H-II Transfer Vehicle Safety Design


Courtesy JAXA/NASA

KATSUSHI SHIBATA[*1] **KOICHI MATSUYAMA**[*2]
KAZUMI MASUDA[*3] **YOICHIRO MIKI**[*1]
HIDEYUKI YAMAGUCHI[*4] **HIROSHI SASAKI**[*5]

The H-II transfer vehicle (HTV) is an inter-orbit cargo transfer spacecraft launched by the H-IIB launch vehicle. It carries both pressurized and unpressurized cargo to the International Space Station (ISS), and is used to dispose of material no longer needed at the ISS. System requirements exist for achievement of the HTV mission and safety requirements exist for each phase of HTV operations, including launch, berthing with the ISS, and atmospheric re-entry. This paper describes the safety and reliability aspects of the HTV systems, which have been part of the design right from the start of development.

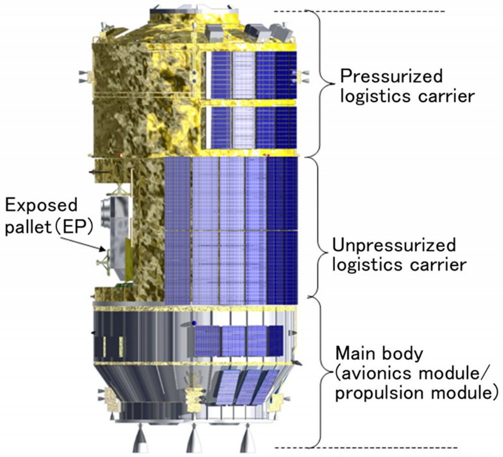
1. Introduction

After more than ten years of development, the first flight of the H-II transfer vehicle, HTV1, was launched on September 11, 2009, and HTV2 was launched on February 22, 2011 by H-IIB launch vehicles. Both missions were successful. These HTVs transported supplies and disposed of discarded goods as originally planned. Mitsubishi Heavy Industries Ltd. (MHI) was responsible for the system design, and coordinated the development of the HTV under the supervision of the Japan Aerospace Exploration Agency (JAXA). The HTV launches are planned once a year and a total of the launches will be six. Starting with the third launch, MHI is responsible for the HTV production, composed of pressurized and unpressurized logistics carriers, the avionics module, and the propulsion module.

2. HTV Configuration

Figure 1 shows a schematic diagram of the HTV.

(1) Cargo capacity for the space station
    Supplies : approximately 6,000 kg
        Pressurized cargo : Maximum 5,200 kg
        Unpressurized cargo : Maximum 1,500 kg
(2) Target orbit (space station orbit)
    Altitude : 350 - 460 km
    Angle of orbit inclination : 51.6º (circular orbit)
(3) Main specifications
    Overall length : Approximately 10 m
    Maximum diameter : Approximately 4.4 m
    Total weight : Approximately 16,500 kg
(4) Mission length
    Planned flight time : Approximately 100 hours
    Emergency standby time : Over 1 week
    Duration of stay at the ISS :
        Approximately 30 days maximum



Courtesy of JAXA

Figure 1 HTV schematic diagram

---

*1 Engineering Manager, Guidance & Propulsion Division, Aerospace Systems
*2 Guidance & Propulsion Division, Aerospace Systems
*3 Deputy General Manager, Guidance & Propulsion Division, Aerospace Systems
*4 Manager, Space Systems Engineering Department, Space Systems Division, Aerospace Systems
*5 Japan Aerospace Exploration Agency

The vehicle consists of four modules: a pressurized logistics carrier for transporting pressurized cargo, an unpressurized logistics carrier for transporting cargo open to space, an avionics module with aviation electronics function, and a propulsion module equipped with propulsion system. The combination of the avionics and propulsion modules make up the main body. This corresponds to the bus module of a satellite, where basic subsystems such as the navigation and guidance control subsystem, propulsion subsystem, communication subsystem, data handling subsystem, and battery subsystem are installed. The pressurized logistics carrier has a hatch and Common Berthing Mechanism (CBM) compatible with the ISS modules so that large items of pressurized cargo can be transferred and manned activity can be conducted in the module as it is in the Japanese Experiment Module (JEM). The unpressurized logistics carrier is the module that carries unpressurized cargo on the exposed pallet (EP). It has a large opening to insert and extract the EP as well as a mechanical system to secure the EP.

Figure 2 illustrates a typical HTV operation sequence. After the HTV is launched by the H-IIB launch vehicle, it transmits and receives data via the US Tracking and Data Relay Satellite (TDRS), and flies autonomously while determining its own position using its global positioning system (GPS). The HTV adjusts its position to the phase (orbital position) and altitude of the ISS, which orbits the Earth every 90 minutes. The HTV communicates directly with the ISS when it is in range, and stops 10 m below the ISS. The ISS manipulator then grasps the HTV and berths it with the ISS.

Pressurized cargo is transported through the hatch of the pressurized logistics carrier by the ISS astronauts while unpressurized cargo is transported after EP is opened by the ISS manipulator. When returning to Earth, unneeded equipment and waste material from the ISS are loaded into the HTV for disposal. The HTV and its contents burn up due to frictional heat during atmospheric re-entry after departing from the ISS.

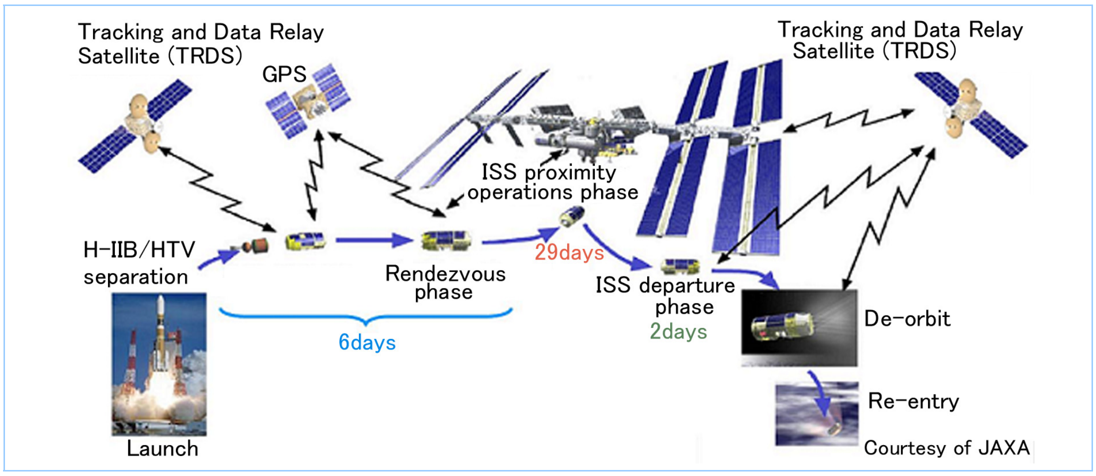


Figure 2 HTV operations sequence

3. System Design

3.1 General

The HTV mission is to transport six tons of supplies to the ISS and dispose of materials discarded from the ISS. The system is designed to be quite reliable, but it must also be capable of accomplishing its mission successfully even in the case of one fault or failure (one fail operative, 1FO). The safety requirements for each phase of HTV operations are described below.

(1) Safety in the launch area

As in the launch of conventional satellites, security of the HTV launch and operations in the launch area is necessary. A high level of safety requirement is imposed for the launch of the H-IIB vehicle to prevent death and injury of people as well as to ensure the safety of the ISS.

(2) ISS safety requirement

Because the HTV approaches and docks with the ISS that is manned system and ISS crews work in the pressurized cargo areas, the safety requirements are much more stringent than those imposed on conventional satellites. The general ISS safety requirements are as follows:

(a) Even if two failures or faults occur, they must not lead to a catastrophic hazard such as injury or death of the ISS crew or loss of the ISS (two fail safe, 2FS).

(b) Even if one failure or fault arises, it must not lead to a critical hazard such as injury of the ISS crew or damage of the ISS.

(3) Safety requirement for atmospheric re-entry

The HTV conducts deorbit maneuver after departing the ISS, re-enters the Earth's atmosphere, and burns up over the South Pacific Ocean. This raises the requirement for monitoring the final maneuvers and conducting a safety assessment in case the final maneuvers fail and HTV debris falls to Earth.

The system configuration and resource allocation were determined based on these system and safety requirements. The system configuration was designed using reliability analysis and failure mode effect analysis (FMEA) to clarify where the risks lay. Using FMEA, possible failure modes were thoroughly investigated, and the effect of a failure and the presence of single-failure points were assessed in advance. The system configuration was assessed by classifying the failure modes into three groups depending on the seriousness of the effect: loss of the ISS and its manipulator, loss of function to support the HTV and ISS mission, and performance degradation. These categories were also used to establish quality grades for the selection of parts.

Safety reviews of the resulting system design were performed at each phase of the design process in conjunction with a design review, and the review results were confirmed by JAXA. Safety aspects related to the ISS were also reviewed by the National Aeronautics and Space Administration (NASA).

3.2 System configuration

In general, double or greater redundancy was used throughout except for sub-systems such as the vehicle structure and mechanism where redundancy was not possible. This included 1FO for mission requirements and 2FS for ISS safety. A triply redundant configuration was used for functions related to ISS safety that ensures safety and detects second failure by using the third system in the redundant configuration. Sufficient design margins or safety factors were used to design for minimum risk for sub-systems where redundancy was not possible. In addition, a fracture control plan was used in the manufacture of the vehicle structure and pressure vessel, which are considered high-risk items. The various sub-systems are described below.

(1) Guidance and navigation control

The guidance and navigation control system includes one guidance control computer with three central processing units (CPUs) and two input/output (IO) controllers for self-diagnosis by majority voting, and one proprietary controller for use when aborting form the ISS. This system provides guidance control using the guidance control sensor shown in **Table 1**. Despite any combination of two failures that may occur during the approach to the ISS, safe departure from the ISS is still possible using the third set of redundant equipment. The proximity communication equipment described below measures the relative distance from and relative velocity toward the ISS. This measurement is used to assess the safety of the approach to the ISS. Even if a failure occurs during the final maneuver for re-entry, changing the system to continue the maneuver and re-enter over the designated target area is still possible.

Table 1 Guidance control sensor

Guidance control sensor	Redundancy	Remarks
Acceleration sensor (X/Y/Z)	3	
Gyroscope (pitch/yaw/roll)	3	
GPS receiver	2	Determination of location and velocity using GPS Determination of relative distance and velocity using data from the GPS receiver in the ISS
Earth sensor	2	Determination of attitude based on the center of the earth
Rendezvous sensor	2	Determination of relative distance and velocity from the ISS by an irradiating reflector on the ISS with a laser

(2) Propulsion system

(a) Thrust generation

The thrust system consists of four main thrusters for large orbit transfers and departure from the ISS, and 28 reaction control system (RCS) thrusters (14 units as a primary system and 14 units as a secondary system) for the control of translation and rotation. The thrust system also has redundant shutoff and pressure valves for 1FO/2FS purposes. The maximum load capacity of MON3/MMH propellant is approximately 2.4 tons. Primary and secondary RCS thruster systems meet the 1FO requirement during the approach to the ISS, and if both systems fail, the main thruster can be used during abort from the ISS to meet the 2FS requirement. If one of the two main thrusters fails during the atmospheric re-entry maneuvers, the other two will be activated to complete the maneuvers successfully.

(b) Propellant leakage

The HTV propellant is harmful to humans. Even if a small amount of propellant adheres to a spacesuit during extravehicular activities, it could be harmful when brought aboard the ISS. Therefore, the forward thruster near where extravehicular activities would be performed has triple valves to prevent massive leakage, and the thruster cannot be activated when crew are outside the ISS, even if two failures occur. These countermeasures also ensure the safety of the ground crew during activities at the launch area.

(c) Explosion

If the pressure in the propellant supply system exceeds the maximum design value, it could, in the worst-case scenario, cause an explosion and structural failure of the ISS, as well as injuring or killing the crew. Serially redundant regulators and shut-off valves in the upper stream are used to avoid such a situation. Furthermore, the system also includes a rupture disk. This disk blows out to prevent excessive pressure on the equipment when the internal pressure exceeds the maximum design value. For the safety purpose of propulsion system, the propellant can be disposed of if, for some reason, the HTV cannot be departed from the ISS after docking.

(3) Data handling system

The data handling system processes the command and telemetry data packets via a 1553B bus for inter-satellite and proximity communications, communication with the ISS while the HTV is berthed, and via an umbilical cable during pre-launch activity. This system performs fault detection and recovery functions for all systems except the guidance and navigation control system. It also warns of any unusual circumstances and switches between different sets of equipment when failures occur.

The data handling system consists of a primary system, a secondary system, and one emergency system that provide the minimum capability of departing from the ISS safely even when two failures occur.

(4) Communication system

The communication system consists of two types of devices: two inter-satellite communication devices for communication with ground equipment via a data relay satellite or geostationary satellite, and two proximity communication devices for communication via communication devices in the JEM. Although the proximity communication devices are used only during the approach to the ISS, heartbeat signals pass between the ISS and HTV to switch the communication devices in case of unusual circumstances. When communication cannot be established due to two failures, the approach to the ISS is aborted, and the HTV is automatically injected into a suitable safe orbit to retreat from the ISS. Although the HTV communicates with the ISS via two 1553B buses while it is docked, the proximity communication device is used as backup for second failure to meet the 2FS requirement.

(5) Electrical power system

Electrical power on the HTV includes 50-V and 120-V systems with enough redundancy to meet the 1FO/2FS requirements. **Table 2** shows how electricity is supplied in each mode. In an early design, the 50-V system had one bus because it was treated as part of the structure, but after discussion with NASA, the configuration was changed to have two independent bus bars to enable departure from the ISS if one bus failed.

Solar array panels are mounted on the body of the HTV because a deployment mechanism has the risk of failure.

Table 2 Electrical power system mode

Electrical power system mode	Contents	Remarks
Secondary battery mode	Electrical power supply from the solar array panel or secondary battery discharging. Surplus power from the solar array panel charges the secondary battery.	
Primary battery mode	Electrical power supply from the primary battery	Used when the electrical power supply from the secondary battery mode falls below the power consumption.
ISS mode	Conversion of electrical power from 120 V received from the ISS to 50 V while docked, and electrical power supply	This mode also distributes electrical power to 120-V equipment.
Umbilical mode	Electrical power supply from an external power source of the ground support equipment before launch	

(6) Thermal control system

The thermal control system keeps the temperature of the equipment and supplies in the HTV within the permissible temperature range. The heater control system is redundant so that the loss of one part would not create a hazard due to freezing or overheating of the propellant.

(7) Structural system

The HTV structural system based on minimum risk design has sufficient strength and stiffness to withstand the forces on it during ground service, launch, flight, and docking with the ISS. A debris bumper is installed to protect the HTV from space debris because the HTV is essentially part of the ISS while docked.

(8) Carrier function – Pressurized logistics carrier

The pressurized logistics carrier requires control of cabin pressure, temperature, air conditioning, and lighting. It is composed of a minimum of equipment to satisfy 1FO/2FS because part of the backup function is provided by the ISS and its crew.

Special care was taken to avoid sharp edges, pinching, electric shock, heat, and noise because the inside of the pressurized logistics carrier is used for intra-vehicular activity. A smoke detection sensor and flame retardant material are used to help prevent fires in the pressurized logistics carrier, and the power divider is mounted outside to reduce the chance of fires.

(9) Carrier function – Unpressurized logistics carrier

The unpressurized logistics carrier has facilities for removing the EP from the HTV and putting it back, and for distributing power to the EP. There is also way to separate the HTV from the ISS manipulator forcefully as an extreme action if something goes wrong when the HTV is grappled by the manipulator. The controller is doubly redundant to satisfy 1FO, and is designed for 2FS so as not to permit unexpected release of the EP or forced separation from the manipulator, even if two failures occur.

Backup by the ISS crew is possible in the case of mechanical system failure, and the equipment that the crew would require in such a case is mounted on and extravehicular activity area is provided on the external surface of the HTV. The EP is pulled in and out of the unpressurized logistics carrier on guide rails and wheels, much like a desk drawer. Wheels on the EP and solid lubrication on the wheels and rails makes the extraction and insertion processes smooth.

(10) Resources

(a) Propellant load capacity

The propellant load capacity is calculated from the ISS orbital altitude, the approach orbit, operation time, thruster operation, HTV weight, and expected disturbances. Extra propellant is loaded to meet the 1FO/2S requirements in case a second attempt is required in either the approach to or departure from the ISS. If the actual launch weight has not reached the maximum value after all the cargo is loaded, extra propellant is added to increase operational flexibility.

(b) Main batteries

Primary batteries are used to provide power to the HTV when power from the solar array panel alone is not sufficient. The electric generating capacity of the solar array panel depends on the HTV attitude and sun direction, and power consumption depends on the combined requirements of the cargo and the heating system. Therefore, the number of primary batteries required to meet the 1FO/2FS conditions was calculated, assuming the worst case of sun direction and temperature for the standard flight profile, including equipment failure and a retry of the approach to or departure from the ISS. The first flight, HTV1, carried eleven primary batteries (including for demo flight), and HTV2 and subsequent flights carried seven. The actually power consumption was less than the capacity of the batteries on board because they were selected for the worst-case scenario.

4. Conclusion

The HTV is the first large spacecraft produced in Japan that is neither a rocket nor a satellite. It was developed cooperatively with JAXA and NASA. The HTV configuration was complicated by the safety considerations required to support human space activities. Because the HTV was designed for intra-vehicular crew activities, we plan to use the knowledge and experience acquired during the HTV development to design advanced versions such as an unmanned or manned return capsule and an inter-orbit transfer vehicle for platforms other than the ISS.

References

1. Miki, Y. et al., Development of the H-II Transfer Vehicle (HTV), Mitsubishi Heavy Industries Technical Review Vol. 47 No. 1 (2010) pp.70-76