSTRUCTION TO INSTALLATION)

ID	Activity List	Duration	Precedent ID	Relationship	Lead / Lag
1	**Project Initiation and Planning**	14	0		
2	**Requirement Gathering and Analysis**	14	1	FS	0
3	**Vendor and Material Selection**	14	2	FS	0
4	**Installation and Configurations**	21	3	FS	0
5	**Testing**	7	4	FS	0
6	**Go Live**	7	5	FS	0
7	**Post-Review**	7	6	FS	0

X. TIME: NETWORK DIAGRAM (PDM) - CONSTRUCTION TO INSTALLATION



XI. QUALITY: POLICIES AND RULES FOR THE USE OF TURNSTILE

1. General Entry Policy

- All individuals entering the campus must use the turnstile system for access control.
- Entry is restricted to students, staff, and visitors with authorized credentials (e.g., valid ID or QR code).
- Authorized personnel must ensure that their credentials are used only by themselves. Sharing or misusing credentials is strictly prohibited.

2. Temporary Access Rules

- Students who forget their ID cards can request a temporary QR code through the student portal. This QR code is valid for a single day.
- Visitors must pre-register online to receive a time-sensitive QR code valid for their visit. Access is granted only during the specified time frame.

3. Anti-Sneak and Anti-Trailing Measures

Advanced Sensor Technology:

- The system employs infrared and microwave motion sensors combined with machine-learning algorithms to analyze behavioral patterns at entry points.
- Sensors differentiate between legitimate entries and irregular activities, such as multiple individuals attempting to pass through on a single authorization.

Real-Time Analysis:

- A dedicated processing unit integrated into the turnstile system monitors entry data in real-time.
- Suspicious activity, such as simultaneous or close-proximity entries, triggers an automatic flag within the security management system.

Automated Security Alerts:

- Alerts are instantly transmitted to campus security via the central access control software, highlighting the location and type of incident (e.g., unauthorized trailing detected).
- Event logs are automatically recorded for further analysis and disciplinary action, ensuring accurate incident tracking.

Preventive Mechanism:

- Turnstiles are equipped with dual-door mechanisms or locking barriers that activate when a trailing attempt is detected, temporarily denying access and requiring manual intervention by security personnel.

4. Emergency Access Protocol

Automatic Unlocking Mechanism:

- Turnstiles are integrated with the university's fire alarm and emergency management systems.
- Upon detecting a fire alarm, power failure, or other emergency signals, the system triggers an emergency override to unlock all barriers simultaneously.

Fail-Safe Design:

- In power outages, the turnstiles utilize backup power supplies or mechanical fail-safe mechanisms to ensure barriers automatically disengage, maintaining compliance with egress regulations.

Routine Testing and Drills:

- Maintenance teams, in collaboration with campus security, conduct monthly simulation tests to verify the functionality of the emergency response protocol.
- Logs from these tests are reviewed to address any identified system deficiencies promptly.

5. Maintenance and Diagnostics

Self-Diagnostic System:

- Embedded Internet of Things (IoT) sensors continuously monitor hardware performance (e.g., motor functionality, sensor alignment, and barrier operation).
- The system is programmed to detect anomalies, such as unexpected mechanical resistance, temperature deviations, or communication errors with the central control unit.

Automated Alerts:

- In case of malfunctions, alerts containing diagnostic data are sent via the campus network to the maintenance team's dashboard, detailing the specific component and nature of the issue.

Preventive Maintenance Scheduling:

- Data from self-diagnostic systems are aggregated and analyzed to predict component wear-and-tear trends, enabling predictive maintenance scheduling to minimize downtime.

Tampering Protection:

- Turnstiles are equipped with tamper sensors that detect unauthorized physical interference or software access attempts.
- Any tampering attempt triggers an immediate alert, locking the system and notifying security personnel.

Penalties for Unauthorized Actions:

- Campus security is authorized to impose penalties, including fines and potential suspension, for individuals who deliberately damage or attempt to bypass the turnstile system.

6. Security and Privacy

- Data collected by the turnstile system (e.g., entry logs) will be stored securely and used solely for access control and security purposes.

- The system will comply with applicable data protection laws to safeguard personal information.

7. Weather-Resistant Usage

- Outdoor turnstiles must be maintained to withstand weather conditions. Regular inspections will ensure operational durability and safety.

8. Reporting Issues

- Users encountering technical difficulties or malfunctions should report them immediately to the campus IT support.
- Suggestions for improving the system can be submitted to the campus security office.

9. Code of Conduct

- Users must queue in an orderly manner to prevent congestion.
- Harassment, physical obstruction, or any behavior that disrupts the use of turnstiles is prohibited and subject to disciplinary measures.

XII. COMMUNICATIONS: PRODUCTION SCHEDULE (CONSTRUCTION TO INSTALLATION)

Phase 1: Pre-Implementation (Planning Phase)

Week 1-2

- **Activity:** Announce the project.
  - **Content:** Publish initial communication about the turnstile upgrade, objectives, and timeline via email, posters, and social media.
  - **Responsibility:** Campus Communications Office.
  - **Channel:** Email, SLU website, bulletin boards, social media platforms.
  - **Deadline:** End of Week 2.

Week 3-4

- **Activity:** Stakeholder briefing.
  - **Content:** Conduct meetings with students, faculty, and staff to present project details and collect feedback.
  - **Responsibility:** Project Manager and Communications Lead.
  - **Channel:** In-person meetings, webinars, official notices.
  - **Deadline:** End of Week 4.

Phase 2: Implementation (Execution Phase)

Week 5

- **Activity:** Update progress.
  - **Content:** Share updates about installation and testing progress.
  - **Responsibility:** Campus Communications Office.
  - **Channel:** Weekly email updates, website announcements.
  - **Deadline:** End of Week 5.

Week 6-8

- **Activity:** Inform users about disruptions.
  - **Content:** Notify campus users of expected interruptions or testing schedules during turnstile installation.
  - **Responsibility:** Communications Team and IT Department.
  - **Channel:** SMS notifications, social media, and on-site announcements.
  - **Deadline:** Rolling throughout the implementation phase.

Phase 3: Transition (Post-Implementation Phase)

Week 9

- **Activity:** Announce system go-live.
  - **Content:** Publish the official announcement about the operational start of the upgraded turnstile system.
  - **Responsibility:** Campus Communications Office.
  - **Channel:** Email, website, bulletin boards, social media.
  - **Deadline:** Day before the system goes live.

Week 9-10

- **Activity:** Provide user training resources.
  - **Content:** Distribute guides, tutorials, and FAQs on using the new system (e.g., QR codes, visitor passes).
  - **Responsibility:** IT Department and Communications Team.
  - **Channel:** Printed materials, online resources, in-person support stations.
  - **Deadline:** Day before the system goes live.

Week 10-11

- **Activity:** Collect feedback.
  - **Content:** Conduct surveys and feedback sessions to assess user experience and identify areas for improvement.
  - **Responsibility:** Project Team and Communications Team.
  - **Channel:** Online forms, in-person focus groups.
  - **Deadline:** End of Week 11.

Ongoing Communication (Maintenance Phase)

Frequency: Monthly or as needed.
Activity: Share updates on maintenance, policy changes, or system improvements.

A. **Responsibility:** Campus Communications Office.
B. **Channel:** Email, website, bulletin boards.

XIII. COMMUNICATION LETTERS

XIV. HR: HIRING PROCEDURES (CONSTRUCTION AND/OR INSTALLATION)

Step 1: Job Posting

The process begins by drafting job descriptions for roles like "Turnstile Technician" and "IT Integration Specialist," specifying duties, skills, and project duration. These descriptions will be reviewed and approved by the Project Manager and HR Department, then posted on external platforms such as JobStreet and LinkedIn. This step will be completed by <no date yet>. The HR Department is responsible for managing this phase.

Step 2: Candidate Sourcing & Pre-Screening

HR will source candidates through internal databases, referrals, and job boards. Resumes will be reviewed to shortlist candidates based on qualifications and experience, particularly in access control systems, RFID, and IT integration. A checklist will ensure alignment with project needs. The sourcing and pre-screening will conclude by <no date yet> with shortlisted candidates notified by <no date yet>. The HR Department will oversee this process.

Step 3: Screening

Shortlisted candidates will undergo initial phone or video screenings to assess their technical knowledge and communication skills. This will be followed by technical assessments, including practical tests focused on access control, IoT integration, and troubleshooting. This step will take place from <no date yet> to <no date yet>. The HR Department, supported by the Technical Team, will manage this phase.

Step 4: Interview Process

Formal interviews are scheduled between <no date yet> and <no date yet>, conducted by a panel comprising the Project Manager, IT Department Head, and HR Representative. Structured interviews will assess candidates on technical expertise, project fit, and contribution potential.

Step 5: Selection & Final Approval

The interview panel will meet on <no date yet> to review feedback and rank candidates. A decision meeting will finalize selections, with approvals from the Project Sponsor or Authorized University Representative. Offer letters will be issued by <no date yet>, detailing job titles, compensation, and start dates. Candidates have until <no date yet> to accept. The HR Department, alongside the Project Manager, will handle this step.

Step 6: Onboarding

Onboarding will begin on <no date yet>, including contract signing, IT setup, and a project overview covering roles, security protocols, and responsibilities. The HR Department and IT Support Team will oversee the onboarding process.

XV. HR: CONTRACTS

SLU Turnstile System Upgrade Project Contract

Saint Louis University
Turnstile System Upgrade Project Contract
Contract No.:
Date:

1. Scope of Work:
The Contractor agrees to provide services for the Turnstile System Upgrade, including:

- Installation of 8 RFID-enabled turnstiles with integrated QR code readers.

- Configuration of anti-sneak and anti-trailing features.
- Deployment of self-diagnostic IoT sensors for real-time monitoring.
- Integration with existing campus security systems.
- Comprehensive testing of the emergency response mechanism.

2. Project Timeline:
Start Date: <no date yet>
Completion Date: <no date yet>

3. Payment Terms:
Total Contract Value: 280,000
Payment Schedule:

- 30% (90,000) upon contract signing
- 40% (100,000) after installation and initial testing
- 30% (90,000) upon project completion and final review

4. Confidentiality:
The Contractor agrees to maintain the confidentiality of all information related to SLU's security systems and procedures.

5. Termination Clause:
Either party may terminate this agreement with a 30-day written notice under the following conditions:

- Breach of contract terms
- Mutual consent of both parties
- Non-performance by either party

6. Liability and Indemnification:
The Contractor shall indemnify SLU against any claims, damages, or losses resulting from the execution of services under this contract.

Signatures:

Adlei Vic Lao-e	Rev. Fr. Gilbert B. Sales, CICM
Project Manager	SLU President

Ms. Jenifer Balagot Head of the Finance Department

XVI. PROCUREMENT: REQUEST FOR QUOTATIONS (SUPPLIERS)

XVII. RISK: PROBABILITY/IMPACT MATRIX

XVIII. COST: LIST OF EXPECTED EXPENSES