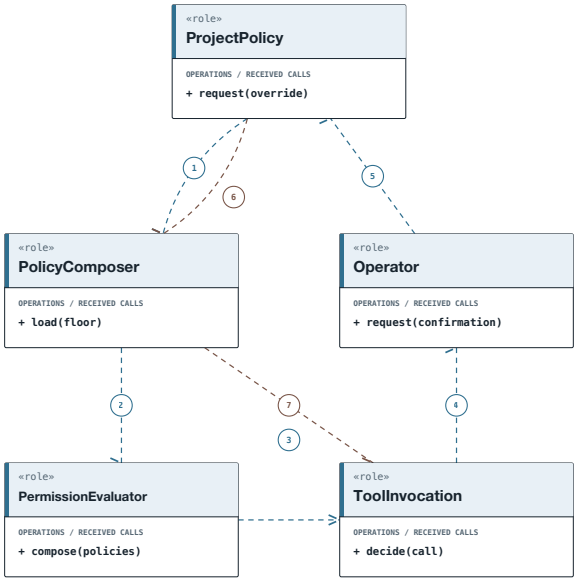
P22 Policy floor

Primitive / UML CLASS VIEW / ANALYTICAL MODEL

Preserve minimum restrictions across customization.

UML CLASS VIEW

dashed arrow: call dependency · brown: return/failure · analytical, not an observed trace



POINTCUT / PATTERN INTERFACE

CONTEXT	Multiple general, project, user, or session policies are merged.
TRIGGER	A proposed action is authorized under composite policy.
STRUCTURE	Minimum floor rules, merge operator, and privileged override path.
EFFECT	Composition cannot weaken protected restrictions without explicit authority.

CONTRACT / REQUIRED BEHAVIOR

REQUIRES	Rule identity and priority or set semantics are defined.
ENSURES	The merged result is at least as restrictive as every floor obligation.
INVARIANT	Local customization cannot silently erase a protected deny rule.
VIOLATION	Conflicts produce deny, escalation, or explicit configured precedence.

RELATIONSHIPS / ANALYTICAL CALLS

number · caller → callee · message

1 ProjectPolicy → PolicyComposer load(floor)
2 PolicyComposer → PermissionEvaluator compose(policies)
3 PermissionEvaluator → ToolInvocation decide(call)
4 ToolInvocation → Operator request(confirmation)
5 Operator → ProjectPolicy request(override)
6 ProjectPolicy ↩ PolicyComposer apply(override)
7 PolicyComposer ↩ ToolInvocation deny(failure)

VARIATION / TEST / NEGATIVE CONTROL

VARIATION	Intersection, ordered layers, scoped profiles, and administrative overrides.
TEST_OBLIGATION	Test widening, conflicting rules, missing policy, and privileged override.
NEGATIVE_CONTROL	A single configurable allowlist has no composition floor.