Space Vehicle Powerdown Philosophies Derived from the Space Shuttle Program

Mark Willsey and Brad Bailey
NASA Johnson Space Center
Houston, TX
mark.w.willsey@nasa.gov
brad.r.bailey@nasa.gov

ABSTRACT

In spaceflight, electrical power is a vital but limited resource. Almost every spacecraft system, from avionics to life support systems, relies on electrical power. Since power can be limited by the generation system's performance, available consumables, solar array shading, or heat rejection capability, vehicle power management is a critical consideration in spacecraft design, mission planning, and real-time operations.

The purpose of this paper is to capture the powerdown philosophies used during the Space Shuttle Program. This paper will discuss how electrical equipment is managed real-time to adjust the overall vehicle power level to ensure that systems and consumables will support changing mission objectives, as well as how electrical equipment is managed following system anomalies. The focus will be on the power-related impacts of anomalies in the generation systems, air and liquid cooling systems, and significant environmental events such as a fire, decrease in cabin pressure, or micrometeoroid debris strike.

The evolution of the powerdown procedures will also be examined. Deactivating electrical equipment not only changes vehicle electrical and thermal loads, but also affects vehicle operability and fault tolerance across many systems and may require crew actions. Designing a powerdown procedure is an iterative interdisciplinary process involving analysis engineers, flight control teams, and Space Shuttle crews. The original powerdown procedures were written before the first Shuttle flight, and as the crew size increased, missions became longer, Orbiter equipment was upgraded, and flight data became available to update or verify electrical and thermal models, the powerdown procedures were continuously revisited.

Finally, considerations for executing powerdowns by crew action or by ground commands from Mission Control will be presented, and general lessons learned from 30 years of Space Shuttle powerdowns will be discussed, including an in depth case-study of STS-117. During this International Space Station (ISS) assembly mission, a failure of computers controlling the ISS guidance, navigation, and control system required that the Space Shuttle's maneuvering system be used to maintain attitude control. A powerdown was performed to save power generation consumables, thus extending the docked mission duration and allowing more time to resolve the issue.

Space Vehicle Powerdown Philosophies Derived from the Space Shuttle Program

Mark W. Willsey* and Brad Bailey†
NASA Johnson Space Center, Houston, Texas, 77058

This paper will focus on how powerdowns are used to manage electrical equipment in real-time to ensure that consumables support changing mission objectives and duration, as well as how electrical equipment is managed following system anomalies to safe or prevent a system failure. This paper will also provide general lessons-learned, an in depth case study of the powerdown used on STS-117, and will present the pros and cons of the two different methods of executing a powerdown, crew action and ground commands from Mission Control.

Nomenclature

ABS = Ammonia Boiler System
AC = Alternating Current
ARS = Air Revitalization System
CMG = Control Moment Gyros
DC = Direct Current
ECLS = Environmental Control and Life Support
EECOM = Electrical, Environmental, and Communications
EGIL = Electrical Generation and Illumination
EPDC = Electrical Power Distribution and Control
EPS = Electrical Power Systems
FC = Fuel Cell
FCL = Freon Coolant Loops
FES = Flash Evaporator System
GNC = Guidance, Navigation, and Control
GSE = Ground Support Equipment
ISS = International Space Station
LCVG = Liquid-Cooled Ventilation Garments
MADS = Modular Auxiliary Data System
MCC = Mission Control Center
MDM = Multiplexer/Demultiplexer
MET = Mission Elapsed Time
MMOD = Micrometeorite Orbital Debris
MOD = Mission Operations Directorate
OCAC = Orbiter Cabin Air Cleaner
OPCL = Orbit Pocket Checklist
PRSD = Power Reactant Storage and Distribution
QDM = Quick Don Mask
SMCC = Service Module Central Computers
SMTC = Service Module Terminal Computers
STS = Space Transportation System
UHF = Ultra High Frequency
WCL = Water Coolant Loops

* Space Shuttle Flight Controller, Electrical Systems, 2101 NASA Parkway ATTN: DS43.
† Space Shuttle Flight Controller, Environmental Systems, 2101 NASA Parkway ATTN: DS44.

I. Introduction

IN spaceflight, electrical power is a vital but limited resource. Almost every spacecraft system, from avionics to life support systems, relies on electrical power. Since power can be limited by the generation system's performance, available consumables, solar array shading, or heat rejection capability, vehicle power management is a critical consideration in spacecraft design, mission planning, and real-time operations.

The purpose of this paper is to capture the powerdown philosophies used during the Space Shuttle Program. This paper will discuss how electrical equipment is managed real-time to adjust the overall vehicle power level to ensure that systems and consumables will support changing mission objectives, as well as how electrical equipment is managed following system anomalies. The focus will be on the power-related impacts of anomalies in the generation systems, air and liquid cooling systems, and significant environmental events such as a fire or a decrease in cabin pressure.

The evolution of the powerdown procedures will also be examined. Deactivating electrical equipment not only changes vehicle electrical and thermal loads, but also affects vehicle operability and fault tolerance across many systems and may require crew actions. Designing a powerdown procedure is an iterative, interdisciplinary process involving analysis engineers, flight control teams, and Space Shuttle crews. The original powerdown procedures were written before the first Shuttle flight, and as the crew size increased, missions became longer, Orbiter equipment was upgraded, and flight data became available to update or verify electrical and thermal models, the powerdown procedures were continuously revisited.

Finally, considerations for executing powerdowns by crew action or by ground commands from Mission Control will be presented, and general lessons learned from 30 years of Space Shuttle powerdowns will be discussed, including an in depth case-study of STS-117. During this International Space Station (ISS) assembly mission, a failure of computers controlling part of the ISS guidance, navigation, and control system required that the Space Shuttle's maneuvering system be used for attitude control. A powerdown was performed to save power generation consumables, thus extending the docked mission duration and allowing more time to resolve the issue.

II. Space Shuttle Systems Overview

Before describing the details of the powerdown philosophies of the Space Shuttle, it is important to have a basic understanding of the related Shuttle systems. Section II will provide this overview.

A. Electrical Power System (EPS) Overview

The Shuttle's Electrical Power System (EPS) is responsible for energy storage, power production, and power distribution to the entire Space Shuttle. The EPS is composed of three major subsystems which are shown in Fig. 1 and described below.

1. Power Reactant Storage and Distribution (PRSD)

The PRSD subsystem is responsible for energy storage. Cryogenic hydrogen and oxygen are stored in tanks and distributed to the three fuel cells to generate electrical power. Additionally, the PRSD subsystem distributes oxygen to the Environmental Control and Life Support System (ECLSS) to be used for crew breathing.

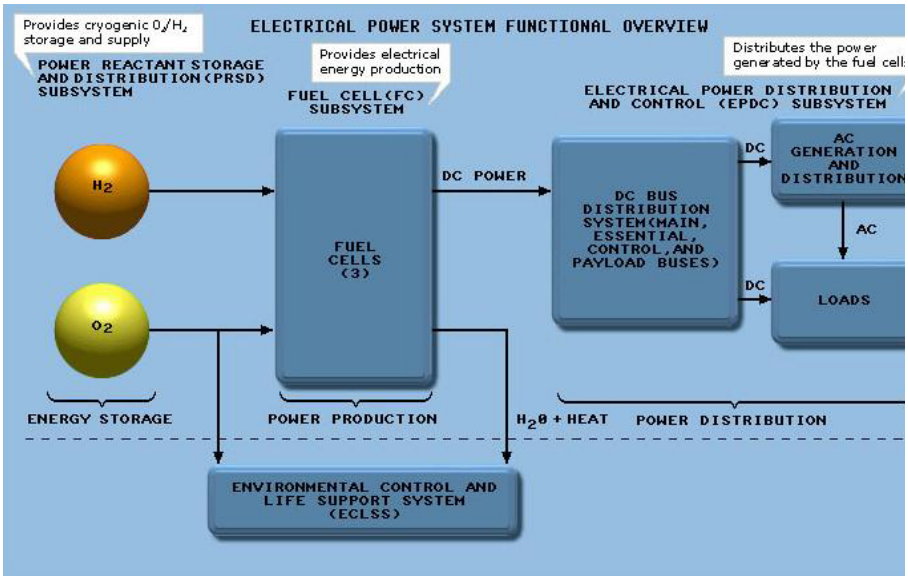

Figure 1. Electrical Power System Functional Overview. *Subsystem interfaces of the Electrical Power System.*[1]

2. Fuel Cells

The Fuel Cell subsystem is responsible for generating all of the vehicle's electrical power through a chemical reaction. Hydrogen and oxygen are used to produce water and direct current (DC) electricity. The electrical power is distributed via the Electrical Power Distribution and Control subsystem, and the water is sent to the Environmental Control and Life Support (ECLS) System to be used for vehicle cooling or as drinking water for the crew.

3. Electrical Power Distribution and Control (EPDC)

The EPDC is responsible for converting some of the direct current (DC) power to alternating current (AC) power and distributing both DC and AC power throughout the vehicle[2].

B. Environmental Control Systems

The Space Shuttle's Environment Control System is responsible for collecting and rejecting heat from the shuttle's electrical equipment and cabin atmosphere. This is accomplished through three subsystems, the Air Revitalization System (ARS), Water Coolant Loops (WCL), and Freon Coolant Loops (FCL).

1. Air Revitalization System (ARS)

The Air Revitalization System conditions the cabin atmosphere by removing heat, CO_2, water, and other contaminates from the air. The cabin fan circulates air throughout the cabin, collecting heat from the crew and cabin air-cooled equipment, and passes it to the Water Coolant Loops through the cabin heat exchanger. To maintain a comfortable "shirt sleeve" cabin temperature, the cabin temperature controller varies the amount of airflow passed over the cabin heat exchanger.

There are also three avionics bays in the cabin which house various air and water-cooled electrical equipment. Although the avionics bays are not hermetically sealed, they are considered thermally separated from the habitable volume. Avionics bay fans circulate air over the air-cooled equipment before passing it through a heat exchanger which transfers the heat to the Water Coolant Loops. There is no active control of the avionics bay air temperature; the air is simply circulated at a constant rate.

2. Water Coolant Loops (WCL)

The Water Coolant Loops run throughout the cabin to collect heat from the ARS heat exchangers mentioned above, as well as equipment mounted on cold plates, and transfer the heat to the Freon Coolant Loops via a heat exchanger referred to as the Interchanger. The Water Coolant Loops also chill the potable water supplied to the galley, provide cool water to the liquid-cooled ventilation garments (LCVG) worn under the Extravehicular Mobility Units while connected to the shuttle's airlock, and thermally condition the flight deck windows to prevent condensation. The temperature of the Water Coolant Loops is actively controlled by varying the amount of flow through the interchanger. There are two fully redundant loops, but only one is active at a time. Water is used as the working fluid in the cabin since it is not toxic (as opposed to Freon).

3. Freon Coolant Loops (FCL)

The heat collected by the ARS and Water Coolant Loops is ultimately transferred to the Shuttle's external Freon Coolant Loops. These loops also provide cooling to equipment such as the fuel cells, payloads, and other equipment located in the payload bay and aft compartments. Freon is used as the working fluid in the Freon loops because it resists freezing at the very low temperatures possible when exposed to deep space. On orbit, most of the collected heat is rejected to space by radiation through the radiators mounted inside of the payload bay doors. When the radiators are not available, such as when the payload bay doors are closed or when the radiators cannot provide sufficient cooling, supplemental cooling is provided by the Flash Evaporator System (FES).

The FES rejects heat by taking advantage of the vacuum of space to flash evaporate water at low pressure, absorbing heat from the Freon Coolant Loops. The water used by the FES is provided by the Fuel Cells. This water is stored in supply water tanks and may also be drank by crewmembers or transferred to ISS. Since the amount of water produced by the Fuel Cells and the amount water consumed by rejecting heat through the FES are both correlated to vehicle power levels, management of vehicle power levels is crucial in maintaining sufficient water consumables.

During entry, the Ammonia Boiler System (ABS) rejects heat when the atmospheric pressure is too high for the FES to operate. The ABS works similarly to the FES, only using a limited supply of ammonia which can evaporate under atmospheric conditions. Before launch and after landing, heat is rejected to Ground Support Equipment (GSE) via fluid-fluid GSE heat exchanger[3].

III. Space Shuttle Powerdown Philosophies

A powerdown on the Space Shuttle can be defined as deactivating non-essential electrical equipment. Since all electrical equipment generates heat when running, and the production of electricity generates heat, deactivating electrical equipment decreases the heat load and electrical demand.

Specifically for the Space Shuttle, since oxygen and hydrogen are used by the fuel cells to produce electricity, a powerdown reduces the rate at which the fuel cells consume the limited amount of hydrogen and oxygen that exists on any particular mission. Since oxygen (and sometimes hydrogen) is usually what limits the length of each mission, reducing the rate at which it is consumed, enables the Space Shuttle to stay on-orbit longer.

Another benefit associated with a decreased electrical demand is that the fuel cell output voltage increases as the load on the fuel cell decreases. If the electrical demand (output current) is high enough, the fuel cell output voltage will fall below the range where the equipment is certified to operate. So by deactivating low-priority equipment, the fuel cell output voltage will increase which improves its supportability of additional critical equipment.

A powerdown may be performed for any combination of four basic reasons: 1) to reduce heat load, 2) to reduce the rate at which consumables are consumed in order to extend the mission, 3) to improve voltage supportability, and 4) to deactivate equipment that is or could become a safety risk. These reasons are explained in detail below.

A. To Reduce Heat Load

The Environmental Control System must reject all of the heat produced by the Orbiter. The vast majority of this heat is the result of the production and use of electricity. Therefore, it is necessary to maintain a vehicle power level that is lower than the Environmental Control System's heat rejection capability. If the overall heat rejection capability is degraded, the total vehicle power level must be reduced. However, if only a portion of the system is degraded, only the affected components must be powered down. In the latter case, it may be possible to switch to redundant equipment that still has good cooling, resulting in no loss of capability and no reduction in the vehicle's total power level. Some examples are discussed below.

1. Complete Loss of Vehicle Cooling

In this situation, there is no way to reject heat from any of the vehicle's powered equipment. Therefore, it is imperative to reduce the vehicle's power level as much as possible, preserve entry-critical equipment, and land as quickly as possible. For the Shuttle, a loss of two Freon Coolant Loops will result in a complete loss of vehicle cooling.

The loss of two Freon Coolant Loops requires the most extreme powerdown for a loss of cooling. Analysis indicates that the orbiter will only survive for approximately 120 minutes from the time that both Freon Coolant Loops are lost. The limiting factor is the fuel cells which will overheat and fail catastrophically. Therefore, the crew is instructed to take the earliest possible deorbit opportunity, even if it requires a bailout and loss of the Orbiter.

The basic powerdown philosophy for this situation is to assume that no other failures have occurred to the Orbiter's systems and powerdown to a zero-fault-tolerant state for entry. This means that there is no redundant equipment powered and any failure of the zero-fault-tolerant equipment will result in a loss of crew and vehicle. Examples of equipment affected are having only a single Guidance, Navigation, and Control (GNC) computer operating during entry, and using only Ultra High Frequency (UHF) communications which only provides intermittent communication through ground sites and no vehicle data to the Mission Control Center. All of the avionics required for such an entry are powered up in a single avionics bay so that the other bays may be powered down completely (fans, smoke detectors, etc).

2. Loss of Cooling to a Portion of the Vehicle

Since the fluids capable of withstanding the wide temperature range of the space environment are often highly toxic, it is often desired to operate a low-toxicity fluid inside the habitable volume which transfers heat to a separate fluid outside the habitable volume where human exposure is not a concern. Additionally, various electronic equipment designs may require air or liquid cooling. The result of these design concerns is often an active thermal control architecture which consists of an air-liquid-liquid scheme. Consequently, failure of the air or internal liquid loop may result in complete loss of cooling to a portion of the vehicle. Listed below are a few examples of these scenarios specific to the Space Shuttle.

A loss of two Water Coolant Loops is the second-worst loss of cooling situation behind loss of two Freon Coolant Loops. In this scenario, cooling cannot be provided to the crew cabin. Therefore, maintaining a cabin temperature at which the crew can safely fly the vehicle is what determines the maximum amount of time the crew

may remain on orbit. Although cabin depressurization/repressurization cycles are used to extend this time by expelling hot, humid air and replacing it with cool, dry air, analysis indicates that a landing must occur within four hours of such a failure.

In this procedure, only the air and water-cooled equipment in the cabin are configured for a zero-fault-tolerant entry. Since the Freon Coolant Loops are still available, additional Freon-cooled equipment is actually powered up in order to maintain a power level to sustain safe fuel cell operation.

Similar to the Loss of Two Freon Coolant Loops procedure, all of the equipment required for a zero-fault-tolerant entry is powered up in a single avionics bay and the remaining avionics bays are powered down. This includes a similar single GNC computer and only intermittent ground site UHF communications configuration. The extended time on orbit (four hours versus two) allows for two situations: 1) If the deorbit opportunity is soon enough, the crew will stay configured for entry, possibly cycling between redundant equipment to take advantage of the thermal capacitance of the avionics bays. 2) If more time on orbit is required to reach a deorbit opportunity, equipment, including all of the vehicle's computers, will be powered down to preserve it for entry. This equipment will be repowered shortly before deorbit.

If both cabin fans are lost, cooling to the crew and cabin air cooled equipment is lost. Similar to losing both Water Coolant Loops, the time on orbit is limited by the cabin temperature at which the crew can safely fly the vehicle. According to analysis, this time is approximately four hours. However, since the avionics bays still have cooling, there are a few changes to the deorbit configuration. The procedures for this scenario simply minimize the powered equipment in the cabin to minimize the cabin air temperature, and cycle redundant critical equipment to make use of the components' thermal capacitance.

3. Degraded Vehicle Cooling

It may also be possible for a spacecraft's cooling system to be degraded as opposed to failed completely. This may be a result of anything from a pump or fan operating at a reduced flow rate to a failure of the vehicle's radiative, evaporative, or sublimative cooling systems. The result is that the heat generated by the production and use of electrical power must be kept at a level below that which the environmental systems can reject. Here are a few Space Shuttle examples of this type of failure.

As mentioned in the Systems Overview, both of the Shuttle's Freon Coolant Loops are required to reject the heat produced at nominal power levels. If one of these loops is lost, the maximum heat rejection capability is cut in half and a powerdown below the supportable level must be performed. Since the Shuttle does not normally operate near its maximum capability the actual reduction in power is not that severe. Procedurally, low priority equipment is powered down first (unused laptops turned off, lighting minimized, etc). If the power level must be further reduced, progressively more critical equipment is powered down until a sustainable power level is reached.

There is one notable variation to losing a Freon Coolant Loop. To mitigate the risk of micrometeoroid orbital debris (MMOD) striking a radiator panel and causing a fluid leak, a modification was made to the Shuttle fleet which provides the ability to isolate the radiators from the rest of the loop, stopping such a leak. Of course this would also cause a loss of the radiator on that loop, which is the primary means of heat rejection. This will increase the cooling demand on the Flash Evaporator System (FES), which will increase water use. Since water production and the vehicle's primary heat load are a function of the power produced by the fuel cells, a balance exists between the water produced and the water demanded by the FES. If this balance cannot be achieved and a net-negative water rate exists, the amount of time until the vehicle must land is dictated by the amount of water stored in the supply water tanks.

Since the Freon Coolant Loop that has lost its radiator is increasing the demand on the FES, it is desired to deactivate this loop as soon as practical. Then, the Loss of One Freon Coolant Loop powerdown is initiated since this is effectively the situation as long as the loop with the isolated radiator is off. The complication of this failure scenario comes from determining whether or not it is safe to stay on orbit. The deciding factor is the amount of water in the supply water tanks that can be used for cooling in the event that the radiator on the other loop is lost.

B. To Reduce the Rate Consumables Are Used to Extend the Mission

Powering down decreases the rate at which the fuel cells consume the limited amount of cryogenic oxygen and hydrogen onboard. By powering down, time can be added to the mission by making the limiting consumable last longer.

For example, in the event that it is desirable to add an additional day to the end of a mission, but consumables (oxygen and/or hydrogen) do not support this at the planned power levels, a powerdown could be implemented to reduce the power level, slow the consumables usage rate, and add an additional day. The Mission Phase Powerdowns (see Section V, Paragraph A) discuss these types of powerdowns in more detail.

A list of equipment which can be powered off to gain margin was created and documented in the Shuttle Flight Rules to minimize the amount of rationalization required in real-time. Specifically, to extend the mission, the following may be powered off to gain margin: crew convenience items (such as some lighting and fans for crew comfort), electronics for automatically controlling equipment when a manual capability exists (manually operating heaters, manually managing the communication systems), and telemetry electronics that provide continuous insight into system health parameters (telemetry multiplexer/demultiplexers (MDMs), will be cycled on and off to take snapshots of data). This equipment is discussed in more detail in Section V, Paragraph A, Subheading 3.

The list of equipment in the Flight Rules is not a complete deactivation of all non-essential equipment though. It does not power off items with insignificant power consumption such as clocks and single pieces of telemetry because in most cases, the cryo savings of manually managing these small pieces of equipment is considered not worth the crew's time.

C. To Improve Voltage Supportability

The voltage at the fuel cell output terminals is inversely-related to the load it powers. At 16 kW, one fuel cell alone is not able to provide sufficient voltage to its sub-buses causing equipment to undervolt. Additionally, because heat is one of the byproducts of the fuel cell reaction, the more load a fuel cell powers, the hotter the fuel cell. An overheating fuel cell will eventually lose structural integrity which would lead to the catastrophic mixing of oxygen and hydrogen. As a result, the fuel cell can only operate at 16 kW for 10 minutes before the load would need to be reduced to the continuous operating limit of 12 kW. These constraints govern how the load on each fuel cell is managed.

Typically, each of the three fuel cells is connected to one of the three main electrical buses that distribute power to the electrical equipment on the orbiter. This equipment may receive power from just one of the main electrical buses or may have the capability to receive power from multiple buses. Typically, there is a little more than 2 kW worth of equipment operating that is capable of receiving power from only one of the main electrical buses. Following the loss of a fuel cell, one of the remaining fuel cells will be connected to the failed fuel cell's main electrical bus so that it powers both buses and no specific functionality is lost with the loss of one fuel cell.

Following the loss of one FC, the crew will power the vehicle down so that the total load on the remaining two fuel cells is less than 18 kW. The reason 18 kW is targeted is to protect for the next worst failure. If the fuel cell that is connected to only one main electrical bus were to fail, then that main bus would be unpowered dropping more than 2 kW, and the total vehicle power level would drop below the 16 kW limit of the remaining fuel cell. Note that a failure of the fuel cell connected to the two buses is not the next worst failure strictly from a voltage supportability perspective since losing this fuel cell will cause two main buses to become unpowered, dropping the total power well below the 16 kW that results from losing only one main bus.

The operational philosophy for the loss of two fuel cells is much simpler. After the loss of two fuel cells, the vehicle is completely dependent on the last fuel cell for survival, so the vehicle power level is reduced below the fuel cell continuous operating limit of 12 kW as soon as possible.

Additionally, when trying to keep the fuel cell under its rated load, it is important to remember that some loads cycle, and others are used only during certain phases of flight, so the target voltage must be far enough under the rated load that buses will not undervolt when additional equipment is activated.

D. To Deactivate Equipment That Is or Could Become a Safety Risk

There are situations where operating certain equipment could pose a safety risk. Fire and physical damage are obvious examples, but other factors such as changes in cabin pressure may also place operational limitations on this equipment. Below are a few examples of situations where a powerdown is warranted.

1. A Confirmed Smoke or Fire Event

Although the cabin atmosphere is carefully managed to reduce the amount of oxygen available to sustain a fire, risk of fire in the crew cabin cannot be completely mitigated. Fires and smoke events (the release of smoke without the presence of flame) are detected either by smoke detectors or by crew members smelling the smoke. Redundant smoke detectors are located in each avionics bay, and there are three cabin smoke detectors located in the ducts of the cabin air revitalization system.

If any of the smoke detectors or the crew detects the presence of smoke, and the crew can locate the source of the smoke or Mission Control detects failing equipment, that equipment will be unpowered immediately. If the source of the smoke is not immediately obvious, the crew will first ensure that they have safe air to breath by donning quick don masks (QDM), and then take appropriate actions to fight the fire before performing any powerdowns.

After crew safety is ensured, attention can be turned to performing the appropriate powerdown. In the case of avionics bay fire or smoke events, all equipment in the affected bay will be powered down, including the smoke detectors and fans. This is done even if a single piece of equipment is known to be the source of the smoke or fire since collateral damage may have occurred.

In most cases, all of the equipment in the affected avionics bay will remain unpowered until entry. During preparations for entry, a procedure exists to repower the equipment necessary for a single-fault-tolerant entry. This will repower any equipment necessary to ensure that a safe entry can be accomplished even after a single failure of entry-critical hardware (such as a vehicle computer). Of course, any piece of equipment that failed at the time of the fire or smoke event will not be repowered since it may have been the source of the event.

In the case of a cabin fire, it is not feasible to powerdown all equipment in the cabin after a smoke or fire event. Powerdowns for cabin fires are handled on a case-by-case basis by Mission Control.

Although the underlying philosophy of powerdowns for smoke and fire events is to unpower any equipment that has failed or may have sustained collateral damage and terminate the mission as soon as it is safe to do so, there are some exceptions. If the event is obviously caused by non-critical hardware that can be easily be left unpowered for the duration of the mission, that single piece of equipment can be unpowered and the mission can continue. This was the case on STS-28 when a printer cable shorted and momentarily released smoke and "four or five burning red embers" before being unplugged. The cable simply remained unplugged and the mission continued with no further action.[4]

Some leeway is also given when it comes to terminating a mission for an avionics bay fire. The flight control team may decide that it is prudent to inspect the affected avionics bay to determine if the event was isolated to a single piece of equipment. If it can be determined that there is no collateral damage, the affected equipment can remain unpowered and the mission may continue.

2. Loss of Smoke Detection Capability to an Enclosed Portion of the Vehicle

Although it would take multiple failures, there is a possibility that all the smoke detectors in a certain area are lost. In the cabin, the crew would be able to detect smoke by smell, so no powerdown is required. In the avionics bays, loss of smoke detection requires that steps be taken to mitigate the risk of fire. This includes a powerdown.

In microgravity, there are no buoyancy effects that drive the convection that would continuously feed oxygen to a fire when gravity is present. Therefore, the main purpose of a loss of smoke detection powerdown is to stop the forced airflow provided by the fans, thereby stopping the flow of oxygen to any would-be fire. Consequently, any equipment that is cooled by the fans must be unpowered. Equipment cooled by other means, such as water-cooled equipment, may remain powered.

Note that the intent of a loss of smoke detection powerdown is not to minimize the amount of powered equipment that may start a fire. This equipment is still considered reliable. Rather, the intent is to remove the ability of a fire to sustain itself.

Since the equipment in an avionics bay without smoke detection is still reliable, the affected bay's fan and equipment can be repowered in order to provide fault tolerance for entry. To provide fire protection during the relatively short time that the fan is on, a fire extinguisher is discharged into the affected bay. Since the fire suppressant from the extinguisher eventually dissipates into the cabin, leaving the avionics bay below the concentration required to suppress a fire, this is only done for entry and is not effective during obit operations.

3. A Change in Cabin Pressure

Because much of the electrical equipment in the orbiter is air cooled and the ability of the cabin air to remove heat is directly related to cabin pressure, there are operational constraints on some cabin equipment below certain pressures. Although the orbiter is designed to autonomously maintain cabin pressure only at either a nominal pressure of 14.7 psi (sea level) or at 8 psi for emergencies, the crew can manually maintain cabin pressure at pressures in between these values. The lowest pressure at which the cabin is nominally maintained is at 10.2 psi. This pressure is often used when shuttle-based extra-vehicular activities (EVA) are required in order to reduce the risk of decompression sickness (the bends) in the extra-vehicular crewmembers. To support these operations, all of the equipment in the orbiter is certified to operate down to a pressure of 10.2 psi. However, in certain contingency situations like a cabin leak or toxic atmosphere, it is necessary to power down any equipment not certified to go below this pressure.

The docking electronics located in the external airlock are a special case. All of these components are Russian-built and are certified down to at least 8 psi. Since the airlock and cabin atmospheres can be separated by closing a hatch, i.e. maintained at different pressures, and the docking electronics are only powered for docking operations,

they are managed separate from the cabin electronics. Powering down of docking equipment is managed on a case-by-case basis.[5]

IV. Executing a Powerdown

Space Shuttle powerdown steps can be executed one of two ways: by the crew onboard, or by the Mission Control Center (MCC) via ground commands. Each method is described below.

A. Crew

Once the MCC decides a powerdown is necessary, MCC will read the powerdown steps to the crew. Upon hearing the powerdown steps, the crew will usually repeat them back to the MCC. Then, MCC will verify that the crew has read back the correct steps and will give the crew permission to perform the powerdown. The crew may need to move to the correct area of the cabin (may not always be accessible on ascent and entry since the crew is seated and restrained), find the panel, and then execute the actions specified while MCC watches data to verify the correct actions were executed.

The pros of having the crew work the powerdown is that it maintains a high level of situational awareness for the crew and can be done independently of the data link required for the MCC to send commands to the vehicle (note: the crew can initiate a powerdown without MCC). The cons of needing the crew to work the powerdown are that the powerdown cannot be performed if the crew is asleep, busy, or if the actions required are at an inaccessible location. Additionally, physiological factors such as acceleration forces, crew well-being (consciousness, fatigue, sickness ...), orientation, reach, and visibility may make it more difficult to perform the powerdown. Lastly, it takes a relatively long time (compared to a ground command) once MCC decides a powerdown is necessary until it is actually performed. As a result, many pieces of equipment that draw small amounts of power, such as timing clocks and single pieces of instrumentation, are not commonly powered down in order to gain an extension day.

B. Ground Command

Once the MCC decides that a powerdown is necessary, the command will be sent during a period of good communication. The MCC will verify the command and inform the crew for their situational awareness.

The pros of this method of powering down are that they can be performed during crew sleep, when the crew is busy or restrained to a certain location, it does not rely on the crew's physiological conditions, and it can be performed quickly. The major cons of this method are that it relies on having command capability and that this capability only exists for a limited amount of equipment.

Due to the primitive software and computers that existed in the 1970s, most equipment on the shuttle can only be activated and deactivated by the crew via onboard switches. However, there are some items, such as the flight data recorder called the Modular Auxiliary Data System (MADS) which can be activated and deactivated by ground commands. With the advances in software and computers, future spacecraft will likely have more ground commanding capability and less onboard switches, but each method has its pros and cons and should be considered during vehicle design.

V. Types of Shuttle Powerdown Procedures

A. Mission Phase Powerdowns

The amount of required powered equipment varies throughout a mission and is dependent on the mission phase. For example, more powered equipment is required during launch than is required during relatively quiescent operations while docked to the ISS. As a result, several powerdowns and powerups have been written to configure the vehicle systems for the appropriate phase of flight. These powerdowns, usually agreed to preflight, save power-producing consumables but come with tradeoffs and are discussed in further detail below.

1. Group A Powerdown

This powerdown is a standard switch list for on-orbit operations. This powerdown deactivates equipment that is used during ascent and not required on-orbit. Some of this equipment will be used for entry, so the tradeoff is that this powerdown will require crew time to perform the powerdown and then reactivate the required equipment before entry.

2. Group B Powerdown

This powerdown which is only implemented after Group A, increases the mission duration by deactivating equipment that is seldom used on orbit. In general, the equipment included in this powerdown does not increase vehicle risk, but requires crew time to power it up and down before and after the activities for which it is required. It was originally intended to be a nonstandard avionics configuration to be used on power-critical missions not normally involving payload deploys, rendezvous, proximity operations, or use of the robotic arm. However, the Group B powerdown became the standard on-orbit config because conserving the limited amounts of oxygen and hydrogen became important and longer missions meant that the crew had more time to perform powerup and powerdown procedures.

The other on-orbit activities which require the Group B powerup are major vehicle maneuvers, system checkouts the day before entry, transitions between computer software modes, and the entry preparations. The Group B Powerdown procedure can be seen in Fig. 2.

PRIORITY PWRDN GROUP B

PNL	GRP B PWRDN (LOW LEVEL)	PWRUP
	NOTE KU-BD and S-BD FM sw: As reqd to conserve energy and accomplish mission objectives, MCC will cmd	
	1. Turn off all lights except Middeck lts 6,7,8 (no lts for single-shift sleep, one for split-shift sleep)	As reqd
C3	2. MSTR MADS PWR – OFF (as reqd, cycle ON per FLIGHT PLAN)	ON
A14	3. RCS/OMS HTR L POD (two) – A AUTO, B OFF R POD (two) – A AUTO, B OFF	MCC call
GALLEY	4. H2O HTR (two), OVEN FAN – OFF (1)	ON (1)
O14, O15, O16:E	5. cb DDU L,R,AFT (six) – op	cl
	If GPC MODE 2 – RUN: 6. Perform G2 SET CONTRACTION (ORB OPS, DPS), then:	(2)
O15:F	7. MMU 2 – OFF (1 of 2 off)	ON
	8. Minimize PGSC use	
O14,	9. Pri RJDF DRIVER,LOGIC (eight) – OFF	ON
O15,	10. Pri RJDA DRIVER,LOGIC (eight) – OFF RJDA 1A L2/R2 DRIVER – ON	ON
O16:F	11. Use only one IDP with three MDUs max. All IDPs and MDUs OFF for single-shift sleep; otherwise – ON	ON
	12. GNC 21 IMU ALIGN IMU 2 STBY – ITEM 22 EXEC	(3)
	13. COLOR PRINTER – OFF	(4)

(1) Insert drink package to keep water tank pump from cycling (water temp may decrease slightly); if repowering Galley, remove drink package

(2) If reqd, go to G2 SET EXPANSION (ORB OPS, DPS)

(3) Recover IMU 2 (MAL, GNC FRP-3)

(4) MCC will instruct crew when to turn COLOR PRINTER ON

Figure 2. Group B Powerdown Procedure.[6]

3. Group C Powerdown

This powerdown, also implemented only after Group A but independently of Group B, is typically planned for mission extension days for weather or other factors preventing an on time landing, but may be implemented at other times if the benefit outweighs the risks and operational impacts. This powerdown is more extensive than the Group B powerdown. In general, the tradeoff of this larger powerdown results in a slight increase in vehicle risk, more crew convenience items being deactivated, and more of an impact to crew time. The Group C powerdown is planned for extension days because there are no mission objectives that must be accomplished during extension days. However, if sufficient margin exists at the end of the mission, the Group B powerdown is preferred on extension days over Group C. Examples of equipment and its associated impacts are described in the next paragraph. The entire procedure is shown in Fig. 3.

Multiplexer/Demultiplexers (MDM) FF2, FF4, and FA4: Deactivating these MDMs results in the loss of continuous jet propellant leak detection. Instead, crew visual reports and data snapshots acquired by periodically reactivating MDMs will be used for leak detection.

Orbiter Cabin Air Cleaner (OCAC): The OCAC is a fan that provides airflow between the Shuttle's middeck and flight deck. It improves air quality by providing thermal mixing, preventing buildup of carbon dioxide pockets, and filtering airborne dust and debris. It is not required equipment, but is crew a preference item; however, it is usually flown since in addition to improving air quality, it reduces the need for avionics air filter cleaning and produces white noise that makes it easier for the crew to sleep.

Multifunction Display Units (MDU): MDUs are computer monitors that can be configured to display a variety of data such as flight instruments and system displays. They can be cycled on and off as required.

Payload MDM 2: Deactivating this MDM results in the loss of some commanding capability and telemetry. Specifically, it results in the loss of commanding to the Orbiter's closed circuit television, a data recorder, a payload signal processor, and commanding through antenna electronics. The agreement is that this MDM would be repowered to regain any of this capability, if needed.

Star Trackers: Star Trackers are used to recalibrate and realign the navigation system of the shuttle to assist in identifying the exact location of the Shuttle. Unpowering a star tracker increases the probability that a star will be missed which would require a maneuver to attitude for an inertial measurement unit align which would result in lost propulsion.

In addition to the on orbit activities that cannot be performed while in a Group B powerdown state, hydraulic circulation pump operations, auxiliary power unit operations, payload bay door operations, the K_u band antennae operations, and some payload operations cannot be performed while Group C equipment are powered down.[6-7]

PRIORITY PWRDN GROUP C

PNL	GRP C PWRDN (MSN EXT)	PWRUP
	1. Perform PRIORITY PWRDN GROUP 1,2	
	If prior to first deorbit prep:	
	2. Perform PRIORITY PWRDN GROUP 3A, then:	
	3. Turn off all lights except two Middeck lts (use no lts for single-shift sleep or split-shift sleep)	
GALLEY	4. H2O HTR (two), OVEN FAN – OFF (1)	ON (1)
	5. MDUs: Cycle ON when reqd	
O14, O15, O16:F	6. Pri RJDF DRIVER,LOGIC (eight) – OFF	ON
	7. Pri RJDA DRIVER,LOGIC (eight) – OFF RJDA 1A L2/R2 DRIVER – ON	ON
O6	8. MDM PL2 – OFF (2)	ON (3)
A14	9. RCS/OMS HTR L POD (two) – A AUTO, B OFF R POD (two) – A AUTO, B OFF	MCC call
A1L	10. PL DATA INTLVR PWR – OFF S-BD PL PWR SYS – OFF CNTL – PNL,CMD (4)	MCC call MCC call
A1R	11. FM PWR – OFF CNTL – PNL,CMD	1 (5)
O6	12. √UHF MODE sel – OFF	
	13. KU-BAND SYS – max 2 hr ON/day (5)	
O14, O15, O16:E	14. cb DDU L,R,AFT (six) – op	cl
	15. COLOR PRINTER – OFF	MCC call

(1) Insert drink package to keep water tank pump from cycling (water temp may decrease slightly); if repowering Galley, remove drink package

(2) Before powering off PF2 MDM, √MCC for Antenna Electronics 1 activation

(3) SM I/O RESET

(4) If PDI and/or PSP pwrd off, expect 'S62 BCE BYP PL', 'S62 BCE BYP PDI' and/or 'S62 BCE BYP PSP' msgs

(5) As reqd, MCC will command

Figure 3. Group C Powerdown Procedure.[6]

PRIORITY PWRDN GROUP 1

PNL	GRP 1 PWRDN	PWRUP
	1. Minimize ltg	
	2. Use only one IDP with three MDUs max	
	If GPC 2 – RUN:	
	3. Perform G2 SET CONTRACTION (ORB OPS, DPS), then:	(1)
O15:F	4. MMU 2 OFF – (1 of 2 off)	ON
	5. GNC 21 IMU ALIGN IMU 2 STBY – ITEM 22 EXEC	(2)

(1) If reqd, go to G2 SET EXPANSION (ORB OPS, DPS)

(2) Recover IMU 2 (MAL, GNC FRP-3)

PRIORITY PWRDN GROUP 2

PNL	GRP 2 PWRDN	PWRUP
O6	1. S TRK PWR -Y,-Z (two) – OFF	As reqd
	2. Perform GPS PWRDN (ORB OPS, GNC) for GPS 2	(1)
	3. MDM FF2,4 (two) – OFF FA4 – OFF	ON (2)
C3	4. MSTR MADS PWR – OFF	ON
L1	5. FLASH EVAP CNTLR PRI (two) – OFF SEC – OFF TOP EVAP HTR NOZ (two) – OFF DUCT sel – OFF	(3) (4) Two ON (3) ON
	NOTE RMS temps no longer avail on A8U; however, MCC has insight	
MA73C:F A8L	6. cb AC1 RMS PRI ΦA – op 7. PORT RMS HTR A(B) – OFF	
	* If PDRS PORT TEMP msg (MA tone only): * * Within 30 min, PORT RMS HTR A(B) – AUTO * * On MCC call: * * PORT RMS HTR A(B) – OFF; repeat as reqd *	
OCAC	8. Use only one orbiter PGSC If OCAC flown: 9. OCAC PWR – OFF	ON

(1) Perform GPS PWRUP (ORB OPS, GNC) for GPS 2

(2) GNC I/O RESET

(3) Perform TOPPING FES STARTUP, using Pri A/B (ORB OPS, ECLS)

(4) SEC CNTLR ON only if both primary controllers failed

Figure 4. Priority Powerdown Group 1 & 2.[6]

B. Contingency Powerdowns

In the event of contingencies such as a partial loss of cooling, change in cabin pressure, loss of a power source, or the presence of a fire, it may become necessary to powerdown equipment. As a result, powerdowns have been pre-written to strategically reduce the power level to an appropriate level, or to deactivate specific pieces of equipment. For example, in the event air-cooling is lost in a particular avionics bay, air-cooled equipment may need to be deactivated while water-cooled equipment in that bay can be left operating. Examples of situations where contingency powerdowns have been prewritten for that specific situation include: Loss of Cabin Pressure, Total Loss of Vehicle Cooling (Loss of 2 Freon Loops), significant loss of power generation capability (Loss of 2 of 3 Fuel Cells), fire damage to a section of the spacecraft (Avionics Bay fire powerdowns), and others.[5]

For situations where the need for additional powerdowns beyond Groups A, B, or C exceed the safety risks associated with decreased operability due to additional powerdowns, a series of powerdown groups were written based on priority. These powerdowns have been organized by six numbered groups (see Groups 1 and 2 in Fig. 4). The powerdown philosophy here is that the lowest numbered powerdown will be executed first, if an additional powerdown is still needed, the next numerical powerdown group will be executed until the desired power level is reached.[6]

VI. STS-117 Powerdown

A. Summary

STS-117 was an International Space Station (ISS) assembly flight that launched in June of 2007. It carried the second starboard truss segment and a set of solar arrays. On Flight Day 5, the Russian Service Module Central Computers (SMCC) and Service Module Terminal Computers (SMTC) all went down due to a failure of their respective power supplies. This resulted in the loss of several systems, in particular the loss of Russian thruster

attitude control on the ISS. The Russian thrusters work with the Control Moment Gyros (CMG) to maintain attitude control. The CMGs can counteract external torque until they become saturated by reaching their full range of motion, when they must be "desaturated" by the Russian thrusters. Additionally, without thrusters, the ISS cannot perform large attitude maneuvers. When docked to the ISS, the Shuttle's thrusters can be used in place of the Russian thrusters for maneuvers, but not CMG desaturation capability.

After about a day of working to fix the Russian computers, it became clear that there was no quick fix and a dilemma arose. With the Shuttle set to undock in less than a week, if the Russian computers could not be fixed and the thrusters regained, the ISS was in danger. To prepare for undocking the Shuttle, attitude control would need to be dropped, then the accelerations caused by the Shuttle undocking would make it impossible for the ISS to resume attitude control without the Russian thrusters. Loss of attitude control meant unreliable and unpredictable power generation and communication between ISS and Mission Control. Additionally, it would be dangerous for any vehicles to dock to or undock from the ISS if it did not have attitude control. These factors caused engineers to explore new methods of attitude control such as commanding Russian Progress directly from the ground instead of through the SMTCs and also reducing Shuttle attitude deadbands so that control could be passed directly from the Shuttle to CMG Momentum Management without large torques. The latter technique was used for all subsequent Shuttle missions, saving Russian propellant. Complications arose because, if these new and uncertified methods of attitude control did not work, loss of attitude control would cause the loss of the ISS and possibly the loss of the crew as a result of undocking the Soyuz without ISS attitude control. For the safety of the ISS crew, serious consideration was given to undock and abandon ISS before the Shuttle undocked.

PP3A	PRIORITY PWRDN (Recoverable) (On MCC call only)	PWRUP
FLT DECK/MIDDECK		√MCC
	1. Exit programs, pwr dn all non-essential PGSCs	
L11	2. DC PWR CAB PL1 – OFF	
If addnl pwrdn reqd:		
	3. Go to PRIORITY PWRDN 3B (PP3B)	

Figure 5. Priority Powerdown PP3A. *This powerdown was written preflight specifically for STS-117 and is referenced in Step 2 of the Priority Powerdown Group C powerdown which is a generic procedure.*[8]

MSG 061A - MODIFIED GROUP C POWERDOWN PROCEDURE

Please perform the following Modified Group C Powerdown Procedure **on MCC GO**.

PNL	PWRDN	NOTES
	1. Minimize Lighting Turn off all lights except two Middeck lts (use no lts for single-shift sleep)	
	2. Use only one IDP with three MDUs max	1
O6	3. MDM PL2 – OFF	2
	4. S TRK PWR -Y – OFF	3
	5. MDM FF2,4 (two) – OFF	
O16:F	6. ASA 3 – ON, then ASA 4 – OFF, then	4
O6	MDM FA4 – OFF	
	7. PGSC Required: OCA, KFX, WLES (STS-7) All other PGSCs – OFF, ON as required	
	8. COLOR PRINTER – OFF, ON as required	
OCAC	9. OCAC PWR – OFF	5
SSV	10. SSV Pwr – OFF	
	11. Perform GPS PWRDN (ORB OPS, GNC) for GPS 2	6

1. Reference the IDP/CRT 1(2,3) POWER OFF/ON Cue Card provided in the FD7 Execute Pack (MSG049A)
2. Before powering off PF2 MDM, √MCC for Antenna Electronics 1 activation
3. GNC will request that the -Y star tracker be powered on for approximately two orbits about every other day. This is required to obtain star vector information for IMU alignment verification.
4. Power on ASA3 to maintain elevon park before FA4 is powered down.
5. The OCAC can be re-enabled for crew sleep as needed, to help in minimizing CO_2 pockets.
6. Powerdown GPS 2 and Pre-amps since it will be unavailable when FF2 is powered down.

Figure 6. STS-117 Modified Group C Powerdown. *This powerdown was the first unplanned powerdown on STS-117 that was developed, uplinked, and then implemented on the morning of Flight Day 7 (~MET 005/14:00).*[9]

On this mission, cryogenic oxygen was the consumable limiting how long the Shuttle could remain docked to the ISS. On Flight Day 6, the Electrical Generation and Illumination (EGIL) flight control team responsible for managing the cryogenic oxygen, was asked to come up with a plan that would save oxygen and extend the mission. Within minutes, the EGIL team was able to calculate the size of the powerdown needed to stretch out the limited amount of oxygen remaining and add an additional day for more troubleshooting. The EGIL team then asked all flight control disciplines to review the Group C Powerdown procedure and report back any additions, deletions, or modifications to the steps needed to execute the powerdown procedure. This powerdown (see Fig. 6) was then executed after the Flight Director gave the official "go".

Soon after this first powerdown, the EGIL team was asked for a plan to add yet another day to the mission. Since it would have been impossible to achieve an extra day by powerdowns alone, the ISS program

decided to "loan" the Shuttle its precious oxygen to allow for more troubleshooting. With the ISS oxygen and further powerdowns, a second additional day was possible (see Fig. 7). For this second round of powerdowns, a variety of low-power equipment was unpowered in this powerdown. The reason the equipment in this powerdown was not included in the Group C powerdown is because in most scenarios, the benefit of deactivating these pieces of equipment is not worth the effort required to power them down. In addition to adding capability for two additional days, consideration was even given to giving up some of the Shuttle's extension days (reserved in the event of bad weather on entry day) in exchange for more docked days to troubleshoot the Russian computers. Even more drastic powerdowns were being considered to buy back hours of time on orbit such as unpowering the computer that runs the software to perform fault detection and annunciation to the vehicle systems, and requiring manual antennae management for communication. Fortunately, before these drastic powerdowns needed to be implemented, the Russian computers were repaired and the ISS was saved four days after the initial failure and three days before the original planned undocking.[12-14]

These powerdowns gave the Russians more time to work at repairing their computers before contingency plans would need to be implemented. It also gave NASA engineers, mission managers, and flight controllers, more time to evaluate different options for alternate methods of attitude control and to develop contingency plans. The impact that these powerdowns had on the overall vehicle power level can be observed in Figs. 9-12.

MSG 074A - FD08 PRE-SLEEP POWERDOWNS

PNL	PWRDN	NOTES
O6	1. GPC PWR 2 - OFF	
	2. MDM FA3 – OFF	
O14:B	3. cb MNA MSN TIMER FWD - op	
	cb MNA EVENT TIMER AFT - op	
O15:B	4. cb MNB EVENT TIMER FWD - op	
	cb MNB MISSION TIMER AFT – op	
	cb MNB OI TIRE PRESS - op	
O16:F	5. ASA 3 – OFF	
O16:E	6. cb MNC RCS/OMS PRPLT QTY GAUGE - op	
R14:A	7. cb MNA ADC 1A/2A - op	
	8. cb MNB ADC 1B/2B cb - op	
L4:J	9. cb AC3 φA SIG CONDR HUM SEP - op	
	B SIG CONDR IMU FAN - op	
ML31C	10. VAC VENT NOZ HTR - OFF	
MO69M	11. √LEH O2 8 vlv - CL	
Ergometer	12. Turn the cycle ergometer power switch off. With subsequent operation, use in unpowered manual mode.	

NOTES:

Prior to use, GPC 2 will need to be IPLed (15 minutes) to protect against low probability double bit error induced by radiation hit without scrub logic.

Figure 7. STS-117 Flight Day 8 Powerdown: *These additional powerdown steps were uplinked as a crew message and implemented before the crew went to sleep on Flight Day 8 during STS-117 (~MET 007/03:00).*[10]

MSG 103 - MODIFIED GROUP C POWERUP

PNL	PWRUP
O6	1. MDM PL2 - ON
	2. MDM FF2,4 (two) - ON
	3. MDM FA3,4 (two) - ON
	4. S TRK PWR -Y - ON
	-Z - ON
	5. GNC I/O RESET
	6. SM I/O RESET
O16:E	7. cb MNC RCS/OMS PRPLT QTY GAUGE - cl
	8. ASA 4 - ON
O15:B	9. cb MNB OI TIRE PRESS - cl
	EVENT TIMER FWD - cl
	MSN TIMER AFT - cl
O14:B	10. cb MNA MSN TIMER FWD - cl
	EVENT TIMER AFT - cl
L4:J	11. cb AC3 ϕA SIG CONDR HUM SEP - cl
	ϕB SIG CONDR IMU FAN - cl
R14:A	12. cb MNA ADC 1A/2A - cl
	MNB ADC 1B/2B - cl
SSP1	13. OIU PWR - OIU 1 ON (tb-UP)
SSV	14. SSV PWR - ON
	OUTRATE - 3
	15. Perform GPS PWRUP (ORB OPS, GNC) for GPS 2
ML31C	16. VAC VENT NOZ HTR - ON
Ergometer	17. Use cycle ergometer as required
OCAC	18. OCAC PWR - ON as required

Figure 8. STS-117 Modified Group C Powerup. *This powerup was performed before undocking to backout of the unplanned powerdown actions and prepare for undocking.*[11]

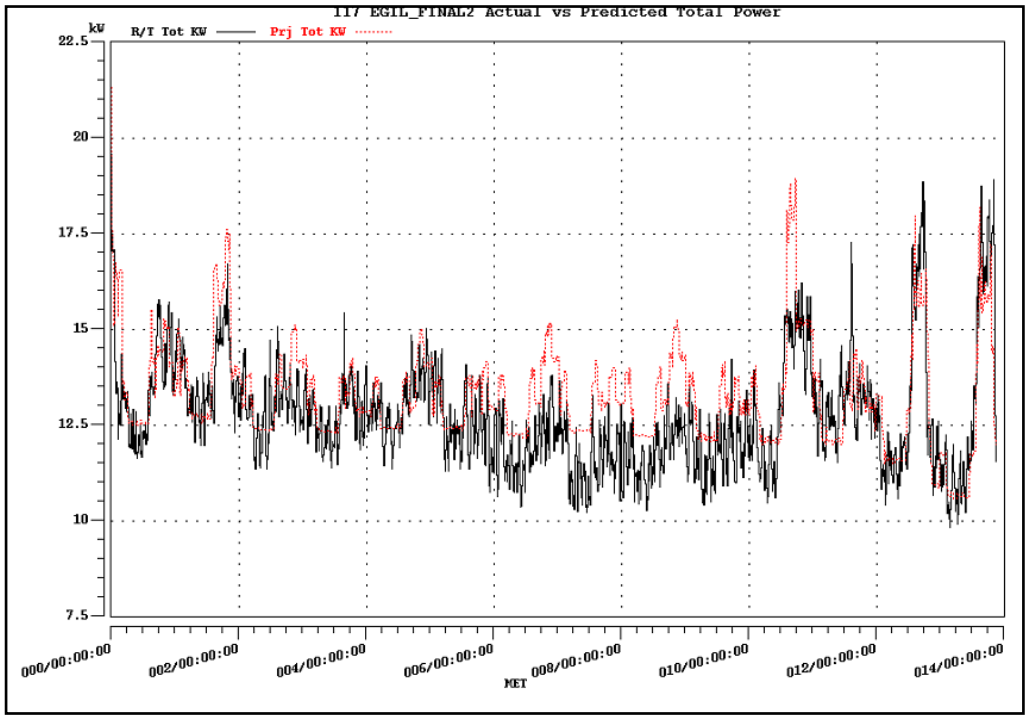

Figure 9. STS-117 Actual versus Predicted Power for the Entire Mission. [15]

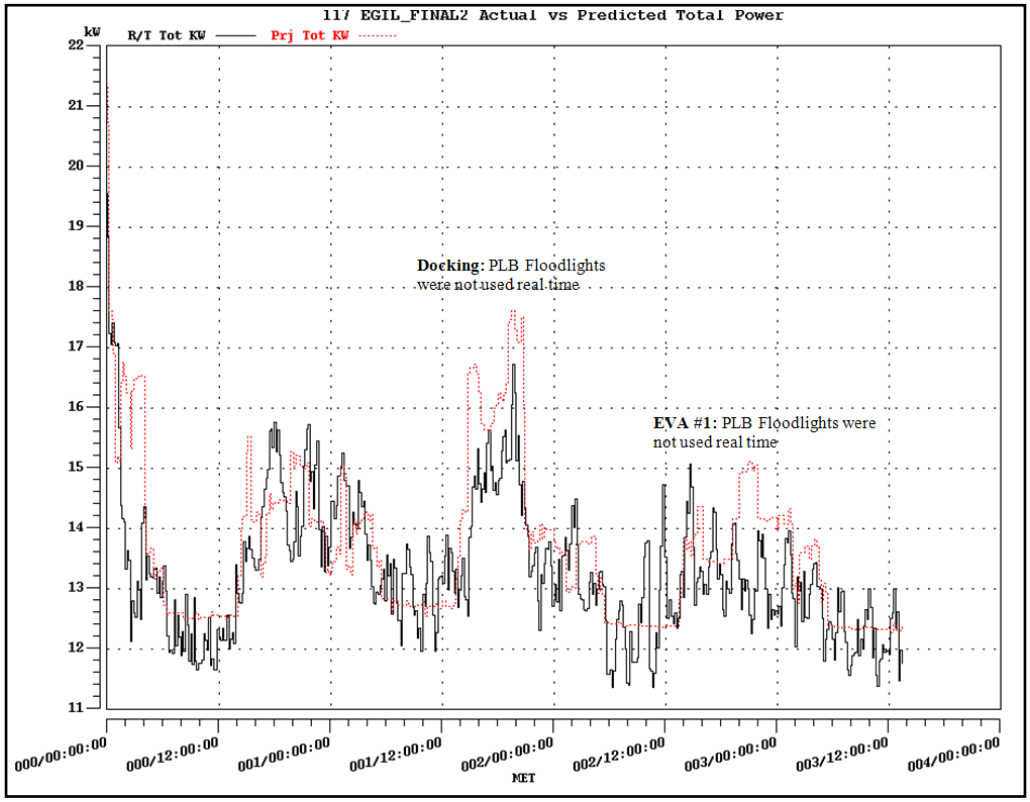

Figure 10. STS-117 Annotated Comparison of Preflight versus Actual Power for the first 96 hours. *Before any of the unplanned powerdowns, the actual power level was very close to the predicted power level.* [15]

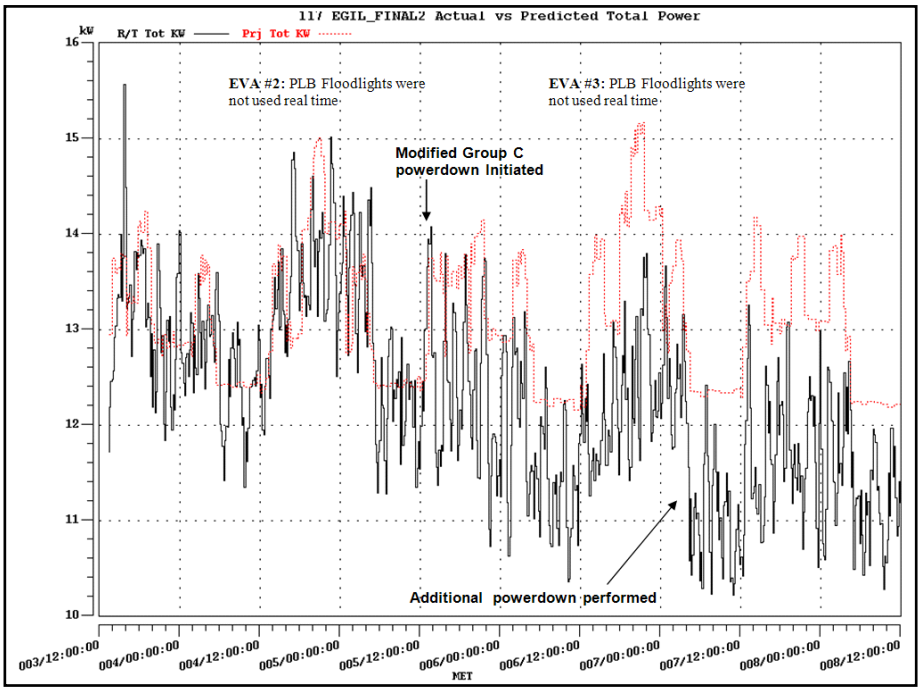

Figure 11. STS-117 Annotated Comparison of Preflight versus Actual Power from FD05 to FD10. *After the Modified Group C powerdown, the actual power level dropped noticeably below the predicted power level. The actual power level dropped again after the additional powerdown was performed.* [15]

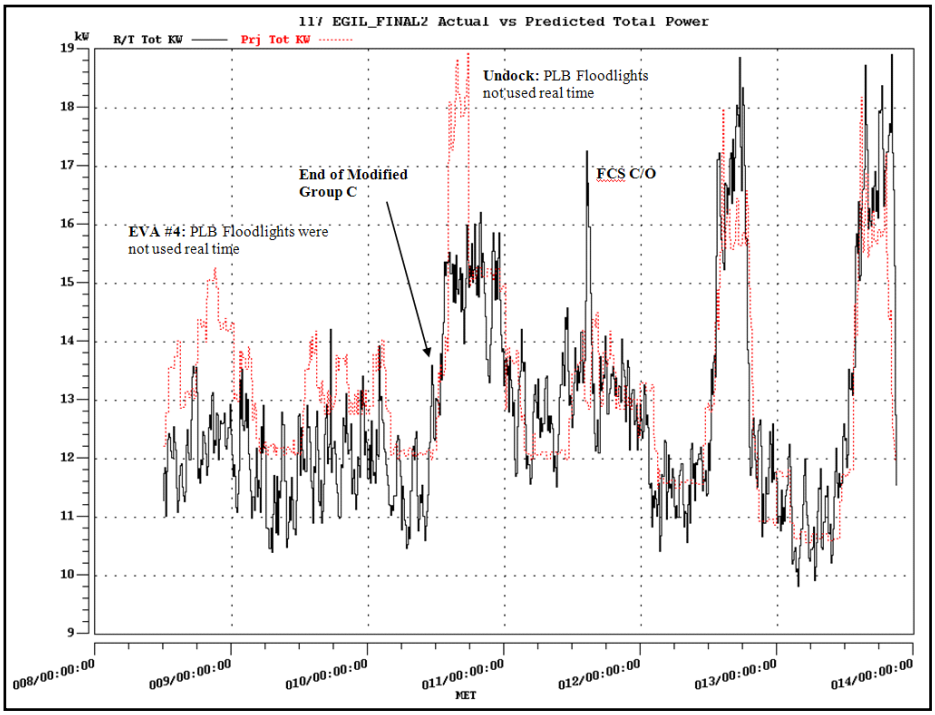

Figure 12. STS-117 Annotated Comparison of Preflight versus Actual Power from Flight Day 10 to End of Mission. *Once the powerdown was no longer needed, systems were powered up to backout of the earlier powerdown actions to regain capability that was given up to powerdown.* [15]

B. Commentary

For the most likely and most severe contingency situations, EGIL maintains prewritten powerdown procedures that have been coordinated across all disciplines to ensure safety. When a powerdown is required, EGIL selects the appropriate powerdown procedure that maintains a balance of power level, operability, and safety. The Shuttle philosophy for managing power is to only have equipment running that is needed. As a result, deactivating a piece of equipment has some impact or it should not be on. The flight control team uses the powerdown procedures as a baseline to reduce the power level precisely to the desired level so as to not give up unnecessary capability or safety margin.

Since it is not practical to write and maintain powerdown procedures that apply to every situation for every mission, the powerdown procedures were written for generic situations, assuming an otherwise healthy vehicle. On STS-117, there were several flight-specific conditions that required the procedure to be reviewed before implementation. On STS-117, the Group B powerdown had been performed after docking. To preserve functionality of equipment required for STS-117's mission, the Group C powerdown was modified before it was executed. Figure 5 contains the payload powerdown that was developed preflight specifically for STS-117 and is referenced in step 2 of the Group C powerdown. The procedures in Figs. 2-5 were used as a baseline to create Fig. 6 which is the Modified Group C Powerdown that was implemented on STS-117 after accounting for all flight-specific considerations. It can be observed that not all steps of the Group C powerdown were performed. Some steps that were in the Group C powerdown would have been undesirable if performed such as step 10 which would have resulted in the loss of some data and commanding capability that the ISS needed. Other steps were not performed by the crew because they could be managed by MCC using ground commands. Even other steps had already been performed in the Group B powerdown that occurred after docking. The modified Group C powerdown also accommodated for the flight-specific onboard laptop configuration. Even though the procedure developed preflight was not implemented as written, it served as a great baseline that safely lowered the power level and saved time by minimizing the real-time rationalization required since the safety analysis and risk trades for that equipment had been performed preflight by the appropriate disciplines.

When the unexpected happens, such as what happened on STS-117, flight controllers and engineers will be extremely busy performing risk trades for a number of scenarios, performing tests, running models, and doing analysis. As a result, having precoordinated powerdown procedures for the most likely and most severe scenarios provides a calmer and more organized environment which maximizes the probability of quickly and safely powering down.

VII. Powerdown Procedure Development and Maintenance

The original shuttle powerdown procedures were written before the first shuttle flight. The procedures assumed two crew members per flight and relied on the predictions of the thermal models. After the fourth flight in 1982, later space shuttle missions had between four and seven crew members. Since the human body generates about 50W of heat while resting, a larger crew size meant a change in the thermal assumptions that were used to create the original powerdown procedures. Additionally, flight data existed which was able to update or verify the thermal models that were used to write the original powerdown procedures.

After the Challenger accident in 1986, there was a 2½ year gap before the next flight. NASA's Mission Operations Directorate (MOD) decided to use some of this time to perform a two-year exhaustive review of the powerdown procedures and assumptions in order to create more reliable procedures that would serve as a new baseline for the duration of the Shuttle Program. Since deactivating a piece of equipment affects many factors such as vehicle electrical load, thermal load, operability, fault tolerance, requires crew action in most cases, and sometimes has environmental affects, the review was a complicated and iterative process involving a wide range of personnel such as power and thermal analysis engineers, flight control teams across all disciplines, and astronauts who would be performing the majority of the powerdown actions.

In the example of the loss of all vehicle cooling, the vehicle has a fixed and limited amount of time where it can operate above rated thermal limits before it overheats and catastrophic consequences occur. So it is essential to invest time and resources to have good powerdown procedures ready to quickly and safely powerdown the vehicle while still allowing enough operability to powerup entry critical systems when required.

The two-year review performed after Challenger was a successful review that gave a good new baseline for powerdown procedures. As the vehicle received new upgrades and new information was learned, the powerdown procedures were continuously modified throughout the duration of the Shuttle program as time permitted.

VIII. Considerations from an Apollo Flight Controller

In an interview of former Apollo Electrical, Environmental, and Communications (EECOM[‡]) flight controller John Aaron who was heavily involved with the Apollo 13 powerdown of the command module, Aaron said they were able to powerdown the command module and move the crew into the lunar module in about 90 minutes. After Apollo 13, a procedure was written to powerdown the command module, and in these sims, they were never able to powerdown the vehicle as quickly as they were able to do it on Apollo 13 in real-time. He said that during formal mission simulations, it often took two to three hours to powerdown the command module. Aaron said, "… And it just shows you that the steps you absolutely have to do is often a shorter list than the steps you'd like to do. It's kind of the bureaucratic tax on engineering. If you've got time, you'll take time."

Aaron described the detail about how the command module powerup procedure was written. It started with all of the subsystem disciplines in a room discussing which equipment should be powered down. The room was in disagreement on a lot, so John Aaron told the room he would write down his ideas and then let everyone review them later. He and another EECOM, Jim Kelly, started working backwards by looking at which equipment needed to be on from landing to entry interface and how much time would elapse between these two events. Only when they had this first draft complete, did they allow the other subsystem experts to review their power timeline. He described this as an iterative process. Once the flight controllers had a good list of actions needed to be performed, they drafted the circuit breakers and switch throws that would be necessary for the crew to execute this powerdown and had astronaut Ken Mattingly, who had trained with the Apollo 13 crew, practice the powerup in the simulator. Mattingly would report which steps of the powerup he needed more/less time to perform and the powerup procedure was further improved.[16]

IX. Conclusion

This paper has shown, using examples from the Space Shuttle Program, that there are a variety of considerations for managing a spacecraft's electrical power level. Although it is undesirable to deviate from the well-analyzed preflight plan, this paper has shown that this is often necessary in order to ensure crew safety and a successful mission. It has shown the value of having thought through the prioritization of electrical equipment across all spacecraft systems in order to protect for unforeseen changes in mission duration due to landing weather or to expeditiously respond to system failures and changes in mission objectives, as was the case with STS-117 and Apollo 13.

Although the technologies of the Space Shuttle limited discussion of more advanced ground commanding capabilities and automated fault detection and powerdown technologies, the authors hope that future spacecraft operators will find value in lessons that were learned during this 30-year program. The most valuable of these lessons is that every situation is unique. The electrical and thermal analysis, interdisciplinary prioritization of equipment, and thorough procedure verification provide a guideline of how to proceed with a powerdown. The actual circumstances that will necessitate powering down will inevitably involve unforeseen circumstances that must be accounted for.

[‡] The Apollo EECOM systems were split up during the Space Shuttle Program. During the Shuttle program, EECOM was for Emergency, Environmental, and Consumables Manager.

Acknowledgments

The authors would like to thank the current and former members of the NASA flight control team that assisted in the editing and development of this paper especially Paul Felker, Christi Worstell, Darren Fasbender, Justin Pochynok, Mark Welch, David Randall, and Jennifer Kimball.

References

[1]Mission Operations Directorate - Spaceflight Training. "Shuttle Electrical Power Systems (EPS)." Computer-Based Trainer, NASA, Houston, 2006 (unpublished).

[2]Mission Operations Directorate. *EGIL Console Handbook.* NASA, Houston, 2007 (unpublished).

[3]Mission Operations Directorate. *Environmental Systems Console Systems Handbook.* NASA, Houston, 2008 (unpublished).

[4]Mission Operations Directorate - EECOM. "MNC UTIL OUTLET/TELEPRINTER SHORT" *Anomaly Report,* NASA. Houston, 1989 (unpublished).

[5]Mission Operations Directorate. "SECTION A10 - PL PWRDN (3,4)," *Orbit Pocket Checklist*. October 18, 2006. http://www.nasa.gov/centers/johnson/pdf/359853main_OPCL_G_M_10.pdf (accessed August 5, 2011).

[6]Mission Operations Directorate. "SECTION A11 - PRIORITY PWRDN PROCEDURES (3,4)," *Orbit Pocket Checklist*. October 18, 2006. http://www.nasa.gov/centers/johnson/pdf/359853main_OPCL_G_M_10.pdf (accessed August 5, 2011).

[7]Mission Operations Directorate. "A2-134 ON-ORBIT CRYO MARGIN BUYBACKS," *Space Shuttle Operational Flight Rules, Volume A,* NASA, Houston, 2009 (unpublished).

[8]Mission Operation Directorate. "SECTION 2 PL PWRDN - ORBIT," *STS- 117 Payload Powerdown.* NASA, Houston, 2006 (unpublished).

[9]Mission Operations Directorate. "MSG 061A - MODIFIED GROUP C POWERDOWN PROCEDURE" *Joint Execute Package Development and Integration (JEDI): STS-117/13A.* NASA, Houston, 2007 (unpublished).

[10]Mission Operations Directorate. "MSG 074A - FD08 PRE-SLEEP POWERDOWNS" *Joint Execute Package Development and Integration (JEDI): STS-117/13A.* NASA, Houston, 2007 (unpublished).

[11]Mission Operations Directorate. "MSG 103 - MODIFIED GROUP C POWERUP" *Joint Execute Package Development and Integration (JEDI): STS-117/13A.* NASA, Houston, 2007 (unpublished).

[12]Mission Control Center, *Mission Highlights.* June 5-22, 2007. http://www.nasa.gov/mission_pages/shuttle/shuttlemissions/sts117/news/status_archive_1.html (accessed August 5, 2011).

[13]Mission Operations Directorate - EGIL. "STS-117 EGIL Console Log." NASA, Houston, 2007 (unpublished).

[14]Mission Operations Directorate - INCO. "STS-117 INCO Console Log." NASA, Houston, 2007 (unpublished).

[15]Pochynok, Justin. *STS-117 EPS Consumables Analysis Postflight Report.* NASA, Houston, 2007 (unpublished).

[16]Aaron, John W., interview by Kevin M. Rusnak. *Oral History 2 Transcript.* January 21, 2000. http://www.jsc.nasa.gov/history/oral_histories/AaronJW/JWA_1-21-00.pdf (accessed August 5, 2011).