Appendix C

Extended Example: Simplified Aid for EVA Rescue (SAFER)

The example presented in this appendix is based on NASA's Simplified Aid for EVA Rescue (SAFER). SAFER is a new system for free-floating astronaut propulsion that is intended for use on Space Shuttle missions, as well as during Space Station construction and operation. Although the specification attempts to capture as much as possible of the actual SAFER design, certain pragmatically motivated deviations have been unavoidable. Nevertheless, the SAFER example contains elements typical of many space vehicles and the computerized systems needed to control them.

C.1 Overview of SAFER

SAFER is a small, self-contained, backpack propulsion system enabling free-flying mobility for a crewmember engaged in extravehicular activity (EVA) that has evolved as a streamlined version of NASA's earlier Manned Maneuvering Unit (MMU) [MMU83]. SAFER is a single-string system designed for contingency use only. SAFER offers sufficient propellant and control authority to stabilize and return a tumbling or separated crewmember, but lacks the propellant capacity and systems redundancy provided with the MMU. Nevertheless, SAFER and the MMU share an overall system concept, as well as general subsystem features. The description that follows draws heavily on the SAFER Operations Manual [SAFER94a] and on the SAFER Flight Text Project development specification [SAFER94b], excerpts of which have been included here as appropriate.

C.1.1 History, Mission Context, and System Description

SAFER is designed as a self-rescue device for a separated EVA crewmember in situations where the Shuttle Orbiter is unavailable to effect a rescue. Typical situations include whenever the Orbiter is docked to a large payload or structure, such as the Russian Mir Space Station or the International Space Station Alpha. A SAFER device would be worn

by every crewmember during these types of EVAs. As noted in [WB94], a crewmember engaged in EVA, who becomes separated from an Orbiter or a space station, has three basic options: grappling the Orbiter or station immediately using a "shepherd's crook" device, rescue by a second crewmember flying an MMU (Manned Maneuvering Unit)[1] or self-rescue using a propulsive system. The first option is not realistic in all situations; it assumes a near-optimal response by a tumbling astronaut. The second option is also unrealistic, in this case because it assumes constant availability of both the MMU and the second crewmember during all EVA, since reaction time is critical to successful rendezvous with a drifting crewmember. The third option, a propulsive self-rescue system, is the most viable and therefore the one ultimately selected.

As described in [WB93], the simplest self-rescue system is the Hand-Held Maneuvering Unit (HHMU) or "gas gun" flown on Gemini and Skylab, and the "Crew Propulsive Device," a redesign of the Gemini HHMU flown on the STS-49. Tests on these units indicated that the HHMUs were adequate for short translations, but required the crewmember to visually determine and effectively nullify tumble rates about all three axes – a challenging proposition even with good visual cues. As a result, recommendations based on the STS-49 tests included an automatic detumble capability for all self-rescue devices.

While the HHMU lacked automatic detumble and other capabilities necessary for a general-purpose self-rescue system, the MMU was too well-endowed. The MMU performed the first self-propelled untethered EVA during the STS-41B mission in 1984, participated in the Solar Maximum Mission spacecraft repair on a subsequent 1984 shuttle flight, and was used to capture the Palapa B-2 and the Westar-VI communications satellites on yet another shuttle flight that same year [WB94, p. 4]. However, the MMU's versatility, redundancy, and physical bulk made it unsuited as a general-purpose self-rescue device. Nevertheless, so many MMU features have been incorporated into SAFER (ranging from the hand controller grip design to the gaseous-nitrogen (GN_2) recharge-port quick-disconnect and the GN_2pressure regulator/relief valve), that SAFER has been described as a "mimimized derivative" of the MMU [WB94, p. 2].

SAFER fits around the Extravehicular Mobility Unit (EMU) primary life support subsystem (PLSS) backpack without limiting suit mobility (Figure C.1). SAFER uses 24 GN_2thrusters to achieve six degree-of-freedom maneuvering control. A single hand controller attached to the EMU display and control module is used to control SAFER operations. Propulsion is available either on demand, that is, in response to hand controller inputs, or through an automatic attitude hold (AAH) capability. Hand controller inputs can command either translations or rotations, while attitude hold is designed to bring and keep rotation rates close to zero. SAFER's propulsion system can be recharged during an EVA in the Orbiter payload bay. The SAFER unit weighs approximately 85 pounds and folds for launch, landing, and on-orbit stowage inside the Orbiter airlock.

[1] Or, similarly, by a robotic-controlled MMU. However, such a system has apparently not yet been developed and is not likely to be available in the near-term.

C.1.2 Principal Hardware Components

The SAFER flight unit consists of three assemblies: the backpack propulsion module, the hand controller module (HCM), and a replaceable battery pack. SAFER also requires several items of flight support equipment during a Shuttle mission. For the purpose of this discussion, only the propulsion and hand controller modules need be included.

C.1.2.1 Backpack Propulsion Module

The propulsion module is the primary assembly of the SAFER system, attaching directly to the EMU PLSS backpack. Figure C.2 shows the structures and mechanisms contained within the propulsion module. Four subassemblies are identified: main frame structure, left and right tower assemblies, and the avionics box. A lightweight, aluminum-alloy frame holds SAFER components, while external surfaces are formed by an outer aluminum skin. With the exception of the upper thrusters mounted to the tower assemblies, all propulsion subsystem components are housed in the main frame.

The tower assemblies have hinge joints that allow them to be folded for stowage. Towers are unfolded and attached to PLSS interfaces in preparation for an EVA. Latches on the towers hold SAFER firmly to the PLSS. Hinge joints accommodate GN_2 tubing, electrical power, and signal routing to the upper thrusters.

Housed in the avionics box are the control electronics assembly, inertial reference unit, data recorder assembly, and power supply assembly. The avionics box is attached to the bottom of the main frame, as depicted in Figure C.2. Data and power connectors provide an interface to the main frame. Connectors are also provided for the HCM umbilical and ground servicing equipment.

Within the main frame, high-pressure GN_2 is stored in four cylindrical stainless-steel tanks. Pressure and temperature sensors are placed directly adjacent to the tanks and these parameters are displayed to the SAFER crewmember on the HCM. Other components attached to the main GN_2 line are a manual isolation valve, a quick-disconnect recharge port, an integrated pressure regulator and relief valve, and downstream pressure and temperature sensors.

After passing through the regulator/relief valve, GN_2 is routed to four thruster manifolds, each containing six electric-solenoid thruster valves. A total of 24 thrusters is provided, with four thrusters pointing in each of the $\pm$X, $\pm$Y, and $\pm$Z directions. Thruster valves open when commanded by the avionics subsystem. When a valve opens, GN_2 is released and expanded through the thruster's conical nozzle to provide a propulsive force. The avionics subsystem can command as many as four thrusters at a time to provide motion with six degrees of freedom ($\pm$X, $\pm$Y, $\pm$Z, $\pm$roll, $\pm$pitch, and $\pm$yaw). Figure C.3 illustrates the thruster layout, designations, and directions of force.

C.1.2.2 Hand Controller Module (HCM)

A SAFER crewmember controls the flight unit and monitors its status by means of the hand controller module (HCM). Two distinct units are found in the HCM: a display

and control unit, and a hand controller unit. Both units are mounted together, as shown in Figure C.4, with an internal connector joining the two units electrically.

Various displays and switches are located on the display and control unit and positioned so that they can be viewed from any head position within the EMU helmet. These displays and switches include

1. **Liquid crystal display.** A 16-character, backlit LCD displays prompts, status information, and fault messages to the crewmember.

2. **Thruster cue light.** A red LED lights whenever a thruster-on condition is detected by the control software. This light is labeled "THR."

3. **Automatic attitude hold light.** A green LED labeled "AAH" lights whenever attitude hold is enabled for one or more rotational axes.

4. **Power/test switch.** A three-position toggle switch labeled "PWR" is used to power on the flight unit and initiate self-test functions. The three positions are "OFF," "ON," and "TST."

5. **Display proceed switch.** A three-position, momentary-contact toggle switch is used to control message displays on the LCD. This switch, which is labeled "DISP" on the HCM, is normally in the center null position. When pushed up/down, the switch causes the LCD to display the previous/next parameter or message.

6. **Control mode switch.** A two-position toggle switch is used to configure the hand controller for either rotational or translational commands. This switch is labeled "MODE," with its two positions labeled "ROT" and "TRAN."

The hand controller grip is compatible with an EMU glove. It is mounted on the right side of the HCM with an integral push-button switch for initiating and terminating AAH mode. A four-axis mechanism having three rotary axes and one transverse axis is the heart of the hand controller. A command is generated by moving the grip from the center null position to mechanical hardstops on the hand controller axes. Commands are terminated by deliberately returning the grip to its center position or by releasing the grip so that it automatically springs back to the center.

As shown in Figure C.5, with the control mode switch in the TRAN position, $\pm$X, $\pm$Y, $\pm$Z, and $\pm$pitch commands are available. $\pm$X commands are generated by rotating the grip forward or backward, $\pm$Y commands by pulling or pushing the grip right or left, and $\pm$Z commands by rotating the grip down or up. $\pm$pitch commands are generated by twisting the grip up or down about the hand controller transverse axis.

As shown in Figure C.6, with the control mode switch in the ROT position, $\pm$roll, $\pm$pitch, $\pm$yaw, and $\pm$X commands are available. $\pm$roll commands are generated by rotating the grip down or up (same motion as the $\pm$Z commands in TRAN mode). $\pm$yaw commands are generated by pulling or pushing the grip right or left (same motion

as the ±Y commands in TRAN mode). The ±pitch and ±X commands are generated as in TRAN mode, thus making them available in both TRAN and ROT modes.

An electrical umbilical connects the HCM to the propulsion module, attaching to a connector on the avionics box. This umbilical is connected prior to launch and is not intended to be disconnected in flight.

C.1.2.3 Battery Pack

The battery pack, which provides power for all SAFER electrical components, connects to the bottom of the propulsion module, as shown in Figure C.2. Two separate battery circuits are found in the battery pack, both containing multiple stacks of 9-volt alkaline batteries. One battery circuit powers the thruster valves, offering 30–57 volts to the power supply assembly, which produces a 28-volt output for opening valves in pulses of 4.5 milliseconds duration. Energy capacity is sufficient to open the thrusters 1200 times and thereby drain the GN_2 tanks four times. The other battery circuit powers the avionics subsystem (i.e., the remaining electrical components), producing 16–38 volts for the power supply for a cumulative power-on time of 45 minutes. A temperature sensor in the battery pack is used for monitoring purposes. Flight procedures allow for battery pack changing during an EVA.

C.1.2.4 Flight Support Equipment

Besides the SAFER flight unit, several types of flight support equipment are needed during SAFER operations. These items include a special plug to attach the hand controller module to the EMU display and control module, a recharge hose for GN_2 tank recharging during an EVA, the Orbiter's GN_2 system to provide GN_2 via the recharge hose, a SAFER recharge station having handrails and foot restraints to facilitate the recharging procedure, an airlock stowage bag for storing SAFER when not in use, and a battery transfer bag for storing extra battery packs during an EVA. None of these support items will be considered any further in this appendix.

C.1.3 Avionics

SAFER's avionics subsystem resides mostly in the backpack module beneath the propulsion components. Included are the following assemblies:

1. **Control Electronics Assembly (CEA).** Found in the avionics box, the CEA contains a microprocessor that takes inputs from sensors and hand controller switches, and actuates the appropriate thruster valves. The CEA has a serial bus interface for the HCM umbilical as well as an interface for ground support equipment.

2. **Inertial Reference Unit (IRU).** Central to the attitude hold function, the IRU senses angular rates and linear accelerations. Three quartz rate sensors, rate

noise filters, and associated rate measurement electronics provide angular rate sensing up to ±30 degrees per second. A separate sensor exists for each angular axis (roll, pitch, yaw). In addition, a temperature sensor is paired with each of the three rate sensors, enabling the avionics software to reduce rate sensor error caused by temperature changes. An accelerometer senses linear acceleration up to ±1 g along each linear axis (X, Y, Z). These accelerations are recorded by the data recorder assembly for post-flight analysis.

3. **Data Recorder Assembly (DRA).** SAFER flight performance data is collected by the DRA. Saved parameters include data from rate sensors, accelerometers, pressure and temperature transducers, and battery voltage sensors. The DRA also records hand controller and AAH commands and thruster firings. Data may be recorded at one of three rates: 1 Hz, 50 Hz, or 250 Hz. A suitable rate is chosen automatically based on which control mode is in use.

4. **Valve Drive Assemblies (VDAs).** Four valve drive assemblies are used to actuate the GN_2 thrusters. A VDA is located with each cluster of six thrusters (in each tower and on the left and right sides of the propulsion module main frame). VDAs accept firing commands from the CEA and apply voltages to the selected valves. VDAs also sense current flow through the thruster solenoids, providing a discrete signal to the CEA acknowledging thruster firing.

5. **Power Supply Assembly (PSA).** Regulated electrical power for all SAFER electrical components is produced by the PSA. Two battery circuits provide input power, and the PSA serves as a single-point ground for all digital and analog signal returns.

6. **Instrumentation Electronics.** A variety of sensors is included in the SAFER instrumentation electronics. A subset of the sensed parameters is available for display by the crewmember. Table C.1 lists all the SAFER sensors.

C.1.4 System Software

The avionics software is responsible for controlling the SAFER unit in response to crewmember commands. Two principal subsystems comprise the system software: the maneuvering control subsystem and the fault detection subsystem. Maneuvering control includes both commanded accelerations and automatic attitude hold actions. Fault detection supports in-flight operation, pre-EVA checkout, and ground checkout.

C.1.4.1 Software Interfaces

Digital interfaces to SAFER components enable the CEA's microprocessor to achieve control. Four classes of inputs are monitored and accepted by the avionics software:

Parameter measured	Sensor type	Displayed?
GN_2 tank pressure	Pressure	Y
GN_2 tank temperature	Temperature	Y
GN_2 regulator pressure	Pressure	Y
GN_2 regulator temperature	Temperature	Y
Roll rate	Angular rate	Y
Pitch rate	Angular rate	Y
Yaw rate	Angular rate	Y
Electronics battery volts	Voltage	Y
Valve drive battery volts	Voltage	Y
Battery temperature	Temperature	Y
X acceleration	Linear acceleration	N
Y acceleration	Linear acceleration	N
Z acceleration	Linear acceleration	N
Roll rate sensor temperature	Temperature	N
Pitch rate sensor temperature	Temperature	N
Yaw rate sensor temperature	Temperature	N

Table C.1: SAFER sensor complement.

1. **Hand controller switches.** Indications of switch operation cover both toggle switches and those embedded within the hand grip mechanism.

2. **Avionics transducers.** Sensor inputs are converted from analog to digital form before software sampling.

3. **Thruster-on discrete.** This input is a binary indication of at least one thruster valve being open.

4. **Serial line.** Ground checkout operations send data through this input.

Similarly, four classes of outputs are generated by the avionics software:

1. **Hand controller displays.** Both LEDs and a 16-character LCD display are included to present status to the crewmember.

2. **Thruster system.** Digital outputs are delivered to the valve drive assemblies to actuate individual thruster valves.

3. **Data recorder system.** Selected data items are recorded for post-flight analysis on the ground.

4. **Serial line.** Ground checkout operations receive data through this output.

C.1.4.2 Maneuvering Control Subsystem

Figure C.7 breaks down the SAFER software architecture in terms of its primary modules. Those modules comprising the maneuvering control subsystem collectively realize SAFER's six degree-of-freedom propulsion capability. Both rotational and translational accelerations will be commanded by the software. Rotations resulting from the AAH function are invoked automatically by the software in response to rotation rates sensed by the inertial reference unit. Special cases result from the interaction of the AAH function and explicitly commanded accelerations.

Translation commands from the crewmember are prioritized so that only one translational axis receives acceleration, with the priority order being X, Y, and then Z. Whenever possible, acceleration is provided as long as a hand controller or AAH command is present. If both translation and rotation commands are present simultaneously, rotation takes priority and translations will be suppressed. Conflicting input commands result in no output to the thrusters.

The SAFER crewmember can initiate AAH at any time by depressing or "clicking" the pushbutton on the hand controller grip. Whenever AAH is active in any axis the green LED on the HCM illuminates. When the button is double clicked (two clicks within a 0.5 second interval), AAH is disabled for all three rotational axes. If AAH is active, and the crewmember issues a rotational acceleration command about any axis, AAH is immediately disabled on that axis. When this occurs, the remaining axes remain in AAH. On the other hand, if AAH is initiated simultaneously with a rotational command from the hand controller, the rotational command will be ignored and AAH will become active in that axis. This feature is necessary so that a failed-on HCM rotational command cannot permanently disable AAH on the affected axis.

AAH implements an automatic rotational deceleration sufficient to reduce axis rates to near-zero levels. Continuous thruster firings are commanded to reduce rotation about an axis whenever its rate is sensed to be above 0.2 degree per second. Once the rates have fallen below 0.3 degree per second, thrusters are fired only as needed to maintain attitude within approximately ± 5 degrees. Thrusters are not fired when attitude is within a ± 2 degree deadband.

Rate sensors, rate noise filters, and associated rate measurement electronics exhibit significant offset errors, which are largely a function of rate sensor temperature. Offset reduction is used to minimize the negative effects of rate offset errors. Temperature measurements are periodically sampled and net offset errors estimated. Such estimates are subtracted from the noise filter rate measurements to minimize rate offset errors. Net offset errors are independent for each axis, reaching an average of 0.2 degree per second and resulting in an average drift of the same magnitude.

Acceleration commands from the hand controller and from the AAH function are combined to create a single acceleration command. Thruster select logic is provided to choose suitable thruster firings to achieve the commanded acceleration. Thruster selection results in on-off commands for each thruster, with a maximum of four thrusters turned on simultaneously. Thruster arrangement and designations are shown in Fig-

ure C.3, while Tables C.2 and C.3 specify the selection logic. These tables are specified in terms of three possible command values for each axis: negative thrust, positive thrust, or no thrust at all.

C.1.4.3 Fault Detection Subsystem

The fault detection subsystem performs four testing functions: a self test, an activation test, a monitoring function, and a ground checkout function. The fault detection subsystem also manages the display interface, performing the computation of parameters and construction of messages for the HCM LCD.

The self test provides an overall functional test of the SAFER flight unit without using any propellant or external equipment. To carry out the test, the crewmember is led through a checklist of prompts displayed on the HCM LCD. If a particular test is unsuccessful, a failure message is displayed. The following tests are performed during self test:

1. Thruster test
2. Hand controller controls and display test
3. Rate sensor function test

The activation test checks the functionality of the SAFER flight unit in an operational mode, being invoked to check the function of the pressure regulator. A minimal amount of propellant is used and no external equipment is required. The test consists of commanding 20 millisecond thruster pulses in translational and rotational axis directions, with opposing thrusters fired as well so no net acceleration results.

A continuous fault check of the SAFER subsystems is performed by the monitoring function, comprising the following tests:

1. Leak monitoring
2. Battery voltage checks
3. Tank pressure and temperature checks
4. Regulator pressure and temperature checks
5. Battery pack temperature check

Status information resulting from continuous monitoring is displayed on the HCM LCD during SAFER flight. The following items are displayed in order:

1. Default display, showing GN_2 and power percent remaining
2. Pressure and temperature
3. Rotation rate

X	Pitch	Yaw	Always turned on	On if no roll command
−	−	−	B4	B2 B3
−	−		B3 B4	
−	−	+	B3	B1 B4
−		−	B2 B4	
−			B1 B4	B2 B3
−		+	B1 B3	
−	+	−	B2	B1 B4
−	+		B1 B2	
−	+	+	B1	B2 B3
	−	−	B4 F1	
	−		B4 F2	
	−	+	B3 F2	
		−	B2 F1	
		+	B3 F4	
	+	−	B2 F3	
	+		B1 F3	
	+	+	B1 F4	
+	−	−	F1	F2 F3
+	−		F1 F2	
+	−	+	F2	F1 F4
+		−	F1 F3	
+			F2 F3	F1 F4
+		+	F2 F4	
+	+	−	F3	F1 F4
+	+		F3 F4	
+	+	+	F4	F2 F3

Table C.2: Thruster select logic for X, pitch, and yaw commands.

Y	Z	Roll		Always turned on	On if no pitch or yaw
−	−	−	NA		
−	−		NA		
−	−	+	NA		
−		−		L1R	L1F L3F
−				L1R L3R	L1F L3F
−		+		L3R	L1F L3F
−	+	−	NA		
−	+		NA		
−	+	+	NA		
	−	−		U3R	U3F U4F
	−			U3R U4R	U3F U4F
	−	+		U4R	U3F U4F
		−		L1R R4R	
		+		R2R L3R	
	+	−		D2R	D1F D2F
	+			D1R D2R	D1F D2F
	+	+		D1R	D1F D2F
+	−	−	NA		
+	−		NA		
+	−	+	NA		
+		−		R4R	R2F R4F
+				R2R R4R	R2F R4F
+		+		R2R	R2F R4F
+	+	−	NA		
+	+		NA		
+	+	+	NA		

Table C.3: Thruster select logic for Y, Z, and roll commands.

4. Angular displacement
5. Battery voltage
6. High rate recorder status
7. Message display (error queue)

The fault detection system also provides for ground checkout of the SAFER flight unit. This function processes commands for data requests or avionics tests from ground support equipment connected to the CEA's ground servicing serial port.

C.2 SAFER EVA Flight Operation Requirements

The full SAFER system has requirements that cover flight operations as well as support procedures such as pre-EVA checkout, propellant recharging, and battery pack changing. Our SAFER example focuses on a subset of the full requirements, namely, those covering flight operations during an EVA. Furthermore, several requirements are incorporated in modified form to better suit the purposes of the example. The most significant change is that the controller samples switches and sensors on every frame rather than accepting change notifications via a serial line interface. This leads to the conceptually simpler architecture of a pure sampled-data control system.

C.2.1 Hand Controller Module (HCM)

The HCM provides the controls and displays for the SAFER crewmember to operate SAFER and to monitor status.

(1) The HCM shall comprise two units, the Hand Controller Unit (HCU) and the Display and Control Unit (DCU).

(2) The HCM shall provide the controls and displays for the SAFER crewmember to operate SAFER and to monitor status.

C.2.1.1 Display and Control Unit (DCU)

The DCU provides displays to the crew and switches for crew commands to power the SAFER, to select modes, and to select displays.

(3) The DCU shall provide a red LED and shall illuminate it whenever an electrical on-command is applied to any one of the SAFER thrusters.

(4) The DCU shall provide a green LED and shall illuminate it whenever automatic attitude hold (AAH) is enabled for one or more SAFER rotational axes.

(5) The DCU shall provide a 16-character, backlit liquid crystal display (LCD).

(6) The DCU shall display SAFER instructions and status information to the SAFER crewmember on the LCD.

(7) The DCU shall provide a three-position toggle switch to power the SAFER unit on and to control the SAFER test functions.

(8) The power toggle switch shall be oriented towards the crewmember for "TST," in the center position for "ON," and away for "OFF."

(9) The DCU shall provide a three-position, momentary toggle switch to control the LCD display.

(10) The display toggle switch shall remain in the center position when not being used and shall be oriented so that positioning the switch towards or away from the crewmember will control the LCD menu selection.

(11) The DCU shall provide a two-position toggle switch to be used to direct hand controller commands for either full rotation or full translation control mode.

(12) The mode select toggle switch shall be positioned to the crewmember's left for the Rotation Mode and to the crewmember's right for the Translation Mode.

C.2.1.2 Hand Controller Unit (HCU)

The HCU provides those functions associated with the hand controller and the automatic attitude hold (AAH) pushbutton switch.

(13) The HCU shall provide a four-axis hand controller having three rotary axes and one transverse axis, operated by a side-mounted hand grip as depicted in Figure C.4.

(14) The HCU shall indicate primary control motions when the grip is deflected from the center or null position to mechanical hard-stops.

(15) The grip deflections shall result in six degree-of-freedom commands related to control axes as depicted in Figures C.5 and C.6.

(16) The HCU shall terminate commands when the grip is returned to the null position.

(17) The HCU shall provide a pushbutton switch to activate and deactivate AAH.

(18) The pushbutton switch shall activate AAH when depressed a single time.

(19) The pushbutton switch shall deactivate AAH when pushed twice within 0.5 second.

C.2.2 Propulsion Subsystem

SAFER thrusters are actuated by the control electronics assembly (CEA) using the valve drive assemblies (VDAs).

(20) The propulsion subsystem shall provide 24 gaseous nitrogen (GN_2) thrusters arranged as shown in Figure C.3.

(21) The VDAs shall accept thruster firing commands from the CEA and apply appropriate voltages to the selected thrusters.

(22) The VDAs shall have the capability of sensing current flow through the thruster solenoids and providing discrete signals to the CEA indicating such an event.

(23) The propulsion subsystem shall provide two transducers to monitor tank pressure and regulator outlet pressure.

(24) The propulsion subsystem shall provide two temperature sensors to measure tank temperature and regulator outlet temperature.

C.2.3 Avionics Assemblies

The avionics subsystem includes several assemblies housed within the backpack propulsion module, each having a digital interface to the CEA.

C.2.3.1 Inertial Reference Unit (IRU)

(25) The IRU shall provide angular rate sensors and associated electronics to measure rotation rates in each angular axis (roll, pitch, yaw).

(26) The IRU shall provide a temperature sensor for each angular rate sensor to allow temperature-based compensation.

(27) The IRU shall provide accelerometers to measure linear accelerations in each translation axis (X, Y, Z).

C.2.3.2 Power Supply Assembly (PSA)

(28) The power supply shall provide a voltage sensor to measure the valve drive battery voltage.

(29) The power supply shall provide a voltage sensor to measure the electronics battery voltage.

(30) The power supply shall provide a temperature sensor to measure battery pack temperature.

C.2.3.3 Data Recorder Assembly (DRA)

(31) The DRA shall accept performance data and system parameters from the CEA for storage and post-flight analysis.

(32) The DRA shall write formatted data on nonvolatile memory devices.

C.2.4 Avionics Software

Executing on a microprocessor within the control electronics assembly (CEA), the SAFER avionics software provides the capability to control SAFER flight maneuvers, to check out functionality and detect faults in SAFER, and to display SAFER fault conditions and general health and consumable status.

(33) The avionics software shall reference all commands and maneuvers to the coordinate system defined in Figure C.3.

(34) The avionics software shall provide a six degree-of-freedom maneuvering control capability in response to crewmember-initiated commands from the hand controller module.

(35) The avionics software shall allow a crewmember with a single command to cause the measured SAFER rotation rates to be reduced to less than 0.3 degree per second in each of the three rotational axes.

(36) The avionics software shall attempt to maintain the calculated attitude within ± 5 degrees of the attitude at the time the measured rates were reduced to the 0.3 degree per second limit.

(37) The avionics software shall disable AAH on an axis if a crewmember rotation command is issued for that axis while AAH is active.

(38) Any hand controller rotation command present at the time AAH is initiated shall subsequently be ignored until a return to the off condition is detected for that axis or until AAH is disabled.

(39) Hand controller rotation commands shall suppress any translation commands that are present, but AAH-generated rotation commands may coexist with translations.

(40) At most one translation command shall be acted upon, with the axis chosen in priority order X, Y, Z.

(41) The avionics software shall provide accelerations with a maximum of four simultaneous thruster firing commands.

(42) The avionics software shall select thrusters in response to integrated AAH and crew-generated commands according to Tables C.2 and C.3.

(43) The avionics software shall provide flight control for AAH using the IRU-measured rotation rates and rate sensor temperatures.

(44) The avionics software shall provide fault detection for propulsion subsystem leakage in excess of 0.3% of GN_2 mass per second while thrusters are not firing.

(45) The avionics software shall provide limit checks for battery temperature and voltages, propulsion tank pressure and temperature, and regulator pressure and temperature.

C.2.5 Avionics Software Interfaces

The avionics software accepts input data from SAFER components by sampling the state of switches and digitized sensor readings. Outputs provided by the avionics software to SAFER components are transmitted in a device-specific manner.

(46) The avionics software shall accept the following data from the hand controller module:

- + pitch, – pitch
- + X, – X
- + yaw or + Y, – yaw or – Y
- + roll or + Z, – roll or – Z
- Power/test switch
- Mode switch
- Display proceed switch
- AAH pushbutton

(47) The avionics software shall accept the following data from the propulsion subsystem:

- Tank pressure and temperature
- Regulator pressure and temperature
- Thruster-on signal

(48) The avionics software shall accept the following data from the inertial reference unit:

- Roll, pitch, and yaw rotation rates
- Roll, pitch, and yaw sensor temperatures
- X, Y, and Z linear accelerations

(49) The avionics software shall accept the following data from the power supply:

- Valve drive battery voltage
- Electronics battery voltage
- Battery pack temperature

(50) The avionics software shall provide the following data to the HCM for display:

- Pressure, temperature, and voltage measurements
- Alert indications
- Rotation rates and displacements
- Crew prompts
- Failure messages
- Miscellaneous status messages

(51) The avionics software shall provide the following data to the valve drive assemblies for each of the 24 thrusters:

- Thruster on/off indications

(52) The avionics software shall provide the following data to the data recorder assembly:

- IRU-sensed rotation rates
- IRU-sensed linear accelerations
- IRU rate sensor temperatures
- Angular displacements
- AAH command status

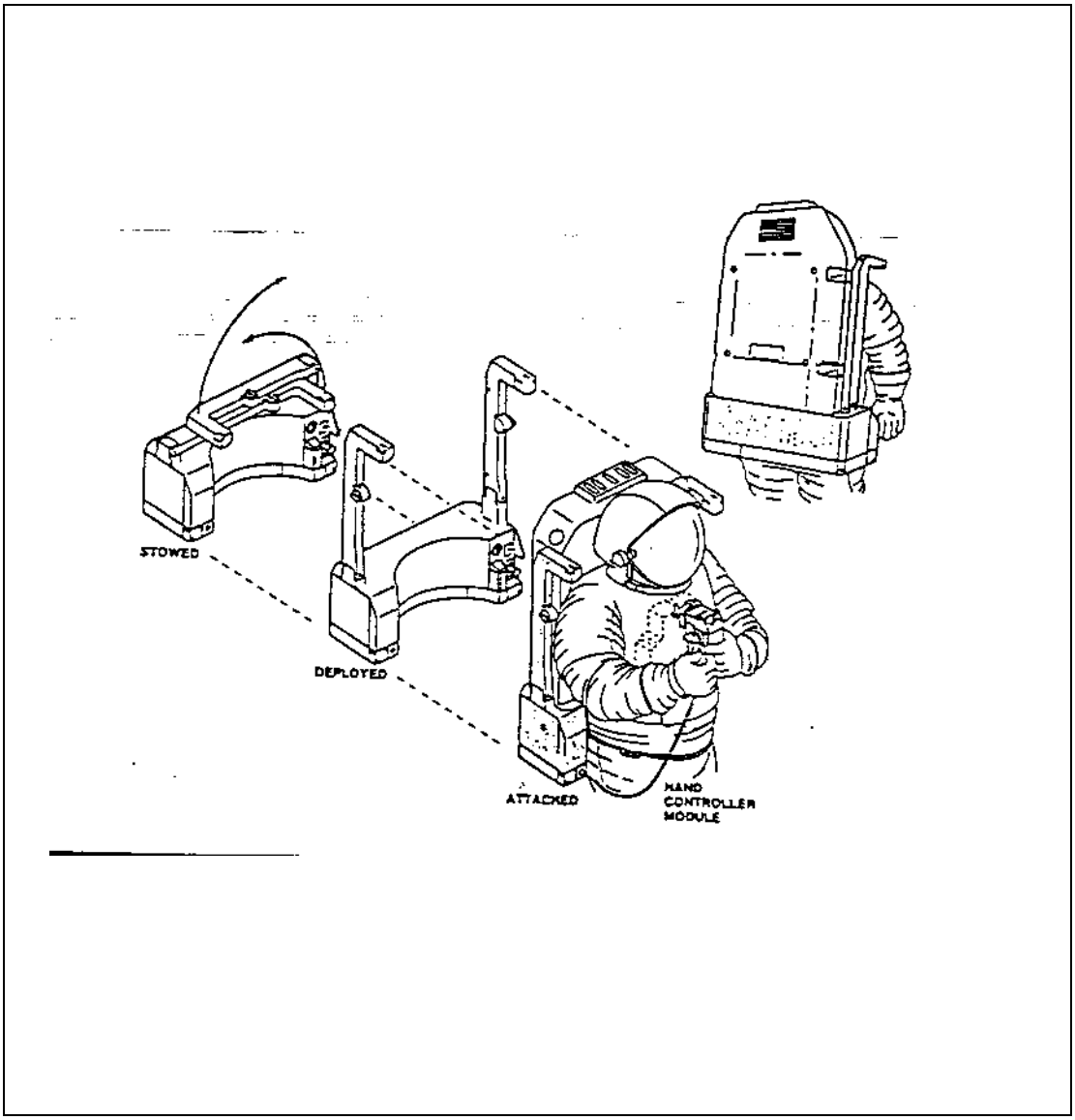

Figure C.1: SAFER use by an EVA crewmember.

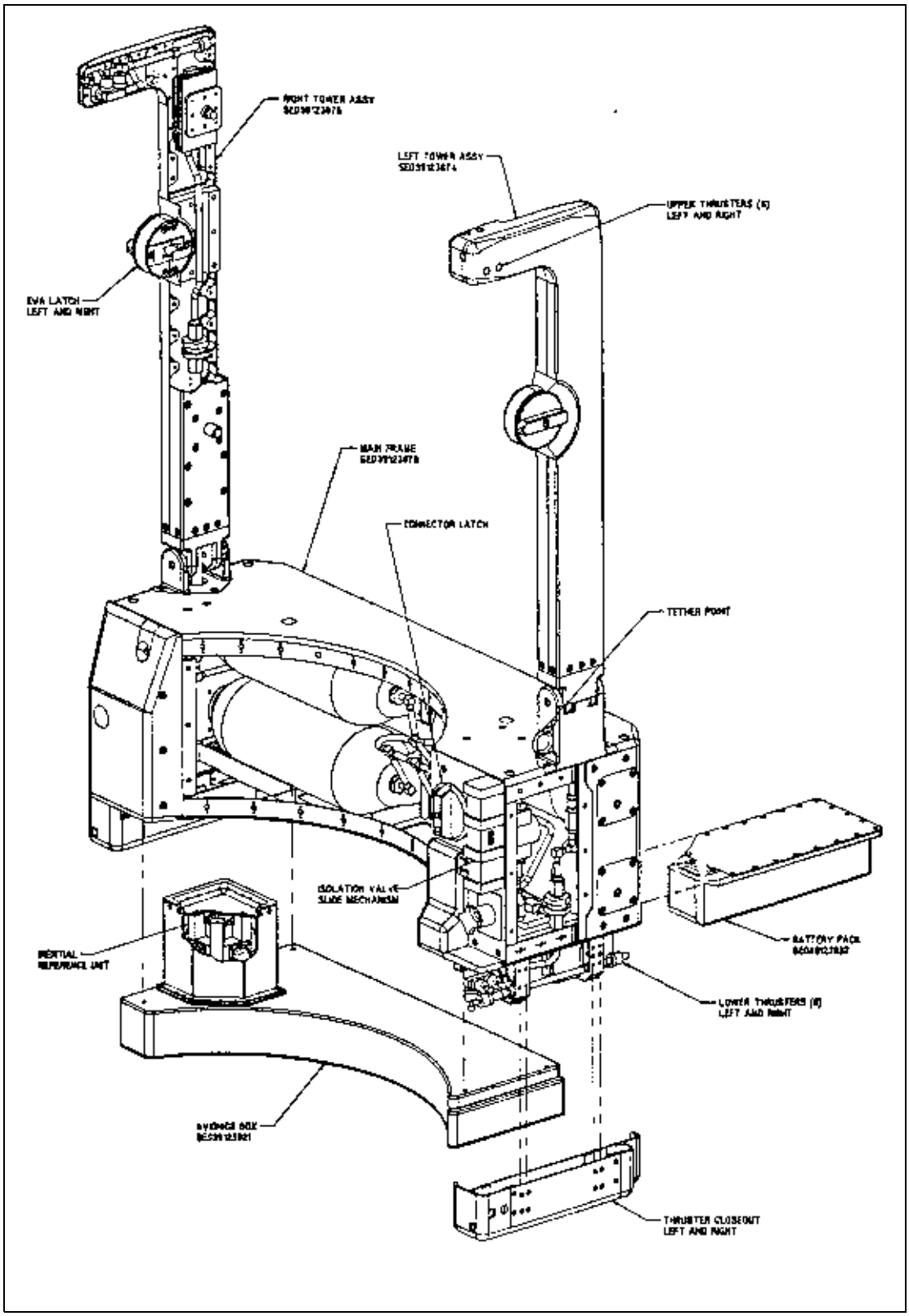

Figure C.2: Propulsion module structure and mechanisms.

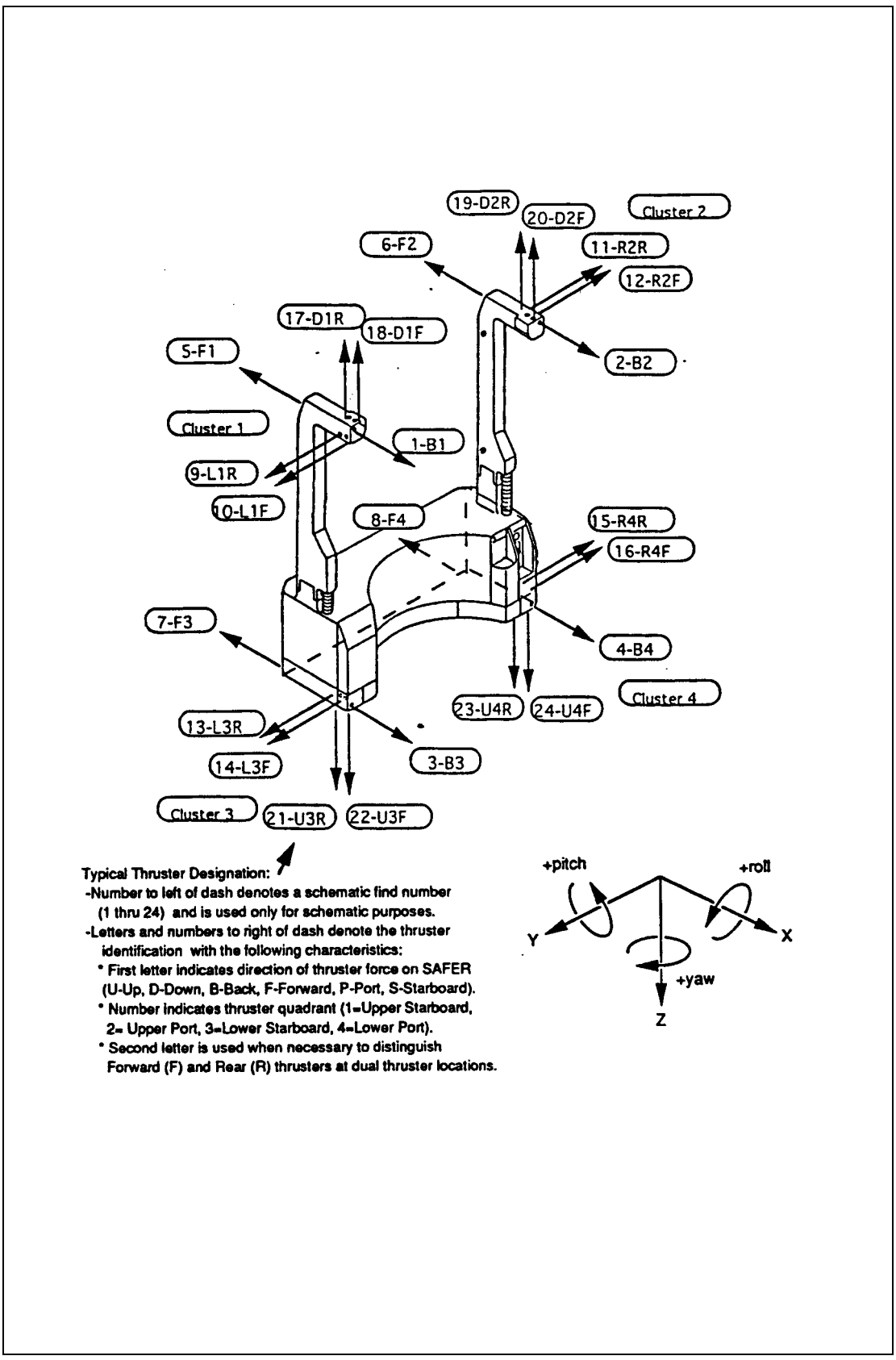

Figure C.3: SAFER thrusters and axes.

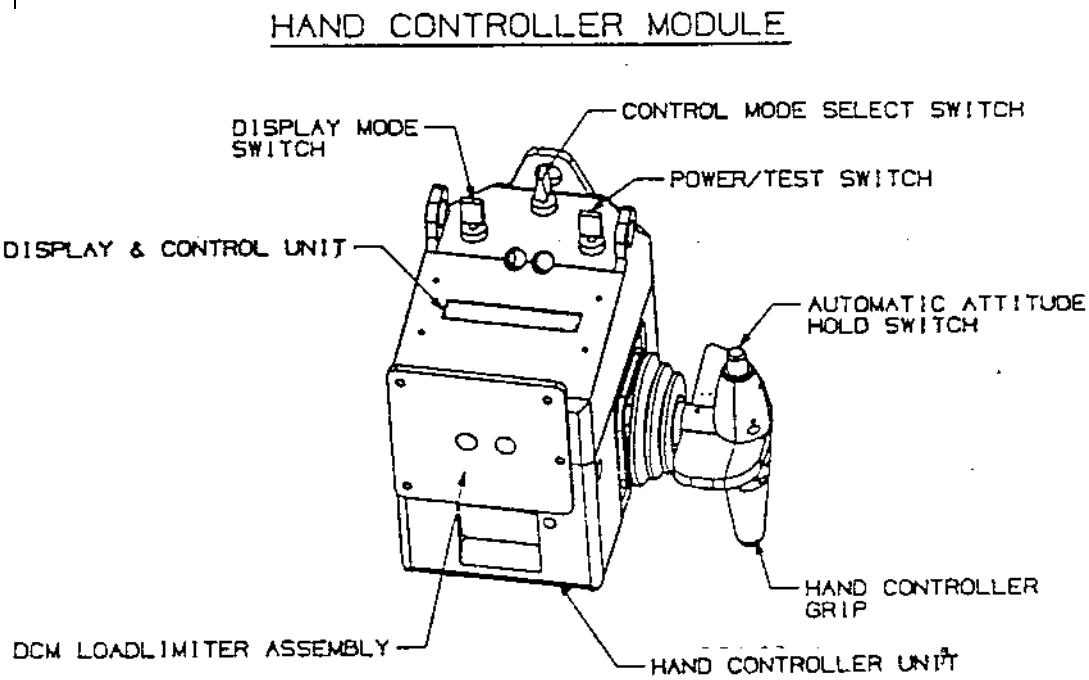

Figure C.4: Hand controller module.

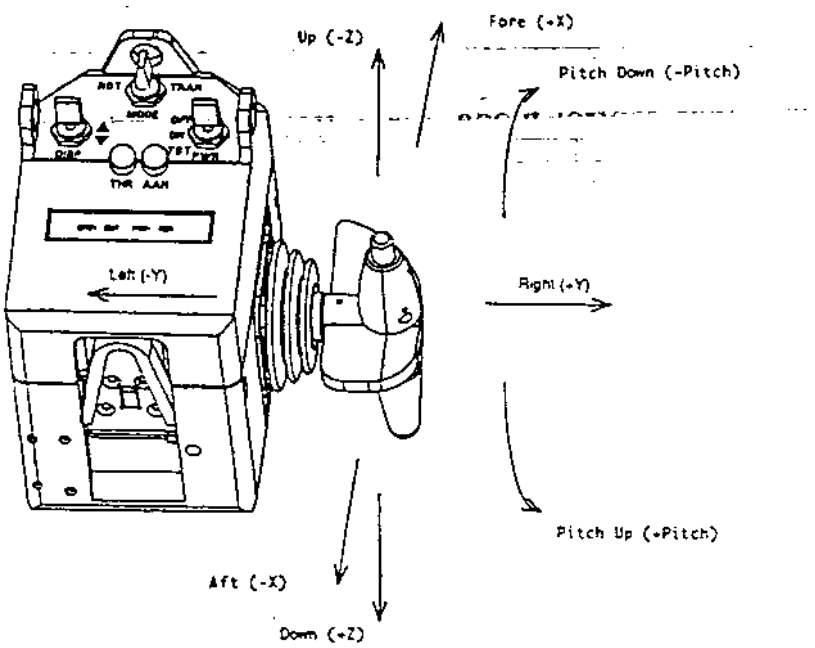

Figure C.5: Hand controller translational axes.

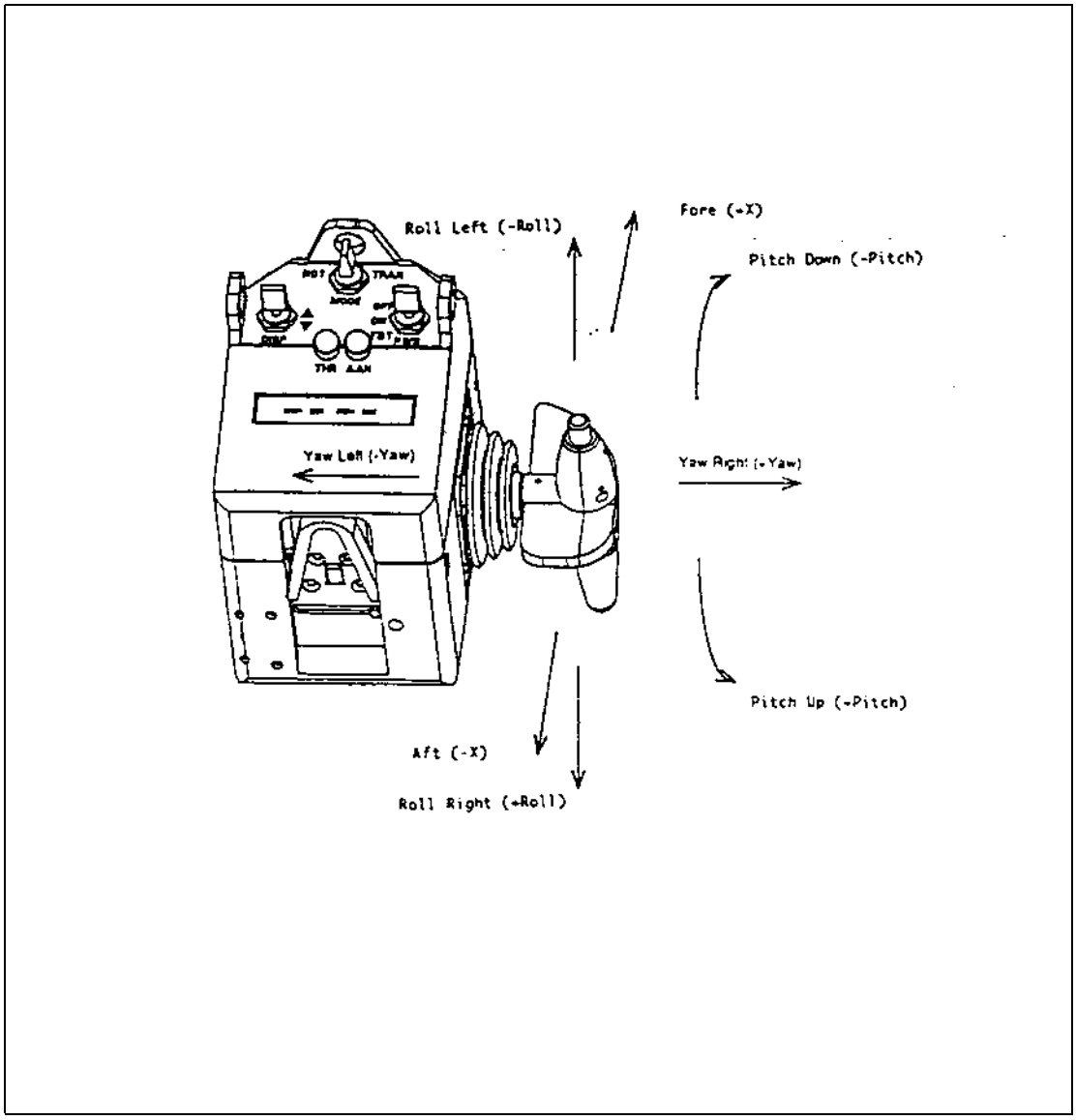

Figure C.6: Hand controller rotational axes.

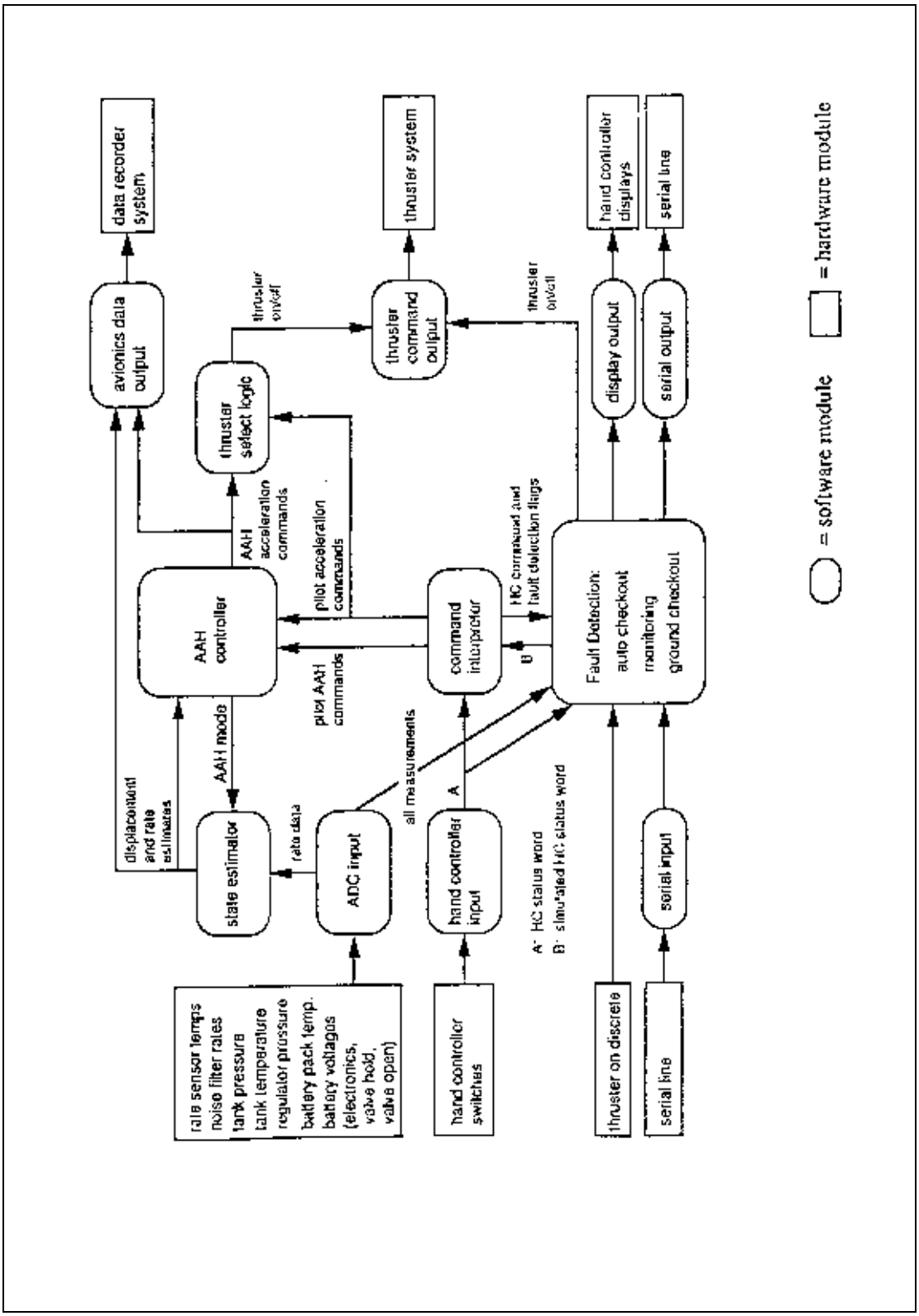

Figure C.7: SAFER system software architecture.

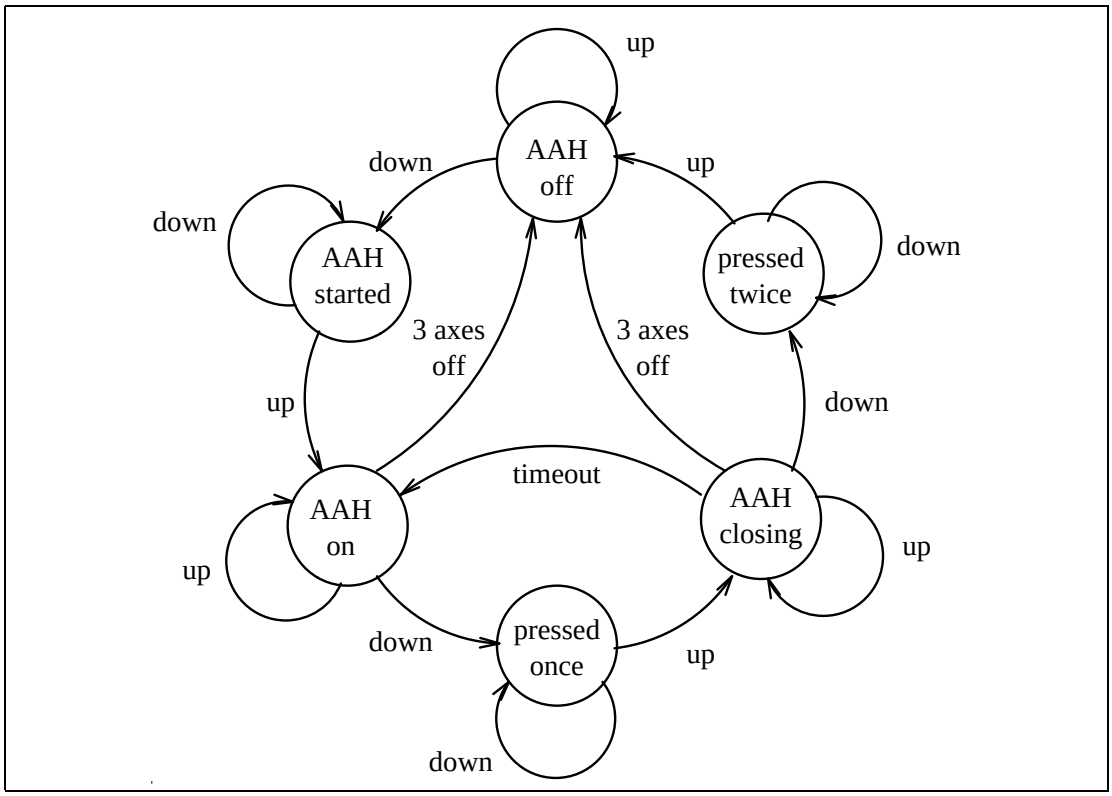

Figure C.8: AAH pushbutton state diagram.