

System Failure Behaviour Aid

We can essentially define our application as a state machine at the time of writing this aid. For example, the "states" of the ATR (new, in-progress, complete). With this in mind, our system test cases define the end system behaviour when doing work.

Continuing with our ATR-related example, when the transporter is logged into the application, all ATR functionality is reactive to the transporter's instructions; this means that the ATR state defines what actions can be taken and each action defines a set of possible responses.

We define the following ATR actions:

1. Start a new ATR (ATR new state)
2. Editing an existing ATR (ATR in-progress state only)
3. Saving an existing ATR (ATR to be in-progress state still)
4. Saving an existing ATR (ATR to be in complete state now)
5. Deleting an existing ATR (ATR in-progress state only)

We define the following system responses:

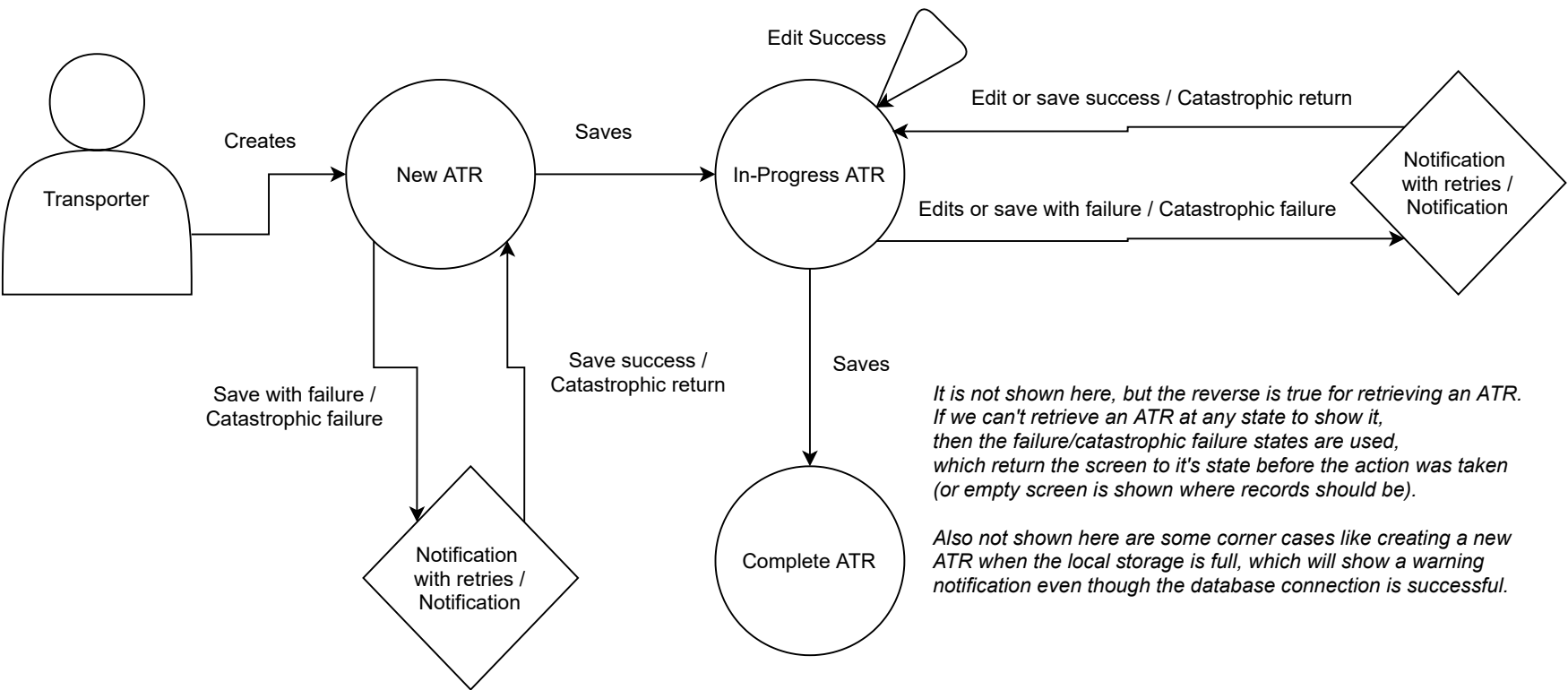
1. Successful
2. Failure with retries and notification
3. Catastrophic failure with notification

We define a catastrophic failure as an unrecoverable situation. One such situation is when we cannot save locally (something internally has gone wrong which cannot be resolved at runtime).

At best in such a situation, we can tell the transporter what we were trying to do and what we thought went wrong. To resolve such a situation, perhaps a new version of the app is needed with a patch (using information reported to the transporter).

These situations occur when communicating with external software required for basic operations and the operation has failed. Our design designates a single point for failure in communication: the database interface. Because we have the single interface to the database(s), we can define the same behaviour for any action that goes through the interface. This is evident in the diagram below.

Simple state diagram showing the general case of notifications for ATR actions (example)



The behaviour expected is described by the system test case, and each test case either is reflected in the above or it is a variant of the above.