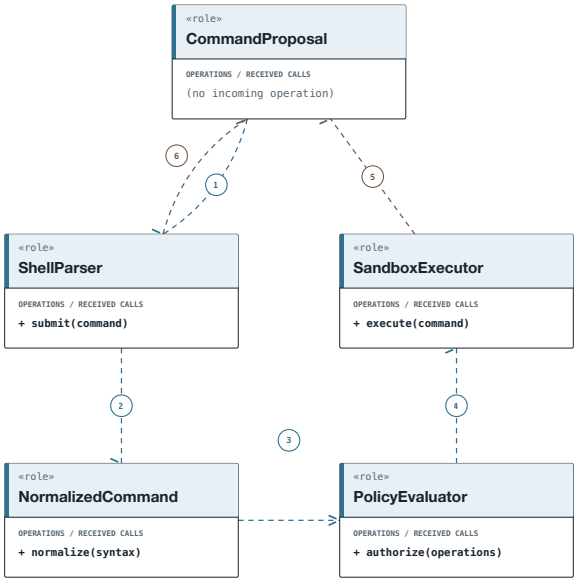
P21 Syntax-aware command permissioning

Primitive / UML CLASS VIEW / ANALYTICAL MODEL

Inspect command structure before execution.

UML CLASS VIEW

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



POINTCUT / PATTERN INTERFACE

CONTEXT	An agent proposes a shell command with security-relevant structure.
TRIGGER	The command is about to be parsed, classified, or executed.
STRUCTURE	Shell parser, normalized command tree, policy evaluator, and execution handoff.
EFFECT	Authorization uses parsed operations and a parse failure cannot fall through to execution.

CONTRACT / REQUIRED BEHAVIOR

REQUIRES	The command is representable by a parser or rejected before execution.
ENSURES	Every subcommand and redirection is covered by a policy decision.
INVARIANT	Parsed intent and executed command refer to the same normalized operation.
VIOLATION	Unsupported syntax fails closed or requests explicit review.

RELATIONSHIPS / ANALYTICAL CALLS

number · caller → callee · message

1 CommandProposal → ShellParser submit(command)
2 ShellParser → NormalizedCommand normalize(syntax)
3 NormalizedCommand → PolicyEvaluator authorize(operations)
4 PolicyEvaluator → SandboxExecutor execute(command)
5 SandboxExecutor ↩ CommandProposal return(result)
6 ShellParser ↩ CommandProposal reject(parse_error)

VARIATION / TEST / NEGATIVE CONTROL

VARIATION	Tree-sitter or shell AST, policy language, command aliases, and escalation.
TEST_OBLIGATION	Test pipes, substitutions, quoting, malformed input, and policy bypass attempts.
NEGATIVE_CONTROL	A substring denylist is not syntax-aware permissioning.