



ADVANCED REACTOR SAFEGUARDS & SECURITY

Project: Glasshouse

Red Teaming To Analyze Observability and Control Pathways in A/SMR Remote Access

PRESENTED BY

Charles Nickerson

04/30/2026

INL/MIS-26-92179



Red Team: Where can I convert access into control?

Remote access enables control escalation



	CLASS 1 REMOTE MONITORING ONLY	CLASS 2 REMOTE ALLOW LISTED COMMANDS	CLASS 3 REMOTE CONTROL OF NON-SAFETY SYSTEMS	CLASS 4 REMOTE CONTROL OF SAFETY SIGNIFICANT AND IMPORTANT TO SAFETY SYSTEMS	CLASS 5 REMOTE CONTROL OF RELATED SAFETY SYSTEMS
WHAT IT MEANS	Observe operational data and system status. No commands are sent to the environment.	Execute predefined, allow listed commands to perform specific, limited actions.	Interactively control systems that are not safety significant and not important to safety.	Interactively control systems that are safety significant and important to safety.	Interactively control systems that are part of or directly related to safety functions (e.g., SIS logic, trips).
WHAT IT DOES NOT INCLUDE	No command execution or configuration changes.	No interactive control. No file transfer or configuration changes outside the allow list.	No access to safety significant or important to safety systems.	No direct changes to related safety systems (e.g., SIS logic or trip functions).	No unsupervised or standing access. Access is time-bound and purpose-limited.
ARCHITECTURAL FOCUS	Read-only visibility. Strict data one-way flow into the organization.	Command allow listing, validation, and constrained execution paths.	Session mediation, activity logging, least functionality, network segmentation.	Strong authentication, session recording, operator approval, change controls.	Maximum assurance: just-in-time access, dual authorization, continuous monitoring.
INBOUND PATH EXAMPLE	Data diode / one-way gateway or read-only replication	Secure gateway with command allow list enforcement	Mediated remote access gateway	Highly controlled gateway with operator verification	High-assurance, just-in-time access with dual authorization
OVERSIGHT LEVEL	LOW Observe Only	LOW-MEDIUM Constrained Commands	MEDIUM Controlled Access	HIGH Restricted & Monitored	HIGHEST Critical Control



As the potential impact increases, so do the architectural controls, session governance, and oversight requirements.

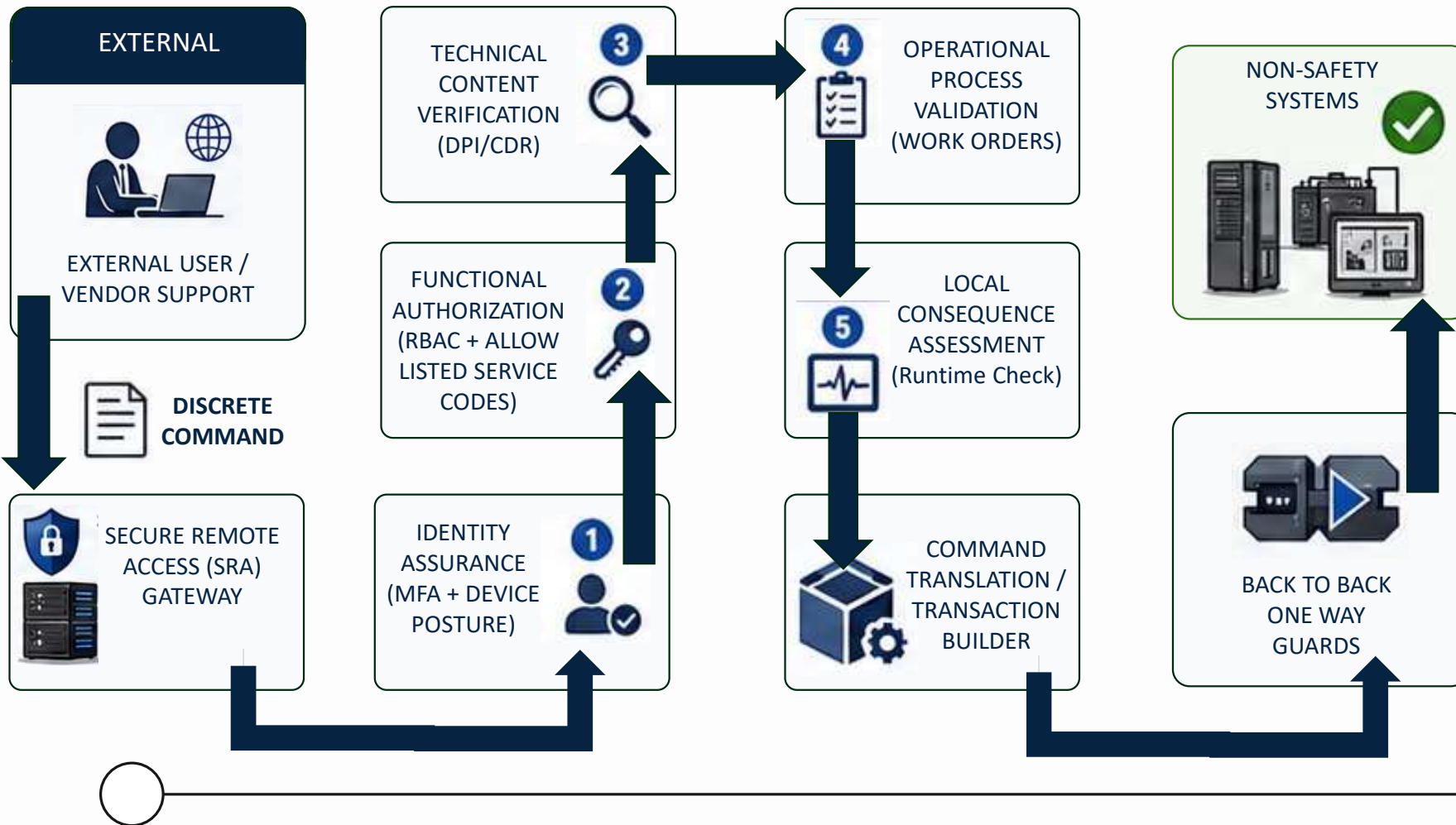


Red Team: What Does Class 2 Architecture Look Like?

Constrained logic becomes exploitable design



- ONLY PRE-APPROVED SINGLE COMMANDS EXECUTE.
- NO INTERACTIVE SESSIONS

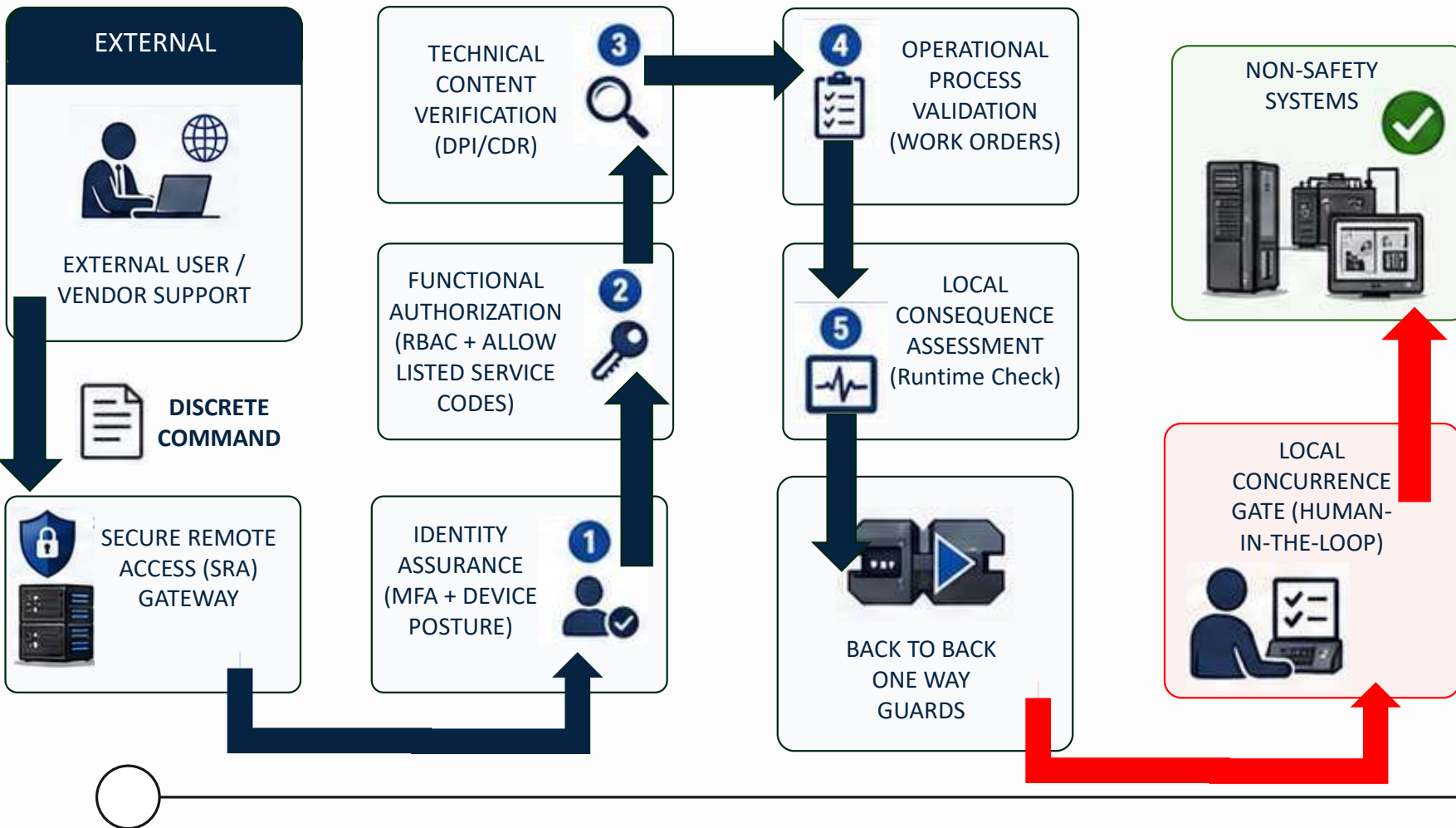


Red Team: What Does Class 3 Architecture Look Like?

A Complex Pathway To Trigger Allow-Listed Commands

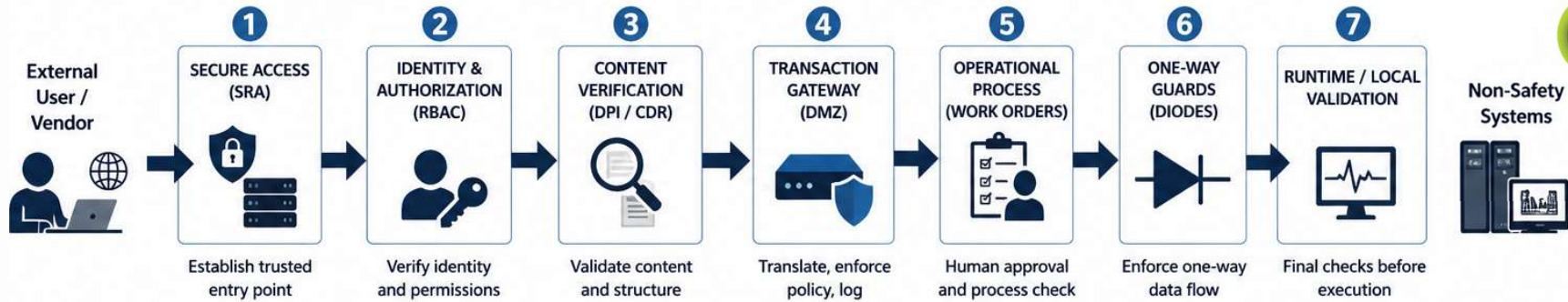


- CONSTRAINED REAL-TIME CONTROL OF NON SAFETY SYSTEMS ONLY.
- LOCAL AUTHORITY RETAINED



Red Team: How do I move through the Architecture?

Layered Controls Become Sequential Opportunities



ATTACKER PERSPECTIVE – OPPORTUNITIES TO MOVE FORWARD



1. The architecture is a sequence of control decisions rather than a single barrier. Each layer evaluates and passes forward only what meets defined criteria creating a path rather than a wall.



2. Trust is established at access and propagated through downstream controls. Systems rely on prior validation of identity, device, and role, so approved trust carries forward.



3. Constraints (RBAC, allow-lists, technical controls) define and enforce allowable behavior. This reduces risk but also creates predictable operating space to work within.



DEFENSIVE FOCUS – HOW WE STRENGTHEN THE PIPELINE



1. Continuously validate trust across layers, not just at the point of entry. Reassess identity, device posture, and behavior throughout the pipeline to detect drift or misuse (maloperations).



2. Evaluate commands and actions in context rather than just for correctness or compliance. Consider operational impact, asset criticality, and system state before allowing execution.



3. Incorporate cumulative, cross-system, and time-based effects into monitoring controls. Detect patterns and sequences that are invisible when analyzing individual events in isolation.



Red Team: How do I manipulate the defender's view?

Looking for observability and detection gaps



- 1. Selective Visibility (Exploit What Isn't Measured) |**
Operate outside the defender's field of view.
- 2. Log Shaping (Control The Narrative of Events) |** Attacker goal is to make recorded history incomplete or misleading.
- 3. Telemetry Manipulation (Break Reality <-> Data Alignment |** Attacker goal is to create mismatch between physical and reported states.
- 4. Threshold Gaming (Live Inside "Normal" |** Attacker goal is to avoid triggering detection logic.
- 5. Noise Engineering (Hide Signal in Volume) |** Reduce analyst attention and bury malicious activity
- 6. Context Manipulation (Influence Human Interpretation) |** Shape how the Human-In-The-Loop interpret data.
- 7. Process Exploitation (Abuse Trusted Workflows) |** Hide inside legitimate procedures.
- 8. Trust Anchor Subversion |** Undermine what defenders inherently trust.

