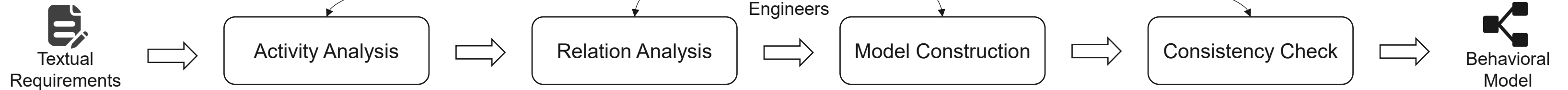


Human Experts on Behavioral Modeling



Textual Requirements

When the device is started, it should first perform **SIM card authentication** to verify the validity and legitimacy of the SIM card. **If the SIM card is invalid or not recognized**, the user will be prompted and subsequent operations will be blocked. **After the authentication is passed**, the device should **start the multi-factor authentication process** (such as **password**, **fingerprint**, **facial recognition**), and at least two authentication methods must be passed according to the security level set by the user. **Each authentication step should include a timeout and error handling mechanism**. **If multiple authentications fail** (such as more than 3 times), the device should lock the user account and **issue a warning notification**. **After successful authentication**, the device should record detailed information about the authentication event, including time, authentication method, and results, for subsequent security review and log analysis.

Activity Analysis

- SIM card authentication
- Start multi-factor authentication
- Issue a warning notification
- Password recognition
- Abort operation
- Authentication passed
- ...

Relation Analysis

Condition Branches: **Level 1**

Branch I: prompt user → abort operation → end

Branch II: start multi-factor authentication → **[Loop Structure]**

→ authentication passed → record authentication event details → regular re-authentication

Loop Branches: **Level 2**

Loop start → authentication type passed → **[Fork Structure]**

→ authentication failure counts → **[Condition Structure]**

Fork Branches: **Level 3**

...

Repeat the Decomposition Process

Condition Branches: **Level N**

Branch I: record authentication method

Branch II: timeout and error handling → authentication failure times +1

Model Construction

SIM Card Authentication

if SIM card is invalid/not recognized

Prompt the user

Abort operation

else

Initiate multi-factor authentication

while number of passed authentication methods < 2

fork

Password recognition

if authentication passed

Record the passed authentication method

else

Timeout and error handling

Authentication failure count+1

...

fork

Facial recognition

if authentication passed

Record the passed authentication method

else

Timeout and error handling

Authentication failure count+1

if authentication failure count > 3

Lock user account

Issue a warning notification

endif

Authentication passed

Record detailed information of the authentication event

Consistency Check

- ☑ Activity Analysis Check
- ☑ Relation Analysis Check
- ☑ Construction Syntax Check
-

Behavioral Model

