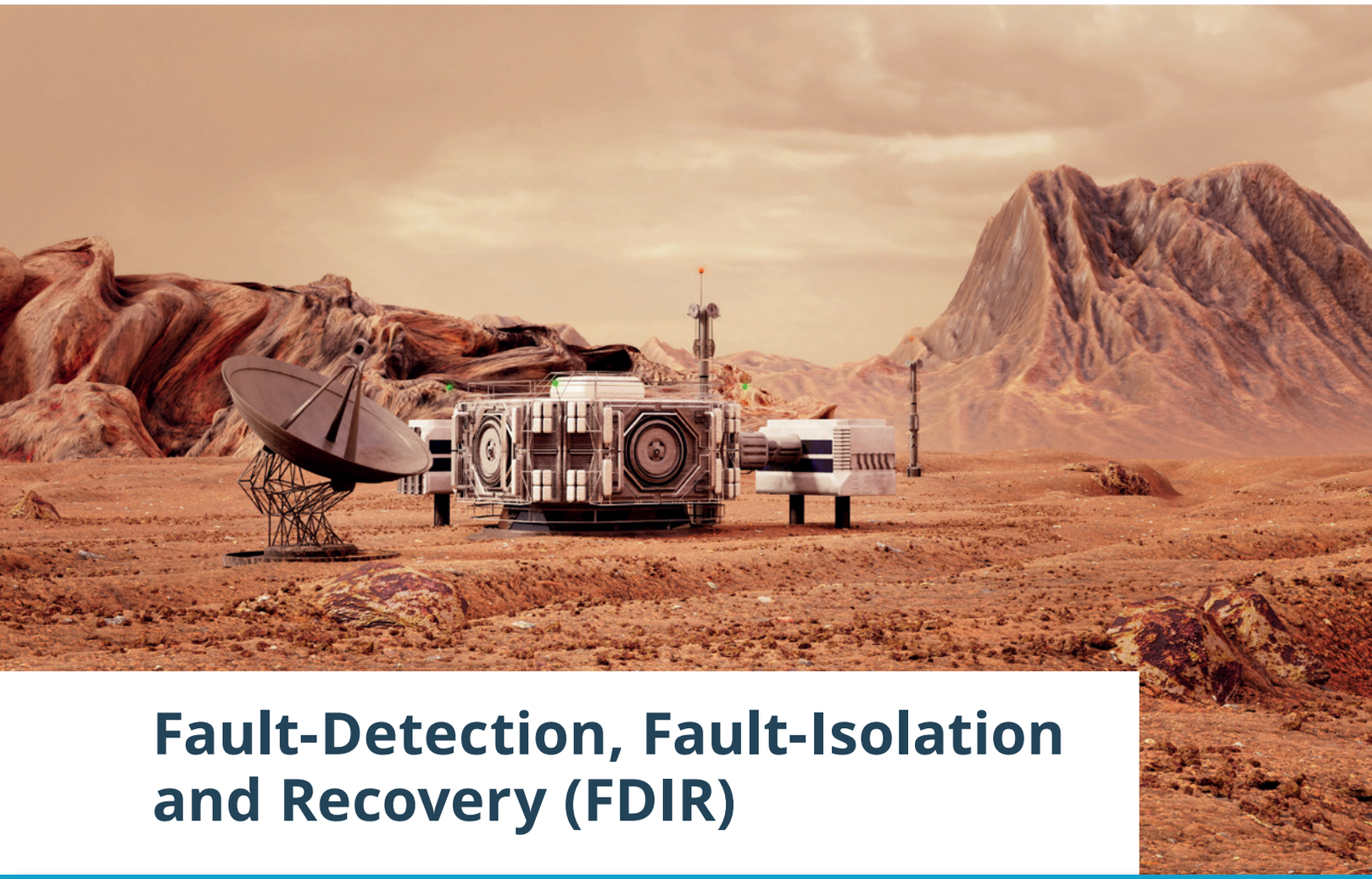
SYSGO
EMBEDDING INNOVATIONS



Fault-Detection, Fault-Isolation and Recovery (FDIR)

PikeOS RTOS & Hypervisor
Space Systems ready for Future Missions

The need to have a working system also in case of faults is a key factor for the space segment systems, as this needs to pursue the mission objectives in any case, also when part of the satellite or probe is no longer working due to a malfunction of any type. For this reason, all space segment systems have a function which implements the FDIR (Fault Isolation, Detection & Recovery) capability for the critical functions (e.g. not all functions are subject to this capability).

PikeOS supports out of the box some key features of the FDIR needs: The capability to run applications in strongly isolated containers (partitions) - like that an application error is ensured not to be able to propagate to other partitions - and the capability to fine grain monitor the application's behaviour (see also redundancy section) to identify faults in an easy manner thanks to its Health Monitoring subsystem.

The latter is a) fully configurable (i.e. can acquire only the needed data); b) compliant to ARINC 653 (for Avionics), but usable by any Guest OS in the partitions, and c) can take actions to applications, partition and module level.

For the following use cases we will suppose to have trouble with a subsystem which will be called ALPHA.

FAILURE DETECTION OF SUBSYSTEM ALPHA

To avoid to detect the fault of a subsystem when it is needed, the FDIR master component periodically requests a status report from the subsystem ALPHA, where the subsystem also provides vital data. This allows the component to perform a functional monitoring (so not only the fact that the system is able to respond is monitored).

In case the subsystem is implemented into a PikeOS partition, the DETECTION function can be achieved via PikeOS' internal monitoring capabilities of the partitions (see Figure 1).

FAILURE ISOLATION OF SUBSYSTEM ALPHA

Once the fault is detected, then it shall be "isolated" – which is a synonym for removing the subsystem ALPHA from the functional chain and verifying that no error propagation occured. While removing from the functional chain is an application level capability, the error propagation avoidance is something which depends on the architecture.

Using PikeOS, with its strongly separated partitions we can ensure, when the subsystem is implemented into a PikeOS partition and that no error will propagate to another partition.

FAILURE RECOVERY OF SUBSYSTEM ALPHA

As the function under the FDIR hood is a critical one, simply removing it from the functional chain is not a really applicable solution – as the system still needs it. So, for each of the possible critical function we need to have a clear recovery possibility. One of the possible recovery mechanisms is the redundancy.

Another one is to be able to activate an alternate function, which allows nevertheless to provide a degraded version of the lost capability. E.g. in the launcher, in case the referential inertial system is lost during the mission. Then the system will use a table-based navigation (e.g. it will navigate "blindly" based only on time).

PIKEOS SOFTWARE ARCHITECTURE

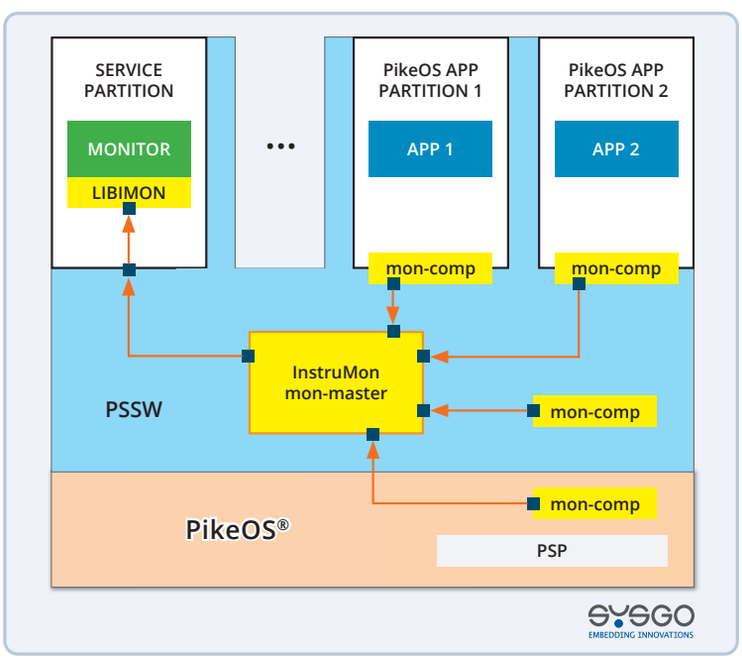


Figure 1

Founded in 1991, SYSGO became a trusted advisor for Embedded Operating Systems and is the European leader in hypervisor-based OS technology offering worldwide product life cycle support. We are well positioned to meet customer needs in all industries and offer tailor-made solutions with highest expectations in Safety & Security. More information at www.sysgo.com/space

SYSGO Headquarters
+49 6136 9948 500

SYSGO France
+33 1 30 09 12 70

SYSGO Czech Republic
+420 222 138 111

sales@sysgo.com

www.sysgo.com