衛星内の情報伝達経路モデルに基づく不具合分析支援に関する研究

2020 年 12 月 01 日　　03-183005 西本 慎吾

概要

近年，大学や高専などの教育機関や，民間企業による超小型衛星の開発，およびそれを利用した事業の展開が盛んになっている．一方で，超小型衛星の信頼性の低さが問題となっている．軌道上故障に関する調査の結果信頼性の低さの原因として，設計および製造過程における不良が多いことが分かっており，地上試験によって不具合の改修，対策を十分に行うことが重要である．しかし，衛星のような複雑なシステムでは，一つの不具合事象に対して多くの故障が考えられ，不具合事象から故障箇所の特定を行うことは非常に多くの知識と経験を必要とする．そこで，本研究ではコンポーネント間の接続関係モデル，情報伝達経路モデルを用いて衛星の故障候補の検証手順（打つべきコマンド，確認事項）を探索し，それらをコマンドの安全性及び，故障候補切り分け能力を示す指標と共に提示することで，不具合分析を支援する手法を提案する．本手法を用いて，簡易的な衛星モデルに対して不具合分析を実践することで，コマンドによる故障箇所の特定作業が体系化できること，設計不備の発見につながることを確認した．

1　序論

1.1　研究背景

超小型衛星開発に大学などの参加が増加している中，信頼性の低さが問題となっている [1)]．軌道上故障の調査の結果，衛星の故障原因の多くは設計・製造過程にある [2)] ことが分かっており，それらの多くは地上試験によって確認することができるものであるという調査結果が出ている [3)]．

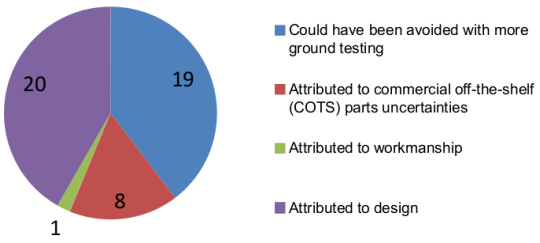

図 1　超小型衛星の故障原因に関する調査結果 [2)]

1.2　問題提起

以上より，地上試験での不具合分析が不十分になっていることが，超小型衛星の信頼性の低さの原因の一つである．地上試験での不具合分析を十分に行うためには以下の 2 点の作業に高い知識と経験が必要とされる．

- 故障仮説生成
- 故障箇所特定

まず，故障仮説の生成は FTA(Fault Tree Analysis) などを用いて不具合事象から考えられる故障モードを網羅的に洗い出す．衛星は内部機器の物理的相互作用が複雑に絡み合っているため，人による思い付きでは網羅的に行うことは困難である．

また，故障箇所の特定は衛星から得られる情報を元に衛星の安全を確保しながら行う必要がある．実ミッションで使用するコマンドとテレメトリは膨大な数であるため，その中から切り分けを行うための情報を選択し，仮説の検証を行う作業は無駄やヒューマンエラーを生むきっかけとなる．

これらの課題に対して，下表 1 に示すように，故障候補の洗い出しを網羅的に行う研究が盛んにおこなわれている．一方で，不具合分析の大きな課題の一つである検証過程に関して取り組んだものは少ない．

表 1　不具合分析手法の比較

手法	故障網羅性	手法の目的
GDE	低	故障仮説生成
GDE+ [4)]	中	故障仮説生成
網状故障解析 [5)]	中	異常モード洗い出し
故障オントロジー [6)]	高	故障仮説生成
本手法	中	故障箇所特定支援

1.3　本研究の目的

以上より，衛星の故障箇所を特定する作業を体系化し，不具合分析経験の少ない人が十分に不具合分析を行える様に支援することが必要である．よって，本研究では以下の機能を満たす不具合分析手法の提案を目標とする．

- 故障候補を確認するためのコマンドおよびテレメトリを提案する．
- 上のコマンドに対して優先度と共に提示する．

また上記の機能を実現するために，本手法は以下の 3 点から構成されている．

- 衛星内部機器の接続関係モデル及び情報伝達経路モデル
- 故障箇所の特定を行うために必要なコマンド及びテレメトリの探索アルゴリズム
- コマンドの安全性及び，故障候補切り分け能力を示す指標

2　情報伝達経路モデルに基づく対話的不具合分析手法の仕様

2.1　不具合分析アルゴリズム

本手法による不具合分析の流れを下図 2 に示す．本研究の対象は色付けているところであり，人間と対話的に故障箇所の特定を行う．これにより 実機の情報をシステムに反映しながら故障箇所を絞り込むことができる．

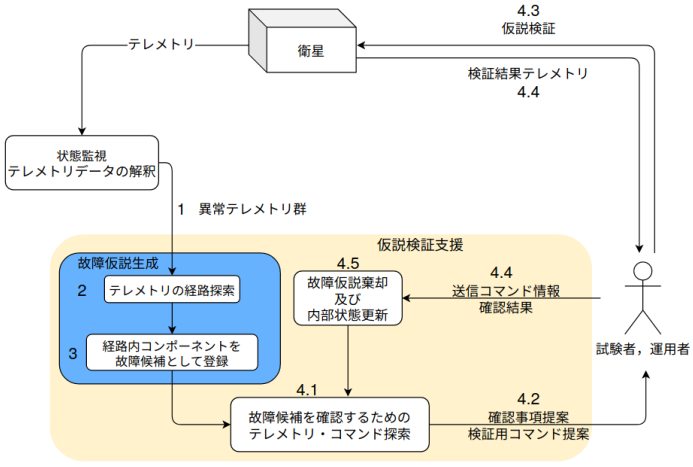

図 2　本手法による不具合分析の流れ

2.2　モデル

上述したアルゴリズムで故障個所の特定を行うために使用するモデルに関して以下に示す．

2.2.1　コンポーネント間接続関係モデル

來村ら [7] は拡張デバイスオントロジーとして，機器間の接続関係を「ポート」と「導管」という概念を用いて表現している．これを元に，コンポーネントの接続関係を表す「リンク」(表 2) を定義した．各リンクには正常確率を属性として持ち，これを用いて後ほど述べるコマンドの故障候補切り分け能力を定量化している．また，表 3 のように各コンポーネントがリンクを属性として持ち，コマンドの情報伝達で使用するリンク (コマンドリンク) とテレメトリの情報伝達で使用するリンク (テレメトリリンク) を区別している．

表 2　リンク定義

ID	Link_name	Compo1	Compo2	Medium	Probability
19	PCU-XTx	PCU	XTx	Power	0.5
20	TOBC-HTR_PROP	TOBC	HTR_PROP	Power	0.5
21	TOBC-HTR_PANEL	TOBC	HTR_PANEL	Power	0.5
22	TOBC-HTR_BAT	TOBC	HTR_BAT	Power	0.5
23	TOBC-HTR_CAM	TOBC	HTR_CAM	Power	0.5
24	TOBC-TS_PROP	TOBC	TS_PROP	Signal	0.5
25	TOBC-TS_PANEL	TOBC	TS_PANEL	Signal	0.5
26	TOBC-TS_BAT	TOBC	TS_BAT	Signal	0.5
27	TOBC-TS_CAM	TOBC	TS_CAM	Signal	0.5
28	AOBC-AOCS	AOBC	AOCS	Signal	0.5
29	AOBC-AOCS	AOBC	AOCS	Power	0.5
30	MIF-XTx	MIF	XTx	Signal	0.5
31	MIF-CAM	MIF	CAM	Signal	0.5
32	HTR_PROP-PROP	HTR_PROP	PROP	Heat	0.5

表 3　コンポーネント定義

Component	Com_linkID	Tel_linkID
GS	1	
MOBC	7,8,9,10,11	6
PCU	11,12,13,14,15,16,17,18,19	11
TOBC	20,21,22,23,24,25,26,27	8
AOBC	28,29	
MIF	31	30
XTx		3,7
STx		2
SRx	4,5	

2.2.2　情報伝達経路モデル

以下の表 4,5 のようにコマンドおよびテレメトリを定義した．それぞれ情報伝達の経路を上述のリンクによって表現している．また，コマンドの属性として「影響を与えるテレメトリ」及び「種別」を定義している．これらによって，コマンドが起こす状態変化を表現し，内部状態の更新を行っている．

また，テレメトリのモデルでは，テレメトリが変化するトリガの種類を指定しており，これによって故障箇所特定に必要な情報取得のために取る行動を決めることができる．ここでは簡単のため，軌道運動などによる状態変化は考慮せず，時間とコマンドだけによる状態遷移を考えている．

表 4　コマンドモデル

ID	CommandName	impact_TEL_ID	type	path				
19	HTR_CAM_OFF	5,6,10,18,22	ACTION	1	4	8	23	35
20	HTR_BAT_OFF	5,6,10,19,23	ACTION	1	4	8	22	34
21	AOCS_ON	5,7,11,25	ACTION	1	4	9	29	
22	AOCS_OFF	5,7,11,25	ACTION	1	4	9	29	
23	RW_START	5,7,11,26	ACTION	1	4	9	28	
24	RW_STOP	5,7,11,26	ACTION	1	4	9	28	
25	M_DATA_DOWN	5,8	GET	1	4	10	31	
26	GET_PANEL_TEMP	5,6	GET	1	4	8	25	

表 5　テレメトリモデル

ID	TelemetryName	TransitionTrigger	path				
10	TOBC_Current	Command	13	11	6	2	
11	AOBC_Current	Command	14	11	6	2	
12	MIF_Current	Command	15	11	6	2	
13	SRx_Current	Command	17	11	6	2	
14	STx_Current	Command	18	11	6	2	
15	XTx_Current	Command	19	11	6	2	
16	PANEL_Temp	Command	41	25	8	6	2
17	PROP_Temp	Command	40	24	8	6	2

コマンドおよびテレメトリの機能モデルでも状態量の更新に関して説明するために必要．

2.3　評価指標の提案

本手法の対象は地上試験における支援であるが，不具合分析に利用する情報の粒度がコマンドとテレメトリのみであるため，軌道上不具合発生時の故障箇所特定にも利用可能である．そこで，以下では地上試験及び軌道上での運用時の両方で重要となる指標を提案し，本手法が両状況で使い分け可能なフレームワークであることを示す．

2.3.1　コマンドの衛星生存性への副作用

まず，生存への副作用を示す指標として，以下の 3 点を与える．

- コマンドを打つ前の電力状態と，コマンドを打つことによって発生する電力消費量
- 姿勢変化を起こすか否か
- コマンド送信によって変化するテレメトリの数

前者 2 点の電力と姿勢による制約から来る指標は運用時に特有のものであり，コマンドを打つことで衛星の安全を脅かすことがないように危険な動作を明示的に示すことで，未熟な運用者による誤ったコマンド送信を防ぐ目的がある．また，不具合発生時は衛星の状態に対する把握が不十分であるため，衛星の状態を大きく変化させるコマンドは危険であるといえる．そのため，コマンドによって発生する状態変化の大きさを定量的に示す指標として 3 点目の指標を与えている．

2.3.2　コマンドの故障候補切り分け能力

運用時は可視時間が限られており，その時間内に不具合の改修を行わなければミッション失敗につながるような，時間制約を考慮した不具合分析を行う場面が考えられる．その際には，少ないコマンド数で効率的に故障個所の特定を行えることが望ましい．

まず，一つのコマンドで切り分けられる故障候補の数を表す指標に関して述べる．以下の図 3 に示すような故障候補 (太矢印) がある場合を考える．あるリンク (l_i) の状態を確認するためにはその経路 (R_j) 内にある他のリンクが正常である必要がある．よって，

$$P(l_i|\mathrm{R}_j) = \prod_{m\in\mathbb{F}_j, i\neq m} P(l_m = \mathrm{normal}) \qquad (1)$$

の確率でリンク l_i を確認できる．ここで $\mathbb{F}_j$ は R_j 内の故障候補リンクの集合，$P(l_m = \mathrm{normal})$ は上述した各リンクの正常確率を表している．$P(l_i|\mathrm{R}_j)$ はコマンドが形成する各径路すべてに対して求まるのでそれらの最大値を取りコマンド (C_k) による l_i の確認可能性は

$$P(l_i|\mathrm{C}_k) = \max\{P(l_i|\mathrm{R}_j)\} \qquad (2)$$

となる．

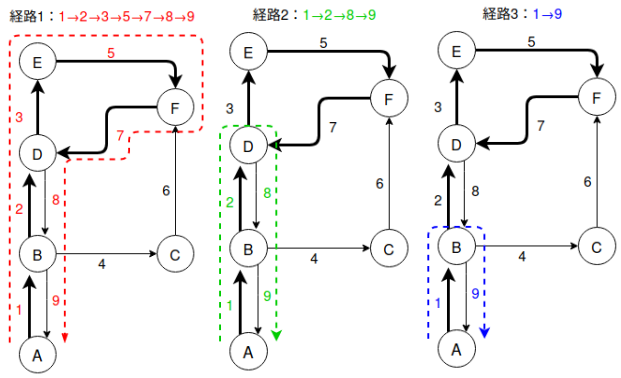

図 3　故障候補とそれを確認するための情報伝達経路の例

また，これが各リンクに対して求められるのでそれらの平均を取り，「平均確認可能性 ($P_m(\mathrm{C}_k)$)」及び C_k によって確認可能なリンクの数を表す「確認可能リンク数 ($E(\mathrm{C}_k)$)」が以下のように求まる．ここで，$\mathbf{N_{F_k}}$ はコマンドが形成する経路内にある全ての故障候補の数を表す．

$$P_m(\mathrm{C}_k) = \frac{1}{\mathbf{N_{F_k}}} \sum_{i=1}^{\mathbf{N_{F_k}}} P(l_i|\mathrm{C}_k) \tag{3}$$

$$E(\mathrm{C}_k) = \mathbf{N_{F_k}} P_m(\mathrm{C}_k) = \sum_{i=1}^{\mathbf{N_{F_k}}} P(l_i|\mathrm{C}_k) \tag{4}$$

式 (3),(4) がどちらも高いコマンドを選択することで，一つのコマンドでより多くの故障候補を絞り込むことが可能である．

次に，あるコマンドから検証を開始した時に，最終的に故障箇所の特定を行うまでにかかるコマンドの総数に関して述べる．以下の図 4 に示すように，あるコマンドによる検証を考えると各テレメトリの結果によって検証結果が異なる．この時，故障候補が残っている場合にはそれに応じたコマンドの探索を行う必要がある．そのため，図 4 中の Case に応じて最終的故障箇所を切り分けるまでのコマンドの総数が異なり，各 Case になる確率を求めることによって検証のために使用するコマンドの数を見積もることができる．

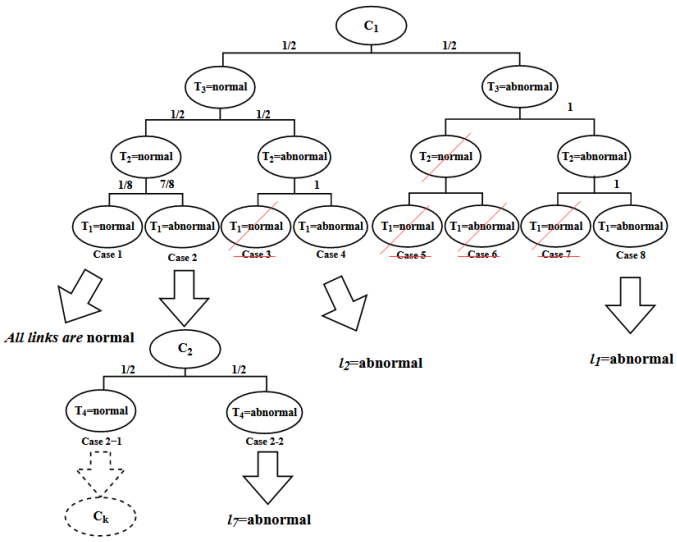

図 4　検証プロセスの全体像

まず，各テレメトリが正常値を示すか否かは各リンクごとの正常確率を用いて以下の式 (5), (6) のように算出でき，これを元に図 4 の各 Case になる確率が求まる．

ここで，T_j は ID が j のテレメトリを表しており，経路 (R_j) の添え字と対応している．

$$P(\mathrm{T}_j = \text{normal}) = \prod_{i \in \mathbb{F}_j} P(l_i = \text{normal}) \tag{5}$$

$$P(\mathrm{T}_j = \text{abnormal}) = 1 - P(\mathrm{T}_j = \text{normal}) \tag{6}$$

これを用いて以下の式 (7) のように検証にかかるコマンド数の期待値が求められ，これを「検証コマンド総数」と定義する．ここで，$\mathbb{C}$ は検証が終了した結果の各場合 (Case) の集合である．

$$N(\mathrm{C}_k) = \sum_{\text{Case } i \in \mathbb{C}} P(\text{Case } i) N_{\text{Case } i} \tag{7}$$

検証コマンド総数が少ないコマンドを選択することによって，全体的にかかるコマンドの数の期待値が小さい検証プロセスを選択することができ，時間制約を考えた場合に重要な指標であると言える．

2.3.3　評価指標の使い分け

以上で示した指標の使い分けに関して以下の表 6 に示す．地上試験時は電力と姿勢による制約はほぼ考えなくてよい．また，効率性を重視したい場合は $P_m(\mathrm{C}_k)$, $E(\mathrm{C}_k)$ が高く，$N(\mathrm{C}_k)$ が小さいコマンドを選択すれば良い．

表 6　地上試験と運用時での指標の優先度 (赤：安全重視，黒：効率重視)

	電力	姿勢	影響 TEL 数	$P_m(\mathrm{C}_k)$	$E(\mathrm{C}_k)$	$N(\mathrm{C}_k)$
地上試験	-	-	中, 低	低, 高	低, 高	低, 高
運用時	高, 低	高, 低	中, 低	低, 中	低, 中	低, 高

3　本手法による不具合分析の実践と評価

3.1　問題設定

以下の図 5 のような簡易衛星モデルを用いて本手法による不具合分析を実践した．実践例として以下の 2 点の故障状態を仮定し，本手法による不具合分析を実践した．

- ヒータの接触不良
- 温度計故障

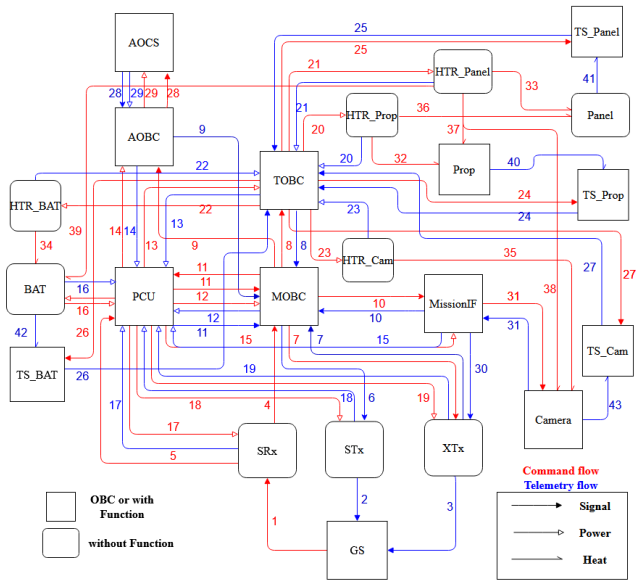

図 5　簡易衛星モデル

3.2　実践結果

3.2.1　ヒータの接触不良

```
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 6　テレメトリによる確認事項の提示

```
 Check telemetries which influenced by initial Command state

COMtarget: [1, 4, 8, 20, 32] TELtarget: [40, 24]
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 7　初期コマンドを用いた確認

```
COMtarget: [32] TELtarget: [40, 24]
COM 13 HTR_PANEL_ON
        {'candidate link number': 2, 'Check link number': 1.0, 'Mean Probability of check': 0.5, 'total_COM_number': 2.0}
        {'impact TEL num': 8, 'Remaining Power': 3.8, 'Power consume by this COM': 2, 'Attitude': 'Keep'}
COM 18 HTR_PROP_OFF
        {'candidate link number': 3, 'Check link number': 0.75, 'Mean Probability of check': 0.25, 'total_COM_number': 1.875}
        {'impact TEL num': 6, 'Remaining Power': 3.8, 'Power consume by this COM': -1, 'Attitude': 'Keep'}
Please select Command above(input ID) >>13
Command 13 ( HTR_PANEL_ON ) & Telemetry 17 ( PROP_Temp ) can verify following links
 COMlink: [] TELlink [40, 24]

Please check PROP_Temp
Input result(OK or NG)>>OK
COMlink: [] & TELLink: [40, 24] were verified
selected Command: [14, 13] remaining Command: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 2
5, 26, 27, 28, 29, 30]
COMtarget: [32] TELtarget: []
COM 18 HTR_PROP_OFF
        {'candidate link number': 1, 'Check link number': 1, 'Mean Probability of check': 1.0, 'total_COM_number': 1.0}
        {'impact TEL num': 6, 'Remaining Power': 3.8, 'Power consume by this COM': -1, 'Attitude': 'Keep'}
Please select Command above(input ID) >>18
Command 18 ( HTR_PROP_OFF ) & Telemetry 17 ( PROP_Temp ) can verify following links
 COMlink: [32] TELlink []

Please check PROP_Temp
Input result(OK or NG)>>NG
selected Command: [14, 13, 18] remaining Command: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 17, 19, 20, 21, 22, 23, 24, 2
5, 26, 27, 28, 29, 30]
COMtarget: [32] TELtarget: []
nothing can verify
finish
faulty COMlink: [32] faulty TELlink: []
```

図 8　コマンド探索結果及び検証過程

3.2.2　温度計故障

4　結論

4.1　本研究で得られた知見

本研究では，衛星の情報伝達経路モデルを用いてコマンドによる故障箇所特定のプロセスを体系化する手法を提案し，テストケースで実践しその有効性を検証した．本手法を用いて最終的な故障箇所の特定を行うことができる故障モードの多くは接続関係に関する故障であり，コンポーネント自体の故障状態に関しては対応できない．また，不具合分析過程を体系化して，それを用いたコマンドの選択をすることによって故障箇所の推論に必要な情報を集めるような働きをしていると言える．

テレメトリを発行している機器の故障の場合は，そのコンポーネントからの情報ラインに冗長系がなければかなり多くの故障候補が残ってしまう．

4.2　今後の展望

今後，接続関係の異常だけでなく，実問題に近い故障状態も扱えるようにするために，扱う状態量をより詳細にモデル化していく必要がある．また，テレメトリと状態量の対応付けを考えることによって異常状態をリンクとして表現するのではなく，各コンポーネントの機能の異常を特定できると考えている．

また本手法では，簡易的に故障候補の洗い出しを情報伝達の経路のみに絞っていたが，）で提案されているオントロジーを用いることで，細かい粒度の特定を目標に行っていく必要がある．

リンクの正常確率として，より実機で用いているコンポーネントの信頼度に近い値を考えることで，モデルが複雑になった際により効率的な故障箇所特定を行えると考えている．

最後に，本研究において使用したモデルは手作業にて構築したが，実ミッションでの適用を考慮すると手作業によるモデル化は人為的ミスや，コストを考えると現実的ではない．今後，設計情報などから必要な情報を抽出してモデルを自動生成できるように工夫する必要があると考えている．

参考文献

1) M Langer and J Boumeester. Reliability of CubeSats Statistical Data, Developers' Beliefs and the Way Forward. *Proceedings of 30th Annual AIAA/USU Conference on Small Satellites*, pp. 1–12, 2016.
2) Catherine C Venturini. Improving Mission Success of CubeSats. Technical report, 2017.
3) Hirobumi SAITO. Secondary Analysis on On-Orbit Failures of Satellite. *JOURNAL OF THE JAPAN SOCIETY FOR AERONAUTICAL AND SPACE SCIENCES*, Vol. 59, No. 690, pp. 190–196, 2011.
4) Peter Struss and Oskar Dressier. "Physical Negation" - Integrating Fault Models into the General Diagnostic Engine. Vol. 89, pp. 1318–1323, 1989.
5) Kota Yamaguchi and Hori Koichi. Fault Network Analysis of Artificial Satellite Using Ontology. pp. 1–4, 2014.
6) 來村徳信, 西原稔人, 植田正彦, 池田満, 小堀聡, 角所収, 溝口理一郎. 故障オントロジーの考察に基づく故障診断方式：網羅的故障仮説生成. PhD thesis, sep 1999.
7) Yoshinobu Kitamura and Riichiro Mizoguchi. *A Framework for Systematization of Functional Knowledge based on Ontological Engineering*. PhD thesis.