JOURNAL OF SPACECRAFT AND ROCKETS
Vol. 29, No. 4, July–August 1992

Expert Systems for Automated Maintenance of a Mars Oxygen Production System

Jen-Kuang Huang,* Ming-Tsang Ho,† and Robert L. Ash‡
Old Dominion University, Norfolk, Virginia 23529

Application of expert system concepts to a breadboard Mars oxygen processor unit have been studied and tested. The research was directed toward developing the methodology required to enable autonomous operation and control of these simple chemical processors at Mars. Failure detection and isolation was the key area of concern, and schemes using forward chaining, backward chaining, knowledge-based expert systems, and rule-based expert systems were examined. Tests and simulations were conducted that investigated self-health checkout, emergency shutdown, and fault detection, in addition to normal control activities. A dynamic system model was developed using the Bond-Graph technique. The dynamic model agreed well with tests involving sudden reductions in throughput. However, nonlinear effects were observed during tests that incorporated step function increases in flow variables. Computer simulations and experiments have demonstrated the feasibility of expert systems utilizing rule-based diagnosis and decision-making algorithms.

Nomenclature

A_d = orifice area of the flow controller, in.^{2}
C_c = fluid capacitance of the cell, (g/h)/(mbar/s)
C_d = discharge coefficient
D_{P_n} = pressure-flow-rate offset of pipeline n, mbar
F_n = mass flow rate of pipeline n, (g/h)
F_{1d} = rate of change of feed-gas flow rate (g/h)/s
H = feedback transfer function of the flow controller, V/(g/h)
I_n = fluid inertance of pipeline n, mbar/[(g/h)/s]
I_z = generated current across the zirconia membrane, mA
K,P = parameters of the flow controller dynamics
P_c = pressure in the cell, mbar
P_d = delivery pressure, psig
P_n = pressure in pipeline n, mbar
P_p = pressure in the primary bottle, psig
P_r = pressure in the reserved bottle, psig
P_t = pressure in the ballast tank, mbar
P_z = pressure in the zirconia tube, mbar
R_n = overall fluid resistance of pipeline n, mbar/(g/h)
T_c = average temperature in the cell, K
T_d = upstream stagnation temperature, K
T_n = temperature in pipeline n, K
V_s = flow-rate set point of feed gas, V
V_z = applied voltage across the zirconia membrane, V
V_{zc} = maximum allowable voltage across the zirconia membrane, V

I. Introduction

RECENT studies have identified lunar bases and manned Mars exploration as desirable and achievable goals for the U.S. Space Program within the next 20–50 years.[1,2] Unlike the Apollo program, these new initiatives will focus on long-duration missions and permanent facilities and operations on the surface of those planetary bodies. However, the goal of long-duration human space operations has a profound impact on mission design. Because the continued high cost of space transportation makes it very expensive to resupply extraterrestrial outposts with consumables from Earth, the attainment of self-sufficiency on the Moon and Mars will become major avenues in space science, exploration, and commerce.[2] The advent of long-duration missions and permanent, isolated standby facilities requires further development of concepts in automated maintenance and repair, reliability, and longevity of systems. Research on continuous life support systems is far ahead of other elements at this time, but the fully closed ecological system approach must be augmented. There are too many ways for a closed ecology to become disrupted and fail, requiring emergency resupply of basic items ranging from oxygen to water and food. It is important to identify and develop the critical technology providing autonomous operation of chemical processes in space that evade nonrepairable failures for a long-duration mission.

Unlike the scientific aspects of an extraterrestrial research station, the production of commodities from in situ resources will involve continuous or repetitive operations that need cost-effective automated operation and maintenance. On the other hand, production of large quantities of oxygen for fuel or for life support may be vital for survival and these systems must be extremely reliable and robust. Furthermore, simple chemical processors offer near-term benefits for early lunar and Mars missions if they are ultrareliable and require minimal human interaction. The research reported here is directed toward establishing the framework and methodology required to operate a mission critical system autonomously. The use of the Martian atmosphere as a feedstock for the production of oxygen has been under investigation for some time.[3-5] Since Mars' atmospheric composition is known accurately[6] and is not sensitive to a landing site, it is an ideal feedstock for early missions using in situ resources. Furthermore, the yttria stabilized zirconia cell that can be used to remove oxygen from heated Mars atmosphere has been demonstrated.[7] However, in order for the technology to become accepted as a viable option for supporting early missions to Mars, it is necessary to demonstrate that these systems can be operated reliably for long periods of time and with minimum human intervention.

Our goal is to establish the reliability of a Mars oxygen separation system. Although Mars' atmosphere must be extracted and oxygen must be liquefied and stored, a variety of hardware elements can be used between atmospheric collection and storage.[4,5,8] However, the oxygen extraction process using heated Mars atmosphere and a zirconia-based electrochemical cell has been identified as the preferred oxygen separation element. Since pumps, compressors, refrigerators, and power

Received Sept. 21, 1990; revision received Feb. 20, 1991; accepted for publication May 1, 1991.

*Associate Professor, Department of Mechanical Engineering and Mechanics. Member AIAA.
†Graduate Research Assistant, Department of Mechanical Engineering and Mechanics. Member AIAA.
‡Professor, Department of Mechanical Engineering and Mechanics. Member AIAA.

generating equipment are accepted elements in processing plants and since a multiplicity of options are available for each element, our research has focused only on developing a well-controlled and reliable oxygen separation system that can be operated as an endurance test bed.

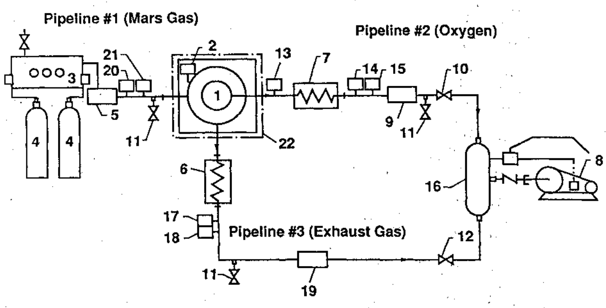
In addition to space systems, expert systems technology has been applied extensively to many fields, including chemical plants and power plants, in the past 10 years.[9,10] Expert systems can deliver human expertise to provide several functions like maintenance, operation, prediction, control, and design and enhance the performance and reliability of the processing unit or control system. However, a recent survey[9] showed that over 95% of the expert systems applied to chemical plants are less than two years old and over 90% of those applications relied on shells, not languages. The survey also reported that most of the expert systems (54%) were used for system diagnosis and prescription. This indicates that expert systems technology is still in its infant stage and more experienced knowledge-based maintenance and more flexible tools are required. It is noted that automated maintenance by expert systems in a variety of terrestrial applications other than chemical plants is also being studied actively.[11,12]

One of the main problems associated with maintenance of dynamic systems is system failure detection and isolation (FDI). Various hardware devices and software algorithms providing FDI capability have been proposed.[10,13] Determination of failure threshold, which is a common problem for all FDI designs, has been studied[14]; application of these methods to chemical plants needs further study. Current methodologies in space system design rely on redundant elements in critical areas to enhance FDI capability. In addition to hardware redundancy, expert systems require analytical redundancy that utilizes the analytical relationships between different elements in the system to detect and identify the component failure. In that way, system performance can be improved without increasing hardware elements. This technique will be discussed in the present application.

The objective of this work is to develop a preliminary expert system to provide the automation of housekeeping functions such as self-health checkout, emergency shutdown, failure detection, and isolation and active control action for the Mars oxygen production system.

II. Mars Oxygen Production System

In order to place the expert system research in context, a brief discussion of the Mars oxygen production system is required. The processing system[15] is shown schematically in Fig. 1. Since it is a prototype machine to be used mainly for testing and demonstration, it is also called the Mars oxygen demonstration (MOD) system. A continuous supply of simulated Mars atmosphere (95.32% CO_2, 2.7% N_2, 1.78% Ar, 0.13% O_2, and 0.07% CO by volume) is provided to the cell via gas storage bottles and a manifold system. The feed-gas mass flow rate is controlled by a mass flow controller, and the electrochemical cell is operated at a pressure of 50–120 mbar, which is considered to be the nominal operating pressure range for the Mars system. The feed gas and cell are maintained at a temperature of 1000–1200 K. The electrochemical cell separates oxygen from the feed gas and pumps the ionic oxygen across the membrane, utilizing collection pressures on the order of 10 mbar. (It is desirable to collect oxygen at a pressure above Mars ambient so that leaks do not cause collected oxygen to become contaminated with Mars atmosphere.) Both the exhaust gas and oxygen leaving the cell are monitored through separate mass flow meters. In the present system configuration, both gas streams are recombined in a ballast tank and expelled to the atmosphere through a vacuum pump. Additional system components include an oven for maintaining the cell temperature and heat exchangers for protecting downstream flow measuring devices. Feed gas, exhaust gas, and collected oxygen can be sampled to verify that the system is operated properly. The various gas stream pressures are regulated



LIST OF COMPONENTS

ITEM NO.	DESCRIPTION	SENSORS
1	Zirconia Cell / Voltage & Current Sensors	V_z, I_z
2	Cell Pressure Transducer / Thermocouple	P_c, T_c
3	Mars Gas Manifold / Pressure Gauge	P_d
4	Mars Gas Bottles / Pressure Transducers	P_p, P_r
5	Mars Gas Flow Controller / Flow Meter	F_1
6	Exhaust Gas Heat Exchanger	
7	Oxygen Heat Exchanger	
8	Vacuum Pump / Pressure Transducer	P_t
9	Oxygen Flow Meter	F_2
10	Oxygen Outlet Valve	
11	Sampling Valves	
12	Exhaust Gas Outlet Valve	
13	Zirconia Cell Pressure Transducer	P_z
14	Oxygen Pressure Transducer	P_2
15	Oxygen Thermocouple	T_2
16	Damping Tank	
17	Exhaust Gas Pressure Transducer	P_3
18	Exhaust Gas Thermocouple	T_3
19	Exhaust Gas Flow Meter	F_3
20	Mars Gas Pressure Transducer	P_1
21	Mars Gas Thermocouple	T_1
22	Oven System	V_o, I_o

Fig. 1 Schematic diagram of Mars oxygen production system.

through a series of manual valves, which can be tuned prior to endurance testing. Temperatures are measured using chromel/alumel and copper/constantan thermocouples, and those data are supplied to an IBM PC/AT computer through a Keithley 500 data acquisition system. In addition, mass flow rates, cell voltage, and gas line pressure measurements are provided to the computer through the data acquisition system. The computer can control the feed-gas mass flow rate as well as shut down the power supplies for the cell and for the oven.

III. Expert Systems Approach

Utilizing Fig. 1, the development of a knowledge-based expert system for failure detection and isolation will be discussed. The goal of the project was to provide autonomous maintenance for the oxygen production unit during long-duration tests of up to one year. In this section, the system operating conditions and parameters are first defined from experimental data. Then, failure modes for a specific set of operating conditions have been defined and rule-based diagnostic and decision-making algorithms are developed to handle the necessary housekeeping functions.

A. System Operating Conditions and Parameters

The definition of the system operating conditions is based on the experience in construction and operation of the Mars oxygen production system. However, different operating condition sets can be determined according to several kinds of operating criteria, such as optimal conversion rate of CO_2 to O_2 or maximum oxygen production, which can be obtained from a specified constant feed-gas flow rate. For a set of operating condition definitions, system parameter data, including pressure, flow rate, temperature, voltage, and current, are collected from sensors and stored in an array in a microcomputer by the data acquisition system. By design, some system parameters can be adjusted each time the system is initialized and, hence, are called independent system parameters. These parameters include cell temperature T_c, cell voltage across the sealed tubular zirconia membrane V_z, the set point for the feed-gas mass flow rate F_1, feed-gas delivery pressure P_d, cell operating pressure P_c, and oxygen collection pressure at the zirconia tubular membrane P_z.

Determination of the best initial input parameters has been a part of the optimization study. Several tests were performed to determine the suitable initial system parameters and the results are discussed in Sec. V. One of the most sensitive system parameters is the oven temperature T_c, which is controlled by an oven heating subsystem. In order to maintain the ionic resistance of the zirconia cell below 15 Ω, it was determined that T_c should be between 1000 and 1200 K. However, the higher oven temperatures lowered the allowable cell voltage that could be maintained across the zirconia cell. A critical voltage V_{zc} existed for the particular cell operating temperature, above which damage occurred to the cell. If the applied voltage V_z exceeds V_{zc}, oxygen atoms in the zirconia matrix will be drawn from the cell, destroying its ionic conductivity. The value of the critical voltage had to be determined experimentally.

The optimal mass-flow-rate set point for the feed gas F_1 can also be determined by experimental testing. Tests performed for feed-gas flow rate between 50 and 150 standard cubic centimeters per minute (sccm) showed that, for fixed cell pressures, higher feed-gas flow rates produced higher current. However, the conversion efficiency (percentage of oxygen collected) was higher for lower feed-gas flow rates. Therefore, the mass flow set point for the feed gas was chosen to be 50 sccm in order to maximize conversion efficiency. The feed-gas delivery pressure was set to be 40 psig according to the specifications of the flow controller. The corresponding nominal sensor values and allowable tolerances for each set of operating condition definitions are given in Sec. V.

Once the system parameters have been set, the other system parameters can be determined by the system characteristics. These dependent system parameters are pressure in the feed-gas pipeline P_1, pressure in the oxygen pipeline P_2, pressure in the waste-gas pipeline P_3, pressure in the ballast tank P_t, waste-gas flow rate F_3, current across the sealed tubular zirconia membrane I_z, and oxygen flow rate F_2.

B. Failure Modes

For each set of operating condition definitions, failure modes for the subsystems have been identified and are listed in Table 1. For either sensors or leakage, 16 additional failure modes were also identified.[17] The corresponding isolation levels and required control actions issued from expert systems commands are also provided. The control actions are determined by examining the following criteria.

1) If a failure will damage any other subsystem or component when the failure is not able to be treated immediately after it happens, the control action for the failure mode is set to be "shutdown system."

2) If a failure will cause the oxygen pipeline to be contaminated, the control action for the failure mode is set to be shutdown system.

3) The control action for any other failure mode that is not so critical as criteria 1 and 2 is set to be "alarm signal."

Among the identified failure modes, two kinds of failure modes are critical and deserve more attention, i.e., failure of the zirconia cell and mechanical failures that produce large fluid line leaks (see Fig. 1). The cell may be damaged by either using an excessive cell voltage from the power supply subsystem or by being heated to higher temperatures than its set point. If the oxygen cell is damaged, no oxygen will be produced and the expert system will invoke shutdown procedures immediately. However, since multiple oxygen cells are planned in the future applications, the expert system should be able to isolate the damaged cell and reconfigure the overall cell network to enable continued operation. The expert system may even follow some testing procedures to make sure that the damaged cell has actually failed. The second critical mode is a major leakage in a flow line. Because the pressure inside the system is far below atmospheric pressure during terrestrial testing, a significant leak will draw external air into the system and the line pressure will increase rapidly toward 1 atm. A large leakage in pipeline 1 or pipeline 3 (see Fig. 1) will degrade the oxygen production seriously and make the pressure difference across the zirconia tube large, possibly causing the tube to fail mechanically; thus, the whole system should be shut down immediately. On the other hand, if the leak is small, it is considered to be noncritical and only an alarm signal will be issued. A leakage in the zirconia tube or pipeline 2, even a small leakage, is considered to be critical because it might cause the oxygen in pipeline 2 to be contaminated.

C. Expert System Methodology

Forward chaining and backward chaining are two basic types of inference engines used in expert systems. Forward chaining starts from the beginning, collects information based on the rules in the knowledge base, and reaches conclusions based on this information. Backward chaining takes all of the possible conclusions and then tries to verify each one by work-

Table 1 General system failure modes

Failure mode	Isolation level	Automatic action
G01 T_c too high	Oven subsystem	Shutdown oven
G02 T_c too low	Oven subsystem	Alarm signal
G03 V_z too high	Power 1 subsystem	Shutdown power
G04 V_z too low	Power 1 subsystem	Alarm signal
G05 V_z unstable	Power 1 subsystem	Alarm signal
G06 V_z bad connection or clip oxidized	Cell subsystem	Shutdown system
G07 Z-cell degraded	Cell subsystem	Shutdown system
G08 V_z short circuit	Cell subsystem	Shutdown system
G09 manifold switch F	Manifold subsystem	Alarm signal
G10 P_r too low	Manifold subsystem	Alarm signal
G11 P_d too high	Manifold subsystem	Shutdown system
G12 P_d too low	Manifold subsystem	Alarm signal
G13 F_1 too high	DAC subsystem	Shutdown F_1
G14 F_1 too low	DAC subsystem	Alarm signal
G15 V_w set point high	Pipe network	Alarm signal
G16 V_w set point low	Pipe network	Alarm signal
G17 V_0 set point high	Pipe network	Alarm signal
G18 V_0 set point low	Pipe network	Alarm signal
G19 pump degraded	Vacuum subsystem	Shutdown system
G20 PST-10 failure	Power subsystem	Shutdown system
G21 PST-15 failure	Power subsystem	Shutdown system
G22 FMS ground error	Power subsystem	Alarm signal

ing backward to known facts. In this research, forward chaining first goes through some block diagrams that represent the failure detection and isolation algorithm and then acquires sensor data—when the algorithm calls for it—until certain failure modes are reached. Backward chaining gathers all of the sensor data, creates a sensor pattern file, and then compares the pattern file with each pattern file of failure modes until a pattern match is found. Whether a system should use forward chaining or backward chaining depends on the number of facts, which are the sensor values, and the number of conclusions, which are the failure modes. Forward chaining works better when there are only a limited number of facts and many conclusions could be reached from these facts. Backward chaining works better when there are only a few possible conclusions with many facts. In this research, the number of failure modes is comparable to the number of sensor values, and so both methods are used. From numerical simulations, the forward chaining method was found to be more efficient but harder to modify. The backward chaining approach was more suitable for experimental tests but was less efficient. In this paper, only backward chaining is implemented for further experiments.

1. Expert System Using Forward Chaining

Corresponding to each failure mode, a set of all known or postulated symptoms has been considered. A knowledge-based expert system is then developed to provide the following: 1) data acquisition and self-health checkout, 2) emergency shutdown, 3) failure detection and isolation, and 4) computer-based simulation and realization.[16] Each element is described separately in the following discussion.

a) Data acquisition and self-health checkout. At prescribed regular intervals, the expert system will perform the following tasks: 1) collect and store system parametric data (pressure, temperature, voltage, flow rate) in an array in computer memory (important parametric data like cell voltage and oven temperature are assumed to be sampled at higher sampling rates than other data); 2) evaluate system performance after each sampling cycle by using the failure detection algorithm described later; 3) update system displays that report system performance; 4) periodically transfer representative parametric data (i.e., statistical average, standard deviation, etc.) to a printer or floppy disk; and 5) if any failure mode is detected, activate the alarm signal and display the corresponding failure messages on the computer screen to advise the operator on whether the system has been shut down due to a critical failure or if certain system adjustments are required.

b) Emergency shutdown. For emergency conditions, the expert system will evoke the shutdown procedures, which may include the following: 1) activation of the local alarm, notifying the immediate area of a system failure; 2) disengagement of power to the system, turning the feed-gas flow controller (item 5 in Fig. 1) off; 3) transfer of all data in the current memory to disk for subsequent failure analysis; 4) initiation of local telephone calls to notify project personnel of a system failure; and 5) transfer of the system from its autonomous control mode to an interactive mode. After system shutdown, the expert system may ask some questions about further diagnosis or repairing procedures and can work interactively with a local or terrestrial control center.

c) Failure detection and isolation. A knowledge-based algorithm for system FDI has been developed and is described by using the block diagrams developed by Huang et al.[16] From the acquired sensor data, the FDI algorithm can identify each existing failure mode under the assumptions that main power, computer, and the data acquisition system never fail and only one failure mode may occur at a time. For those failure modes not considered or those that combine at least two known failure modes, the FDI algorithm can only display the existing symptoms, turn on the alarm, and continue to monitor the system. Any new failure mode found after further testing can be added to the knowledge base. If hardware redundancies (like multiple oven thermocouples) or analytical redundancies are introduced in the future, the FDI algorithm will be modified to interrogate the system in order to detect anomalies and distinguish between sensor failures and subsystem failures.

Because a cell failure is critical, the cell voltage, cell current, and oven temperature are checked more frequently (by a factor of 200). All other parametric data are checked after every 200 sampling cycles of the cell voltage and current. If the cell voltage exceeds V_{zc}, the cell current exceeds 500 mA (maximum measurable current for current measurement design), or the oven temperature exceeds the upper limit, a cell failure is acknowledged and system shutdown procedures are invoked.

If hardware redundancies exist, the FDI algorithm can be modified by assuming that only one sensor fails at a time. Suppose we put three thermocouples at different places inside the oven with the following measurements:

$$[T_{cm_i}] = [k_i]T_c + [v_i], \qquad i = 1,2,3 \tag{1}$$

where T_{cm_i} is the measurement value of each thermocouple, T_c the averaged temperature of the oven, v_i the measurement noise, and k_i the factor related to different spacial placements of the thermocouples. Equation (1) means that the measurement values of the three thermocouples can be expressed as a linear transformation of the averaged temperature of the oven and measurement noise. If three calibrated thermocouples are located at the same spatial point, then $k_1 = k_2 = k_3 = 1$; otherwise k_i can be determined by testing under thermally steady conditions. From Eq. (1), we can derive three parity residuals:

$$[\mathrm{Par}] = [V_{ij}][T_{cm_j}]$$

where

$$[\mathrm{Par}] = \begin{bmatrix} \mathrm{Par}_{12} \\ \mathrm{Par}_{23} \\ \mathrm{Par}_{13} \end{bmatrix} \qquad [V_{ij}] = \begin{bmatrix} 1/k_1 & -1/k_2 & 0 \\ 0 & 1/k_2 & -1/k_3 \\ 1/k_1 & 0 & -1/k_3 \end{bmatrix}$$

These three parity residuals are then compared with three corresponding thresholds Th_{12}, Th_{23}, and Th_{13} to identify any sensor failure. For example, $\mathrm{Par}_{12} > Th_{12}$, $\mathrm{Par}_{23} < Th_{23}$, and $\mathrm{Par}_{13} > Th_{13}$ indicate that thermocouple 1 has failed and T_{cm_1} should not be used. All thresholds are chosen to be 10% of the change of T_c and can be adjusted according to the desired accuracy for each thermocouple. A similar algorithm can be applied to other sensors if the hardware redundancies are available.

A similar FDI algorithm can be used for analytical redundancies. For example, if there is no leakage in the whole system (see Fig. 1) and the cell performs in a nominal condition, then conservation of mass for steady-state operation yields

$$F_1 = F_2 + F_3 = f_2F_1 + f_3F_1 = (f_2 + f_3)F_1$$

with

$$f_2 + f_3 = f_1 = 1$$

and

$$[F_{m_i}] = [f_i]F_1 + [v_i], \qquad i = 1,2,3 \tag{2}$$

where F_{m_i} is the measurement value of each flowmeter and f_i represents the ratio of F_i to F_1. Equation (2) is similar to Eq. (1). Thus, flow conservation can be invoked to identify the failure of one of three flowmeters without having hardware redundancy. However, this method can be applied only by assuming that deviation of F_1 from its nominal set point is small and there is no leakage and no other subsystem failure. Because the system is nonlinear, f_1 cannot be kept constant if F_1 deviates far from its nominal set point. The same problem will occur if leakages or subsystem failures exist in the system. Consequently, this method cannot be used to identify the failures of sensors unambiguously. Instead, we use other system parameters to identify the failure of sensors. If all of the other sensor readings are normal except a particular one that exceeds the range of a preassigned threshold, then it follows that the particular sensor has failed. For most cases, this FDI algorithm assumes that only one failure mode exists at a time.

d) Computer program realization. Based on the FDI algorithm, a computer program has been developed using BASIC language to provide numerical simulations. BASIC programming was chosen in order to interface with the hardware configuration (Keithley 500 data acquisition system) with high-speed data processing deferred for future development. The nominal values and allowable tolerances of the system parameters that are assigned in data files in the program have been provided from experimental data developed in Sec. V.

2. Expert System Using Backward Chaining (or Pattern Matching)

Another methodology of FDI using backward chaining has been developed and is described as follows.

a) Symbolic manipulation. Suppose there are n sensors installed in a system and their output values acquired by the data acquisition system at the instant kT are

$$S_i(kT), \qquad i = 1, 2, \ldots, n; \quad T = \text{sampling period}$$

or simply

$$S_i(k)$$

S_i can be a digital value or can be transferred into a knowledge representative word such as HIGH, LOW, or OK. Failure modes can be tested and the corresponding sensor output values for each failure mode recorded. For example, assume that each failure mode can be identified uniquely by a set of current sensor output values $S_i(k)$, $i = 1, 2, \ldots, n$, i.e.,

$$F_M(k) = f(S_1, S_2, \ldots, S_n)$$
$$F_M(k) = \text{failure mode identified at the instant } kT$$

The value of $F_M(k)$ can be any of the failure modes listed in Table 1, and $F_M(k) = N$ means that the system is in normal operating condition. $F_M(k) = ?$ represents the case in which the current version of the knowledge base cannot identify the failure. It might be a new failure mode that has not been recognized or a failure mode with two or more failure modes happening at the same time. In summary, the failure mode at a discrete time can be identified by examining the pattern of all the sensor outputs.

b) Knowledge and rule base. The threshold of each sensor output for different failure modes may not be the same. Both the upper limit and the lower limit of each sensor output are used for failure mode identification. The relation between failure modes and sensor outputs for the MOD machine have been tested, and 22 rules have been set (see Table 2) for the failure modes shown in Table 1.

c) Testing procedures. In order to determine the thresholds for each failure mode, several testing categories are suggested. Before starting the tests, it is necessary for the system to be operated under normal conditions. The failure tests can be divided into the following steps: 1) statistical tests of sensor readings, 2) tests of each individual general failure mode, and 3) tests of leakage failures. Using the knowledge base and test results, a computer program in BASIC language has been developed for further experiments.

D. Expert System Using Application Software

It is easier to develop expert systems by using expert system shells. The criteria for selecting a competent software package for different jobs have been discussed elsewhere (see, e.g., San Giovanni and Romans[9]). Generally, the problem characteristics have to be considered first. The problem characteristics suggest certain solution features. The solution features together with the desired system features form the basis for choosing a particular shell. For the Mars oxygen production system, we want to diagnose the system failure modes from 16 sensor readings. There are at least 23 possible failure modes. Furthermore, we want the shell to be able to interface with the data acquisition system so that the diagnostic process can be in real time. Because an IBM/PC/AT computer is used, the memory capacity is also a crucial factor. Based on these criteria, an application software called 1st-Class was chosen. The expert system shell 1st-Class can handle up to 32 factors, 32 values, 32 results, and 255 examples, which is enough for our case. A data acquisition program in BASIC was also developed to acquire data without using a lot of memory space and thus enabled the interface between the data acquisition system and the 1st-Class expert system shell.

IV. Dynamic Model of the Mars Oxygen Demonstration System Using Bond Graph

Static and dynamic models of gas behavior in pipelines require complex analysis of fluid dynamics. The bond graph[18]

Table 2 Rule base for failure detection and isolation algorithm[a]

Rule 1:	If all the sensor outputs are normal except a particular one that is out of the normal range, then the particular sensor failed.
Rule 2:	If $T_c > T_c^a$, $I_z > I_z^a$, $V_z < V_z^b$, and $F_2 > F_2^a$, then failure mode G01 is justified.
Rule 3:	If $T_c < T_c^b$, $I_z < I_z^b$, $V_z > V_z^a$, and $F_2 < F_2^b$, then failure mode G02 is justified.
Rule 4:	If $V_z > V_z^a$, $I_z > I_z^a$, $F_2 > F_2^a$, and $P_z > P_z^a$, then failure mode G03 is justified.
Rule 5:	If $V_z < V_z^b$, $I_z < I_z^b$, $F_2 < F_2^b$, and $P_z < P_z^b$, then failure mode G04 is justified.
Rule 6:	If $I_z < I_z^b$, $V_z > V_z^a$, $P_z < P_z^b$, and T_c is normal, then failure mode G06 is justified.
Rule 7:	If $I_z < I_z^b$, $V_z > V_z^a$, $P_z < P_z^b$, and T_c is normal, then failure mode G07 is justified.
Rule 8:	If $I_z > I_z^a$, $V_z < V_z^b$, $F_2 < F_2^b$, and T_c is normal, then failure mode G08 is justified.
Rule 9:	If $P_d < P_d^b$, $P_p < P_p^b$, and $P_r > P_r^b$, then failure mode G09 is justified.
Rule 10:	If $P_r < P_r^b$, then failure mode G10 is justified.
Rule 11:	If $P_d > P_d^a$ and $P_p < P_p^a$, then failure mode G11 is justified.
Rule 12:	If $P_d < P_d^b$ and $P_p > P_p^b$, then failure mode G12 is justified.
Rule 13:	If $F_1 > F_1^a$, $F_3 > F_3^a$, $P_1 > P_1^a$, and $P_3 > P_3^a$, then failure mode G13 is justified.
Rule 14:	If $F_1 < F_1^b$, $F_3 < F_3^b$, $P_1 < P_1^b$, and $P_3 < P_3^b$, then failure mode G14 is justified.
Rule 15:	If $P_c > P_c^a$, $P_1 > P_1^a$, and F_1 and F_3 are normal, then failure mode G15 is justified.
Rule 16:	If $P_c < P_c^b$, $P_1 < P_1^b$, and F_1 and F_3 are normal, then failure mode G16 is justified.
Rule 17:	If $P_z > P_z^a$, $P_2 > P_2^a$, and P_c is normal, then failure mode G17 is justified.
Rule 18:	If $P_z < P_z^b$, $P_2 < P_2^b$, and P_c is normal, then failure mode G18 is justified.
Rule 19:	If $P_c > P_c^a$, $P_z > P_z^a$, and F_1 and F_3 are normal, then failure mode G19 is justified.
Rule 20:	If all sensor readings are normal except P_1, P_2, P_3, P_t, P_p, and P_r, then failure mode G20 is justified.
Rule 21	If F_1, F_2, F_3, P_c, and P_z are almost zero, then failure mode G21 is justified.
Rule 22	If F_1, F_2, and F_3 are negative, then failure mode G22 is justified.

[a]Superscript a, upper limit; superscript b, lower limit.

method is an easier alternative way to derive a mathematical model for the MOD system for further analysis. Because of the small tube diameters and flow rates, it is clear that we are dealing with a laminar, incompressible, and static-pressure dominated gas flow.[17] From that knowledge, we can use the bond graph method to derive a dynamic model for the system. However, there is one complicating factor due to density variations. Although the flows can be considered incompressible, the density of the gas varies with the pressure along the pipeline. Similar to the dynamic models for thermal systems,[18] the pseudo bond graph method was used to represent the relations between system variables. For the MOD system, all of the relations between variables are verified through experimental testing. The proposed block diagram for the flow controller and bond graph of the MOD system are shown in Figs. 2 and 3. In Fig. 2, the discharge coefficient C_d is a function of the orifice area of the flow controller A_d.

The system dynamic equations were derived (see Ref. 17 for their derivation) and can be fully described by four state variables, four state equations, and one output equation. In addition, the temperature keeping subsystem can be modeled as a basic thermal system[19] consisting of a mass block that is assumed to have a nearly uniform temperature T_c and thermal capacity C. The thermal block is assumed to be surrounded by insulation with thermal resistance R. We assume further that the ambient temperature remains a constant T_a, even if heat flows to and from the surroundings. An electric-resistance heating element is embedded in the mass block. By employing the bond graph technique and noting the on-off control incorporated in the oven controller, the following two dynamic equations and control laws can be derived[20]:

$$\dot{T}_c = -(1/RC)(T_c - T_a) + e \cdot i/C \qquad \text{when} \qquad T_c < T_s - \mathrm{d}T$$

$$\dot{T}_c = -(1/RC)(T_c - T_a) \qquad \text{when} \qquad T_c > T_s - \mathrm{d}T$$

where $e \cdot i$ is the electrical power of the oven, T_s the temperature set point, and $\mathrm{d}T$ the deviation threshold for on-off control. Determination of process parameters includes determination of the values of C_c, K, P, H, P_d, R_1, D_{P_1}, I_1, R_3, D_{P_3}, I_3, V_z, T_c, R_z, R_2, D_{P_2}, I_2, . . ., etc. Testing procedures and results are given in Sec. V. Numerical simulations are also provided.

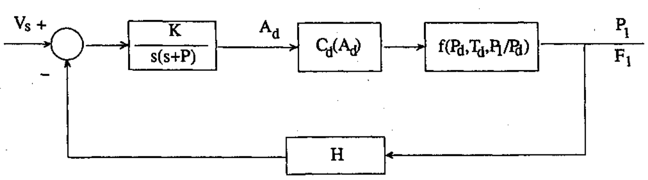


Fig. 2 Block diagram of the flow control.

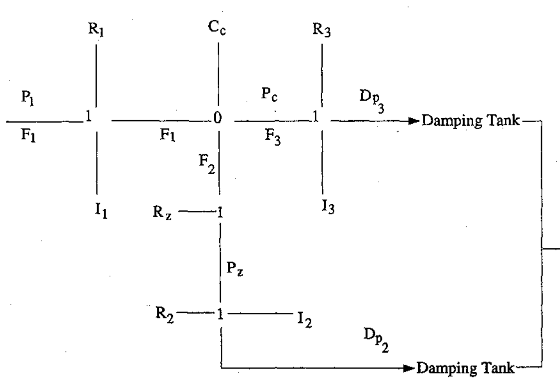


Fig. 3 Bond graph representation of Mars oxygen production system.

Table 3 Control values for input parameters

T_c, K	V_z, V	F_1, sccm	P_d, psig	P_c, mbar	P_z, mbar
900	1.0	50	50	75	50
1000	1.2	100		115	75
1200	1.5	150		125	115
	2.0			150	125
					150

Table 4 Statistics or sensor output values

Sensor	Mean	Standard deviation
T_c, K	1200.241	1.359235
V_z, V	1.014947	0.003172
F_1, g/h	5.406548	0.038737
F_2, g/h	0.026945	0.000856
F_3, g/h	4.726044	0.030729
P_p, psig	934.0432	7.799892
P_c, mbar	124.3519	1.177941
P_c, mbar	127.3614	0.295978
P_z, mbar	48.89628	1.113997
P_1, mbar	192.3832	1.301610
P_2, mbar	7.374239	0.235801
P_3, mbar	99.79853	1.449098

V. Experimental Results and Numerical Simulations

A. Preliminary Evaluation of System Performance

The whole MOD system has been set up and system performance has been evaluated by operating the system using different input parameter sets. Table 3 lists the control values that have been used for each individual input parameter (refer to Sec. III.A.) during testing. Both carbon dioxide and simulated Mars gases were used as feed gases for testing. In addition, a proposed 30-min cell repair test was implemented by reversing the cell polarity, which resulted in conduction of oxygen back into the feed-gas stream[21] and resupplied oxygen to the zirconia. (No observable improvement was achieved by reversing the potential.)

In order to determine the failure thresholds for the expert system, the normal range of each sensor output under normal operating conditions was examined first. That task was accomplished by recording all of the sensor outputs over a 24-h operating period. The mean values and standard deviations s_d for each sensor output were then calculated and are listed in Table 4. It is noted that P_1, P_2, and P_3 are regular pressure transducers that measure gauge pressure instead of absolute pressure. Their readings may vary with barometric pressure. Tests of each individual failure mode were also performed successfully.

B. Experimental Data of System Dynamics

The validity of the dynamic model can be examined through a comparison between the experimental data and the simulation results of the model. The responses of some system parameters, when the flow-rate set point of the flow controller changes instantly from one value to another, are compared between experiments and simulations. Here, the change of the F_1 set point is treated as a step input to the system. Six different test cases were performed.[17]

C. Simulation Results of the System Model

As presented in Sec. IV, the system dynamics can be described by the following four equations with four state variables (P_c, F_1, F_{1_d}, and F_3):

$$\dot{P}_c = (1/C_c)[F_1 - F_2 - F_3]$$

$$\dot{F}_1 = F_{1_d}$$

$$\dot{F}_{1_d} = KV_s\,[g(P_c)] - PF_{1_d} - KH\,[g(P_c)]F_1$$

$$\dot{F}_3 = (1/I_3)[P_c - R_3F_3 - D_{P_3}]$$

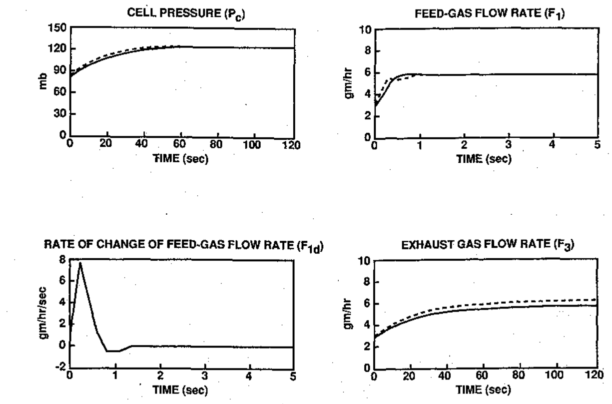


Fig. 4 Numerical simulation (solid line) and experimental results (dashed line) when feed-gas flow rate is increased from 25 to 50 sccm.

where

$$g(P_c) = mC_d(T_d)^{1/2}P_d[(P_1/P_d)^{2/1.3} - (P_1/P_d)^{2.3/1.3}]^{1/2}$$

$$P_1 = P_c + R_1F_1 + D_{P_3} + I_1F_{1_d}$$

and m is an empirical coefficient.

In order to perform numerical simulations, the values of process parameters have to be determined.[17] A software package called DE was used to realize the numerical simulations for this case. The numerical simulation results as well as the experimental data are shown in Fig. 4. Simulation results are comparable to those obtained from experiments.

VI. Concluding Remarks

The hardware setup for a prototype Mars oxygen production system has been built. Several operational tests have been performed to obtain the optimal operating conditions in terms of providing maximum oxygen production or production efficiency. The data acquisition system has been set up to acquire the system data and control the feed-gas flow rate.

Several possible failure modes were tested and algorithms for failure detection and isolation were developed based on the failure tests. From simulations, the method using a forward chaining approach was found to be more efficient but harder to modify. It was determined that the backward chaining method was more flexible for modification and has therefore been implemented for experimental validation. The expert system shell 1st-Class was found to be very helpful in developing a knowledge base, but it presented difficulties in handling numerical data.

An effort has been made to derive the dynamic model of the system using the bond graph method. The results of numerical simulations were compared with the experimental data. Better agreement between the simulation results and the experimental data were achieved for the cases when feed-gas flow rate was decreased rather than increased. For the cases when feed-gas flow rate was increased, the agreement was not good. This phenomenon showed that the model needed to be improved. The model needs to be modified by taking into account real gas behavior such as orifice effects, compressibility, and thermal effects. Since sudden increases in flow variables tend to produce compression waves, nonlinear effects are considered responsible for discrepancies in one type of system behavior that complicates the controller dynamics.

Acknowledgment

This work was supported partially by USRA, the Planetary Society, and NASA Johnson Space Center. Their support is gratefully acknowledged.

References

[1]Paine, T. D., *Pioneering the Space Frontier; Report of the National Commission of Space,* Bantam, New York, 1986, pp. 1–16.

[2]Duke, M. B., "Lunar and Mars Missions, Challenges for Advanced Life Support," Society of Automotive Engineers, Paper 88-0988, July 1988.

[3]Ash, R. L., Dowler, W. L., and Varsi, G., "Feasibility of Rocket Propellant Production on Mars," *Acta Astronautica,* Vol. 5, No. 9, 1978, pp. 705–724.

[4]Ash, R. L., Richter, R., Dowler, W. L., Hanson, J. A., and Uphoff, C. W., "Autonomous Oxygen Production for a Mars Return Vehicle," International Astronautical Federation Paper 82-210, Sept. 1982.

[5]Frisbee, R. H., French, J. R., Jr., and Lawton, E. A., "A New Look at Oxygen Production on Mars—In Situ Propellant Production (ISPP)," AIAA Paper 87-0236, Jan. 1987.

[6]Owen, T., Biemann, K., Rushneck, D. R., Biller, J. E., Howarth, D. E., and Lafleur, A. L., "The Composition of the Atmosphere at the Surface of Mars," *Journal of Geophysical Research,* Vol. 82, No. 28, pp. 4635–4639.

[7]Richter, R., "Basic Investigation into the Production of Oxygen in a Solid Electrolyte Process," AIAA Paper 81-1175, June 1981.

[8]Ash, R. L., Huang, J.-K., Johnson, P. B., and Sivertson, W. E., Jr., "Elements of Oxygen Production Systems Using Martian Atmosphere," AIAA Paper 86-1586, June 1986.

[9]San Giovanni, J. P., and Romans, H. C., "Expert Systems in Industry: A Survey," *Chemical Engineering Progress,* Vol. 9, No. 1, 1987, pp. 52–59.

[10]Malin, J. T., and Lance, N., Jr., "An Expert System Approach to Automated Fault Management in a Regenerative Life Support Subsystem," AIAA Paper 86-0321, Jan. 1986.

[11]Aggarwal, B. B., Giordano, J. C., and Przybylko, S. J., "Knowledge-Based Systems for Rotodynamic Diagnostics," AIAA Paper 86-1678, June 1986.

[12]Liubakka, M. K., Rizzoni, G., and Ribbens, W. B., "Failure Detection Algorithms Applied to Control System Design for Improved Diagnostics and Reliability," Society of Automotive Engineers, Paper 88-0726, Feb. 1988.

[13]Willsky, A. S., "A Survey of Design Methods for Failure Detection in Dynamic Systems," *Automatica,* Vol. 12, No. 6, 1976, pp. 601–611.

[14]Walker, B. K., and Gai, E. G., "Fault Detection Threshold Determination Technique Using Markov Theory," *Journal of Guidance and Control,* Vol. 2, No. 4, 1979, pp. 313–319.

[15]Ash, R. L., Werne, J. A., and Haywood, M. B., "Design of a Mars Oxygen Processor," *Case for Mars III,* Vol. 75, edited by C. Stoker, American Astronautical Society, Washington, DC, 1989, pp. 479–487.

[16]Huang, J.-K., Wei, Y.-H., Ash, R. L., and Ho, M.-T., "An Expert Systems Approach to Automated Maintenance for a Mars Oxygen Production System," Society of Automotive Engineers, Paper 88-1056, July 1988.

[17]Ho, M.-T., "Expert Systems for Automated Maintenance of a Mars Oxygen Production System," M.S. Thesis, Dept. of Mechanical Engineering and Mechanics, Old Dominion Univ., Norfolk, VA, May 1989.

[18]Karnopp, D. C., "State Variables and Pseudo Bond Graphs for Compressible Thermofluid Systems," *Journal of Dynamic Systems, Measurement and Control,* Vol. 101, No. 3, 1979, pp. 201–204.

[19]Collacott, R. A., *Mechanical Fault Diagnosis,* Chapman & Hall, London, distributed in the U.S.A. by Halsted Press, New York, 1977, pp. 16–42.

[20]Rosenberg, R. C., and Karnopp, D. C., *Introduction to Physical System Dynamics,* McGraw-Hill, New York, 1983, pp. 83–106.

[21]Ash, R. L., "Mars Oxygen Production System Design," *Proceedings of the 4th Annual NASA/USRA University Advanced Design Program Conference,* 1988, pp. 1–6.

Alfred L. Vampola
Associate Editor