計測自動制御学会産業論文集
Vol.10, No.11, 91/99(2011)

階層化 FDIR による高安全性航法誘導制御系の提案と宇宙ステーション補給機「こうのとり」での実現

白坂成功*，堀田成紀**，蒲原信治***

Proposal of Highly Safe Guidance Navigation and Control system by Layered FDIR and Realization in H-II Transfer vehicle "KOUNOTRI"

Seiko Shirasaka*, Shigeki Hotta **, Nobuharu Kambara ***

Rendezvous technology has been developed and demonstrated through several technology demonstration missions in the world. However, high safety has to be additionally considered to use rendezvous technology as infrastructure of space activities. In this paper, layered FDIR (Fault Detection, Isolation and Recovery) is proposed to realize highly safe guidance navigation and control system for rendezvous spacecrafts. The layered FDIR can realize both mission continuity and high safety. The method to design the layered FDIR and to incorporate it into control logic is described. It is also described how this layered FDIR was implemented in HTV (H-II Transfer Vehicle) which was launched in 2009. And according to the ground verification results and HTV real flight results, the layered FDIR worked properly.

Key Words : FDIR, Safety, Guidance Navigation and Control, rendezvous, HTV

１．はじめに

これまでの宇宙開発において，あるターゲットとなる宇宙機に対して，別の宇宙機が接近するランデブという技術開発が行われてきた．日本では技術試験衛星 VII 型（ETS-VII）[1]を使った技術実証が行われた．同様に，米国においても，Orbital Express[2]によってランデブ技術の実証が行われた．このようなランデブに必要な２つの宇宙機の協調制御技術[3]そのものについてはすでに実証されたものとなった．しかしながら，これまでのランデブ宇宙機は，ランデブ技術の開発を目的としていたため，技術を実証するためのミッション達成という目標を設定し，ミッション達成を優先とした設計となっていた．このため，軌道上における耐故障機能についても，これまでの衛星開発で実証されてきたものの延長として開発されてきた．しかしながら，国際宇宙ステーション（International Space Station：以降，ISS）をはじめとするように，人類が宇宙空間に滞在し，ランデブ技術をインフラ技術として利用するためには，ミッションの達成のみではなく，高い安全性が要求される．特に，ランデブミッションでは，２つの宇宙機が衝突するという危険性があり，この衝突を避けることは，ミッションの達成と同様に重要なことである．つまり，ランデブ技術を，産業を実現するインフラ技術として利用するためには，これまでの技術実証ミッションでは完全には実現されなかった高安全性を含めたランデブ技術というものが必要である．

本論文では，これまでに実証されてきたランデブ技術に，高い安全性を組み入れる方法として階層化 FDIR（Fault Detection, Isolation and Recovery）を提案する．この階層化

* 慶應義塾大学大学院システムデザイン・マネジメント研究科 横浜市港北区日吉 4-1-1
** 宇宙航空研究開発機構 つくば市千現 2-1-1
***三菱電機株式会社鎌倉製作所　鎌倉市上町屋 325 番地
* Graduate School of System Design and Management, KEIO University, 4-1-1, Hiyoshi, Minato-ku, Yokohama, Kanagawa
** Japan Aerospace Exploration Agency (JAXA), 2-1-1 Sengen, Tsukuba, Ibaraki
*** Mitsubishi Electric Corporation, 325 Kamimachiya Kamakura, Kanagawa
(Received August 20, 2010)
TRIA 011/11/1011@2010 SICE

FDIR は，2009 年 9 月および 2011 年 1 月に種子島から打ち上げられ，ISS にランデブを行った宇宙ステーション補給機「こうのとり」（H-II Transfer Vehicle，以降 HTV）にも利用されている．本論文において，どのように階層化 FDIR を HTV の設計に取り入れたかを説明し，最後にその実証結果を示す．

２． 従来の FDIR

２．１ FDIR とは

人工衛星に代表される宇宙機は，ごく一部の場合を除いて無人のシステムとなっている．また，常に地上でのモニタが可能であるとも限らない．このため，何か故障が発生した場合においても，人間の介入が出来ないことを前提とした設計をする必要がある．特に航法誘導制御系あるいは姿勢制御系において故障が発生し，それに対して迅速な処置がとられなかった場合には，姿勢の喪失や位置のずれが発生し，その結果として通信断絶，電力確保不能などの状態に至る可能性がある．このため，軌道上で発生した故障に対して自動的に処置をするための耐故障性設計を行う．この耐故障設計において最も重要なものが自動で異常を検知（detect）し，異常の影響が広がらないように分離（isolate）し，異常状態から回復（recovery）するための FDIR（Fault Detection, Isolation and Recovery）である．

２．２ 従来型人工衛星の FDIR

従来の人工衛星では，大きく分けて 2 種類の FDIR を実装していることが多い [4), 5)]．具体的には，故障発生時に，まずは FDIR にてミッションの継続を行うことを目指すが，故障が回復できなかった場合には，人工衛星の喪失を防ぐために，通信と電力を確保する安全モードへと移行する．この場合はミッションの継続よりも衛星損失防止が優先される．また，一部の故障モードでは，ミッションの継続困難なことが明らかであるため，即座に安全モードに移行する [4)]．以下に典型的な例を示す．

環境観測技術衛星（ADEOS-II）の姿勢軌道制御系の耐故障設計では，9 種類の機器に対して，28 の故障モードを想定して FDIR を設計している．28 の故障モードのうち 3 種類の故障モードに対しては，即座に安全モードに移行するような設計となっており，残りの 25 種類の故障モードについては冗長系への切り替えによってミッションを継続するような設計となっている [4)]．

また，ADEOS-II 以前の FDIR では，通常 1 つのセンサの出力に対して，ある固定的な閾値を設定しておき，その値を超えたときに故障と断定する方法が一般的であった．たとえば，センサの出力値がある値よりも大きいことがミッションのフェーズから考えられない場合に，その値を閾値として設定しておき，センサの出力値と比較を行うことで異常を検知する．あるいは姿勢は常に一定の範囲に制御されているため，姿勢を閾値と比較することで異常を検知することが可能である．ADEOS-II では，それに追加し，通常の姿勢制御方式である定常航法と，それに GPS の信号を追加した複合航法との比較を実施している．複合航法の姿勢決定値と定常航法の姿勢決定値とを比較し，差があった場合には定常航法への切り替えをおこなっている [4)]．

通常の人工衛星では，軌道上における対有人の安全性要求のような厳しい網羅性を問われるような要求が課せられていないため，通常すべての機器を 2 冗長系用意し，識別された故障モードに対応した FDIR 機能を用意することにより主系に故障が確定した場合には従系に切り替えることを行なっている [12), 13)]．

２．３ 従来型ランデブ宇宙機の FDIR

従来型ランデブ宇宙機の FDIR として，技術試験衛星 VII 型（ETS-VII）ランデブ・ドッキング実験系の FDIR について述べる．ETS-VII は，1997 年に打ち上げられ，1998 年にランデブ・ドッキング実験を行なった．ETS-VII はチェイサ衛星である「ひこぼし」とターゲット衛星である「おりひめ」から構成されており，軌道上で「ひこぼし」が「おりひめ」を分離して，いったん遠ざかったのちに再度接近してドッキングするというランデブ・ドッキング実験を行なった．このランデブ・ドッキング実験系は，将来の有人機への自動ランデブを考慮して，２故障時でも安全性を確保する 2 Fail Safe（以降，2FS）の思想のもとでアーキテクチャが設計されている．基本的な考え方としては，2 故障発生後は，軌道を離脱して衝突ハザードが発生しないように「おりひめ」と「ひこぼし」が離れていくアボートを実施する．実際に軌道上ではスラスタの異常が発生し，FDIR にてスラスタを切り替えてアボートをする事態が発生，FDIR 機能が正常に動作することが軌道上で実証された [6)]．ETS-VII の FDIR としては，2 故障後にもアボートによって退避が可能な 3 系目を持っている点が従来の衛星とは大きく異なるところである．しかしながら，各機器の出力などに対して固定的な閾値を用意し，それとの比較により FDIR を行なっている点については，従来衛星が行なっていた FDIR と大きく異なるものではない．

３．階層化 FDIR による高い安全性の実現

前述したとおり，ランデブ技術をインフラ技術として利用するためには，これまでのミッション達成だけでなく，高い安全性も具備する必要がある．従来の FDIR は，想定される故障モードに対応した対処機能として用意されたものであるため，必ずしも十分に高い安全性を実現しているとは言えないものであった．これに対し，階層化 FDIR では，以下の２つの戦略を持った FDIR を設計することにより，高い安全性とミッション継続性の両方を実現する．

・広いハザード原因をカバー

・ミッション継続のための素早い対処

具体的には，**Fig.1** に示すように，ハザードを引き起こす原因を Fault Tree Analysis (FTA)を使って解析する．

FTA では，左側の現象は，右側の事象の結果として引き起こされると考える．つまり，Cause1 は，Cause1.1 か，あるいは Cause1.2 が発生したことにより引き起こされると考える．更に，Cause1.1 は，Cause1.1.1 か Cause1.1.2，あるいは Cause1.1.3 が発生したことにより引き起こされると考える．このため，通常は FDIR などによって，故障の根本原因（ルートコーズ）である Cause1.1.1，Cause1.1.2，Cause1.1.3 を検知し，分離し，回復する．しかし，FTA は人間が思いつく範囲で原因を洗い出したものであり，必ずしもすべての原因が漏れなく識別されているとは限らない．もし仮に左側の現象を発生する原因に識別漏れがあった場合，その漏れていた原因に対する対処が出来ておらず，その結果としてハザードが発生してしまう可能性がある．そのような予期せぬ故障モードにも対応可能なようにカバレッジを広くするため，なるべく FTA の左側の事象に対応する FDIR を用意するのが安全性の観点からは望ましい．つまり，Cause1 そのものを検知し，安全化することができれば，もし仮に Cause1 を引き起こす原因である Cause1.3 を識別できていなくても，結果として安全を保つことが可能である．しかし，一方で，FTA の右側の事象が発生して，左側の事象が発生するには通常時間的な遅れが生じる．つまり，FTA の左側の事象をベースに FDIR を構成した場合，異常に対する対応が遅い FDIR となってしまい，リアルタイム性の厳しいランデブミッションではミッションの継続自体が困難となってしまう．このため，階層化 FDIR では，ミッション継続性を確保するための早い反応を，FTA の右側の Cause に対応する FDIR で実現し，高い安全性を確保するための故障モードを広くカバーすることを，FTA の左側に対応した FDIR で実現する．Fig.1 では，この FDIR の階層を仮に３段としたが，これは FTA の階層数および FIDR をどこに実現するかに依存するため，FDIR の階層の団数については特に制約があるものではない．

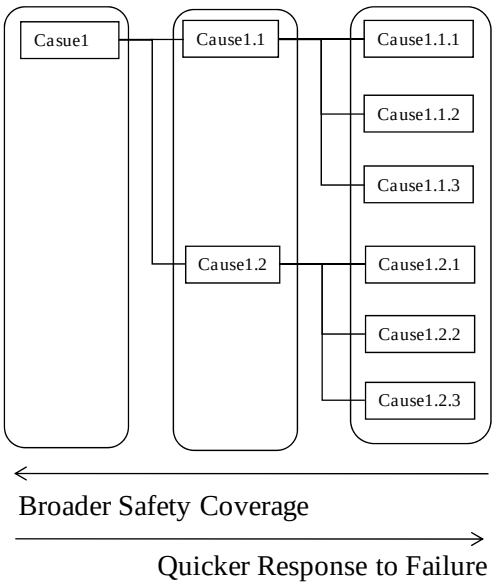

Fig.1 FTA and Layered FDIR

つぎに，この階層化 FDIR を制御系に組み込むための方法を示す．前述したとおり，FTA の右側の事象の結果として，左側の事象が発生する．つまり，右側ほどプリミティブな情報であるといえる．たとえば，宇宙機の姿勢の場合を考える．姿勢は，角速度を計測するジャイロデータを積分することで求めることができる．姿勢が異常になっているかどうかを確認する場合に，ジャイロデータの積分を利用した姿勢角で検知することが可能であるが，ジャイロデータそのものが異常であると，この計算された姿勢角そのものが間違ったものとなる．このように異常なデータを利用しないために，あるデータを使って処理する場合には，そのデータが異常でないかどうかを確認することを行い，異常のないデータを使って処理する必要がある．つまり，FTA で右側にある FDIR を実施し，異常がないことを確認した上で，そのデータを処理して，より左側の FDIR に利用するということになる．これを模式的に表現すると，**Fig.2**(a)コンセプトに示すようになる．ここでの FDIR のレベルは Fig.1 に示したものに対応する．上述したジャイロの場合での具体的な例を Fig.2(b)に示す．まず，ジャイロセンサと搭載計算機は定期的に通信を行っており，規定の通信時間以内にデータ取得ができるかどうかの FDIR を行っている．この通信チェック FDIR 処理で問題ないと判断されたデータのみがつぎの処理であるデータ工学値変換処理へと渡される．このデータ工学値変換処理では，センサから渡される 16 進数のデータを工学的な意味のある数値である規定時間（１周期）当たりの角度変化へと変換される．この角度変化量は，スラスタ推力範囲と慣性質量から範囲が計算される．この範囲外にある場合はセンサが故障していると考えられる．このようなチェックをデータ範囲 FDIR で行う．データ範囲 FDIR で問題なければ，工学値変換された値と現在の姿勢から姿勢推定処理を行う．この推定結果を元に現在の姿勢が異常かどうかの確認（姿勢異常 FDIR）を実施する．姿勢が正常であれば，姿勢制御のための制御量を演算するという流れとなる．

この階層化 FDIR を実際に HTV に適用した．４項ではどのように HTV に適用したかを具体的に示す．

４．階層化 FDIR の HTV への適用

４．１ HTV とは

階層化 FDIR の HTV への適用を説明するために，まず HTV について説明を行う．HTV 全体システムは，H-IIB で打ち上げられ，ISS へ接近していく HTV フライトセグメント，ISS の「きぼう」日本実験棟に設置してある近傍通信システム（Proximity Communication System : PROX）と反射器(レーザレーダリフレクタ)，および HTV を運用するために筑波宇宙センターに設置されている HTV 運用管制室から構成される．

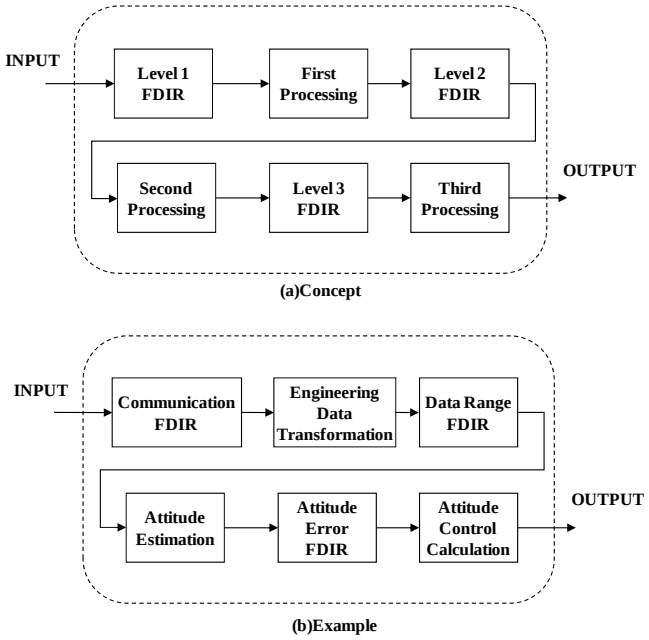

Fig.2 Data Processing using Layered FDIR

HTV フライトセグメントは「補給キャリア与圧部」，「補給キャリア非与圧部」，「曝露パレット」，「電気モジュール」，「推進モジュール」の 4 つのモジュールから構成されている [7]（**Fig.3**）．

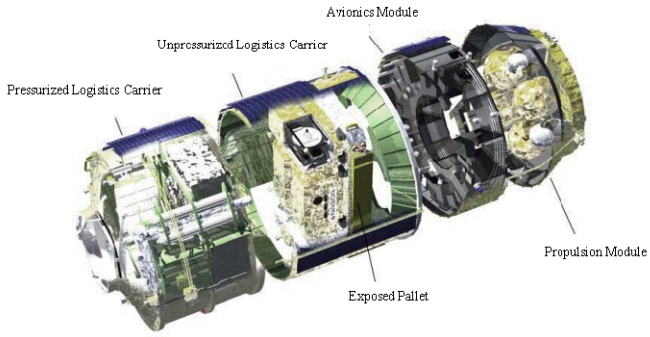

Fig.3 Construction of HTV Flight Segment（HTV1Press Kit[7]）

航法誘導制御系の機器は，電気モジュールに搭載されている．

４．２　HTV の運用

HTV は，H-IIB で打ち上げられた後，GPS 絶対航法と，HTV 地上運用管制設備からコマンドとして送られた ISS のステートベクタを基に差分航法を行い，ISS への接近を行う．この期間をランデブフェーズと呼ぶ．

ISS へ十分に接近した後には，ISS の「きぼう」に搭載された PROX と HTV とが直接通信を行う．この期間を近傍運用フェーズと呼ぶ．近傍運用フェーズでは，PROX に搭載された GPS 受信機で得た GPS 衛星のデータ（GPS データ）を直接 HTV に伝送し，HTV では PROX から受信した GPS データと，HTV で計測した GPS データを利用して GPS 相対航法をおこなう．得られた GPS 相対航法結果を用いて，近傍運用フェーズでは基本的に搭載自動シーケンスにより ISS への接近を行う．GPS 相対航法によって ISS 下方 R バー上 500m の点（RI 点）まで飛行する．

RI 点に到着した後は，ランデブセンサ（レーザセンサ）を使用して，「きぼう」に取り付けられたレーザレーダリフレクタとの相対距離と相対姿勢を計測しながら規定されたコリドー内を ISS へ接近する．HTV は「きぼう」の下方約 10m 付近のキャプチャー点に到達すると自動で相対的に停止する．

キャプチャー点において，相対位置・姿勢の確立が確認されたのち，ISS クルーによって，制御停止コマンド（フリードリフトコマンド）が送信される．HTV はこのコマンドを受信すると，すべての並進制御および姿勢制御を停止する．この状態において，ISS クルーは ISS のロボットアーム（SSRMS）を使って HTV を把持（キャプチャー）する．その後，ISS の「ハーモニー（Node2）」の地球側共通結合機構に結合され（Fig.4），補給キャリア非与圧部にある船外実験機器などおよび補給キャリア与圧部にある船内用物資が運ばれる．

Fig.4　HTV attached ISS（NASA’s Picture）

ISS からの離脱時は，クルーが SSRMS により HTV を ISS 下方約 10m の地点まで移動させ，その後リリースを行う．リリースされた後，ISS クルーにより送信される離脱開始コマンドによって HTV は制御を開始する．HTV は規定された離脱コリドー内を移動し，最終的には ISS から十分に遠ざかった後，地上からのコマンドにより再突入のための一連のマヌーバを実施する．

以上のような運用において，HTV が ISS に接近しているフェーズ，特に近傍運用フェーズでは，計画されたタイミングで計画されたマヌーバを行い，接近を続けることがミッションの成功のために必須となる．このため，たとえ故障があ

っても，なるべく即座にその故障から復帰し，ノミナルの運用を継続することが必要となる．実際，HTV に課せられたミッション要求は 1 Fail Operative（1FO）というもので，1 故障あるいは 1 回の運用ミスがあってもミッションが継続できることである．

４．３　HTV 航法誘導制御系

HTV には，ISS における有人安全性要求が適用されている[8), 9)]．具体的には，ISS の損失や ISS クルーの致命的な怪我などのカタストロフィックハザードに対しては，2 故障もしくは２回の運用ミス，またはそれらのいかなる組み合わせによっても発生させないということが要求となっている．これを 2 Fail Safe（2FS）要求という．HTV が ISS に衝突して ISS ならびにクルーを損失してしまうことが最大の危険（ハザード）と認識されており，この「衝突ハザード」に対する 2FS 要求が航法誘導制御系に課せられた最も大きな要求のひとつである．更に，上述したとおりミッションに対して 1FO 要求がある．これら２つの要求を満たすように HTV の航法誘導制御系のアーキテクチャは構成されている．　HTV 航法誘導制御系を構成する機器を **Table 1** に示す．また全体構成を **Fig.5** に示す[8),10)]．

Table 1 Construction of HTV Guidance Navigation and Control System

Component Name	Acronyms	No.
Rendezvous Flight Software	RVFS	1
Guidance Control Computer /Abort Control Unit	GCC/ACU	1
GPS/INS System	SIGI	3
GPS Antenna Subsystem	GPSL/GPSF/GPSS	2
Rendezvous Sensor	RVS(RVSE/RVSH)	2
Earth Sensor	ESA(ESE/ESH)	2
SIGI/RVS DC/DC Converter	SIGI/RVS-PC	3
Valve Drive Electronics	VDE	3

航法誘導制御系としては，各種センサが計測したデータを基に，GCC/ACU 上のランデブフライトソフトウェアが航法誘導制御の計算を行い，その結果に従ったスラスタの駆動信号を，VDE を経由して推進系のバルブに出力するという処理の流れを持つ．ここでは，以降の説明に必要な範囲において簡単に説明を行う．HTV 航法誘導制御系の詳細については，参考文献８）に詳しい．

（１）誘導制御計算機のアーキテクチャ

誘導制御計算機は GCC（Guidance Control Computer）と ACU（Abort Control Unit）の 3 種類の計算機より構成される．更に，GCC の内部は，3 つの CPU と 2 つの入出力制御器（I/O Controller : IOC）から構成され，内部冗長の構成をとっている．Fig.5 においては，左側の点線で描かれた長方形で示されている．

（２）搭載ソフトウェアのアーキテクチャ

搭載計算機の GCC/ACU には，4 種類のソフトウェアが搭載されている．RVFS（Rendezvous Flight Software），CPU OS，IOC OBS（Onboard Software），ACU OBS（Onboard Software）である．GCC の CPU 部で実行される RVFS は飛行中の航法誘導制御機能を実行するソフトウェアであり，ノミナル時の航法誘導制御に関わる処理を行う．CPU OS は，CPU 部において RVFS を実行する OS として機能する．IOC OBS は，通常は GCC の外部の機器と RVFS と間でのデータのやり取りを処理しているが，CPU が故障した際には IOC 側で対処処置を実行する．ACU OBS は通常は特にミッション上必要な処理は行なっていないが，GCC が故障した際には安全化を行う処理を有している．Fig.5 においては，左側の点線で描かれた長方形内で色付きの長方形で示されている．

（３）バルブ駆動回路（VDE）と推進系のアーキテクチャ

アクチュエータ機能は，VDE とスラスタなどの推進系から構成される．アクチュエータ機能は，ノミナル運用に対して 2 冗長系，安全に対して 3 系冗長系の構成となっている．ノミナル運用に対する 2 冗長系は，GCC 内の IOC より駆動信号を受ける VDE1（A 系および B 系），RCS スラスタ（14 基の A 系および B 系），およびメインスラスタ（4 基）から構成される．上記２系故障時にも安全に退避できるように，ACU より駆動信号を受ける VDE2 とメインスラスタ（4 基）で 3 系目を構成している．Fig.5 においては，右下の点線で描かれた長方形で示されている．

（４）航法誘導制御系センサのアーキテクチャ

HTV 航法誘導制御系のセンサとして，SIGI(Space Integrated GPS and INS)と呼ばれるジャイロ/加速度計/GPSR の 3 つのセンサを統合した機器，RVS（Rendezvous Sensor），ESA（Earth Sensor Assembly）が使用されている．
SIGI 内に含まれたジャイロと加速度計は 3 冗長構成となっているが，SIGI 内の GPSR，RVS，ESA はそれぞれ 2 冗長系構成となっている．Fig.5 においては，右上の点線で描かれた長方形で示されている．

上述してきたように HTV では対有人システムにおける安全性要求である 2FS 要求と，タイムクリティカルな運用を実現する 1FO 要求という 2 つの大きな技術要求がある．これに対応するため，HTV 航法誘導制御系では階層化 FDIR を利用することでこれらの要求を実現した．

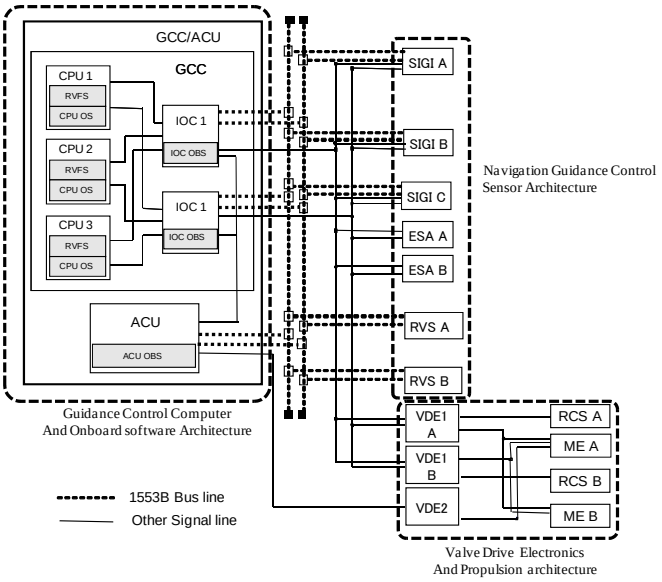

Fig.5 System Block of HTV Guidance Navigation and Control System

４．４　HTV での階層化 FDIR

HTV の航法誘導制御系は，当初より安全性とミッション継続性を考慮した設計を行なってきた．このため，HTV 航法誘導制御系では，FDIR の設計に対して階層化 FDIR というコンセプトを適用した．

安全設計を行うためには，ハザード事象を引き起こす原因（Cause）を識別するために Fault Tree Analysis（FTA)を行った．実際の FTA の一部を簡略化したものを **Fig.6** に示す．Fig.6 では，最下層の故障としては便宜上，故障モードとして１，２という表現をとっているが，実際にはセンサの種類コントローラ，アクチュエータに対応してより多くの故障モードが存在している．

前述した通り，異常に対して素早く対処するために FTA の右側の Cause に対して FDIR を行う必要がある．

HTV では，個々の機器においてすでに存在がわかっている故障モードについては，FTA の右側をカバーする形で「単体 FDIR (Component FDIR)」を実装した．単体 FDIR とは，「機器単体の情報により行う FDIR」ということを意味している．たとえば，機器のアウトプットがあり得ないほど大きな出力となったり，急激に変化したり，あるいは絶対に一定にならないようなときに一定値となってしまうような故障モードは古くから知られており，こういった故障モードをカバーするために用意された FDIR である．この FDIR は Fig.1 と Fig.6 においては最も右側の Cause をカバーするための FDIR であり，Fig.2 では Level1 FDIR に当たるものである．これまでの宇宙機では，この単体 FDIR のみを実装していた．HTV では，各機器の未知の故障モードについては機器間の「比較 FDIR (Comparison FDIR)」によってカバーした．この比較 FDIR は，複数の機器の情報を比較して行う FDIR である．通常，複数の機器の情報を比較できるようにするために，何らかの処理を行ったのちに，その処理結果を比較する．更に，姿勢の異常や加速度の異常など，状態として異常とみなせる事象については，「状況に基づく FDIR(Condition Based FDIR)」として実装した．この比較 FDIR と状況に基づく FDIR は，Fig.1 と Fig.6 においては真ん中の Cause をカバーするための FDIR であり，Fig.2 では Level2 FDIR に当たるものであるまた，たとえば，推進系の微小なリークなどについては，即座に加速がでているとは確認できないため，増速の過不足を即座に判断することが困難である．こういった状況をカバーするために，最終的には軌道自体をチェックして衝突軌道に入っていないことを確認する最終の FDIR（Safety Net FDIR）を用意した．この FDIR は Fig.1 と Fig.6 においては最も左側の Cause をカバーするための FDIR であり，Fig.2 では Level3 FDIR に当たるものである結果的に，この Safety Net FDIR を用意したことで，どのような異常事象であれ，Safety Net FDIR で使用しているデータが正常であれば検知が可能な頑健性の高い FDIR を実装することができた．

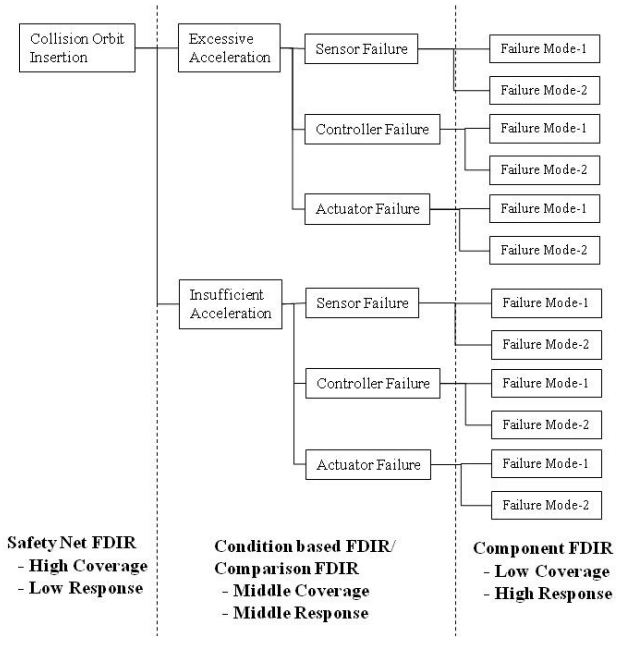

Fig.6 FTA of HTV

上記の階層化 FDIR を，航法誘導制御系の処理に組み入れた状態を **Fig.7** に示す．比較 FDIR は，センサの出力値が正常であって初めて意味があるものである．したがって単体 FDIR をパスしたデータのみが使われるべきである．また，状態に基づく FDIR は，状態の認識にセンサデータを使用するため，単体 FDIR と比較 FDIR をパスしたデータを使うこととなる．同様に上位の Safety Net FDIR は単体 FDIR と比較 FDIR をパスしたデータを使用する．つまり，各階層を確実に動作させることが重要である．

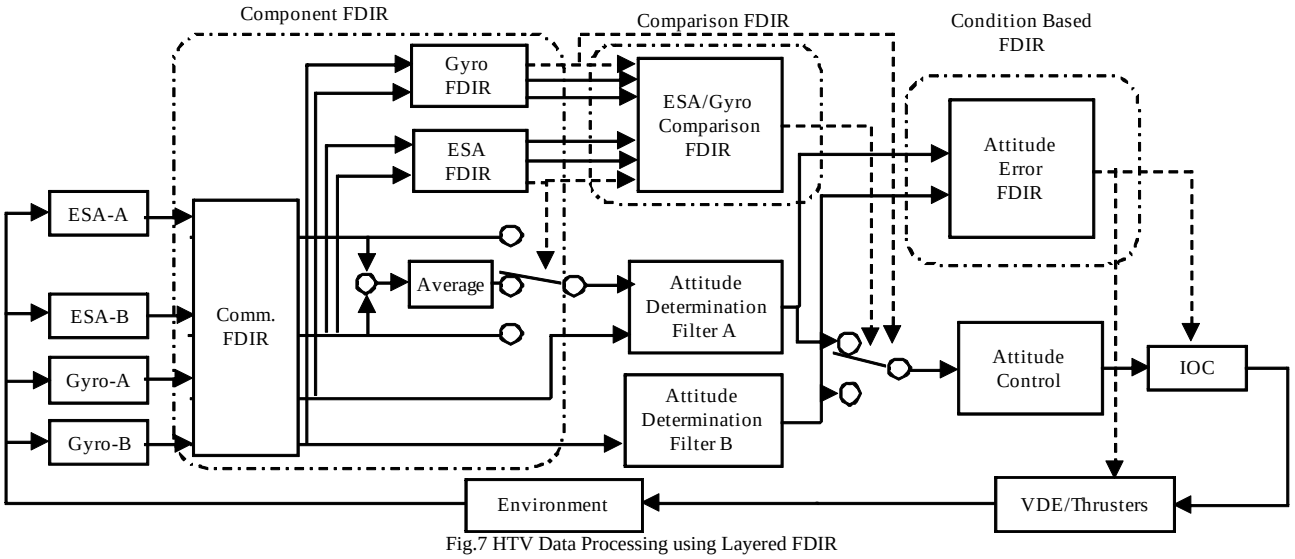

Fig.7 HTV Data Processing using Layered FDIR

ジャイロについては 2 系を同時に動作させている．単体 FDIR を実施するとともに，ESA2 系をふくめて，4 系での比較 FDIR を実施している．また，クリティカルなフェーズではジャイロの 3 系目を使用することで，より確実に正常なセンサを使用できるようになっている．ジャイロも ESA も，１系が故障しても 2 系目があるため，ミッションの継続が可能である．また 2 系目が壊れた場合にはアボートを実施する．アボート時の姿勢制御は，ジャイロあるいは ESA の正常な一方を使用することで行う．

５． 適用結果

５．１ 地上検証の結果

HTV 航法誘導制御系では，階層化 FDIR を利用したために，多くの FDIR を持つこととなった．このため，計画的な検証活動が必要であった [8]．

HTV 航法誘導制御系については，段階的な検証・インテグレーションを繰り返すことで検証を行なった．

搭載ソフトウェアはハードウェアや環境をソフトウェアでシミュレーションし，ソフトウェア総合試験を実施した．これとは並行にハードウェアは製造試験にて検証を行った．搭載ソフトウェアおよびハードウェアを個別に検証した後に，両者の組み合わせ試験として SCLT（Static Closed Loop Test）を，更にセンサなどコンポーネントを接続した DCLT（Dynamic Closed Loop Test），DOLT（Dynamic Open Loop Test）を実施した．SCLT において GCC/ACU および 3 種類のソフトウェアの機能について十分に検証した後に，DCLT にてジャイロ，ESA，RVS に関わる部分の検証を行なった．また DOLT にて GPSR に関わる部分の検証を行った．

前述したような多彩な FDIR を実装しているが，機器の故障のタイミングおよび故障の種類は多数あり，その組み合わせについては無数にあるともいえる．そこで **Fig.8** に示すような試験ケース設定ツリーを用意し，故障発生時のイベント（運用のフェーズ），故障モード，故障の発生タイミング，故障が発生している成分（X,Y,Z）およびエラーケースの組み合わせの中から安全上のリスクの高いものを選択して試験を実施した．

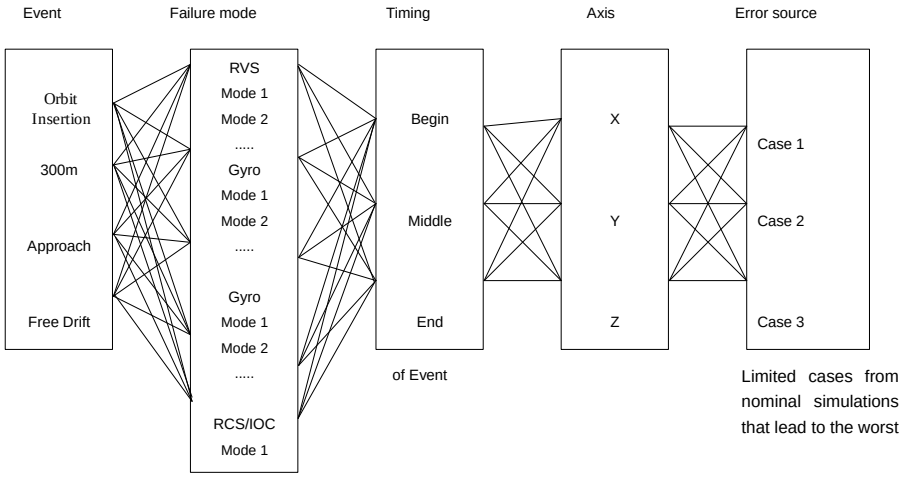

Fig.8 Development of Test Case Setting

その結果，500 ケースを超える試験を実施することとなったが，最終的にはすべての FDIR を検証することができた．例えば，故障発生時のイベント（運用のフェーズ）として最終接近の開始マヌーバ時に，故障モードとして SIGI-A に含まれているジャイロで故障が発生し，故障の発生タイミングとしてはマヌーバの開始時点であり，故障が発生している成分は X 軸周り（つまりロール）であり，エラーケースとしてはジャイロ出力が一定となるような故障モードの組み合わせ時において，故障したジャイロを使われることなく，正常なジャイロデータを使ってマヌーバが正常に終了することが確認できるような試験を実施している．これは単体 FDIR としてのジャイロ FDIR の検証にあたる．また，ジャイロの故障モードとして，単体 FDIR にかからないレベルの異常データによる試験も実施した．この場合には，他のジャイロおよび ESA との比較 FDIR にて検知が行われており，比較 FDIR の検証にあたる．また，スラスタの異常が発生するが，単体 FDIR，比較 FDIR,状況に基づく FDIR のいずれにも検知されない試験ケースを設定し，軌道がずれることによって最終的には Safety Net FDIR にて検知される試験ケースを設定することにより，Safety Net FDIR の検証も実施した．

５．２　軌道上実証結果

HTV は，2009 年 9 月 11 日に種子島宇宙センターから H-IIB ロケットによって打ち上げられた．打ち上げ後は順調に ISS への接近を行い，9 月 18 日に ISS に搭載されたロボットアームによりキャプチャーされ，同日 ISS に結合された（**Fig.9**）．その後，10 月 31 日に ISS から切り離され，離脱を行ったのち，11 月 2 日に大気圏再突入を行い，ミッションを終了した．このミッション期間中，何度か FDIR が動作する機会があったが，いずれも安全性およびミッション継続性を損なうことなく適切に動作している．たとえば，参考文献 9)にも示されているとおり，再突入前日に３つの CPU がエラー表示となる事象が発生したが，これは単体 FDIR および比較 FDIR が設計通りに動作することで HTV の制御を失うことなく，その後の復帰を行うことが可能となった．軌道上においては Safety Net FDIR にかかるような異常は発生しなかった．

６．　まとめ

これまでは技術実証のレベルであったランデブ技術を，実用レベルにするために必要な新たな耐故障機能として階層化 FDIR を提案した．この階層化 FDIR は実際に HTV の航法誘導制御系に利用され，地上検証および軌道上実証で正常に動作していることを示した．

HTV は，ISS が運用されている限り打ち上げられることが決まっており，今後も毎年約 1 機のペースで打ち上げられることとなっている．今回提案した階層化 FDIR は今後の HTV にも利用される予定である．特に，スペースシャトルの退役後，HTV は ISS プログラムにおいて重要な役割を担うこととなる．

更に，宇宙が単なる技術開発から，実用的な産業になるためには，実際の利用のために必要な安全性の確保は重要な項目である．その点でも，今回提案する階層化 FDIR は宇宙の産業化に必要な技術であると考えられる．

Fig.9 HTV before Capture (NASA’s photo)

謝辞

本論文の執筆にあたり貴重なご助言を頂きました慶應義塾大学大学院システムデザイン・マネジメント研究科　狼嘉彰教授に感謝いたします．

参考文献

1）河野，小田，稲葉：ランデブ・ドッキング技術開発の将来展望；計測と制御，Vol.38，No.11，pp.710-712 (1999)

2）Geoffrey C. Hintze et al:AVGS,AR&D for Satellites, ISS, the Moon, Mars and Beyond, Proceeding for AIAA Infotech @ Aerospace 2007 Conference and Exhibit, AIAA2007-2883 (2007)

3）木田隆，山口功：宇宙機の相対運動とその制御－ランデブおよびフォーメーション；システム制御情報学会誌，Vol.49，No.6，pp.229-236 (2005)

4）小島寧, 棚町健彦, 狼嘉彰: 環境観測技術衛星（ADEOS-II）搭載姿勢軌道制御系（AOCS）の対故障設計，；宇宙技術, Vol.3, pp49-58 (2004)

5）As’ad Michael Salkham: Fault Detection, Isolation and Recovery (FDIR) in On-Board Software, Master’s Thesis Charlmers University of Technology (2005)

6）河野功, 杢野正明, 鈴木孝, 小山浩, 功刀信: ETS-VII ランデブ・ドッキング実験の結果；日本航空宇宙学会論文集, 2 Vol.50, No.578, pp.95-102 (2002)

7） HTV-1 ミッションプレスキット: 宇宙航空研究開発機構 (2009)

8）蒲原信治, 鈴木雅晴, 渡部大輔他: HTV 航法誘導制御系における安全設計とその検証； 第 51 回宇宙科学技術連合講演会 (2007)

9）今田高峰, 植田聡史: HTV 誘導制御システムに対する CBCS 安全要求の適用について； 宇宙ステーション講演会 有人宇宙飛行技術シンポジウム講演集 , pp17-20 (2008)

10）青木英剛, 白坂成功, 津屋　直紀他: HTV アビオニクス開発； 第 50 回宇宙科学技術連合講演会 (2006)

11）宇宙ステーション補給機（HTV）技術実証機の国際宇宙ステーション（ISS)離脱及び再突入結果について: 宇宙航空研究開発機構 (2009)

12）福田　盛介, 水野　貴英, 坂井　真一朗, 福島　洋介, 斉藤宏文: れいめい（INDEX）衛星における統合化衛星制御； 航空宇宙学会論文集, Vol.57, No.660, pp.25-31 (2009)

13）Josian Fabrega, Michel Frezet and Jean-LouisGonnaud: ATV GNC During Rendezvous； Proceedings Third International Conference on Spacecraft Guidance, Navigation and Control System, pp.85-93 (1996)

14）Seiko Shirasaka, Taichi Nakamura, Takafumi Chiba, et al. : Architecture of H-II Transfer Vehicle’s Guidance & Control Computer； AIAA Visiting Vehicle Conference (1999)

[著者紹介]

白坂　成功（正会員）

1994 年東京大学大学院工学系研究科宇宙工学専攻修士課程卒業．同年三菱電機株式会社入社．2010 年より慶應義塾大学大学院システムデザイン・マネジメント研究科　准教授　専門は，宇宙工学，システムエンジニアリング．

堀田成紀

1993 年，東京大学大学院工学系研究科宇宙工学専攻修士課程修了．同年三菱電機株式会社入社．現在，宇宙航空研究開発機構　有人宇宙環境利用ミッション本部 HTV プロジェクトチームに出向．専門は，制御工学，軌道力学，運用管制．

蒲原信治

1995 年東京大学大学院工学系研究科修士課程修了．同年三菱電機株式会社入社．

宇宙ステーション補給機(HTV)の開発等に従事．現在，宇宙システム部制御技術課 専門は航空宇宙機の飛行力学，最適制御．