第 1 章

本手法による不具合分析の実践と評価

1.1 概要

不具合分析の具体的な流れをみるために，いくつかの事例を取り上げて実践した結果を示す．以下では，まず実際に故障箇所特定が行えた事例を取り上げる．その結果に関して，コマンドを選択する際に優先する指標を変えることによって検証プロセスが異なることを述べ，評価指標に関する考察を行う．次に，故障箇所の特定を上手くできなかった事例を取り上げ，そこから得られた知見に関して述べる．最後に，本手法によって扱うことのできる故障の種類に関する限界を述べ，発展させるために必要な方針に関して議論を行う．

1.2 実践例

1.2.1 故障箇所の特定ができた例（ヒータの接触不良）

まず，以下の図 1.1 のような故障を考え，不具合分析を行っていく．

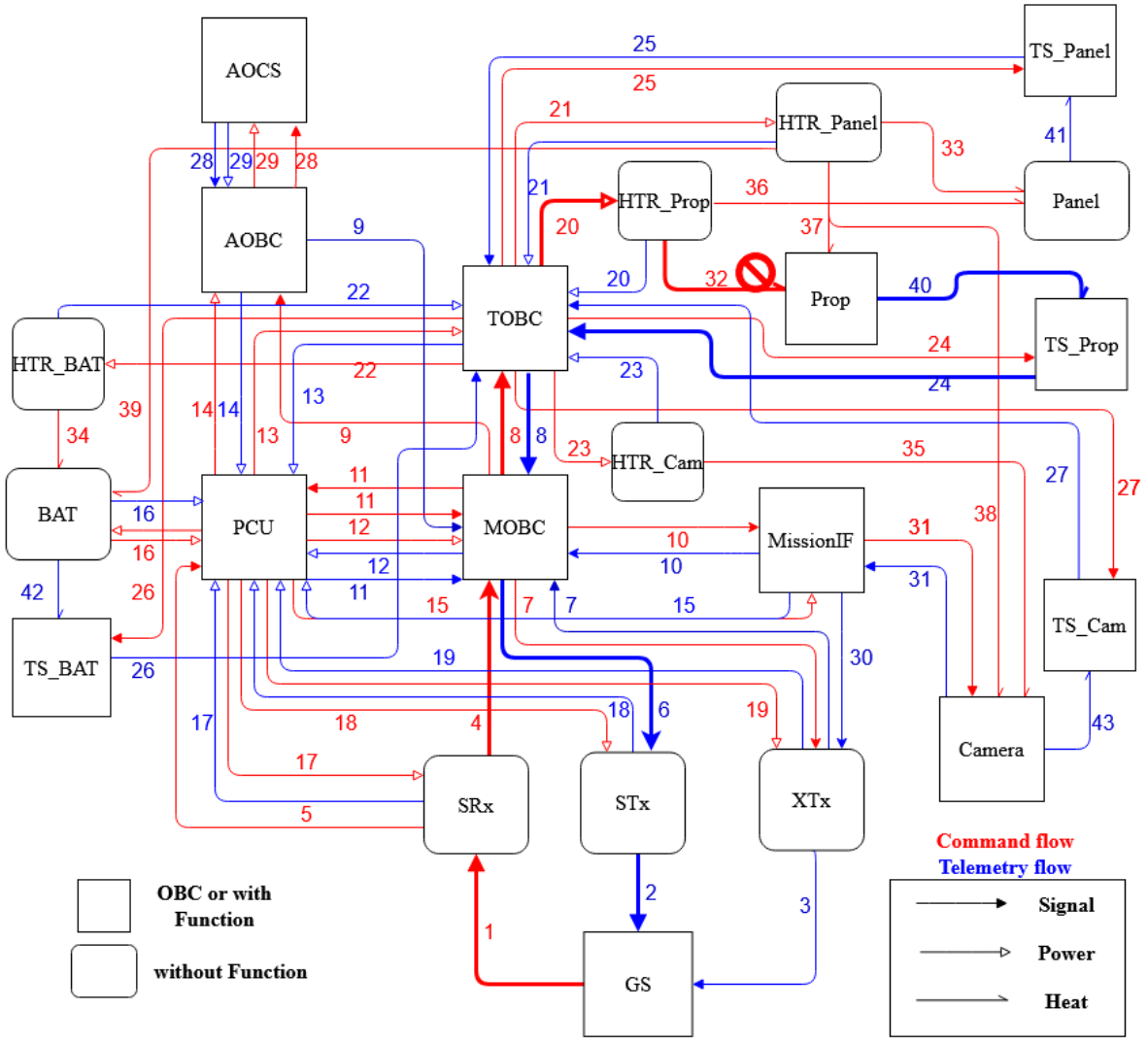

図 1.1　故障箇所：リンク 32(推進系ヒーター推進系間) の時の故障候補

図 1.1 に示すような推進系ヒータ - 推進系間でのヒータ接触不良が発生している場合を考える．この時，異常検知の際の不具合事象としては，

- 推進系ヒータ ON コマンド (ID:14) を送信したのに，推進系温度 (ID:17) が上昇しない

という事象である．

ここで，本手法では前章で述べたように衛星内部コンポーネントの初期状態として，送信したコマンドによってもたらされる状態変化が起こっているものとして与えている．そのため，不具合事象の際に送っているコマンド「推進系ヒータ ON」によって，推進系ヒータは電源 ON 状態であると仮定し，以下の検証用コマンドの探索を行っていることを述べておく．

以下に，この事象に本手法を適用した例を示す．まず，図 1.2 に故障候補の決定及び，テレメトリ情報を用いた確認の段階を示す．故障候補の決定では，不具合事象を検知するきっかけとなったコマンドとテレメトリが形成する経路を探索し，targetTEL，targetCOM として提示している．

その後，時間変化するテレメトリ情報を用いて確認できる故障候補を提示し，返ってくるテレメトリが正常 (OK) か否 (NG) かを入力させることで，切り分けを行っている．今回の例では MOBC 及び TOBC は正常に動作しているはずなので，MOBC カウンタ及び TOBC カウンタは正常 (OK) と入力し，それを元に状態の更新を行っている．

```
targetTEL: [40, 24, 8.0, 6.0, 2.0]
targetCOM: [1, 4, 8, 20, 32]
TELtarget: [40, 24, 8.0, 6.0, 2.0]
Telemetry 1 ( MOBC_Counter ) can verify following links
 [6, 2]

Please check MOBC_Counter
Input result(OK or NG)>>OK
TELlink: [6, 2] were verified
TELtarget: [40, 24, 8.0]
Telemetry 2 ( TOBC_Counter ) can verify following links
 [8]

Please check TOBC_Counter
Input result(OK or NG)>>OK
TELlink: [8] were verified
```

図 1.2　テレメトリによる確認

次に，図 1.3 に示すのが，不具合発生時に送信していたコマンド情報から考えられるテレメトリの変化を用いて故障候補の確認を行う段階である．今回は，初期コマンドとしては異常検知の際に送ったコマンド (推進系ヒータ ON) のみを考えている．確認可能性の高い経路を形成するテレメトリから順に表示され，人間に確認をさせているのが分かる．ここでの確認テレメトリに関しても，今回の例では正常であるため，そのように入力し状態の更新を行っている．

```
 Check telemetries which influenced by initial Command state

Command 14 ( HTR_PROP_ON ) & Telemetry 5 ( MOBC_COM_Counter ) can verify following links
 COMlink: [4, 1] TELlink []
Command 14 ( HTR_PROP_ON ) & Telemetry 6 ( TOBC_COM_Counter ) can verify following links
 COMlink: [8, 4, 1] TELlink []
Command 14 ( HTR_PROP_ON ) & Telemetry 10 ( TOBC_Current ) can verify following links
 COMlink: [8, 4, 1] TELlink []
Command 14 ( HTR_PROP_ON ) & Telemetry 16 ( PANEL_Temp ) can verify following links
 COMlink: [20, 8, 4, 1] TELlink []
Command 14 ( HTR_PROP_ON ) & Telemetry 21 ( HTR_PROP_Current ) can verify following links
 COMlink: [20, 8, 4, 1] TELlink []

Please check MOBC_COM_Counter
Input result(OK or NG)>>OK
COMlink: [4, 1] & TELlink: [] were verified

Please check TOBC_COM_Counter
Input result(OK or NG)>>OK
COMlink: [8] & TELlink: [] were verified

Please check PANEL_Temp
Input result(OK or NG)>>OK
COMlink: [20] & TELlink: [] were verified
COMtarget: [32] TELtarget: [40, 24]
```

図 1.3　初期コマンドを用いた確認

最後に，以下の図 1.4 に示すのが，上記の流れを経て残った故障候補を確認できるコマンドを探索し，

指標と共に提示した結果である．残った故障候補は，

- コマンドリンク 32:推進系ヒータ - 推進系間
- テレメトリリンク 40:推進系 - 推進系温度計間
- テレメトリリンク 24:推進系温度計 - TOBC 間

である．この時，探索結果として表示されたのはコマンド 13(パネルヒータ ON) と 18(推進系ヒータ OFF) であり，これらのコマンドに関する指標が図 1.4 のように示されている．
図中において Pm(C) が「平均確認可能性」，E(C) が「確認可能リンク数」，N(C) が「検証コマンド総数」を表している．またコマンドの衛星生存性への副作用を示す指標に関しては，Remain Power が「コマンド送信前のバッテリ残量」，Power Consume「コマンド送信による消費電力」，Impacted TEL num が「コマンドによって影響を受けるテレメトリの数」，Attitude が「姿勢変化を起こすか否か」を示している．Attitude に関しては，姿勢変化を起こす場合は”Change”，起こさない場合は”Keep”と表示するようにしている．

```
COM 13 HTR_PANEL_ON
         Pm(C): 0.5 , E(C): 1.0 , N(C): 2.0
         Remain Power: 3.8 , Power Consume: 2 , Impacted TEL num: 8 , Attitude: Keep
COM 18 HTR_PROP_OFF
         Pm(C): 0.25 , E(C): 0.75 , N(C): 1.875
         Remain Power: 3.8 , Power Consume: -1 , Impacted TEL num: 6 , Attitude: Keep
```

図 1.4　コマンドの選択肢表示及び検証過程

以下の図 1.5 に，探索されたコマンドに関して各コマンドを選択し検証を行ったプロセスを示す．どちらのコマンドから開始しても最終的に，今回想定した故障箇所である「推進系ヒーター推進系間 (リンク ID:32)」が故障箇所であると特定された．

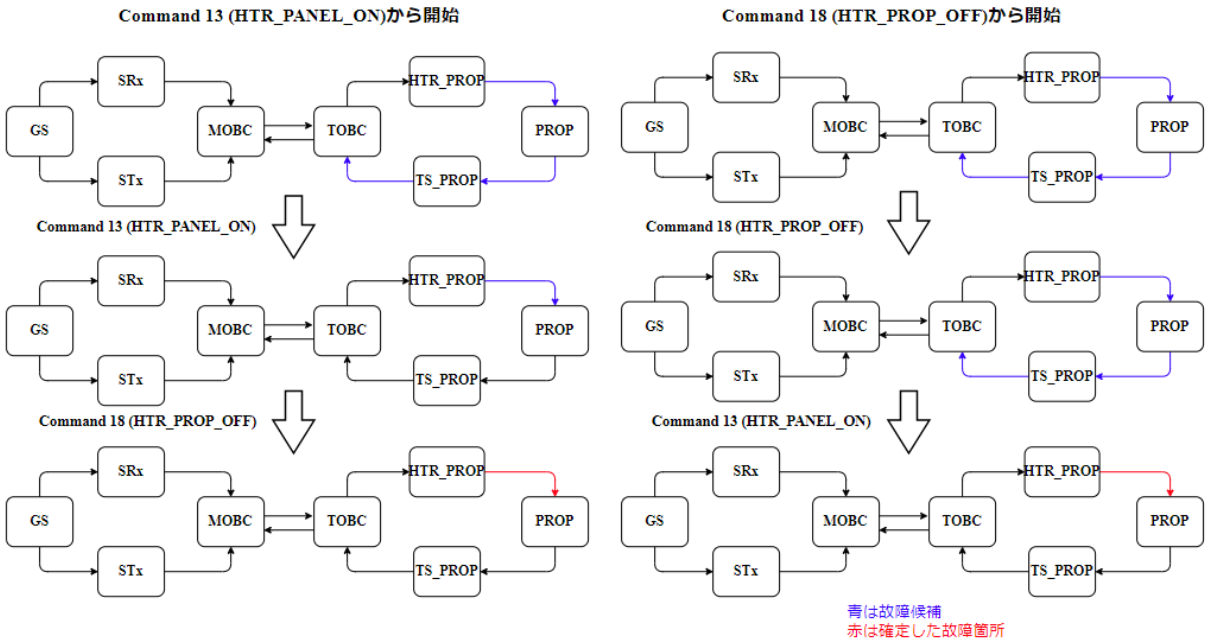

図 1.5　ヒータ接触不良時の各検証プロセスの流れ

1.2.2　評価指標に関する考察

上で示した例 (ヒータ接触不良) に関して，コマンドを選択する際に優先する評価指標によって図 1.5 のように検証プロセスの違いが生じた．この結果の違いに基づき，提示された評価指標が持つ意味を考察する．

図 1.4 にあるように提示された 2 つのコマンドを比較すると，「平均確認可能性」はパネルヒータ ON コマンド (13:HTR_PANEL_ON) が高く，「検証コマンド総数」は推進系ヒータ OFF コマンド (18:HTR_PROP_OFF) が小さくなっている．パネルヒータ ON コマンドから検証を開始した場合，初めに「推進系－推進系温度計間 (テレメトリリンク 40)」,「推進系温度計－ TOBC 間 (テレメトリリンク 24)」の正常が確認できており，1 つのコマンドによる確認で故障候補が 1 つのリンクにまで絞り込めている．最終的に，推進系ヒータ OFF コマンドを送信した際に推進系温度の変化が見られなかったことから「推進系－推進系温度計間 (テレメトリリンク 32)」の異常が確認でき，故障箇所を特定している．
一方で，推進系ヒータ OFF コマンドから検証を開始した場合，1 つ目の検証では推進系温度に変化が見られず，状態変化を確認できないため，故障候補の切り分けをすることができない．一方で，故障候補の中に確実に故障箇所が存在することを確かめることができる．次に，2 つ目のコマンド「パネルヒータ ON」で推進系温度の上昇を見ることができるため，先程のプロセスと同様の切り分けができ，故障箇所の特定ができている．

運用時，通信が不安定であり不具合分析に使える時間が明確でない時には一度のコマンドで多くの確認ができることが望ましい．そのため，図 1.4 において「パネルヒータ ON」コマンドから送信する検証プロセスが良いと言える．これを元に考えると，平均確認可能性が高いコマンドから送ると，一回のコ

マンドで多くの絞り込みが行える可能性が高いと言える．より厳しい時間制約の際には，最後まで検証作業を行うことができるという保証はない．そのため，平均確認可能性が高いコマンドを優先的に選択して各コマンドによって得られる切り分けの効果を大きくすることが望ましい．

一方で検証コマンド総数が小さなコマンドを優先的に選択した場合，少ないコマンド数で絞り込みを行える可能性があるが，この指標はあくまで，故障箇所を特定するまで検証を行うことを前提としてコマンドの数を計算している．そのため，故障状態によっては見積もられた数以上のコマンドを送信する必要があり，時間制約が厳しいときには十分に絞り込みを行えないまま検証作業を終えることになる．このことを踏まえると，検証コマンド総数は不具合分析を最後まで行うことができる保証がある時に，優先的に考えることで，全体で打つコマンドの数を少なくできる可能性があると言える．

1.2.3 本手法と人間の不具合不具合分析の違い

上で示した不具合事象「推進系ヒータ ON コマンドを送った時，推進系温度が変化しない」に関して，想定した故障状態に関する情報を与えずに不具合分析を行う際の過程（送信するコマンド，コマンドを選択する理由，確認するテレメトリ）を不具合分析の経験が豊富な本研究室の先輩方に伺った．
与えた情報としては，以下に示す通りであり，コマンドやテレメトリが通る経路や，コマンドが影響を及ぼすテレメトリに関する情報は与えなかった．

- 衛星システムのコンポーネントの接続関係図
- システムを構成するコンポーネント及びその電源状態
- コマンド及びテレメトリの定義情報（何の機能を持つコマンドなのか，テレメトリに含まれる情報）

質問内容は以下であり，コマンドによる不具合分析を始める段階からの意思決定を対象にしている．

- 不具合分析を開始する際に初めに送信するコマンドとその理由
- 初回の検証で何のテレメトリ情報を確認するか
- 上で送信した結果が正常もしくは異常であった場合に次に選択するコマンド及びその理由
- 2 回目の検証で何のテレメトリ情報を確認するか

以下の図 1.6 に，初回の検証で選択するコマンドの調査結果を示す．本手法で検証用コマンドとして提案された 2 つのコマンド「推進系ヒータ OFF(HTR_PROP_OFF)」と「パネルヒータ ON(HTR_PANEL_ON)」を選択している人が半数以上を占めていることから，今回の問題設定では本手法による検証用コマンドの探索は人間の推論に近いと言える．また，提示された選択肢以外のコマンドを選択する人が一定数いたが，これらを選択した理由を見ると，これらのコマンドによって回答者が確認しようとしている事項は既に確認しているとして問題を設定していたため，問題での前提条件に対する認識の違いによるものであった．また，それらの回答者に関しても 2 回目のコマンド選択では，「パネルヒータ ON」を選択しており，検証用コマンドとして本手法による探索と同じような推論を行っていると言える．

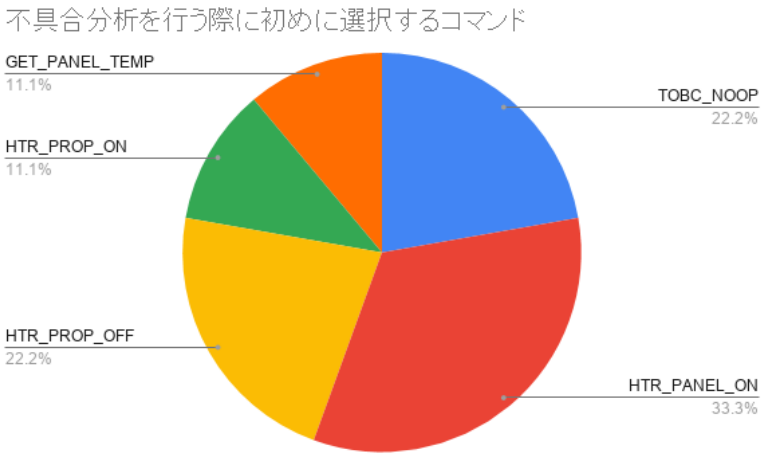

図 1.6　不具合分析時に初めに選択するコマンドの調査結果

また，このコマンドを選択した理由を見ると，「パネルヒータ ON」コマンドを送る人は積極的に故障候補の絞り込みを行う目的で選択しており，「推進系ヒータ OFF」コマンドを送る人は，故障していると考えられる推進系ヒータに通電を続けるのが危険であると考え，安全を考慮してこのコマンドを選択していた．本手法でコマンドの安全性を示す指標として提示するものは，電力と姿勢による制約からくるものと，状態をどれだけ変化させるかという点から提案を行っていた．しかし，不具合発生時に故障箇所が含まれている可能性があることを考えると，そのままの状態を保持することが危険であるという考え方もできる．そのため，安全状態に戻すという視点での指標の提案が必要であると考えている．
また，状態を不具合発生前の状態に戻すコマンド「推進系ヒータ OFF」は同時に，故障候補を検証可能なコマンドであることが分かる．人間による不具合分析ではこのことを意識せずに，故障候補切り分けのための情報を見逃してしまうことも多い．本手法を用いることで，このコマンドも検証用コマンドとして提示することで切り分けのために必要な情報を見逃すことを防ぐことにつながる．

次に，初回の検証結果が異常であった場合に次に選択するコマンドに関して以下の図 1.7 に調査結果を示す．初回に選択するコマンドが本手法で提案したものと一致していたのに対し，次に選択するコマンドは大きなばらつきが見られた．こちらに関しても，これらのコマンドを選択した理由を見ると，故障候補の特定よりも二次故障の発生を防ぐために安全を考慮してコマンドを選択した場合や，故障候補をより網羅的に洗い出したことによる検証プロセスの違いであることがわかった．
前者に関しては，上述したように不具合状態を保持することによる危険を考えており，本手法では扱うことができていない概念である．また後者に関しては，本手法では故障候補の洗い出しは不具合発生時のコマンドとテレメトリが通る経路のみに限定しているが，不具合分析経験が豊富な人による推論では，コマンドによる状態変化を起こすための電力供給源を考えた場合や，コンポーネントの機能単位の回路の故障を疑ったものが見られた．実際の不具合発生時では，このようにコンポーネント間の接続関係だけでない機能間のつながりや，状態変化によって発生する波及効果によって他のコンポーネントに影響を与えることも考えられるため，より網羅的な故障仮説の生成に取り組む必要があると考えている．

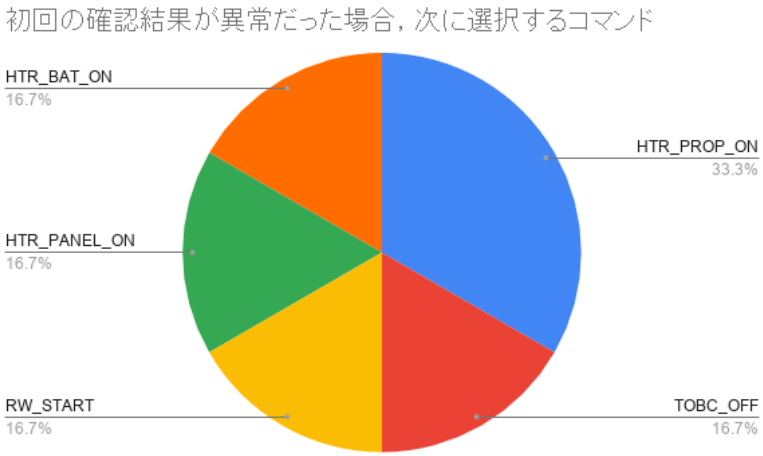

図 1.7　初回の検証で確認したテレメトリが異常であった場合

また，本手法による故障箇所特定は単一故障を前提としたアルゴリズムとなっていたが，複数故障を考慮した分析を行う人も見られた．その場合，安全なコマンドを評価するためには全ての故障候補の組み合わせの場合の数だけコマンドによる影響を考慮する必要がある．それらの組み合わせに対して波及効果までを考え，安全性を評価できるのは人間の強みであると言える．一方で，このように多くの候補を考えることは多くの知識と経験を要する作業である．経験の少ない人物が安全性の評価を十分に行うことを支援するために，複数故障を考慮した検証作業に関しても考慮する必要があることが分かった．

1.2.4　温度計故障に関する検証

次に，以下の図 1.8 に示すような温度計故障（断線）を考え検証を行った例に関して述べる．この時，異常検知の際の不具合事象としては，上の事例と同じく

- 推進系ヒータ ON コマンド (ID:14) を送信したのに，推進系温度 (ID:17) が上昇しない

という事象である．テレメトリの確認や，初期コマンド状態からの確認情報の提示の流れは先ほどの例と同様となる．

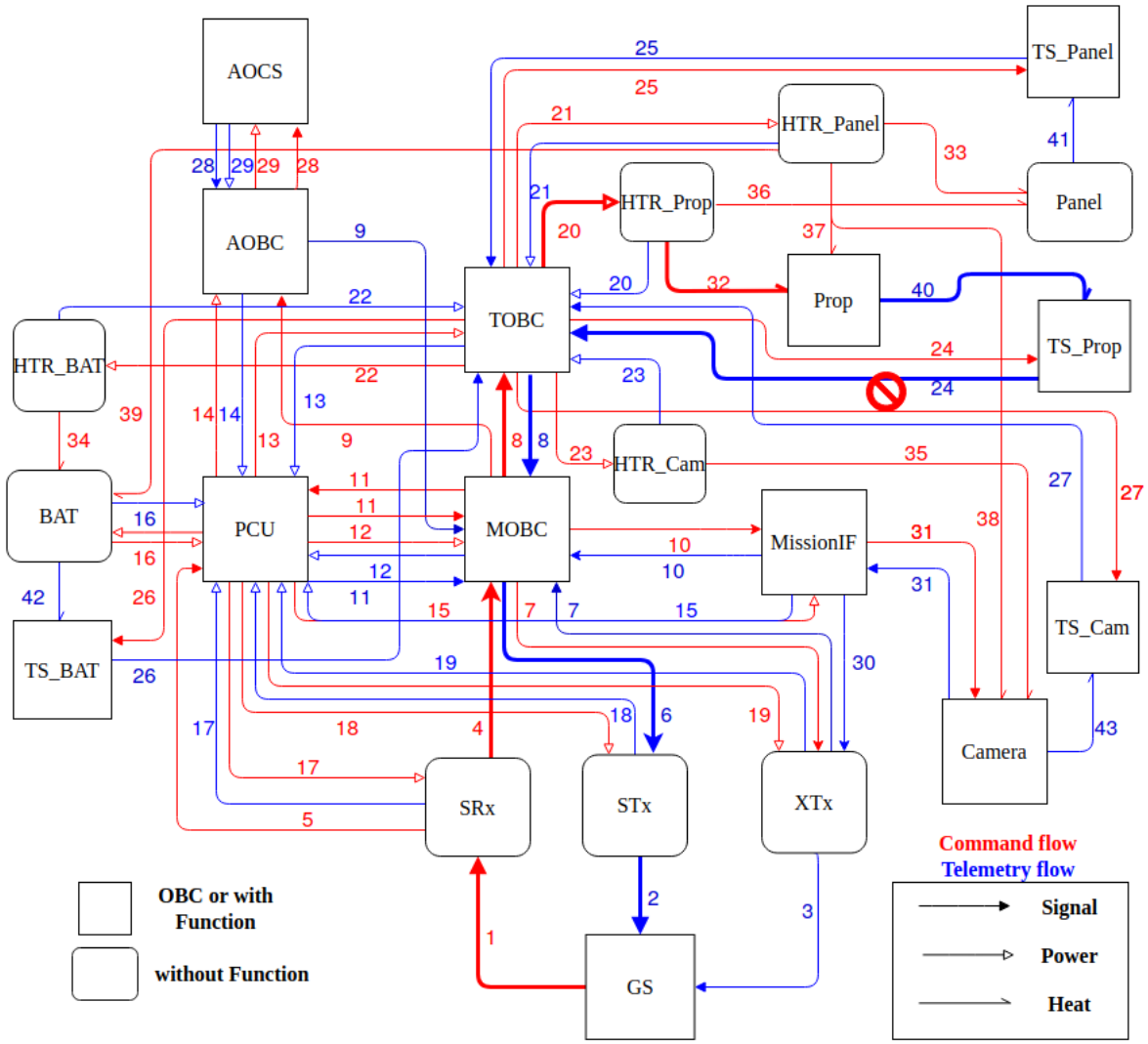

図 1.8　故障箇所：リンク 24(推進系温度計-TOBC 間) の時の故障候補

この時，システムによって洗い出された検証用のコマンドは上の例 (図 1.4) のものと同じであり，どちらのコマンドから検証を始めても結果は同じで以下の図 1.9 のようになった．今回の不具合は温度計の断線であるため，パネルヒータによる推進系温度の変化も推進系ヒータによる推進系温度変化も見る

ことはできないため，提案されたコマンドによって推進系温度計に変化は見られず，異常テレメトリとなる．そのため，どちらのコマンドによる検証でも切り分けを行うことができず，故障箇所の特定を行うことができなかった．このことから，この衛星の設計では今回扱った故障「(推進系) 温度計故障」が発生した際に，本手法を用いて故障特定を行えないことが分かる．

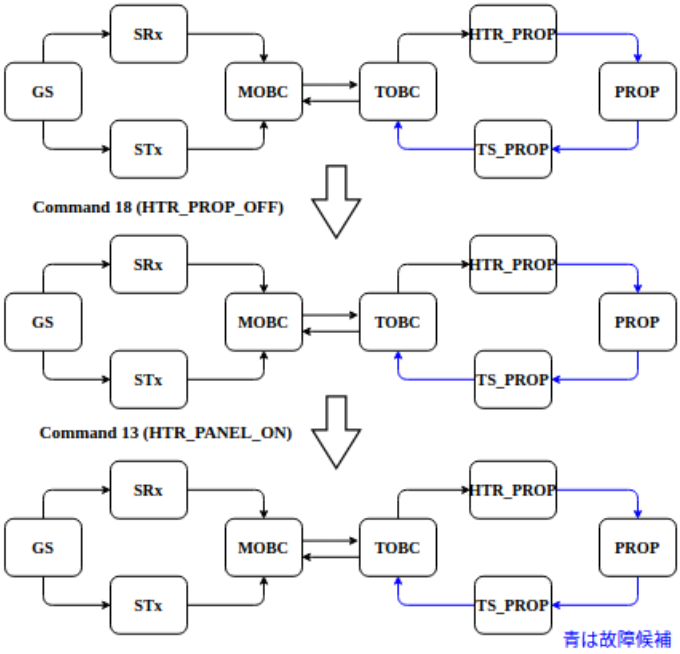

図 1.9　温度計故障時の検証の流れ

一方で，不具合分析の過程で得た情報を用いた人間の推論を組み合わせることで故障箇所を特定することは可能である．まず，今回の事例では，TOBC から推進系ヒータへの電源供給ライン（コマンドリンク 20）が正常であることは「推進系ヒータ電流値」によって確認できており，同時に「パネル温度」の上昇によってヒータが正常に作動していることも確認できるため，推進系ヒータの故障ではないことが切り分けられる．

また，「パネルヒータ ON」によって推進系温度の変化を見ることができなかったことから，「推進系ー推進系温度計間」か「推進系温度計ー TOBC 間」のいずれかに確実に故障箇所があることが推測できる．よって，温度計自体の故障か，TOBC の温度計読み取り回路のどれかが故障していると判断することが可能である．

このように，本システムのみでは故障箇所の特定が行えなかった場合においても，提示された選択肢に従って検証を行うことによって，故障箇所を推論するために必要な情報が取得可能であることがわかる．

また，人間の推論を組み合わせても故障箇所の特定が行えなかった場合には，設計の不備を考えることができる．衛星の地上試験及び軌道上での運用では，基本的には本手法のようにコマンドとテレメトリでのやり取りによって人間との通信を行う．そのため，これらの情報を用いて不具合分析が行えるような，コンポーネントの接続関係，コマンドやテレメトリの設計を行う必要がある．本手法を設計段階

の衛星に対して適用することによって，衛星システムとして不具合発生時の検証能力が十分であるかを確認することが可能である．

実ミッションでは，設計段階において FMEA(Failure Mode and Effect Analysis) などを用いて，衛星システムに起こりうる故障モードを列挙し，それらの故障モードによる影響や，発見のしやすさなどを考え，設計の正しさを確認する．この過程において，FMEA 上で洗い出された故障モードに対して本手法を適用することによって，それぞれの故障モードが発見可能な設計になっているかを確認することができる．