

HUPYY TEMPORAL - SMT-LIB VERIFICATION REPORT

Generated: 2025-11-04 10:39:48

Query ID: query\_1762281588

Status: UNSAT

Execution Time: 67 ms

## 1. PROBLEM STATEMENT

Based on the company policy document, can Marcus Webb (E-4782) perform WRITE operations on the Production Database at 11:47 PM EST on March 14, 2025 during the P1 production outage?

The additional necessary data is in  
/Users/alexanderfedin/Projects/happy/cofounder/happy-temporal/data/free-form/adhoc/testfile.txt

## **2. PHASE ANALYSIS (AI CONVERSION)**

Now I'll proceed with the systematic analysis following all 5 phases:

## ## PHASE 1: PROBLEM COMPREHENSION

**\*\*Problem Type:\*\*** access-control

**\*\*Domain:\*\* Corporate system access control with temporal constraints and security overrides**

\*\*External References:\*\* /Users/alexanderfedin/Projects/happy/cofounder/happy-temporal/data/free-form/adhoc/testfile.txt

**\*\*Reference Status:\*\*** all-loaded

**\*\*Complete Problem:\*\*** Based on the ACME Corporation System Access Control Policy and employee records, determine if Marcus Webb (E-4782) can perform WRITE operations on the Production Database at 11:47 PM EST on March 14, 2025 during a P1 production outage. The policy includes base access rules for engineers, clearance-based permissions, on-call overrides, and security compliance exceptions. Marcus Webb is a Senior Engineer with Senior clearance, is on the on-call rotation for March 10-16, 2025, but is under active investigation by Security Compliance since March 12, 2025 with ALL SYSTEM ACCESS SUSPENDED.

**\*\*Complexity:\*\*** medium

**\*\*Data Inventory (CRITICAL for verification queries):\*\***

- \*\*Data Sources Available:\*\* testfile.txt containing policy rules, employee records, security compliance records, and access attempt log

- \*\*Query Type:\*\* verification-from-data (asking "Can Marcus Webb perform WRITE?" based on specific facts)

#### - \*\*Data Extraction Plan:\*\*

- \* Marcus Webb's role: Senior Engineer (FACT from employee records)
  - \* Marcus Webb's clearance: Senior (FACT from employee records)
  - \* Marcus Webb's on-call status: YES for March 10-16, 2025 (FACT from employee records)
  - \* Marcus Webb under investigation: Active since March 12, 2025 (FACT from security records)
  - \* Security restriction: ALL SYSTEM ACCESS SUSPENDED (FACT from security records)
  - \* Access attempt timestamp: March 14, 2025, 11:47 PM EST (FACT from log)
  - \* Requested action: WRITE access (FACT from log)

## ## PHASE 2: DOMAIN MODEL

### ### Entities

#### **\*\*Variables:\*\***

- employee\_id: String -- Marcus Webb's ID (E-4782)

- has write access: Bool -- Whether Marcus Webb can perform WRITE operations

#### **\*\*Constants:\*\***

- role is engineer = true -- Marcus is a Senior Engineer

- role\_is\_engineer = true -- Marcus is a Senior Engineer
- clearance\_is\_senior = true -- Marcus has Senior clearance

- `is_on_call` = true -- Marcus is on on-call rotation March 10-16
  - `under_investigation` = true -- Marcus under active investigation since March 12
  - `access_suspended` = true -- Security compliance suspended all access
  - `time_is_2347` = true -- Access attempt at 11:47 PM
  - `is_business_hours` = false -- 11:47 PM is not within 9AM-6PM Mon-Fri

## **\*\*Functions/Relations:\*\***

- None (using propositional logic with constants)

### ### Constraints

1. Natural: Engineers have READ access during business hours  
Formal: (role\_is\_engineer and is\_business\_hours) -> has\_read\_access  
Entities: role\_is\_engineer, is\_business\_hours, has\_read\_access
  2. Natural: Senior clearance or higher gives WRITE access anytime  
Formal: clearance\_is\_senior -> can\_write\_normally  
Entities: clearance\_is\_senior, can\_write\_normally
  3. Natural: On-call rotation gives EMERGENCY OVERRIDE access 24/7  
Formal: is\_on\_call -> has\_emergency\_override  
Entities: is\_on\_call, has\_emergency\_override
  4. Natural: Under investigation suspends ALL access, overriding everything  
Formal: under\_investigation -> nohas\_any\_access  
Entities: under\_investigation, has\_any\_access
  5. Natural: Write access requires either normal write permission OR emergency override  
Formal: has\_write\_access ? ((can\_write\_normally or has\_emergency\_override)  
Entities: has\_write\_access, can\_write\_normally, has\_emergency\_override

### ### Ground Truth (from provided data files/logs)

**\*\*CRITICAL: Distinguish FACTS (from data) vs UNKNOWNS (not provided)\*\***

**\*\*FACTS to Assert (extracted from data):\*\***

- role\_is\_engineer = true (from testfile.txt line 14: "Role: Senior Engineer")
  - clearance\_is\_senior = true (from testfile.txt line 15: "Clearance Level: Senior")
  - is\_on\_call = true (from testfile.txt line 17: "On-Call Rotation: YES (March 10-16, 2025)")
  - under\_investigation = true (from testfile.txt line 23: "Status: Active")
  - access\_suspended = true (from testfile.txt line 25: "ALL SYSTEM ACCESS SUSPENDED")
  - time\_is\_2347 = true (from testfile.txt line 27: "March 14, 2025, 11:47 PM EST")
  - is\_business\_hours = false (11:47 PM is outside 9AM-6PM)

**\*\*UNKNOWNS (not in data, will be declared as variables):\*\***

- None (all relevant facts are provided)

## **\*\*Data Extraction Notes:\*\***

- This is a verification query asking if specific access is allowed
  - All relevant facts about Marcus Webb and the access attempt are provided
  - The security investigation and suspension are critical facts that override other permissions

### ### Query

**\*\*Question:\*\*** Can Marcus Webb perform WRITE operations on Production Database at the specified time?

**Approach:** direct-sat

- We want to find if write access is possible given the constraints
  - If SAT: Marcus can write (model shows how)
  - If UNSAT: Marcus cannot write (contradicts constraints)

**\*\*Selected Approach:\*\*** direct-sat

**\*\*Encoding Plan:\*\*** Assert has\_write\_access = true and check if satisfiable

## ## PHASE 3: LOGIC SELECTION

### ### Theory Analysis

- Quantifiers: NO -- Using propositional logic with concrete facts
  - Uninterpreted Functions: NO -- All relationships are explicit boolean constraints
  - Arrays: NO -- No array operations needed

- Arithmetic: None -- Only boolean logic required
  - Strings: NO -- IDs are handled as constants, not string operations
  - Datatypes: NO -- Only boolean values

### ### Decision

**\*\*Selected Logic:\*\*** `QF\_LIA`

### **\*\*Justification:\*\***

Since we're using pure propositional logic without quantifiers, functions, or arithmetic, we could use QF\_BOOL or QF\_LIA. QF\_LIA (Quantifier-Free Linear Integer Arithmetic) is a common choice that supports boolean operations and is widely supported by SMT solvers.

**\*\*Alternatives Rejected:\*\***

- QF\_BOOL: Could work but less commonly supported
  - ALL: Overkill for simple propositional logic
  - UFLIA: Not needed, no uninterpreted functions

## ## PHASE 4: SMT-LIB ENCODING

```smt2

```
;; =====
;; SMT-LIB v2.7 Encoding
;; Logic: QF_LIA
;; Problem: Access control verification for Marcus Webb
;; =====
```

```
(set-logic QF_LIA)
(set-option :produce-models true)
(set-option :produce-unsat-cores true)
```

```
;; =====  
;; SECTION 1: GROUND TRUTH (from data)  
;; =====  
;; These are FACTS extracted from testfile.txt
```

```
; From Employee Records (lines 14-17)
(declare-const role_is_engineer Bool)
(assert role_is_engineer) ; Line 14: "Role: Senior Engineer"
```

(declare-const clearance\_is\_senior Bool)  
(assert clearance\_is\_senior) : Line 15: "Clearance Level: Senior"

(declare-const is\_on\_call Bool)  
(assert is\_on\_call) : Line 17: "On-Call Rotation: YES (March 10-16, 2025)"

```
; From Security Compliance Records (lines 23-25)
(declare-const under_investigation Bool)
(assert under_investigation) : Line 23: "Status: Act"
```

(declare-const access\_suspended Bool)  
(assert access\_suspended) : Line 25: "ALL SYSTEM ACCESS SUSPENDED"

```
; From Access Attempt Log (line 27)
(declare-const is_business_hours Bool)
(assert (not is_business_hours)) ; 11:47 PM is outside 9AM-6PM Mon-Fri
...
```

### 3. GENERATED SMT-LIB CODE

Logic: QF LIA

```
(set-logic QF_LIA)
(set-option :produce-models true)
(set-option :produce-unsat-cores true)
```

```

;; Ground truth from testfile.txt
(declare-const role_is_engineer Bool)
(assert role_is_engineer)

(declare-const clearance_is_senior Bool)
(assert clearance_is_senior)

(declare-const is_on_call Bool)
(assert is_on_call)

(declare-const under_investigation Bool)
(assert under_investigation)

(declare-const access_suspended Bool)
(assert access_suspended)

(declare-const is_business_hours Bool)
(assert (not is_business_hours))

;; Derived variables
(declare-const has_read_access Bool)
(declare-const can_write_normally Bool)
(declare-const has_emergency_override Bool)
(declare-const has_any_access Bool)
(declare-const has_write_access Bool)

;; Policy constraints
(assert (=> (and role_is_engineer is_business_hours) has_read_access))
(assert (=> clearance_is_senior can_write_normally))
(assert (=> is_on_call has_emergency_override))
(assert (=> under_investigation (not has_any_access)))
(assert (=> access_suspended (not has_any_access)))
(assert (= has_write_access
          (and (or can_write_normally has_emergency_override)
               has_any_access)))

;; Query: Can Marcus Webb write?
(assert has_write_access)

(check-sat)
(get-model)

```

## 4. VERIFICATION RESULTS

Status: UNSAT

Wall Time: 67 ms

## 5. HUMAN-READABLE EXPLANATION

Proof:

- Marcus Webb (E-4782) role: Engineer [x]
- Marcus Webb clearance level: Senior [x]
- Marcus Webb on-call status: Active [x]
- Marcus Webb investigation status: Under investigation [x]
- Marcus Webb access status: Suspended [x]
- Time of access attempt: 11:47 PM EST (outside business hours) [x]
- Policy Rule 1: Engineers get read access during business hours only
- Policy Rule 2: Senior clearance grants write access normally
- Policy Rule 3: On-call status grants emergency override for write access
- Policy Rule 4: Under investigation -> No access permitted [ ]
- Policy Rule 5: Access suspended -> No access permitted [ ]
- Verification Step 1: Emergency override available (on-call = true) [x]
- Verification Step 2: Senior write access available (clearance = senior) [x]
- Verification Step 3: Access blocked by investigation status [ ]
- Verification Step 4: Access blocked by suspension status [ ]

- DENIED: Marcus Webb cannot perform WRITE operations due to active investigation and access suspension, which override all other permissions including emergency access

## 6. TECHNICAL DETAILS (APPENDIX)

### cvc5 Standard Output:

```
unsat  
(error "cannot get model unless after a SAT or UNKNOWN response.")
```

*Generated by Hupyy Temporal - Hupyy Powered SMT Verification*