Software Reuse in Safety Critical Ground Systems

Emmanuel Lesser, B.Sc., M.Sc. (Oxon.)
Software S&MA Lead Canadarm3
Safety & Mission Assurance, Robotics & Space Operations
Emmanuel.Lesser@mda.space
www.mda.space

Most ground systems in the space industry have traditionally been considered to be mission critical or not critical. As a result, the software for these systems are often developed for compliance with the lower software criticality classes of the applicable standards. However, ground-based mission control systems used in human spaceflight can be involved in causing and/or controlling critical or catastrophic hazards. This is especially true in missions that rely heavily on software for autonomy (or even AI), where the flight segment and the ground segment form a single integrated system that is safety critical and must be human rated.

Mission control systems often include graphical or even multimodal user interfaces that allow operators to easily access and visualize telemetry, as well as command and control the flight segment in a way that takes into account important human factors considerations. Such interfaces tend to rely on COTS technology and software frameworks, which have not been developed for use in safety critical contexts. Such frameworks are excessively difficult to qualify because they are usually very large and complex, contain closed source components and rely on a software stack that is not adequate for safety critical infrastructure.

In this presentation, we will go over some examples of mission control systems that are safety critical but rely on difficult to qualify user interface technology for command and control. We will discuss what innovative techniques can be put in place to work around this problem, as well as cost effective ways for assuring the required failure tolerance in these systems in order to safeguard human life during the entire mission lifetime.