

This feature entails implementing a set of behaviours on the MVP to cater for handling a set of predefined failure modes on an MVP subarray. The exact scope of functionalities needed for adequate graceful recovery of failures may not be covered during a single PI. Thus it will be narrowed down by setting down a specified list of failure scenarios and appropriate responses for a single PI only.

However, the scenarios specified and functionalities implemented will use the following as a guide:

The main failure modes on the subarray can be classified according to the type of element/s within the subarray failing as follows: 1) those elements (often called capabilities) within a subarray that change or may change when the type of functionality it owns changes (e.g. being reconfigured) 2) those elements that can change when the input array of receptors is updated (e.g. resources are re-assigned) and lastly (3) those structural elements that stay fixed during the entire lifetime of a subarray (e.g. CSP Subarray, Subarray LN etc.). Using this scheme opens up a way for recovering the subarray back to a healthy state as depicted in the table below:

Category	State	Corrective action
Failure in structural elements	<i>healthState</i> =FAILED; TANGO <i>state</i> of one or more elements = FAULT. If ONLINE then <i>obsState</i> = FAULT	Take to OFFLINE, fix faulty element (possibly restarting) and take back to ONLINE.
Failure in resource elements	<i>healthState</i> = DEGRADED or FAILED if condition worse enough (determined by subarray resource assignment). If FAILED and <i>obsState</i> higher than IDLE, then <i>obsState</i> =FAULT.	if <i>obsState</i> = FAULT then reset to IDLE. Reassign resources to remove faulty ones until <i>healthState</i> = OK
Failure in functional or capability elements	failure occurs during SCANNING : <i>healthState</i> = DEGRADED or FAILED as per above. If FAILED then <i>obsState</i> → FAULT and wait for RESET failure occurs during CONFIGURATION : <i>obsState</i> = FAULT and wait for RESET, however health stays OK as the configuration is considered to have not been implemented yet.	FAILED during Config: reset to READY and automatically rollback previous successful configurations to children; configure again using different configuration settings or use current stable config for SCANNING. FAILED during SCANNING: reset to READY and determine if SCAN should be skipped or redone with different configurations. Reconfigure or rollback until <i>healthState</i> = OK.

An initial list of failure scenarios can be found here:

<https://docs.google.com/spreadsheets/d/1fFN9Td13AvCUk-mjr6698dekBuy1QOxYBZZoQwFdVRM/edit#gid=0>

This list implies the following starting points for a list of enhancements to be made or verified on the MVP:

1. The ability to roll back a configuration to a previous one when commanded to rollback
2. Listeners on devices that check for a change in health conditions of children according to their own state
3. Test harness and frameworks that can enable automated testing of falling scenarios

This feature will be tested as follows:

A test for each of the scenarios listed above will be done by setting the state and verifying the expected

result occurs.