社団法人 電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
KBSE2008-23 (2008-11)

組込みシステム非正常系分析における QFD とガイドワードに関する考察

久保 純哉† 井上 富雄† 三瀬 敏朗‡ 新屋敷 泰史‡
橋本 正明† 片峯 恵一† 鵜林 尚靖† 中谷 多哉子§

†九州工業大学 〒820-8502 福岡県飯塚市川津 680-4
‡パナソニック電工株式会社/九州工業大学 〒571-8686 大阪府門真市大字門真 1048
§筑波大学 〒305-8571 茨城県つくば市天王台 1-1-1

E-mail: †kubo@minnie.ai.kyutech.ac.jp

あらまし 組込みソフトウェアの開発においては，システムの障害などを処理する非正常系が，開発規模の約 7 割を占めている．筆者らが既に提案している組込みソフトウェアの非正常系分析手法において，HAZOP (Hazard and Operability Study)のガイドワードは重要な役割を持っている．しかし，ガイドワードの体系は，未整理である．そこで，本稿は，要求された品質とその品質を実現するための機能の関係を示す QFD(Quality Function Deployment)と，ガイドワードの関係を考察する．

キーワード 組込みソフトウェア，非正常系，ガイドワード，QFD

A Discussion on QFD and Guide-Words in Analysis of Unexpected Obstacles in Embedded Systems

Junya KUBO† Tomio INOUE† Toshiro MISE‡ Yasufumi SHINYASHIKI‡
Masaaki HASHIMOTO† Keiichi KATAMINE† Naoyasu UBAYASHI† Takako NAKATANI§

† Kyushu Institute of Tecnology 680-4 Kawazu, Iizuka-shi, Fukuoka, 820-8502 Japan
‡ Panasonic Electric Works, Co..Ltd/Kyushu Institute of Tecnology
1048 Kadoma, Oaza, Kadoma-shi, Osaka, 571-8686 Japan
§ University of Tsukuba 1-1-1 Tennoudai, Tsukuba-shi, Ibaragi, 305-8571 Japan

E-mail: †kubo@minnie.ai.kyutech.ac.jp

Abstract In the development of embedded software, about 70% of the source code of the embedded software is generally allocated to handling unexpected obstacles such as system failure. The authors already proposed an analysis method of unexpected obstacles in embedded systems. The guide-words of HAZOP (Hazard and Operability Study) have an important role in the analysis method. However, the guide-words have not yet been studied satisfactorily. Therefore, this paper dicusses the relationship between the guide-words and QFD (Quaity Function Deployment) which relates the system quality to the function implementing the quality.

Keyword Embedded Software, Unexpected Obstacles, Guide-Words, QFD

1. はじめに

組込みソフトウェア(以下ソフトウェア)を搭載している組込みシステム(以下システム)は，厳しいリソース制約や高い信頼性，リアルタイム性を求められている．組込みソフトウェアはこれらを実現するためにコード量が 1000 万行を超え，大規模化が進んでいる．それにも関わらず開発期間の短縮が求められている．具体的には，ソフトウェアの 80%が，1 年未満の短い開発サイクルとなっている．[1]

ところで，システムは不特定多数の人によって使用され，その設置場所も多様である，これらの要因によってシステムに不具合が生じ，システムが正常に機能しなくなることもある．そのため，ソフトウェアの開発規模の約 7 割が，システムに不具合を発生させない処理，または発生した場合に不具合を他に伝播させない処理に費やされている．しかし，ソフトウェア設計工程において不具合を想定するには，ソフトウェアに関する豊富な知識と経験が必要である．そのため，ソ

フトウェアの経験が浅い技術者は，不具合を見過ごしてしまうこともあり得る．したがって，不具合の起こる条件を明確にできれば，ソフトウェアの品質と開発効率を向上できる．

そこで，筆者らは，不具合の中でも特に想定から漏れ易いものを，「非正常系」と呼ぶ．また，マニュアルに記載されているような，設計時に既に明確になっているソフトウェアの振る舞いを，「正常系」と呼ぶ．その上で，筆者らは，非正常系の分析手法として，IFD(Information Flow Diagram) と ESIM(Embedded Systems Improvement Method)を既に提案している．IFD は，システムの局所的な詳細分析に向いている．一方，ESIM は，システムの全体的な分析に向いている．その両者とも，既存分析手法の FTA(Fault Tree Analysis) や FMEA(Failure Modes and Effects Analysis)，HAZOP(Hazards and Operability Analysis)の考え方を適用している．

HAZOP においては，不具合を想定するのに，「ガイドワード」を用いている．筆者らの研究においおいては，化学プラント設計用の HAZOP のオリジナルなガイドワードに，組込みシステム向きのガイドワードも加えて使用している．そのため，ガイドワード全体がまだ整理できておらず，経験の浅い技術者には，適切なガイドワードを選択するのが困難とも考えられる．また，新たなガイドワードを整えるための指針もない．そこで，筆者らは，非正常系の根底となっている品質と，ガイドワードの適用対象となっている機能の両者に着目した．本稿は，その両者を関係づけるための QFD(Quality Function Deployment)と，ガイドワードに関して考察する．以下，第 2 章に研究の要件を述べる．第 3 章にはガイドワードを説明し，第 4 章に QFD を説明する．その両者の関係は第 5 章に述べ，第 6 章に考察する．

2. ガイドワード

ガイドワードを用いる HAZOP は，化学プラントの危険要因を分析する手法である．そのガイドワードを，システムの分析にも適用する．化学プラントにおいては，化学物質の流れがガイドワードの適用対象である．一方，システムにおいては，情報の流れや，その情報を運ぶキャリア，デバイスを適用対象とする．HAZOP のオリジナルに，システムの熟練技術者が考案したものも加えたガイドワードの例を，表 1 に示す．

表 1 電化製品に適用するガイドワードの例

機器の種別	現象の種別	ガイドワード
一般		no, not, more, less, as well as, part of, reverse, other than
電気回路	挙動	止まる，不安定になる，固定する
	物理的破損	劣化する，特性が変化する，部分的に破損する
	論理的故障	現実と合わない，一致しない，矛盾する
機構部品	挙動	止まる，不安定になる，固定する
	物理的故障	衝突する，磨耗する，汚れる，詰まる
	論理的故障	ずれる，切り替わる，矛盾する
環境	自然環境	温度，輝度，気圧
	機械環境	振動，圧力，加速
	電気環境	電気的雑音，高周波雑音
	負荷環境	過負荷，軽負荷，障害物，逆負荷
	電源環境	電圧低下，電源断，過電圧，瞬時停電
操作環境	設置環境	誤設置，不良位置
	施工環境	誤接続，接続不良，接着不良
	その他	矛盾した運用，衝突，競合，資源不足
操作者	意図	誤操作，偶然，意図的，いたずら
	利用目的	特別な用途，緊急
	特性	年齢，経験，ハンディーキャップ

ガイドワードを適用するには前述のとおり，システムの情報の流れや，キャリア，デバイスを把握していなければならない．それらは，IFD に表現することができる．

IFD は，デバイス・ダイアグラム(DD)とプロセス・ダイアグラム(PD)の 2 つを組み合わせて構成している．IFD は，最初に正常系シナリオを用いて記述する．

DD には，アーキテクチャ設計において決めたデバイスと，そのデバイスを相互に接続するキャリアを図示する．デバイスには，製品内のもの以外にも，その製品に影響する動作環境内のものも記述する．たとえば，光センサを用いて昼夜を判断するシステムであれば，光を発する太陽もデバイスとして記述する．PD は，プロセスの機能を静的に表すための手法である IDEF0 を用いて記述する．そのため，プロセス相互の間を流れる情報も記述できる．DD と PD の関係付けは，プロセスのメカニズムへ，そのプロセスを処理するデバイスを接続することによって行う．なお，IFD は階層化も可能である．

IFD を記述するには，シナリオが必要である．シナリオには，1 章に述べた正常系と非正常系の分けることができる．また，非正常系シナリオのうち，システムに障害を発生させるものを特に障害シナリオと呼ぶ．

ここで，話題沸騰ポット (GOMA-1015 型) 要求仕様書 第 6 版[3]を事例にして，下記の正常系シナリオによって記述した IFD を図 1 に示す．

1　人が操作パネルの保温設定ボタンを押下し，保温温度を設定する．

2　蓋センサが ON であり，水量も温度制御可能な量である．

3　サーミスタがポット内の水温を測る.
4　測定された水温により以下の処理を行い，2 に戻る
　4.1　水温が設定された温度より低くなった場合ヒータの電源を ON にする.
　4.2　水温が設定された温度より高くなった場合ヒータの電源を OFF にする.

図 1 に示した IFD に，ガイドワードを適用して，非正常系を分析する．この IFD に，表 1 の「環境」の「電気環境」に示すガイドワード「電気的雑音」を適用する．その際，水位センサとマイコンの間のキャリアに着目すると，電気的雑音によって情報が反転することを想定できる.その結果,水がないのに空焚きするや，水があるのに加熱しないといった障害を想定できる．このように，ガイドワードの適用によって，障害を想定することができる.

3. QFD

QFD すなわち品質機能展開は，品質展開と，狭義の品質機能展開の 2 つによって構成されている．品質展開は，ユーザの要求を代用特性に転換し，完成品の設計品質を定め，これを各機能部品の品質，さらに個々の部品の品質や工程の要素にいたるまで，これらの間の関連を系統的に展開していくこと，と定義されている．狭義の品質機能展開は，品質を形成する職能ないし業務を目的・手段の系列で、ステップ別に細部に展開していくこと，と定義されている．[4]

品質機能展開を行うことにより，満たすべき品質を，機能として捕らえることができる．そのためには，システムの品質をソフトウェアの要求に変換するための品質展開を行う．品質展開はシステムの要求品質とソフトウェア要求を対応付けるために，図 2 のように 2 次元に展開をする．さらに，システムの要求品質とソフトウェア要求とが対応する交点に，○印を付ける．同図に示すシステム品質特性は ISO 9126 に定められているソフトウェアの品質特性を利用しており，満たすべき品質の重み付けを行い，品質管理のために記述する．[5]

次に，展開されたソフトウェア要求をソフトウェアの要求品質とし，その品質を満たすためのソフトウェア機能を展開する．この 2 つの要求品質展開によって，満たすべき品質を機能に展開することができる.また，組込みソフトウェアの開発には，デバイスとソフトウェアの両方の知識が必要である[6]．そのため，ソフトウェア機能と，それを実行するデバイスの関連付けも行う．以上に述べた品質機能展開図を，図 3 に示す.

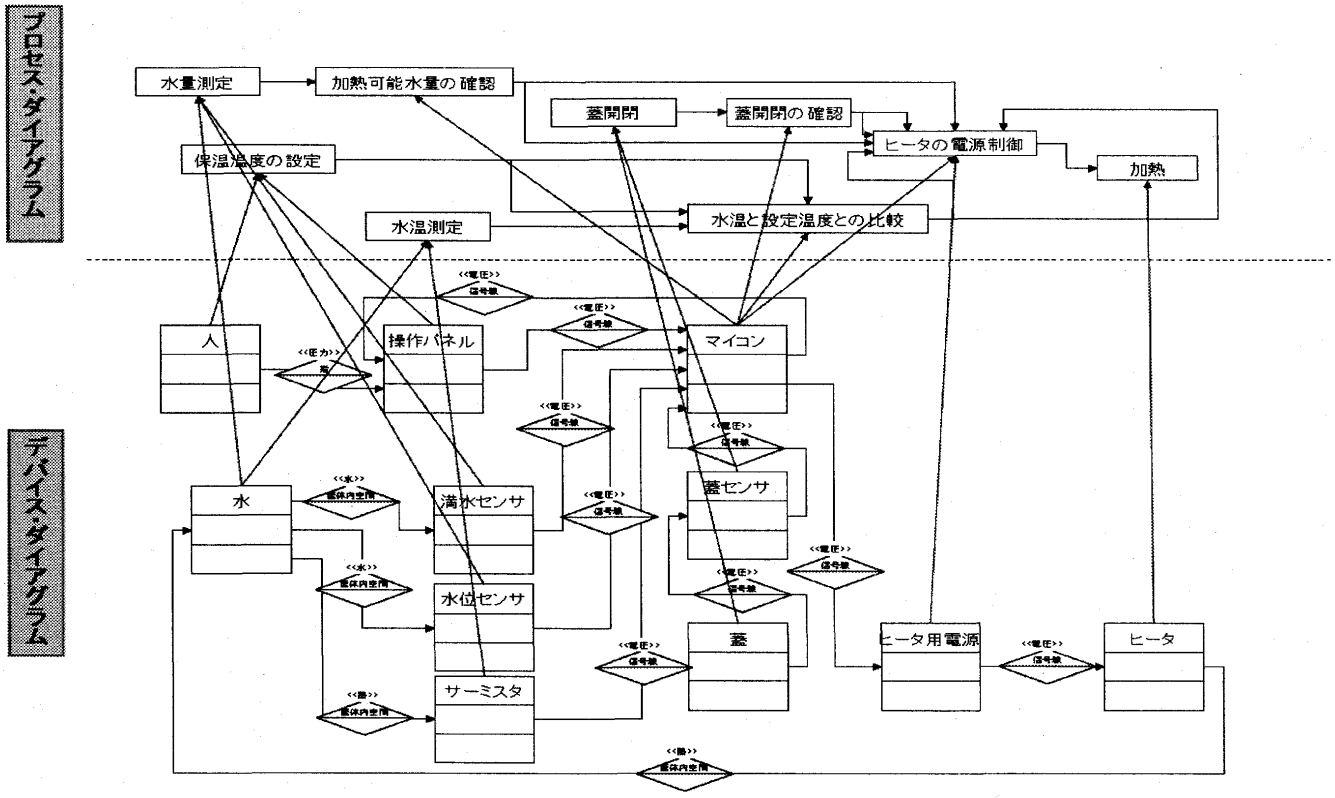

図 1 正常系シナリオに基づくポットの IFD

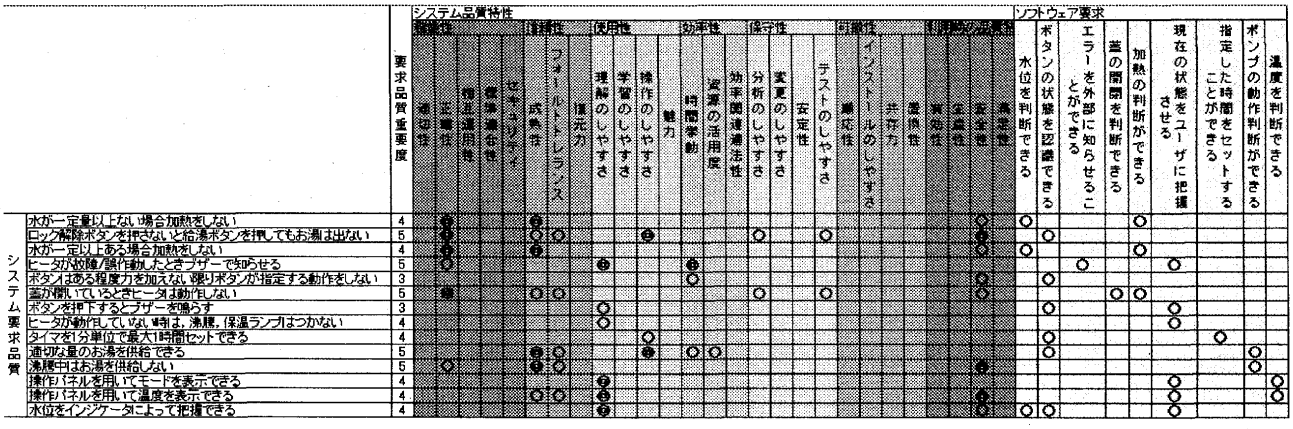

図 2 ポットのシステム要求品質展開

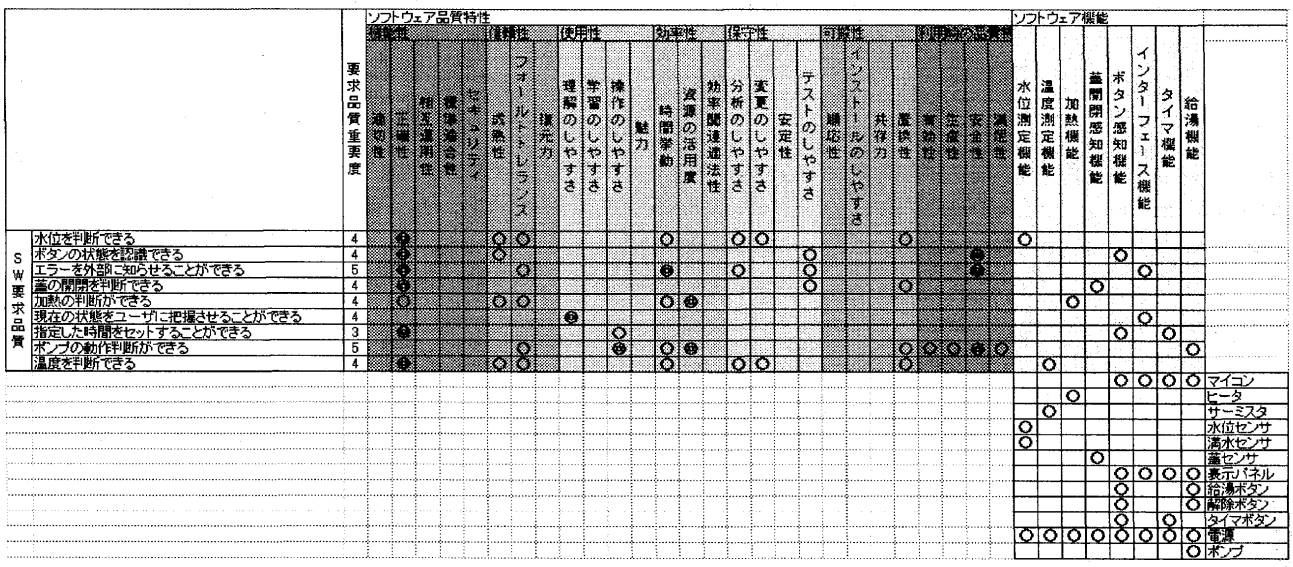

図 3 ポットのソフトウェア要求品質展開

4. QFD とガイドワードの関係

QFD とガイドワードの関係を述べ，その関係を，事例を用いて確認する．

4.1. QFD とガイドワードの見方

QFD によってシステムの品質をソフトウェアの機能に展開し，そのソフトウェアの機能を実行するためのデバイスにも展開できることは，前章に述べた．ところで，ガイドワードは障害が起こり得る機能の逸脱を想定するための言葉である.，そこで，QFD によって展開された機能に着目すると，ガイドワードによって想定される機能の逸脱は，システムが正常な機能を果たしていないことに置き換えできる．システムが正常な機能を果たしていないことを，機能不全と呼ぶ．すなわち，ガイドワードはシステムが機能不全に陥るかもしれないことを想定するための言葉と言い換えることができる．

一方，QFD によって展開されたソフトウェアの機能が，正常に働かないことも，機能不全である．したがって，機能不全の概念によって品質とガイドワードを関係づけると，以下に示す関係が得られる．

品質―機能―機能不全―ガイドワード

この関係によって，品質と，非正常系の関係を想定することができる．

4.2. ガイドワードの絞り込み方

ガイドワードは,表 1 に示すように,機器の種別と，現象の種別に分類されている．機器の種別に示す電気回路や，機構部品は，品質展開した時に現れるデバイスと対応付ける．この対応付けによって，まず大まかなガイドワードの絞込みができる．次に，現象の種別については，挙動や物理的故障はデバイスが原因となっており，論理的破損はソフトウェアが原因となっている．そのため，現象の種別によって，さらにガイドワードを絞り込むことができる．

次に，システムの機能を見ると，デバイスのデバイスが本来の機能を果たすのに必要なエネルギーそのものと，そのエネルギーをコントロールするための情報

処理である観測と演算と制御に分けることができる．観測は，システムやその動作環境の中に存在するデバイスの状態を知るための情報処理である，制御は，デバイスのコントロール情報を伝えるための情報処理である．演算は，観測情報から制御情報を作り出すための情報処理である．たとえば，温度測定機能においては，エネルギーとして温度が存在し，情報処理の種別は観測となる．エネルギーは，表 1 に示す機器の種別が「環境」に関係する．また，情報処理は，「電気回路」の「論理的故障」に関係する．

そこで，以下に述べる手法を取れば，多数のガイドワードの中から，必要なガイドワードを絞り込むことができる．

1　デバイスを，機器の種別の「電気回路」や，「機構部品」等から合致するものから選ぶ
2　システムの機能の特性を，エネルギーと情報処理に分ける
3　着目するデバイスから物理的故障の該当するガイドワードを選ぶ
4　ソフトウェアの面から見たガイドワードは，デバイスの合致する機器種別の論理的破損から選ぶ．また，ソフトウェアの対象としているエネルギーについては，機器の種別である「環境」から選択する

たとえば，温度測定機能においては，デバイスの面から見てサーミスタ自体が「劣化する」や，ソフトウェアの面から見て温度測定が「現実と合わない」といったガイドワードを選ぶことができる．

4.3. 適用事例

事例として，前述のポットに適用する[3]．ポットの要求仕様は，ポット内の水を沸騰して保温し，ユーザによって設定された温度のお湯を提供するものである．また，給湯とは関係ないが，ブザーを鳴らして知らせるタイマにより，調理時間の計測も行う．図 5 にデバイスの構成を示す．

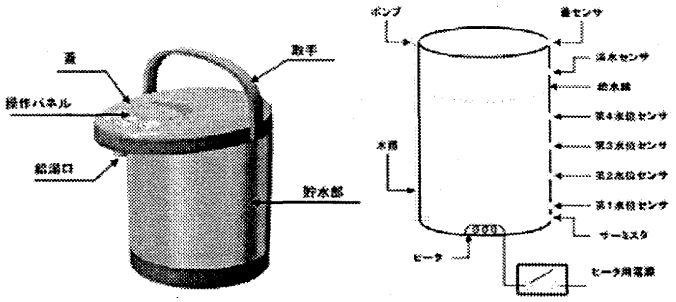

図 4 デバイス構成

このポットの QFD は，図 3 と 4 に示したものである．この図によって，満たすべき品質と，実装すべき機能の対応関係がわかる．次に，個々の機能とガイドワードについて，その関係を確認する．機能と，デバイス・デバイス，機能の対象について，その関係を表 2 に示す．

表 2 デバイスと機能の対象

		ハードウェア	機能の対象	
			エネルギー	処理
ソフトウェア機能	給湯機能	ポンプ，マイコン，給湯ボタン，解除ボタン	モータ，電圧	制御
	水位測定機能	水位センサ，満水センサ	水量	観測
	温度測定機能	サーミスタ	温度	観測
	加熱機能	ヒータ	温度	制御
	蓋開閉感知機能	蓋センサ	電圧，接触	観測
	ボタン感知機能	マイコン，表示パネル，各種ボタン	電圧	観測
	インターフェース機能	マイコン，表示パネル	電圧	制御
	タイマ機能	マイコン，タイマボタン，表示パネル	電圧	演算

給湯機能については，デバイスはポンプと，マイコン，給湯ボタン，解除ボタンの 4 つが該当する．ポンプと，給湯ボタン，解除ボタンは機構部品に該当し，マイコンは電気回路に該当する．ソフトウェアの機能は，ポンプのモータを制御するため，エネルギーはモータの駆動力となり，情報処理は制御となる．ここまでが，前節に述べた手順 1 と 2 に対応する．

次に，着目するデバイスを選択する．今回は，ポンプを選択する．デバイスに関するガイドワードとして，「ポンプが止まる」と，「ポンプが劣化する」を得ることができる．最後に，ソフトウェアに関するガイドワードとして，エネルギーがモータの駆動力の場合は「モータが過負荷状態になる」と，「モータが障害物により回らなくなる」を得ることができる．また，情報処理においては，ソフトウェアの制御がデバイスの動作と合わないといったガイドワードを得ることができる．

加熱機能については，デバイスはヒータなので，電気回路となる．ソフトウェアの機能はヒータを調節し温度を高めるため，エネルギーは熱であり，情報処理は制御となる．デバイスに関するガイドワードとして，「ヒータが不安定になる」と，「ヒータが止まる」，「ヒータが劣化する」を得ることができる．また，ソフトウェアに関するガイドワードとして，エネルギーは熱なので「水温があがらない」を得ることができ，情報処理は制御なので「ヒータの電源が不要な時に切り替わる」も得ることができる．

このように，システムの品質を決めた後，さらに機能に展開することによって，非正常系の分析に適用されるガイドワードを絞り込むことができる．

5. 考察

5.1. ガイドワード絞込みに関する考察

4.1 節に述べた品質とガイドワードの関係が，4.3 節述べた適用事例において成り立っているか確認する．適用事例において，システムの要求品質から展開されたソフトウェアの機能に関係するガイドワードを，4.2

節に述べた方法によって得ることができた．図 3 と 4 に示した品質展開表を用いれば，要求品質とガイドワードを結びつけることができており，4.1 節に述べた関係は満たされている．すなわち，品質を決めた時点において，適用するガイドワードを絞り込むことができる．

しかし，4.2 節に述べた方法によってガイドワード絞り込むには，展開された機能だけではなく，ソフトウェアを搭載しているデバイスも必要である．したがって，デバイスの設計書が必要なため，デバイスが未定なシステム・アーキテクチャ設計前は、ガイドワードを絞り込むことは困難である．

5.2. QFD とガイドワードの関係に関する課題

QFD とガイドワードの関係に関する課題について述べる．今回適用したガイドワードは，そのまとめ方が，表 1 に示すように，QFD と対応していない．そのため，ガイドワードの適用時に技術者のスキルの差が生じる．たとえば，ヒータを電気回路としてとらえるのか，機構部品としてとらえるのかによって適用されるガイドワードが異なる．そのため，今後は QFD に合わせたガイドワードの整理が必要である．

デバイスの繋がりは，IFD においてキャリアで表現されている．障害が発生する原因には，デバイスの故障や，プロセスの破損の他に，キャリアの不具合もある．現在，ガイドワードはデバイスとキャリア共に同じ表にまとめられているが，キャリアのみに着目した整理を，現在研究中である．[7]

6. おわりに

QFD とガイドワードの関係について考察した．品質と機能とガイドワードが，機能不全の概念によって関係するという道筋を立てた．その関係を，適用事例を用いて確認した．今後の研究課題としては，QFD に合わせたガイドワードの整理，デバイス間のキャリアに着目したガイドワードの整理があげられる．

文　献

[1] 経済産業省，”2008 年版組込みソフトウェア産業実態調査”．

[2] Mise, T., Hashimoto, Y., Katamine, K., Shinyashiki, Y., Ubayashi, N., Nakatani, T., ”A Method for Extracting Unexpected Scenarios of Embedded Systems, ” Proc. of the Knowledge-Based Software Engineering (JCKBSE ’06), pp.41-50, August, 2006.

[3] 胡麻印まほうびん，“話題沸騰ポット (GOMA-1015 型) 要求仕様書 第 6 版” SESSAME, October, 2004.

[4] 大藤 正，小野 道照，赤尾 洋二，“品質展開法(1)”，pp.4，(株) 日科技連出版社，東京，2002.

[5] 小松 由香里，吉原 真也，石橋 慶一，秋山 義博，中谷 多哉子，片峯 恵一，鵜林 尚靖，橋本 正明，”QFD による組込みソフトウェア分析・設計の品質管理モデリングに関する一考察” プロジェクトマネジメント学会，March ，2005.

[6] R.Crook, D.Lnce, L.Lin, B.Nuseibeh, “Security requirements engineering: when anti-requirements hit the fan” Proc. Of the 10th Anniversary Joint IEEE International Requirements Engineering Conference (RE ‘02)， pp.203-205，2002.

[7] 谷本 真樹，三瀬 敏朗，新屋敷 泰史，橋本 正明，中谷 多哉子，鵜林 尚靖，片峯 恵一，”情報フロー・ダイアグラムと分析マトリクスを統合した組込みソフトウェア費正常系要求分析手法の適用事例と考察” 知能ソフトウェア工学研究会，November，2007.