RC-004

故障木図からの例外処理の導出による通信プログラム構築手法

A Method to Create Network Communication Programs by Deriving Exception Handling from Fault Tree Diagram

長田 知之† 原内 聡† 北村 操代† 山地 勉‡ 上野 泰秀‡
Tomoyuki Nagata Satoshi Harauchi Misayo Kitamura Tsutomu Yamaji Yasuhide Ueno

1． はじめに

監視制御システムの分野では、高品質なシステムを低コストかつ短期間で構築することが求められている。監視制御システムの生産性向上を阻害する要因の一つに、案件毎の作りこみが発生することが挙げられる。監視制御システムによっては、独自通信プロトコルの作りこみをしなければならない。また通信プログラムは、送受信タイムアウトなどの例外が多い。このため、例外発生時に行うべき例外処理の漏れが発生する可能性がある。例外処理の漏れは、試験時に発見されることが多いため、工程の手戻り削減が課題になっている。

本稿では、これらの課題を解決する通信プログラム構築手法を提案する。本手法では、シーケンス図などで記述された通信プロトコル仕様から、通信プログラムのソースコードを生成する。また、システムの信頼性分析に使用する故障木図から例外処理を導出し正常時処理に付加することで、例外処理の漏れを削減する。

2．課題と従来方式

通信プログラムの構築には、以下の二つの課題がある。一点目は、必要な例外処理の考慮漏れの防止である。通信プログラムでは、正常時処理よりも例外処理の方が多い。一般に独自通信プロトコル仕様では、例外処理について明記されることは少なく、試験時に初めて考慮漏れが発見されることが多くなる。二点目は、正常時処理及び例外処理の再利用性の向上である。独自通信プロトコルでは、正常時処理は同じだが例外処理のみが異なる場合がある。また、作成した例外処理を他のプロトコルでも使用することもある。一般に通信プログラムでは、正常時処理と例外処理の記述が混在しているため、それらを個々に取り出すことは難しい。

通信プログラムを効率的に作成するために、通信プロトコル仕様から通信プログラムのソースコードを生成する手法が提案されている[1-3]。Preccs は、プロセス代数や正規表現に基づいたプロトコル仕様記述言語である[1]。Preccs で記述した通信プロトコル仕様から、生成系が C 言語で記述された通信プログラムを生成する。IBM Rational SDL Suite は、シーケンス図などで記述された通信プロトコル仕様から、C/C++で記述された通信プログラムを生成する通信プロトコル実装環境である[2]。IBM Rational SDL Suite では、High Level Message Sequence Chart[4]を利用することで正常時処理と例外処理の記述を分離することができる一方、Preccs では正常時処理と例外処理は混在してしまう。また、Preccs と IBM SDL Suite 共に、例外処理の漏れ防止については考慮されていない。

正常時処理に対して自動的に例外処理を付加する手法として、寺内らによる手法[3]が知られている。寺内らは、正常時処理を表すシーケンス図と、例外が起こりうる条件とその処理を記述したルールとから、例外処理を付加したシーケンス図を生成する手法を提案している。このルールを用いることで、正常時処理と例外処理の記述を分離することができる。しかし、ルールの作成は難しく、系切換えなどの複雑な例外処理を記述するルールの網羅することは難しい。

新屋敷らは、動作環境も含めたシステムの中を流れる情報に着目して、例外が発生する条件を漏れなく想定する手法を提案している[5]。これにより、例外を網羅することは可能であるが、例外処理の漏れの防止については考慮されていない。

3. 提案手法

本稿では、通信プロトコルの正常時処理をシーケンス図で定義することと、必要な例外処理を故障木図から導出し正常時処理シーケンスに付加することにより、通信プログラムを構築する手法を提案する(図 1)。本手法では、シーケンス図[4]やメッセージ形式定義言語で通信プロトコル仕様を定義し、定義から通信プログラムを生成する。また、監視制御システムの信頼性分析によく用いられる故障木図から、必要な例外処理を導出する。

監視制御システムにおける通信プログラムの開発効率を向上させるため、通信プロトコル仕様から通信プログラムを生成する。プログラミングにより通信プログラムを作成する必要はなく、案件毎の通信プログラム作成コストを低減することができる。

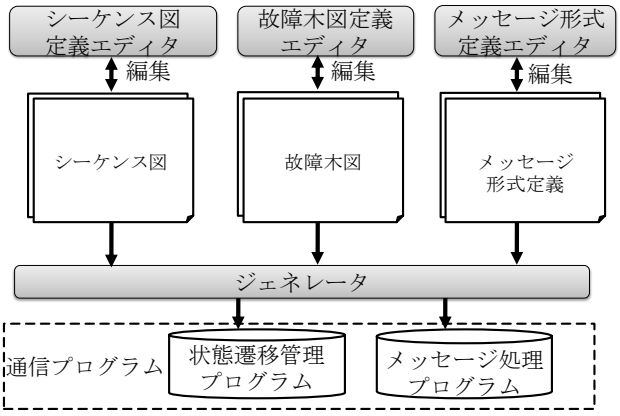

図 1 提案手法

† 三菱電機株式会社 先端技術総合研究所
‡ 三菱電機株式会社 系統変電システム製作所

監視制御システムにおける通信プログラム作成の課題の一点目「必要な例外処理の考慮漏れの防止」と二点目「正常時処理及び例外処理の再利用性の向上」を、故障木図から必要な例外処理を導出し、正常時処理シーケンス図に付加することで解決する。通信プログラムの設計者は、正常時処理シーケンス図と、例外とその要因との因果関係を記述した故障木図、例外要因発生時の条件や処理を記述したシーケンス図を作成し、そして例外要因がシーケンス図上で発生しうる箇所を定義する。これらの情報を基に、例外が発生しうるシーケンス図上の全ての箇所に、故障木図から導出した例外処理を付加する。

故障木図から必要な例外処理を導出し、正常時処理で例外処理が必要な箇所に付加することで、例外処理の漏れを削減する。また、正常時処理と例外処理の記述を分離することができるため、正常時処理と例外処理の記述を再利用することができる。

4. 実現方式

本章では、故障木図から例外処理を導出し、正常時処理シーケンス図に付加する手法について具体的に述べる。

4.1. 正常時処理シーケンス

通信プログラムの設計者は、正常時の処理をシーケンス図で記述する。シーケンス図には、クライアントやサーバなどの通信インスタンス間のメッセージの送受信を記述する。また、メッセージの送受信を伴わない内部処理やタイマの開始・停止などを記述する。メッセージの送受信や、内部処理を総称してシーケンス図のイベントとよぶ。図 2 に正常時処理シーケンスの例を示す。図 2 は通信相手や LAN の監視を行うためのシーケンスである。サーバは定周期に機器から送信される LAN 監視パケットを受信する。タイマ 2 は正常な LAN 監視パケットが一定期間受信されなかった場合に、タイムアウトする。このタイムアウトにより、通信相手である機器が不応答かまたは LAN 断のいずれかであるとサーバは判断する。

4.2. 故障木図

故障木図とは、システムの信頼性分析に用いられる図で、発生が好ましくない事象の発生原因を論理演算で結びツリー形式で表したものである。故障木図は、監視制御システムの設計に先立ち作成されることが多い。故障木図では、例外を表す事象をトップ事象とよぶ。トップ事象は長方形で表され、ツリーの根となる。トップ事象とその発生要因を論理演算で結び、トップ事象が発生する因果関係を表す。ツリーの葉ノードにあたり、それ以上分解できない発生要因を基本事象とよび、丸で囲んで表す。一方、ツリーの中間ノードにあたり、複数の発生要因をまとめるものを中間事象とよび、トップ事象と同じく長方形で囲んで表す。

図 3 は故障木図の例である。図 3 において、LAN 監視パケットが未着という例外は、通信相手が不応答か LAN が断絶することで発生することを示す。

4.3. コンディション・アクション設定

シーケンス図と故障木図が保持する異なる情報を統合するために、コンディション・アクション設定を行う。まず、故障木図中の基本事象と、それが発生する条件(コンディション)をシーケンスを用いて記述したものを関連付ける。また、故障木図のトップ事象や中間事象と、それらが発生した際の例外処理(アクション)をシーケンスを用いて記述したものを対応付ける。

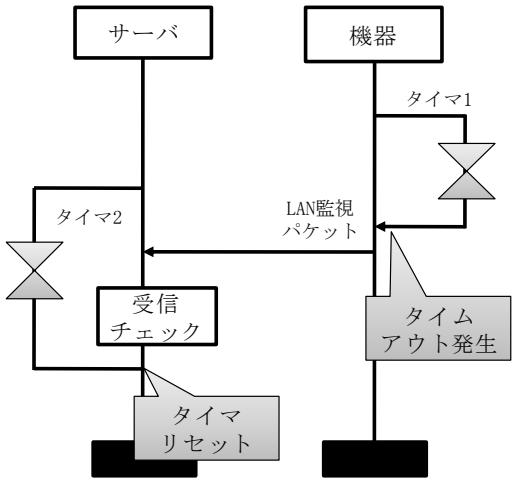

図 2 LAN 監視シーケンス

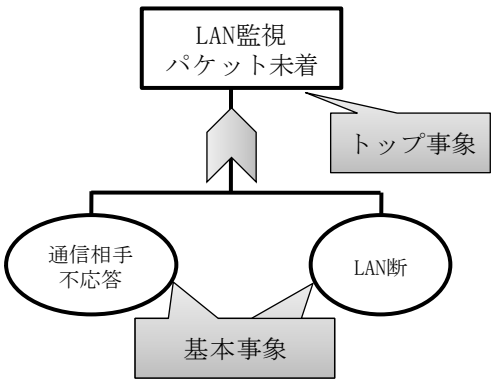

図 3 故障木図

図 4 において、基本事象「通信相手不応答」と「LAN 断」に対しては、発生条件「機器から LAN 監視パケットがサーバに届かないため、サーバのタイマ 2 がタイムアウトする」ことを表すシーケンスを対応付ける(図 4 中(a))。また、トップ事象「LAN 監視パケット未着」には、例外処理「サーバが LAN 障害イベントを発生させる」という例外処理を表すシーケンスを対応付ける(図 4 中(b))。

4.4. マッピング

マッピングでは、故障木図中の基本事象が正常時処理シーケンス図中のどこで発生しうるかを設定する。図 5 では、故障木図における二つの事象「通信相手不応答」と「LAN 断」が、正常時処理シーケンスのサーバにおける「LAN 監視パケット受信」イベントと「タイマ 2 リセット」イベントにマッピングされている。マッピングされたシーケンス図上のイベントを、マッピング点とよぶ。これは機器からサーバへ LAN 監視パケットが送信されない場合か、LAN 監視パケット受信チェックに失敗した際に、事象「通信相手不応答」と「LAN 断」が発生しうることを示す。

ハードウェアの故障など通信プロトコルと関係なく、シーケンス図の任意の箇所で発生しうる基本事象に関しては、シーケンス図中の全てのイベントにマッピングする。また、パケットのパリティ検定違反など、パケット

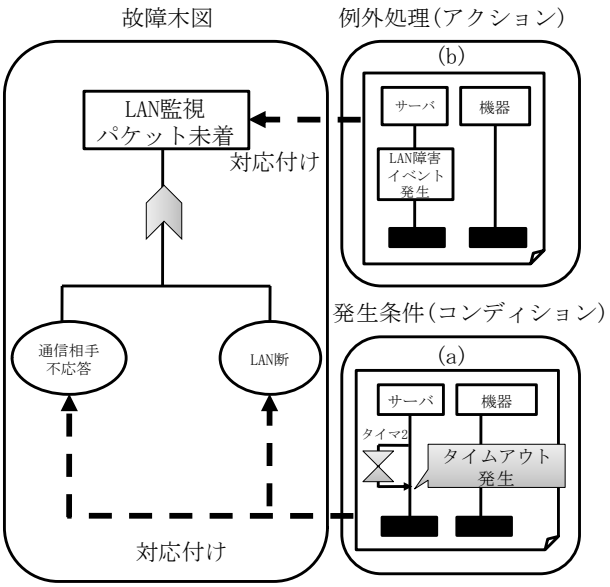

図 4 アクション・コンディション設定

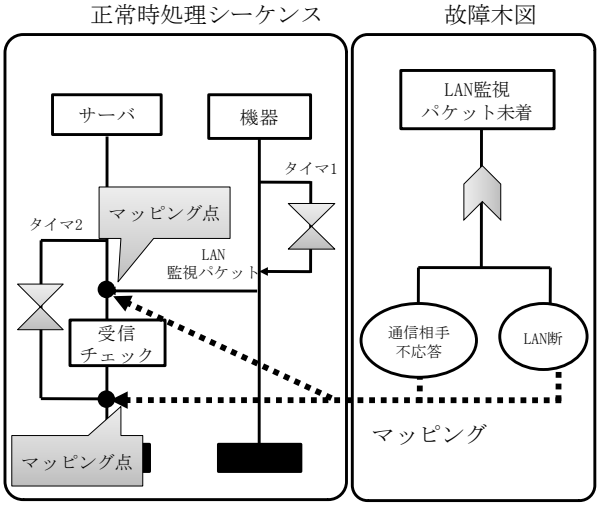

図 5 マッピング

の受信に伴う基本事象に関しては、シーケンス図中のパケット受信イベント全てにマッピングする。これを実現するために、イベント定義情報、事象定義情報及びイベント・事象対応情報を導入する。

イベント定義情報とは、シーケンス図中のイベントが属するグループを示す情報である。表 1 の例では、イベント「LAN 監視パケット受信」は、グループ「パケット受信」に含まれることを示す。

事象定義情報とは、各事象が所属するグループを示す情報である。表 2 の例では、事象「LAN 異常」は、グループ「故障」と「通信断」とに含まれ、事象「パリティ検定違反」はグループ「パケット不正」に含まれることを示す。

イベント・事象対応情報は、事象にマッピングされうるイベントをグループで指定する情報である。表 3 の例では、事象グループ「パケット不正」は、全てのパケットを受信した際に発生しうるので、対応するイベントのグループは「パケット受信」になる。ここで論理式において、イベントグループを論理記号で結ぶことにより、事象と対応するイベントを細かく指定することができる。

以上の定義情報を利用することにより、任意のグループの事象を任意のグループのイベントに自動的にマッピングすることができる。

表 1 イベント定義情報

イベント	グループ1	グループ2	・・・	グループn
LAN監視 パケット受信	パケット 受信	-		-

表 2 事象定義情報

事象	グループ1	グループ2	・・・	グループn
LAN異常	故障	通信断		-
パリティ検定 違反	パケット 不正	-		-

表 3 イベント・事象対応情報

事象グループ	イベント グループG1	イベント グループG2	・・・	イベント グループGn	論理式
パケット 不正	パケット受信	-		-	G1

4.4. 例外処理導出

例外処理導出では、正常時処理シーケンスに対応付けられた故障木図から、必要な例外処理を導出し正常時処理シーケンスに付加する。例外処理導出は以下の各ステップから構成される。

- Step1. 正常時処理シーケンスからマッピング点を一つ選択。
- れた故障木図の事象を取得する。この事象を対象事象とよぶ。
- Step3. 対象事象に対応付けられたアクションを取得する。なお、アクションが設定されていなくてもよい。
- Step4. 対象事象の親ノードの親ノードの事象(上位事象)を新たに対象事象とし、Step3 に移動する。ただし、対象事象が発生したことで上位事象が発生する場合に限る。上位事象が存在しない場合や、対象事象が発生したことで上位事象が発生しない場合は、Step5 に移動する。
- Step5. Step1 で取得したマッピング点でのイベント以降のシーケンスを、Step3 で取得したアクション群で置換する。全てのマッピング点において Step1 から Step4 の処理が行われた場合は終了する。そうでない場合は、Step1 に移動する。

Step4 における、対象事象の上位事象が発生する条件は、親ノードに依存する。対象事象の親ノードが論理和である場合、対象事象が発生すれば、その上位事象は発生する。また、対象事象の親ノードが論理積である場合、対象事象の兄弟ノードの事象が全て発生していれば、その上位事象は発生する。

図 2 の正常時処理シーケンス(LAN 監視シーケンス)にお

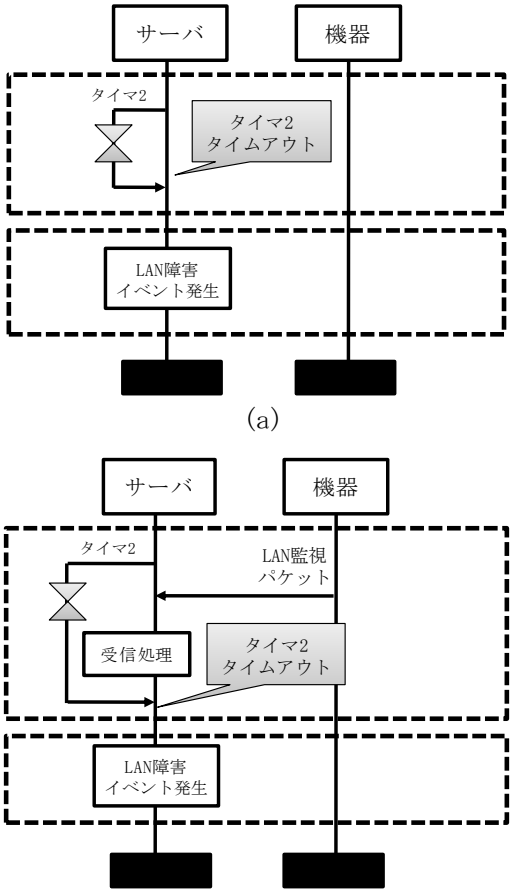

図 6 例外処理付加シーケンス図

いて、図 3 の故障木図と図 4 で示されるコンディション・アクション設定と、図 5 で示されるマッピングにより、図 6 の例外処理付加シーケンス図を生成することができる。

図 6 中(a)のシーケンス図は、図 5 のサーバの LAN 監視パケット受信イベントにおけるマッピング点から生成される。同じく、図 6 中(b)のシーケンス図は、図 5 のサーバのタイマ 2 リセットイベントにおけるマッピング点から生成される。図 6 中(a)は、機器からサーバに対して LAN 監視パケットが送信されなかったため、サーバのタイマ 2 がタイムアウトになったことを示す。図 6 中(b)は、機器からサーバに対して LAN 監視パケットが送信されたが、サーバの受信処理の結果、不正なパケットであると認識されたことを示す。この結果、サーバのタイムアウト 2 がタイムアウトしている。

5. 構築環境の実現例

図 7 に、図 1 におけるシーケンス図定義エディタの画面例を示す。本エディタは、シーケンス図の作成や、コンディション・アクション設定などを容易に行うための専用エディタである。本エディタがシーケンス図の論理的な整合性チェックや、図 1 のメッセージ形式定義との連携を行うことで、効率的にシーケンス図を定義する。

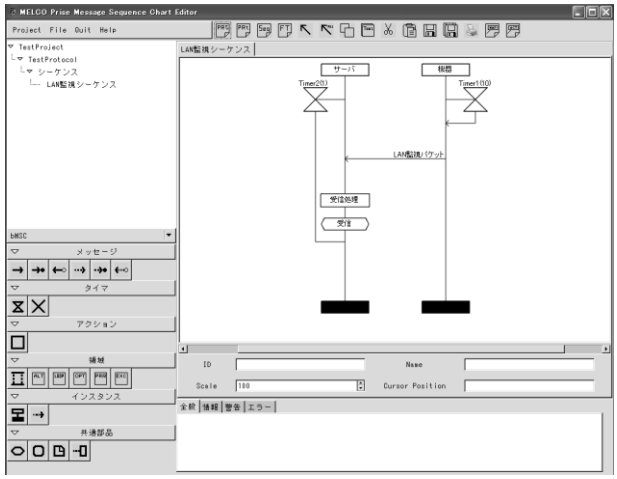

図 7 シーケンスエディタ画面例

6. おわりに

本稿では、監視制御システム向け通信プログラムを、高品質・低コストで開発するための構築手法について述べた。本手法によれば、対象通信プロトコル仕様を熟知した技術者が作成した故障木図から必要な例外処理を導出することで、例外処理の漏れを削減する。また、正常時処理と例外処理の記述を分離することができるため、正常時処理と例外処理の記述を再利用することができる。

今後の課題として、本方式の評価と、UDP プロトコルにおける通番管理など、シーケンス図で記述することが難しい項目への対応が挙げられる。

参考文献

[1] 服部 健太, 数馬 洋一: “正規表現とプロセス代数に基づく通信プロトコルのための仕様記述言語の提案”, 情報処理学会論文誌 47(28), pp.18-pp.29 (2006)

[2] IBM: “IBM Rational SDL Suite”, http://www-01.ibm.com/software/awdtools/sdlsuite/ (2009)

[3] 寺内 敦, 金井 敦: ”MSC とルールを併用した通信サービスの効率的解法”, 情報処理学会第 49 回全国大会, 1-263 (1994)

[4] ITU-T. recommendation Z.120 : ”Message Sequence Chart(MSC)” (2004)

[5] 新屋敷 泰史, 三瀬 敏朗, 片峯 恵一, 鵜林 尚靖, 中谷 多哉子: ”情報フロー・ダイアグラムによる組み込みソフトウェア非正常系の要求分析の一手法”, 情報処理学会論文誌 48(9), pp.2894-pp.2903 (2007)