2026 MIT STAMP WORKSHOP
SEPTEMBER 15-24, 2026

Unifal MG
Universidade Federal de Alfenas

Integrating DevSecOps and STPA for deriving safety, cybersecurity, and data privacy requirements with regulatory traceability: A case study of healthcare software under the Brazilian LGPD

Vinicius Henrique Piotto Boiago
viniciuspiotto.dev@gmail.com

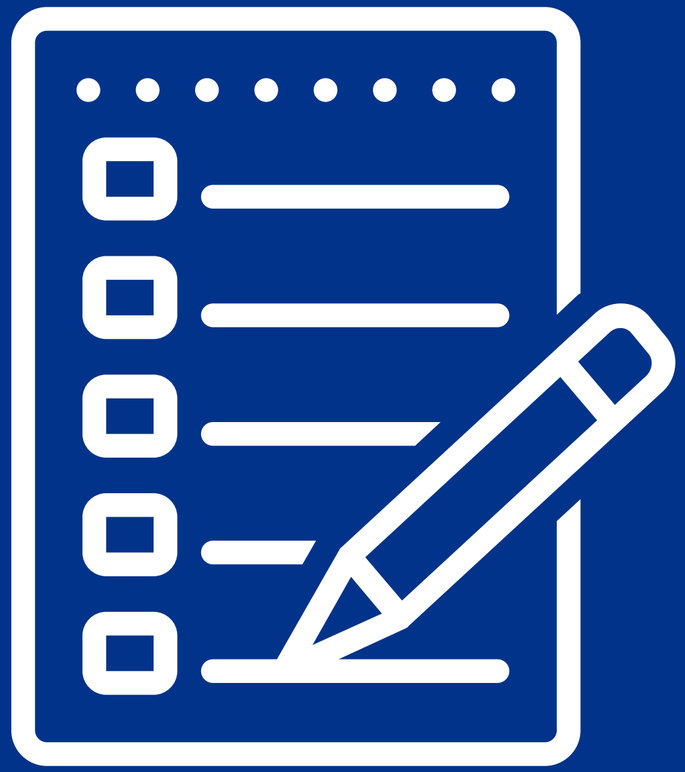
Isabelle Cristinne Pinto Costa
isabelle.costa@unifal-mg.edu.br

Fellipe Guilherme Rey de Souza
fellipeguilhermerey@gmail.com

Rodrigo Martins Pagliares
rodrigo.pagliares@unifal-mg.edu.br

Agenda

- Context and Motivation
- Problem
- Case Study
- Integration Artifacts
- Results and Conclusion



Context and Motivation

Context and Motivation

- DevSecOps pipelines are socio-technical environments whose outcomes depend not only on automated tools but also on human decisions, feedback, organizational policies, configuration, and coordination
- In this work, Trustworthiness is a shorthand for safety, cybersecurity, and data privacy.
- Regulated domains demand compliance with regulatory frameworks.





Problem

Problem

- Compliance alone does not guarantee trustworthy behavior.
- Conventional DevSecOps pipeline tools miss socio-technical and systemic conditions.
  - Limited support for socio-technical flaws and inadequate feedback.
  - Infrastructure as Code (IaC) Scanning, Static Application Security Testing (SAST), Software Composition Analysis (SCA), Dynamic Application Security Testing (DAST).





Case Study

- SisAPEC is an LLM-powered platform designed to support the Nursing Process.
- Implemented in 22 Primary Health Care Units and one hospital in Brazil, under the LGPD.
- Processes sensitive personal, including health data.
- We focus on the DevSecOps processes responsible for the development, verification, deployment, operation, maintenance, and evolution of the platform.



Integration Artifacts (STPA + Regulatory Mapping + Trustworthiness Requirements)

Unacceptable Losses

Loss
L-1: Unauthorized disclosure, exposure, destruction, or loss of control over sensitive personal data.
L-2: Non-compliance with applicable regulatory mandates.
L-3: Loss of institutional reputation and credibility.
L-4: Loss of the system’s ability to support the Nursing Process or maintain continuity of patient care.
L-5: Loss of life or injury to people.

Unacceptable Losses

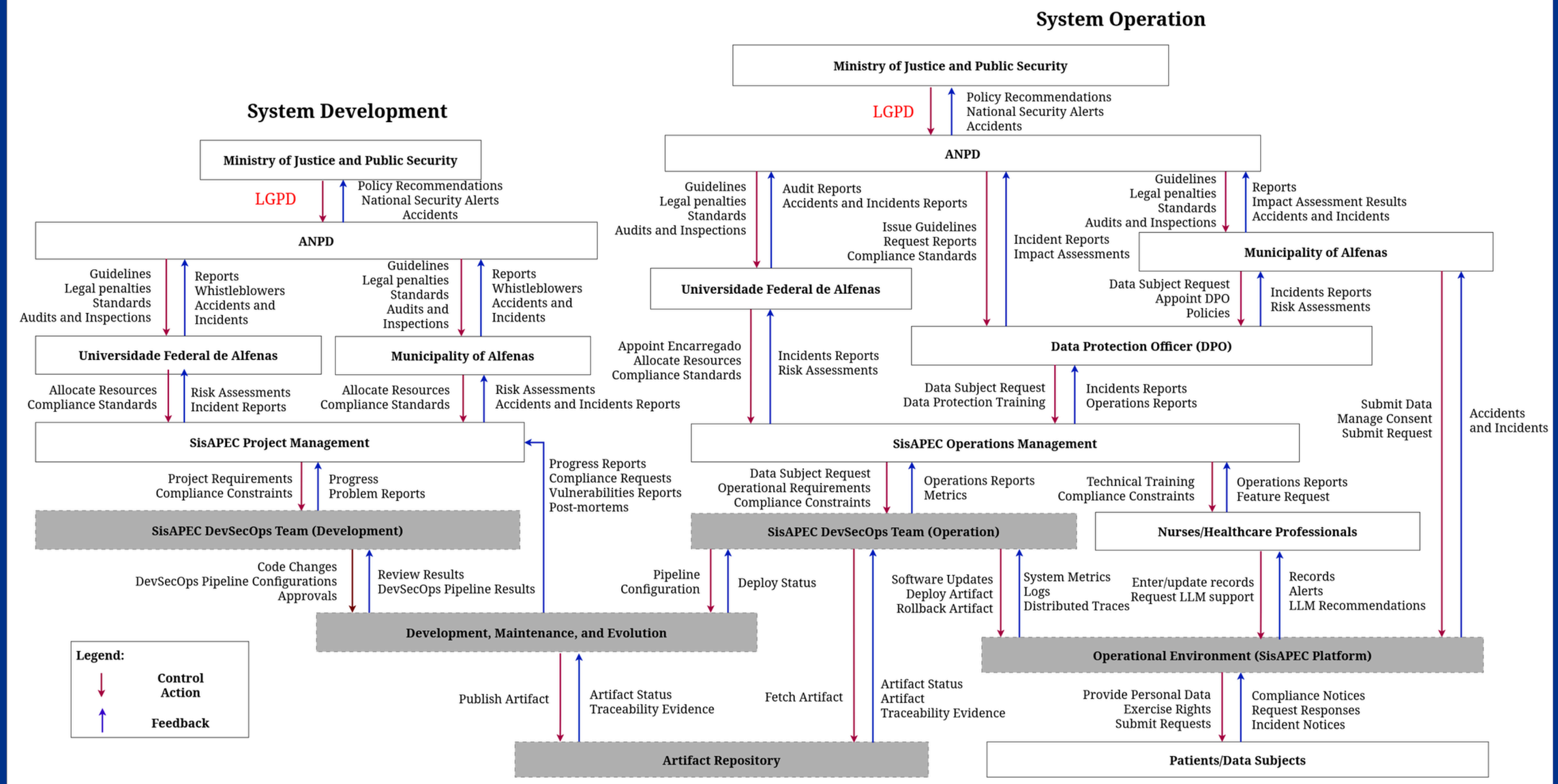
Loss
L-1: Unauthorized disclosure, exposure, destruction, or loss of control over sensitive personal data.
L-2: Non-compliance with applicable regulatory mandates.
L-3: Loss of institutional reputation and credibility.
L-4: Loss of the system’s ability to support the Nursing Process or maintain continuity of patient care.
L-5: Loss of life or injury to people.

Regulatory non-compliance modeled as an unacceptable loss.

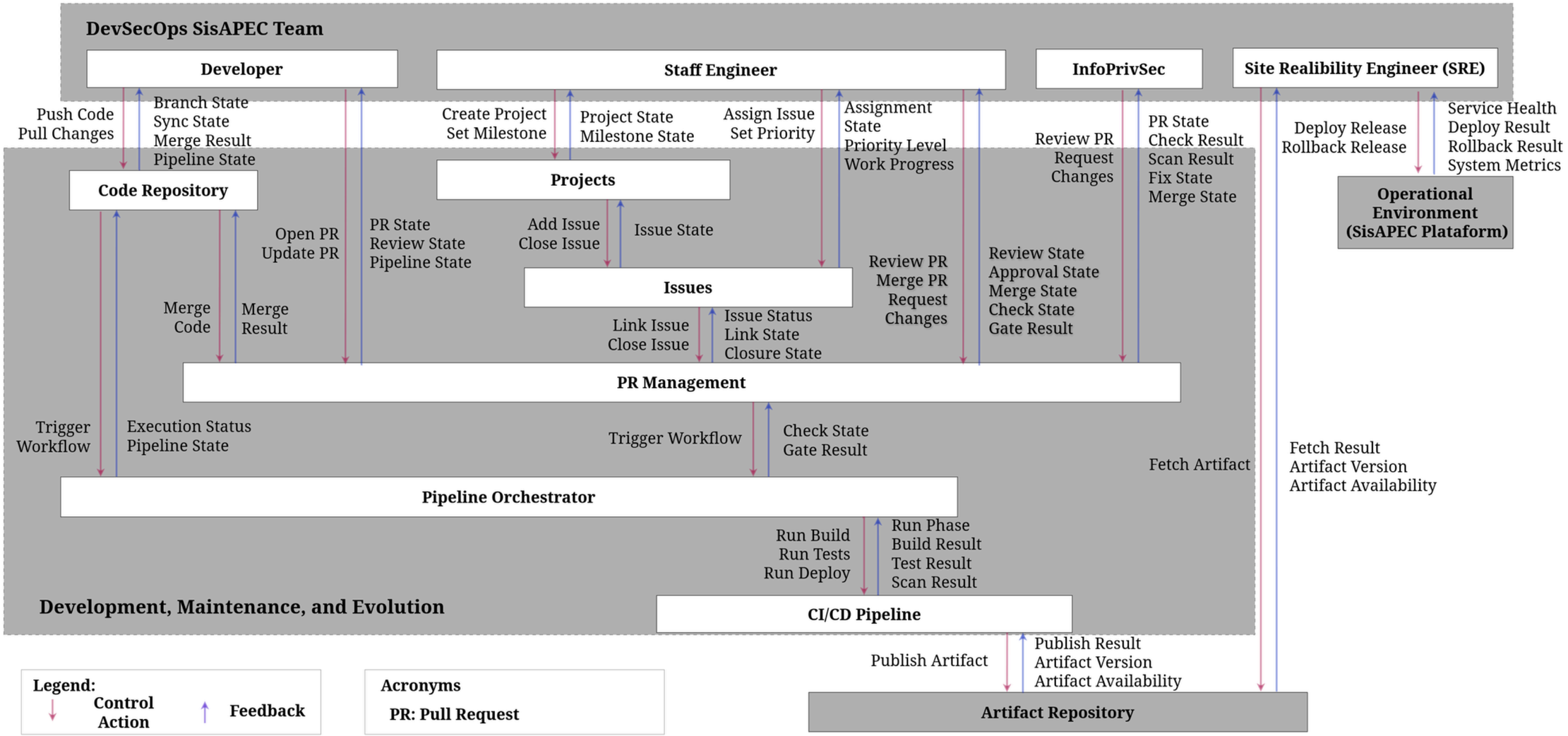
System-level Hazards and Constraints

System-level hazard	System-level constraint
H-1: Sensitive personal data are accessible outside the authorized scope. **[L-1, L-2, L-3]**	**SC-1:** SisAPEC must restrict access to sensitive personal data to authorized users, systems, purposes, and scopes. **[H-1]**
H-2: SisAPEC operates with unapproved or unverified software or configurations. **[L-1, L-2, L-4, L-5]**	**SC-2:** SisAPEC must operate only with software and configurations that have been approved and verified. **[H-2]**
H-3: SisAPEC processes sensitive personal data outside the permitted authorization, purpose, or use constraints. **[L-1, L-2, L-3]**	**SC-3:** SisAPEC must process sensitive personal data only when the applicable authorization, purpose, and use constraints are satisfied. **[H-3]**
H-4: Patient health records do not accurately represent the patient's clinical condition and history. **[L-2, L-4, L-5]**	**SC-4:** Patient health records must accurately represent the information required to support care. **[H-4]**
H-4.1: Patient health records contain incorrect information. **[L-2, L-4, L-5]**	**SC-4.1:** Patient health records must contain correct information or clearly indicate when information has not been verified. **[H-5]**
H-4.2: Patient health records omit information required for care. **[L-2, L-4, L-5]**	**SC-4.2:** Patient health records must include the patient information required to support care. **[H-4.2]**
H-4.3: Patient health records contain outdated information represented as current. **[L-2, L-4, L-5]**	**SC-4.3:** Patient health records must distinguish current patient information from outdated or superseded information. **[H-4.3]**
H-4.4: Patient health records contain mutually inconsistent information. **[L-2, L-4, L-5]**	**SC-4.4:** Patient health records must maintain consistency among related patient health information or clearly indicate unresolved conflicts. **[H-4.4]**

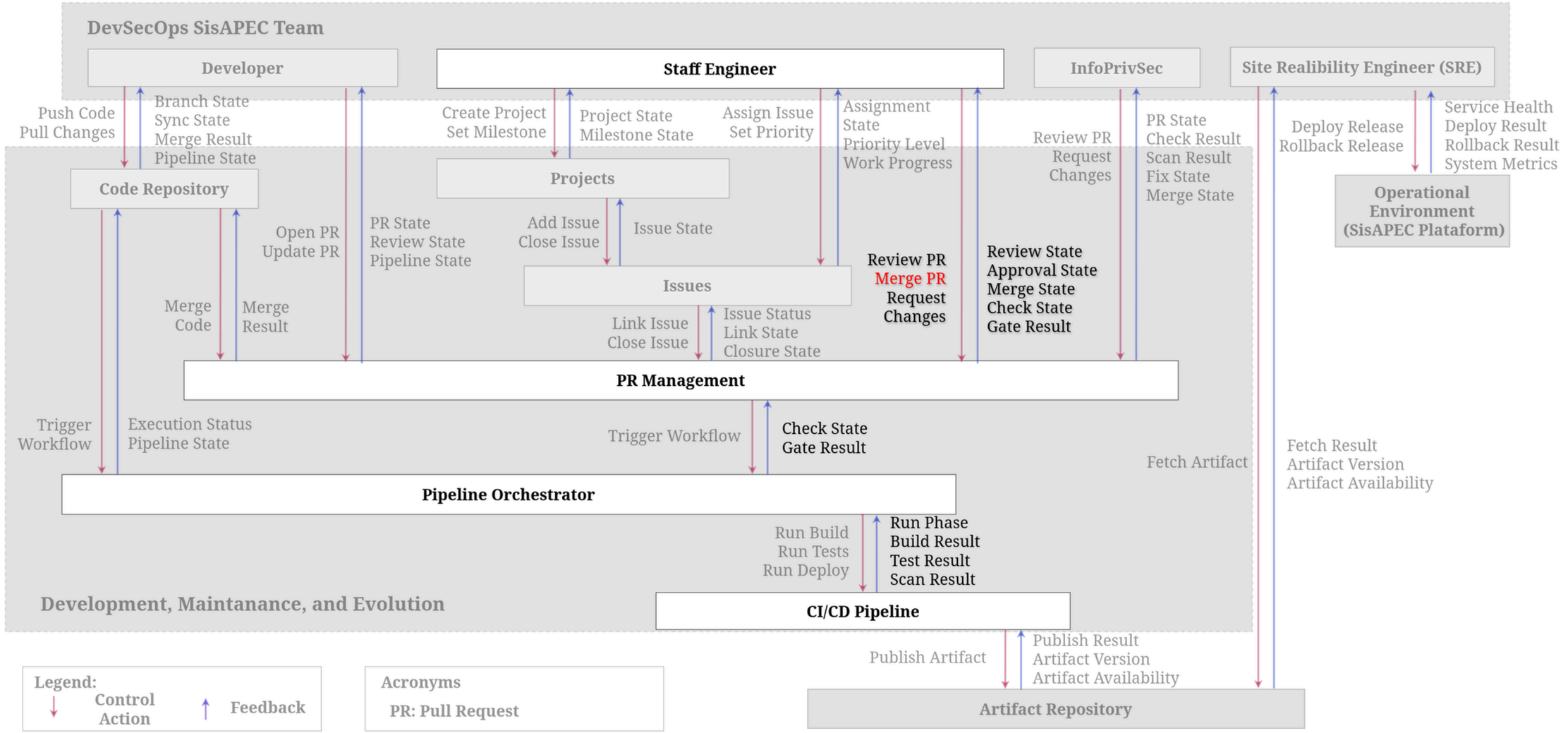
High-Level Socio-Technical Control Structure of SisAPEC



Refined Control Structure of the SisAPEC DevSecOps Processes



Refined Control Structure of the SisAPEC DevSecOps Processes



Unsafe Control Actions of Merge Pull Request

Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
UCA-9.1: Staff Engineer **DOES NOT PROVIDE** Merge Pull Request with a validated critical fix when all approvals and checks are satisfied. **[H-1, H-2]**	**UCA-9.2:** Staff Engineer **PROVIDES** Merge Pull Request during a deployment freeze or maintenance period. **[H-2]** **UCA-9.3:** Staff Engineer **PROVIDES** Merge Pull Request when InfoPrivSec approval does not cover the current commit. **[H-2, H-3]**	**UCA-9.4: Staff Engineer PROVIDES** Merge Pull Request **BEFORE** receiving the required peer approvals**. [H-1, H-2]** **UCA-9.5:** Staff Engineer **PROVIDES** Merge Pull Request **OUT OF ORDER**, **BEFORE** its prerequisite Pull Request are merged**. [H-2]**	N/A

Unsafe Control Actions of Merge Pull Request

Not providing causes hazard	**Providing causes hazard**	**Too early, too late, out of order**	**Stopped too soon, applied too long**
UCA-9.1: Staff Engineer **DOES NOT PROVIDE** Merge Pull Request with a validated critical fix when all approvals and checks are satisfied. **[H-1, H-2]**	**UCA-9.2:** Staff Engineer **PROVIDES** Merge Pull Request during a deployment freeze or maintenance period. **[H-2]** **UCA-9.3:** Staff Engineer **PROVIDES** Merge Pull Request when InfoPrivSec approval does not cover the current commit. **[H-2, H-3]**	**UCA-9.4: Staff Engineer PROVIDES** Merge Pull Request **BEFORE** receiving the required peer approvals**. [H-1, H-2]** **UCA-9.5:** Staff Engineer **PROVIDES** Merge Pull Request **OUT OF ORDER**, **BEFORE** its prerequisite Pull Request are merged**. [H-2]**	N/A

Causal Scenarios and Solutions

Class 2 - Unsafe Feedback Path		
UCA-9.1: Staff Engineer DOES NOT PROVIDE Merge Pull Request with a validated critical fix when all approvals and checks are satisfied		
High-level Scenario	**Refined Scenario (RSC)**	**Refined Solution (RFS)**
Pull Request **to** Staff Engineer **does not adequately indicate** the Pull Request contains a validated critical fix, all required approvals and automated checks are satisfied. The Pull Request Management **actually** contains a validated critical fix, all required approvals and automated checks are satisfied.	**RSC-9.1:** A vulnerability is identified in the SisAPEC patient record retrieval endpoint. The Developer submits a hotfix Pull Request, and the Pipeline Orchestrator completes all automated verification workflows successfully. Pull Request Management displays a passed status, but the Pull Request lifecycle-status feedback lacks any incident severity indicator. Managing multiple concurrent architectural reviews with no automated alerting to compensate for task-switching, the Staff Engineer does not read the Pull Request description's incident reference and treats the merge as routine, batching it with other pending merges and delaying the critical fix by hours while the production system remains exploitable.	**RFS-9.1.1:** Associate remediation Pull Request with the active incident, vulnerability severity, and remediation deadline, and place them in a dedicated merge queue once required checks and approvals pass. **RFS-9.1.2:** Send an immediate high-priority alert for validated critical fixes and escalate unacknowledged alerts to the on-call backup.

Estabilish Regulatory Traceability

Regulatory relationship	Regulatory Framework Articles	Scenario/Solution(s)
Timely remediation of a vulnerability affecting the protection of personal data.	Art. 6º, VII, VIII; Art. 46; Art. 47; Art. 49*	**RSC-9.1/ RFS-9.1.1 and RFS-9.1.2**

- Maps scenarios and solutions to regulatory mandates.
- Selective mapping linked to real regulatory mandates.
- Not every scenario receives a regulatory mapping.



*https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Derived Requirements

Derived Requirement (DR)	Trustworthiness Concerns	Regulatory Framework Articles
DR-1: The Pull Request Management system shall associate a remediation Pull Request with the active incident, vulnerability severity, and exposure SLA, and shall place it in a dedicated merge queue once all required checks and approvals pass. **[RFS-9.1.1]**	Cybersecurity, Data Privacy	Art. 6º, VII, VIII; Art. 46; Art. 47; Art. 49
DR-2: The Pull Request Management system shall send an immediate high-priority alert to the Staff Engineer for a validated critical fix, containing the incident identifier, affected service, exposure window, and mitigation deadline, and shall escalate to the on-call backup if unacknowledged. **[RFS-9.1.2]**	Cybersecurity, Data Privacy	

- Formalize solutions into trustworthiness requirements.
- Structured natural language with "shall" statements.
- Derived from causal analysis, not stakeholder statements.
- Atomic, verifiable requirements keeping full LGPD traceability.

Results and Conclusion

- 71 Unsafe Control Actions from refined control structure of the SisAPEC DevSecOps processes.
- 23 Causal Scenarios without component failure.
- Reveals untrustworthy behavior without individual component failures.
- Regulation-Agnostic.
- Future work: a fully systemic approach for deriving trustworthiness requirement with regulatory traceability.



2026 MIT STAMP WORKSHOP

SEPTEMBER 15-24, 2026

Unifal MG
Universidade Federal de Alfenas

Questions?

Vinicius Henrique Piotto Boiago
viniciuspiotto.dev@gmail.com

Isabelle Cristinne Pinto Costa
isabelle.costa@unifal-mg.edu.br

Fellipe Guilherme Rey de Souza
fellipeguilhermerey@gmail.com

Rodrigo Martins Pagliares
rodrigo.pagliares@unifal-mg.edu.br