Model Checking of Autonomy Models for an In-Situ Propellant Production System

Peter Engrand[1] and Charles Pecheur[2]

[1] NASA Kennedy Space Center, FL 32899 , U.S.A.
peter.engrand-1@ksc.nasa.gov
[2] RIACS / NASA Ames Research Center, Moffett Field, CA 94035, U.S.A.
pecheur@ptolemy.arc.nasa.gov

Utilization of extraterrestrial resources, or In-Situ Resource Utilization (ISRU), is viewed as an enabling technology for the exploration and commercial development of our solar system. A key subset of ISRU is In-Situ Propellant Production (ISPP), which involves the partially autonomous production of propellants for planetary ascent or Earth return. To support the development and evaluation of ISPP technology, the NASA Kennedy Space Center is currently developing an ISPP hardware test bed for Mars missions, that uses carbon dioxide from the Martian atmosphere.

One of the challenges is the ability to maintain continuous plant operation without a Mars-based human presence, despite component failures and operational degradation. As a solution, KSC is employing the Livingstone controller to monitor an ISPP plant. Livingstone is a model-based autonomous health management agent developed at NASA Ames. It uses a model of the controlled system to track the system's behavior for anomalous conditions, diagnose component failures, and provide recovery recommendations.

Because this kind of intelligent systems address a very wide range of possible scenarios, A new approach to verification is needed to provide adequate confidence in their reliability. NASA Ames researchers, in collaboration with Carnegie Mellon University, have developed a translator that converts the Livingstone model and its expected properties into the input syntax of the SMV symbolic model checker. SMV then performs an exhaustive search of all possible executions of that specification and reports any property violation, illustrated by an execution trace that helps to localize the source of the violation.

These verification tools are used at Kennedy to validate the ISPP Livingstone models and provide feedback and suggestions to Ames on how to improve the tools. First experiments have shown that SMV can easily process the ISPP model and verify useful properties such as reachability of normal operating conditions or recoverability from failures. The translator and SMV have been used to verify expected global flow properties in a model representing a portion of the ISPP plant. The verification has pointed out a property violation, due to an improper modeling of flow equations. The latest version of the ISPP model, with 10^{50} states, necessitates some hand tuning of SMV optimizations but can still be processed in less than a minute, thanks to the power of BDD technology. This experience demonstrates how such verification tools can be used for interactive debugging as part of the design process.

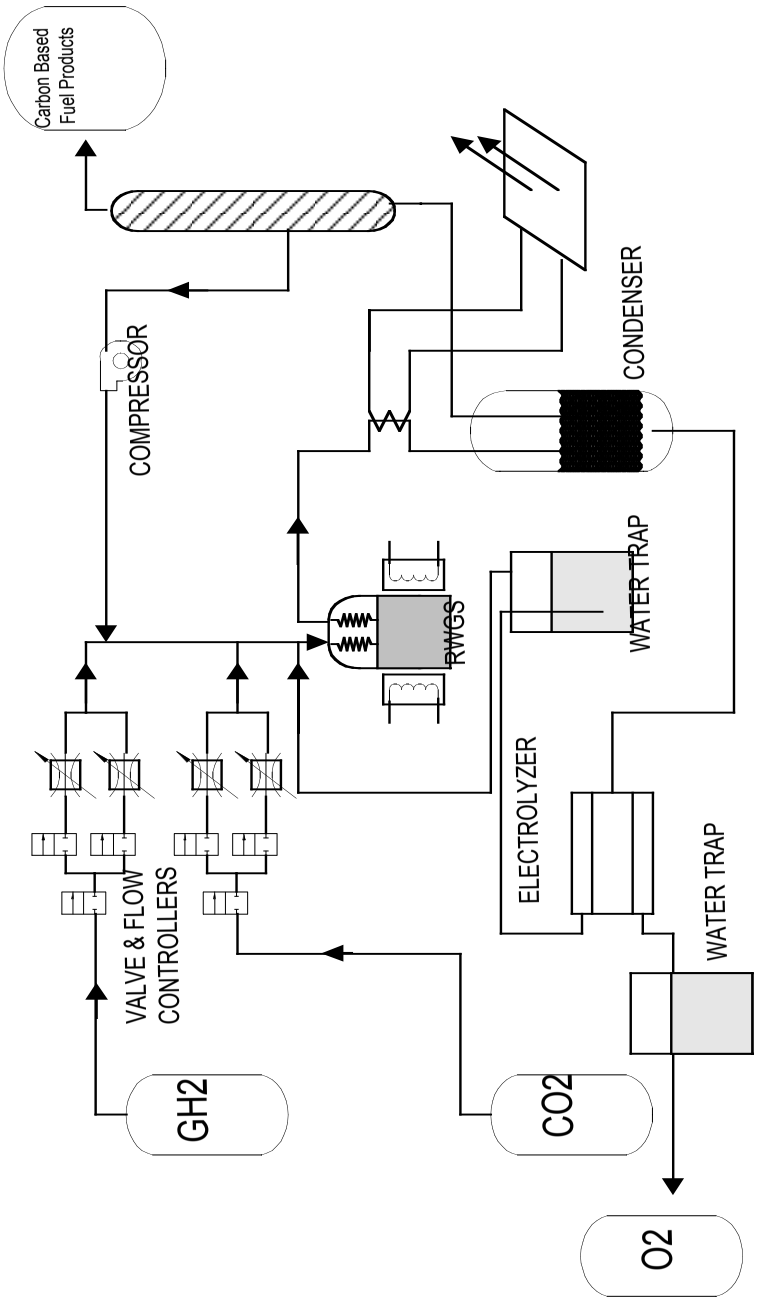

Fig. 1. Reverse Water Gas Shift schema