12-16 July 2015, Bellevue, Washington

Cascade Distillation System Design for Safety and Mission Assurance

Miriam J. Sargusingh[1], and Michael R. Callahan[2]
NASA Johnson Space Center, Houston, TX 77058

and

Shira Okon[3]
Tietronix Software Inc., Houston, TX 77058

Per the NASA Human Health, Life Support and Habitation System Technology Area 06 report "crewed missions venturing beyond Low-Earth Orbit (LEO) will require technologies with improved reliability, reduced mass, self-sufficiency, and minimal logistical needs as an emergency or quick-return option will not be feasible".[1] To meet this need, the development team of the second generation Cascade Distillation System (CDS 2.0) chose a development approach that explicitly incorporate consideration of safety, mission assurance, and autonomy. The CDS 2.0 preliminary design focused on establishing a functional baseline that meets the CDS core capabilities and performance. The critical design phase is now focused on incorporating features through a deliberative process of establishing the systems failure modes and effects, identifying mitigation strategies, and evaluating the merit of the proposed actions through analysis and test. This paper details results of this effort on the CDS 2.0 design.

Nomenclature

AES	=	Advanced Exploration Systems
CDS	=	Cascade Distillation System or Cascade Distillation Subsystem
CDS 2.0	=	Second generation CDS
CTSD	=	Crew and Thermal Systems Division
DFMR	=	Design for minimum risk
ECLSS	=	Environmental Control and Life Support System
FMEA	=	Failure Modes and Effects Analysis
FMECA	=	Failure Modes Effects and Criticality Assessment
FTA	=	Fault Tree Analysis
GUI	=	Graphical User Interface
IBD	=	Internal Block Diagram
JSC	=	Johnson Space Center
LEO	=	Low-Earth Orbit
LSSP	=	Life Support Systems Project
PRA	=	Probabilistic Risk Assessment
RBD	=	Reliability Block Diagram
S&MA	=	Safety and Mission Assurance
SMD	=	State machine diagram
SME	=	Subject matter expert
SysML	=	Systems Modeling Language
XML	=	Extensible Markup Language

[1] Systems Engineer, Crew and Thermal Systems Division, 2101 NASA Parkway/EC2
[2] Principal Investigator, Crew and Thermal Systems Division, 2101 NASA Parkway/EC3
[3] Principal Engineer/SysML Modeler, Tietronix Software, Inc., 1331 Gemini Street, Suite 300

I. Introduction

ADVANCEMENTS in environmental control and life support systems will be necessary in order to make human exploration missions beyond low-Earth orbit (LEO) viable in the next few decades. Without an established supply chain, options for timely emergency supplies, and no quick-return options, the crew will need to be equipped for self-sufficiency like never before. The overall reliability of critical mission systems will be of paramount concern.

The current regenerative life support system aboard the International Space Station relies on system redundancy, spares for replacement at the subsystem and assembly level, emergency stores and resupply to maintain consistent life support for the crew. Even lunar missions had an abort path that could return crew to Earth within a reasonable amount of time to rely on emergency life support resources. A human exploration mission to Mars will not have to the benefit of proximity to Earth or a well-established supply chain; every consumable, including maintenance and emergency resources, will need to be included. "Today, it costs $10,000 to put a pound of payload in Earth orbit." Efforts are being made to reduce this 100-fold by 2025[2,3]. Even so, making a mission to Mars fiscally viable will involve making careful trades between reliability and mass.

As experienced in the Constellation Program, full focus on safety and mission assurance (S&MA) comes at a price. After suffering an architecture design that did not close from a mass perspective, the Constellation program adopted an approach that would balance these seemingly competing objectives.[4] A similar approach is being employed in the design of a flight forward advanced water recovery system based on the cascade distillation technology, referred to as CDS 2.0. Using the experience gained from a CDS prototype ground test system, referred to as the Blue Box, as well as from the Urine Processor Assembly aboard the ISS, a baseline functional architecture was established. This baseline architecture reduced the part count by more than 50%. The project is now in the process of re-integrating components required to meet the S&MA goals of the project.

II. Background

A. Cascade Distillation System

The Cascade Distillation System (CDS) employs thin-film vacuum rotary distillation to recovery water from wastewater. Fig. 1 presents a simple schematic of the CDS. The centrifugal force generated by the rotation is harnessed by pitot pumps within the distiller; this along with a balancing of pressures throughout the system provide the motive force for fluids without the need for additional pumps. The process generates a non-potable water distillate with more than 90% of the contaminants removed; further processing is required to remove the remaining contaminants before the water is safe for consumption. This distillate is generated by evaporating water from the wastewater and condensing the steam. The batch process is stopped with the residual wastewater, or brine, has reached its maximum concentration; over processing could lead to the formation of the solids in the system that could cause performance degradation and/or hardware damage (ref. 5).

The key components of the CDS include the distiller, the heat pump, 3 tanks, the vacuum pump, a trim cooler, feed and product flow regulators and various valves to manage the flow. The system also includes a power distribution system and an embedded controller capable of automating the core batch operation of the CDS without human interaction. Additional instrumentation is needed to support this automation process.

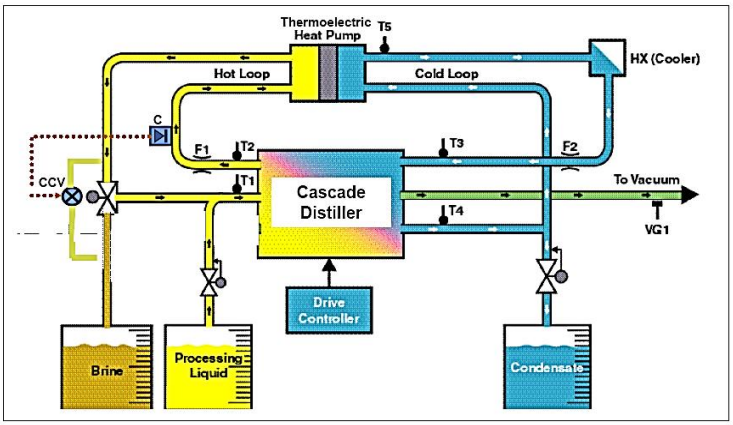


Figure 1. Simplified block diagram of a cascade distillation system. *The blue stream represents the flow of distillate, the yellow stream indicates the flow of waste water, both fresh and partially concentrated, the orange stream represents concentrated brine, and the green stream represents the flow of vacuum.*

The goal of CDS 2.0 development effort is to develop a flight-forward prototype. The resultant hardware will primarily be used in ground testing; there design will support operation aboard the ISS as a payload experiment.

B. Assessing CDS Reliability

Although reliability is recognized by the agency as an important area of advancement, the tools available for evaluating a system for reliability are generally retrospective. The tools consider systems that are well defined and any quantitative analysis requires a significant empirical data set for the components employed in the system. The means by which an emerging system designs with unique prototype level components could be evaluated and optimized for reliability was considered in a series of events hosted by the AES Water Recovery Project in the spring of 2013. This campaign included an educational series in which experts from across the agency and academia provided information on terminology, tools, and techniques associated with evaluating and designing for system reliability. The campaign culminated in a workshop that included members of the Environmental Control and Life Support System and AES communities. The course presented by the JSC S&MA organization included a description of tools for evaluating systems for reliability such as the Probabilistic Risk Assessment (PRA), Failure Modes & Effects Analysis (FMEA), Reliability Block Diagrams (RBD), and fault trees (ref. 6). Given the immaturity of the design, the PRA would not be an effective tool at this stage of the CDS development. It was decided that variations of the latter 3 tools would be used.

III. Assessment

The project opted to focus on developing a failure modes, effect and criticality analysis (FMECA). The CDS 2.0 FMECA was derived from the CDS 2.0 system model generated using the Systems Modeling Language (SysML), a graphical modling language for representing requirements, behavior, structure, and properties of a system and its components.[8]

A. Failure Mode Ranking

Using the FMECA (instead of an FMEA), numerical ratings of the failure mode's effects were rated, allowing for a ranking to be established among the failure modes. The ranking was then used as a basis for addressing the failure mode; i.e. identifying whether the failure mode should be mitigated and to what extent.

1. Consequence Levels

The consequence ratings are tailored to the project based on hazard ratings defined by the International Space Station and by the JSC Crew and Thermal Systems Division (CTSD) Testing Branch. A catastrophic hazard, or Category I hazard, is one that can result in a disabling or fatal personnel injury, or loss of the vehicle (ISS). ISS requires two fault tolerance in these instances. A critical hazard, or Category II hazard, is one that can result in a non-disabling injury, loss of a major ISS life sustaining function or emergency system, or involves damage to the flight vehicle. The system is required to be single fault tolerant in these cases.[9] All other hazards are considered Marginal, Class III, hazards. These are hazards that may lead to major damage to an emergency system, damage to a non-critical ISS element, or minor personnel injury or occupational illness. The CTSD consequence levels are similar, except defined in terms of ground system and facility damage. A fourth class is included in their definition referring to negligible hazards that minor injury to personnel that might require some first aide and minor damage to facilities, equipment or flight hardware.[10] The project incorporated a classification system that addressed payload mission assurance while meeting the spirit of the classifications set by ISS and CTSD. The resultant rating are as follows:

- *Level 1*: A condition that may cause death or permanently disabling injury, facility destruction on the ground, or loss of the ISS.
- *Level 2*: A condition that may cause severe injury or occupational illness, major property damage to facilities, systems, equipment, or flight hardware on the ground, loss of a major ISS element, damage/significant impact to a life sustaining function or emergency system, loss of other ISS payloads, or loss of the CDS.
- *Level 3*: A condition that may cause minor injury or occupational illness, minor property damage to facilities, systems, equipment or flight hardware, damage to non-critical ISS-element, or lost/compromised test objectives.
- *Level 4*: A condition that could cause the need for minor first-aid treatment but would not adversely affect personal safety or health; damage to facilities, equipment, or flight hardware damage beyond normal wear and tear.

2. Failure Mode Ranking

During a deep space human exploration mission, it is likely that a loss of the CDS would be considered a Level 1 hazard. Taking into consideration a baseline functionality only architecture, almost any failure could lead to the loss of CDS functionality, and would therefore be classified as a Level 1 failure mode. In order to provide some resolution to the ranking, consequence levels were established taking into consideration CDS 2.0 as a payload experiment. In this case, loss of CDS operation would be considered a Level 3 consequence.

The objective of the project is to eliminate Level 1 hazards. Design for minimum risk (DFMR) techniques would be utilized in cases where the hazard cannot be eliminated, such as with the CDS 2.0 brine tank which would contain

toxic brine and has the inherent hazard or rupturing or leaking. Mitigation strategies would be considered for Level 2 hazards beyond the requisite fault tolerance and hazard controls. At a minimum, a method of monitoring along and alerting personnel to these hazards will be implemented. Level 3 and 4 mitigation strategies will also be considered, though at a lower priority. The cost associated with implementing these strategies will have to be weighed against the likelihood of the hazards occurring. Without quantitative reliability data, the likelihood ratings are based on subject matter expert (SME) input.

B. Failure Modes, Effects, and Criticalities Modeling Method

The FMECA is derived from specific relationships defined CDS 2.0 SysML model; this method was developed by Tietronix Software, Inc. and described in reference 7. An overview of the FM meta-model describing relationships between model elements is depicted in figure 2.

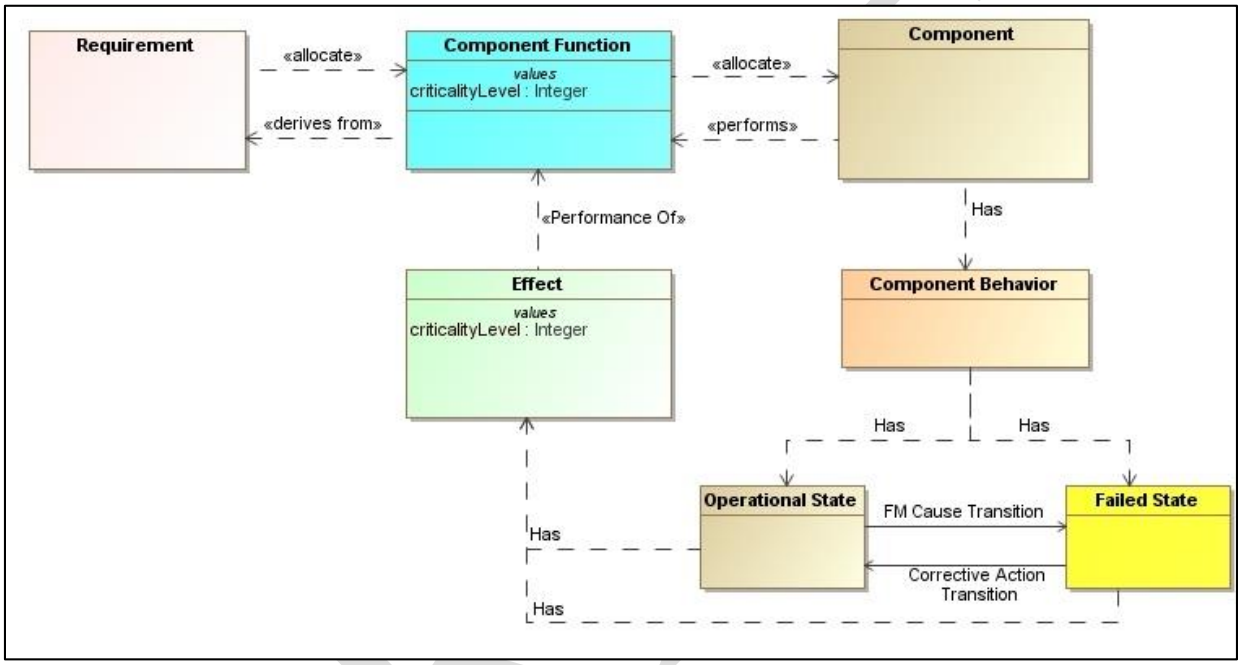
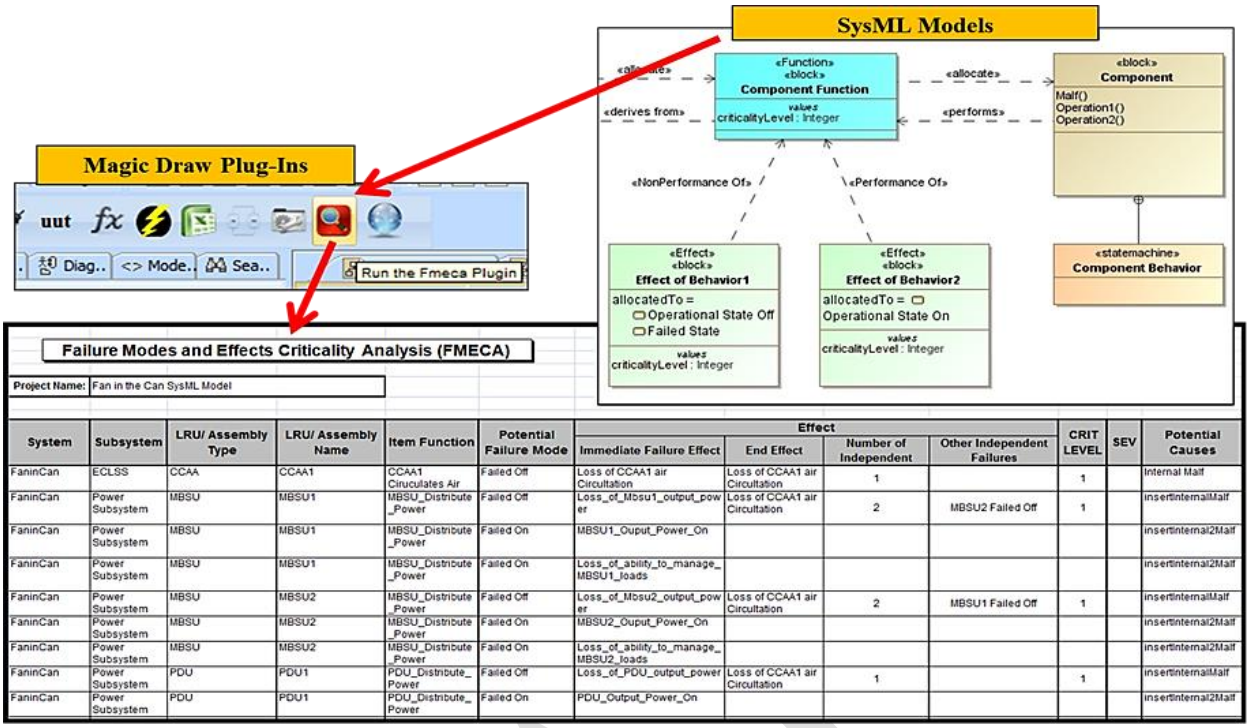


Figure 2: FM Meta-Model

The Internal Block Diagram (IBD) depicts how the components in the design are connected. Each part in the IBD diagram represents a unique hardware component. Functions are represented as blocks with <<Function>> stereotypes applied. The functions are captured as names in the blocks.[11] The behavior of the component is captured in state machine diagrams (SMD) owned by the component. Operational states and potential failed states are identified. Failed states represent potential failure modes, and are modeled as states with a <<FailedState>> stereotype. The immediate effects of each state were identified. The effects describe the performance of the function in a given state. Therefore in the Operational "On" state, the intended function is performed; however in the Operational "Off" state and <<FailedState>> the effect describes the loss or non-performance of the Function. The immediate Effects of the mode states are modeled as blocks with <<Effect>> stereotypes and allocated to states in the state machine models.

State changes between states are accomplished via state transitions. Transitions consist of a trigger and a guard. Triggers can be represented as events (example: operations or signal events). Interactions between state machines are accomplished via broadcasted signal actions from one state and signal event triggers on transitions in another state machine. Broadcasted signal actions are modeled as entry actions to states. Signals broadcasted must be unique to each component.

The FMECA MagicDraw plug-in[12] extracts details about failed states. Failed states represent potential failure modes in the FMECA output. The plug-in traverses behavior diagrams to determine potential failure modes and end effects for analysis and produces the resulting spreadsheet shown in Figure 4.



System	Subsystem	LRU/ Assembly Type	LRU/ Assembly Name	Item Function	Potential Failure Mode	Effect				CRIT LEVEL	SEV	Potential Causes
						Immediate Failure Effect	End Effect	Number of Independent	Other Independent Failures			
FaninCan	ECLSS	CCAA	CCAA1	CCAA1 Circulates Air	Failed Off	Loss of CCAA1 air Circultation	Loss of CCAA1 air Circultation	1		1		Internal Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu1_output_power	Loss of CCAA1 air Circultation	2	MBSU2 Failed Off	1		insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	MBSU1_Ouput_Power_On						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU1	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU1_loads						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed Off	Loss_of_Mbsu2_output_power	Loss of CCAA1 air Circultation	2	MBSU1 Failed Off	1		insertInternalMalf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	MBSU2_Ouput_Power_On						insertInternal2Malf
FaninCan	Power Subsystem	MBSU	MBSU2	MBSU_Distribute_Power	Failed On	Loss_of_ability_to_manage_MBSU2_loads						insertInternal2Malf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed Off	Loss_of_PDU_output_power	Loss of CCAA1 air Circultation	1		1		insertInternalMalf
FaninCan	Power Subsystem	PDU	PDU1	PDU_Distribute_Power	Failed On	PDU_Output_Power_On						insertInternal2Malf

Figure 3: FMECA (Failure Mode and Effects Criticality Analysis) Data Exchange MagicDraw Plug-In

The FTA plug-in[13] derives fault trees from any "Effect" stereotyped block. "Effect" stereotyped blocks represent potential top level events in the fault trees. The FTA plug-in traverses behavior diagrams to extract the fault event paths for analysis. The plug-in creates an XML file of the fault tree that can be imported to fault tree graphical tools.

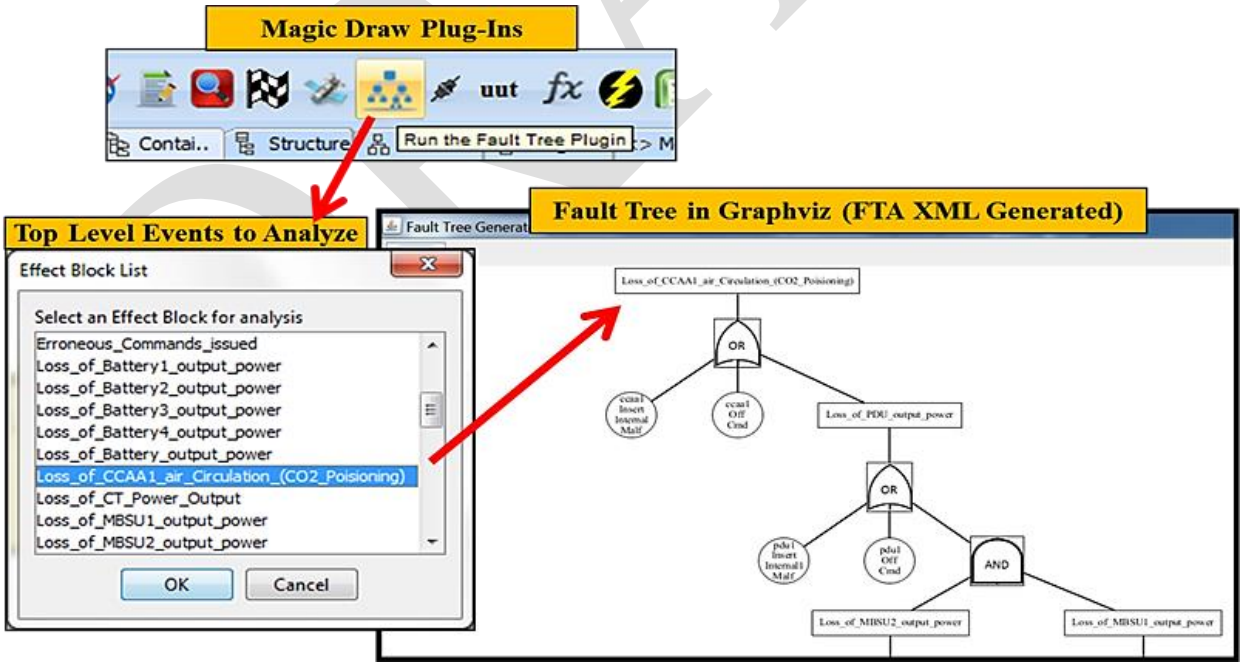


Figure 4: FTA (Fault Tree Analysis) Data Exchange MagicDraw Plug-In

A visual GUI display of the fault tree as a MagicDraw pop-up window is also generated by the plug-in.

{Details on application of this methodology to CDS will be provided in the final manuscript}

IV. CDS FMEA Model

Figure 5. shows the IBD being used to evaluate the CDS 2.0 failure modes' effects and criticalities.

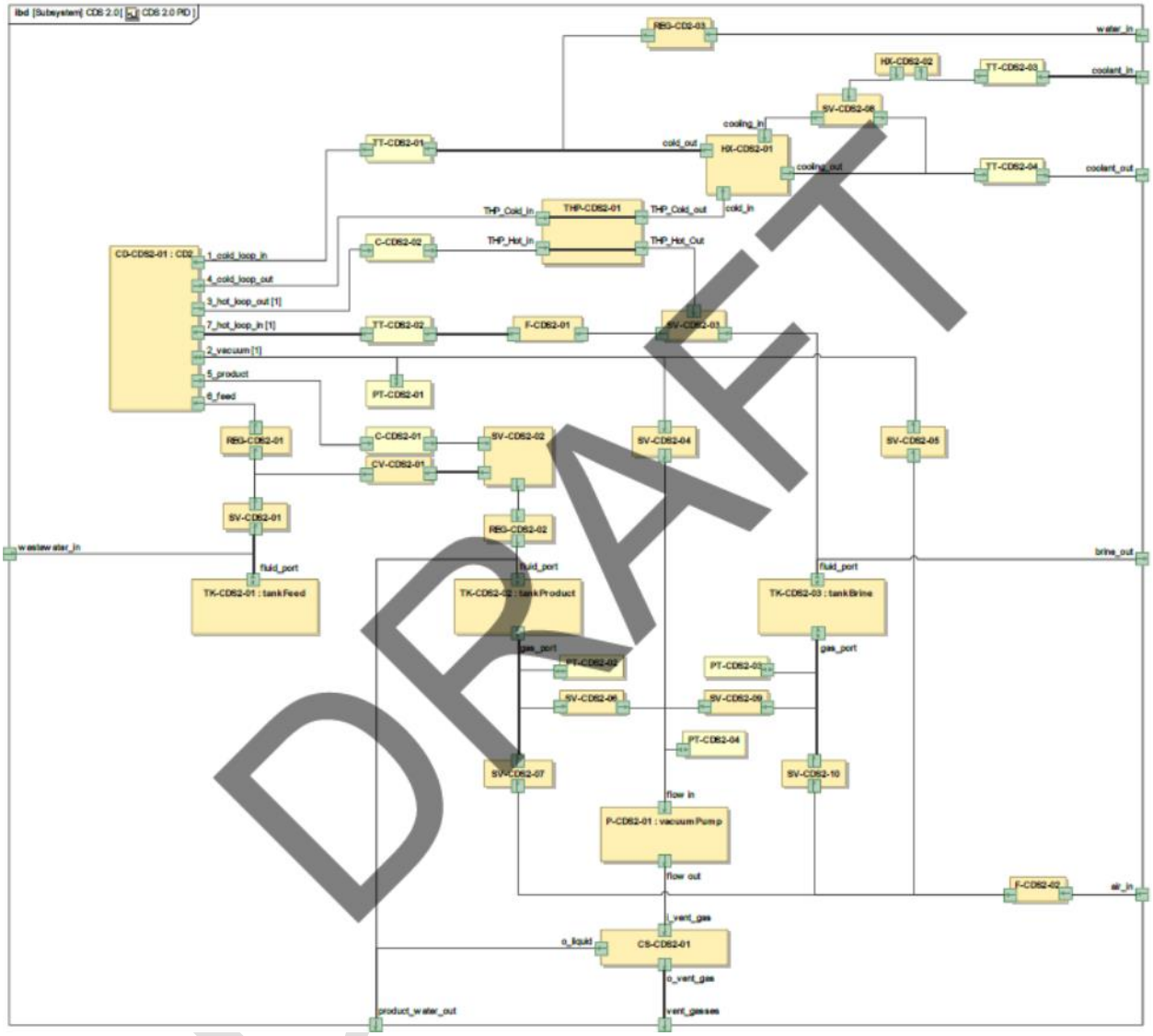


Figure 5 DRAFT. CDS 2.0 Plumbing and Instrumentation Diagram.

Figure 6 shows an example of an state machine model for the vacuum pump (P-CDS2-01). The vacuum pump was attributed 3 states: "Off", "On", and "Failed Off". Other states were considered, but discounted as non-credible. For example, the Failed On state was considered. The only way for the vacuum pump to fail "On" is if power is continuously applied; this is a failure of the avionics or power system not of the vacuum pump itself. The SMD shows that when the vacuum pump is off, it is not pulling vacuum; a placeholder effect of not venting was included to capture potential interaction between the vacuum pump and a vent air conditioner or the environment. In the "On" state, the vacuum pump pull vacuum and vents air. In this state, the vacuum is broadcasting the signal "Vac Pump Pumping". This signal will be received by the CD as one of several signals required for the CD to be in the "Process" state. In order for the vacuum pump to transition between the "On" and "Off" states, a signal must be broadcast from the power distribution module reflecting whether or not power is being provided. The only failed state defined for the vacuum pump is the "FailedOff" state. The only trigger for leading to this state is defined as an internal failure which is

modeled as a behavior of the vacuum pump (missing from the diagram is a transition from "On" to "FailedOff"). Included in this SMD are options for recovering from the failed state.

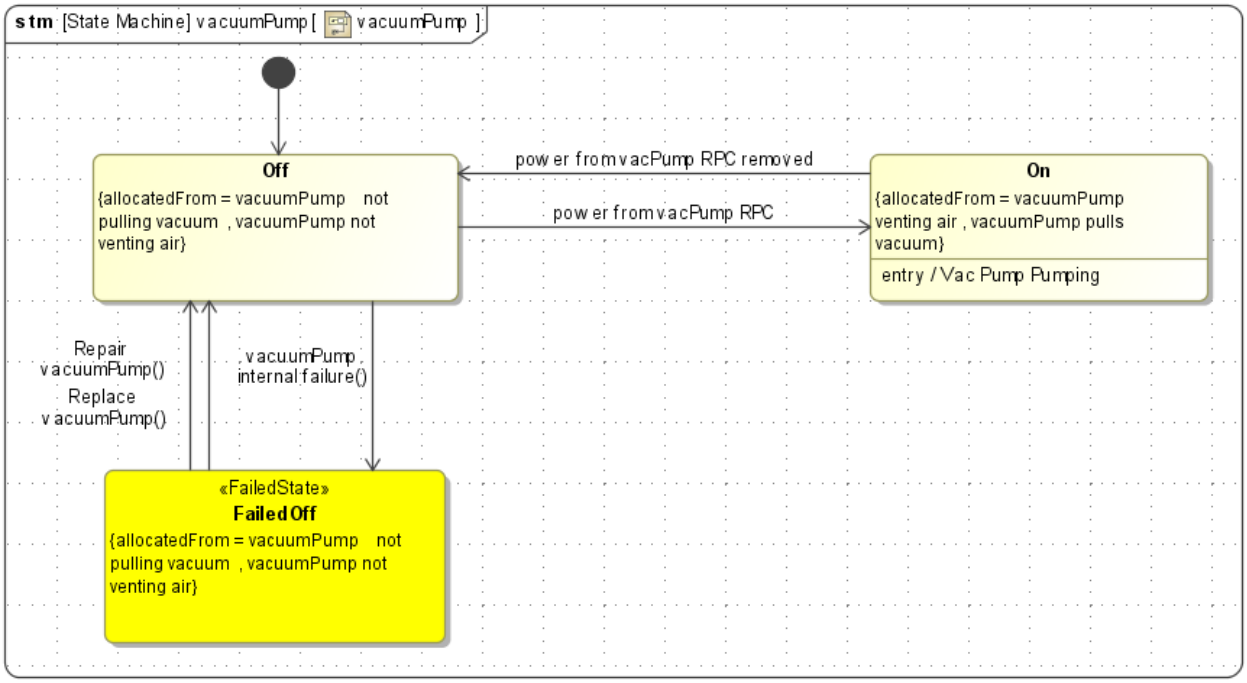


Figure 6. State machine model for the CDS 2.0 vacuum pump.

V. Results

At the CDS 2.0 preliminary design review (PDR), a manual assessment produced 58 potential failure modes. The only Level 1 failure modes identified were associated with the feed and brine tanks, since failure of these devices to contain their fluid could lead to personnel coming into contact with toxic fluids. Since these failure modes cannot be mitigated, a DFMR approach to tank design will be taken into consideration. Options include use of components already certified for the storage and management of toxic fluids aboard the ISS.

Several Level 2 failure modes were identified. These could be classified into the following two groups:

- Failure modes that lead to exposure of personnel and other ISS equipment to uncontained liquids
- Failure modes leading to the formation of solids in the recirculating brind loop that could damage the the heat pump or the distiller.

The Level 3 failure modes could be classified as follows:

- Failure modes leading to corruption or loss of data
- Failure modes that render the CDS incapable of processing wastewater

Level 4 hazards were largely associated with failure modes that could lead to degraded performance, product water contamination or excessive wear on the CDS components.

Note that the FMECA considered the CDS 2.0 functional design. Inherent failures that are not associated with the system functionality, such as electrocution hazards, are not included at this time.

Figure 7 shows a portion of the preliminary FMECA output for the CDS. This portion highlights 2 valves whose function is required for CD operation. Valve v02product opens the product line from the CD to the product tank; if this line isn't open, the CD will not have anywhere to displace the generated distillate and it will cease to function. Valve v04vacCD isolates the CD from the vacuum line; it is required for adequate pressure management. Individually, a failed valve is a level 4 failure, however the model output provides the assigns the level associated with worst case end effect; in this case the loss of distillate, a level 3 failure.

LRU/ Assembly Name	Item Name	Item Function	Potential Failure Mode	Effect				CRIT LEVEL	Potential Causes
				Immediate Failure Effect	End Effect	Number of Independent Failures	Other Independent Failures		
v02product	solenoid_valve_2way		failedClosed	v02product isolates CD from feed tank	CD does not generate distillate	1		3	Int Structure_Failure
v02product	solenoid_valve_2way		failedClosed	v02product isolates CD from feed tank	CD pumps fluids	1		3	Loss of Magnetic Field
v02product	solenoid_valve_2way		failedClosed	v02product isolates CD from feed tank	CD does not generate distillate	1		3	Loss of Magnetic Field
v04vacCD	nc_solenoid_valve		Failed Closed	v04vacCD isolates CD from vacuum	CD pumps fluids	1		3	Loss of Magnetic Field
v04vacCD	nc_solenoid_valve		Failed Closed	v04vacCD isolates CD from vacuum	CD does not generate distillate	1		3	Loss of Magnetic Field
v04vacCD	nc_solenoid_valve		Failed Closed	v04vacCD isolates CD from vacuum	CD pumps fluids	1		3	Int Structure_Failure
v04vacCD	nc_solenoid_valve		Failed Closed	v04vacCD isolates CD from vacuum	CD does not generate distillate	1		3	Int Structure_Failure
v04vacCD	nc_solenoid_valve		Failed Open	v04vacCD opens CD to vacuum		1		4	Int Structure_Failure
v04vacCD	nc_solenoid_valve		Failed Open	v04vacCD opens CD to vacuum		1		4	SpringFailure
v04vacCD	nc_solenoid_valve		Failed Open	v04vacCD opens CD to vacuum		1		4	Contamination

Figure 7. Snapshot of DRAFT CDS model FMECA output.

It is no surprise that each failure shows a value of 1 for the "Number of Independent Failures", given that the design is based on minimum functionality.

{model driven results to be expanded upon in the final manuscript}

VI. Conclusions and Forward Work

{conclusions to be provided in the final manuscript}

Acknowledgments

The authors acknowledge the grand team that has assembled to support the work described in this paper. Wade Bostick of JSC Safety and Mission Assurance directorate has been instrumental in providing guidance in the process, insight into implications for the overall project lifecycle and providing relevant S&MA resources. Mike Malone and Christian Parker have provided guidance on division policy as well as hazard propagation and mitigation. We thank several members of Tietronix Software, Inc. for their support in developing CDS SysML modeling and fault management analysis tools and tailoring those tools for CDS application: Howard Wagner PhD, Michel Izygon, PhD, Larry Garner, and Emmy Chacko. We also thank the participation of the RESCAID STTR team for choosing to utilize CDS as a test case for the application of their fault simulation tool to design optimization: Sudipto Ghoshal, Chuck Domagala and Deepak Haste of QSI, and John Sheppard and Logan Perreault of Montana State University. We also thank Lui Wang, Voung Pham for coordinating the use of the CDS as a test case for the respective SBIR/STTR. Finally, we acknowledge the support of the AES LSSP management, Walter Schneider of Marshall Space Flight Center and Sarah Shull.

References

[1] Hurlbert, K., Bagdigian, B., Carroll, C., Jeevarajan, A., Kliss, M., and Singh, B., "NASA Human Health, Life Support and Habitation System Technology Area 06", April 2012.

[2] "Advanced Space Transportation Program: Paving the Highway to Space", *NASA Marshall Space Flight Center*, URL: http://www.nasa.gov/ centers/marshall/news/background/facts/astp.html prt.htm [cited 20 February 2015].

[3] Joshi, J., Perchonok, M., and Berdich, D., "Sustaining Life -- Where Would a Space Explorer Find Water and Oxygen?" URL: http://www.nasa.gov/audience/foreducators/stseducation/materials/ Sustaining_Life_prt.htm [cited 20 February 2015].

[4] Rhatigan, J. (ed.), "Constellation Program Lessons Learned Volume II", NASA/SP-2011-6127-VOL-2, 2011.

[5] McQuillan, J., Pickering, K. D., Anderson, M., Carter, L., Flynn, M., Callahan, M., Vega, L., Allada, R and Yeh, J., "Distillation Technology Down-selection for the Exploration Life Support (ELS) Water Recovery Systems Element, *40th International Conference on Environmental Systems*", AIAA 2010-6125, AIAA, Reston, VA, 2010.

[6] Sargusingh, M. J., and Nelson, J. R., "Environmental Control and Life Support System Reliability for Long-Duration Missions Beyond Lower Earth Orbit", *International Conference on Environmental Systems; 13-17 Jul. 2014*, ICES-2014-180, Texas Tech University, Department of Civil, Environmental, and Construction Engineering, Lubbock, TX [online collection] URL: http://repositories.tdl.org/ttu-ir/handle/2346/58495 [cited 24 February 2015].

[7] "Phase I MBFME Modeling Methodology", Tietronix Software, Inc., December 19, 2014 (unpublished)

[8] S. Friedenthal, A. Moore, and R. Steiner, *A Practical Guide to SysML*, 2nd ed., Elsevier, Inc., 2012.

[9] "Safety Analysis and Risk Assessment Requirements Document", SSP 30309, Rev. F, NASA International Space Station Program, November 2005.

[10] M. Malone, "Hazard Analysis for the Cascade Distillation Sub-system (CDS) 2.0 Design to Advanced Water Recovery System Development Facility (AWRSDF)", NASA Johnson Space Center, Crew and Thermal Systems Division, Draft revision, September 2014 (unpublished).

[11]Aerospace Ontology {reference to be provided in final manuscript}

[12] FMECA MagicDraw plug-in, Tietronix, Inc., beta version, 22 December 2014.

[13] FTA MagicDraw plug-in, Tietronix, Inc., beta version, 22 December 2014.