B-024

故障木図からのモデル検査式導出手法の提案

A method to derive linear temporal logics from fault tree diagrams

長田知之† 原内聡†
Tomoyuki Nagata Satoshi Harauchi

1. はじめに

監視制御システム(SCADA System; Supervisory Control And Data Acquisition system) は，コンピュータがネットワークで接続された機器と通信を行い，機器の監視・制御を行うシステムである．監視制御システムは，発電所，変電所，上下水処理場やエレベータなど，様々な分野で用いられている．

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，案件ごと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，案件特化の通信プロトコルを作りこむ必要がある．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．

我々はこれらの課題を解決するために，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手法を提案してきた[1]．

本稿では，故障木図から例外処理だけでなく，例外処理が適切に付加されているかを確認する線形時相論理(LTL;Linear Temporal Logic)式[2]を導出する．例外処理が付加された通信シーケンスのモデルを Promela[2]で記述[2]し，モデルが LTL 式で示される性質を満たすか，モデル検査ツール SPIN[2]で網羅的に検査する．これにより，適切に例外処理が付加されているかを確認することができる．

2. 従来手法と課題

文献[1]の手法では，通信プログラムの設計者は，通信プロトコルの正常時の処理を記述したシーケンス図と，例外とその要因との因果関係をツリー形式で記述した故障木図を作成する． 故障木図に対して，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対応付け，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．これにより，例外処理の漏れを削減する．

本手法を高い信頼性が必要な監視制御システムに適用するためには，故障木図から導出した例外処理が適切かどうかを確認する手段が必要である．例外処理が不適切であった場合，この不具合は試験時に発見されてしまい，工程の手戻りが発生してしまう．

3. 提案手法

本稿では，故障木図から例外処理が適切に付加されているかを確認する LTL 式を導出する手法を提案する(図 1). 提案手法では，例外処理が付加された通信シーケンスのモデルを Promela で記述する．また，例外処理が実行された後に成立すべき条件を記述した LTL 式を故障木図から導出する．Promela 記述されたモデルが導出した LTL 式で示された性質を満たすかを，モデル検査ツール SPIN により検査を行う．提案手法によれば，文献[1]の手法により付加された例外処理が適切かどうかを設計段階で確認することができる．

4. 実現方式

故障木図から，例外処理が実行された後に成立すべき性質を記述した LTL 式を導出するアルゴリズムについて，図 2 の通信シーケンス図を例に述べる．

図 2 は，機器が監視制御システムに対して，定期的にヘルスチェックパケットを送信するヘルスチェックシーケンスを示す．

図 3 は図 2 のシーケンスに対する故障木図である．故障木図では，発生が好ましくない事象をトップ事象とよぶ．トップ事象とその発生要因を論理演算子で結び，トップ事象が発生する原因を示す．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ぶ．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ぶ．図 3 の故障木図は，ヘルスチェックパケットが未着というトップ事象は，機器が不応答か LAN が断絶していることを示す．

文献[1]の手法では，故障木図の基本事象に，その事象が発生する条件を記述したシーケンス図を対応付ける．また，中間事象とトップ事象にその事象が発生した時の例外処理を記述したシーケンス図を対応付ける．図 3 では，通信相

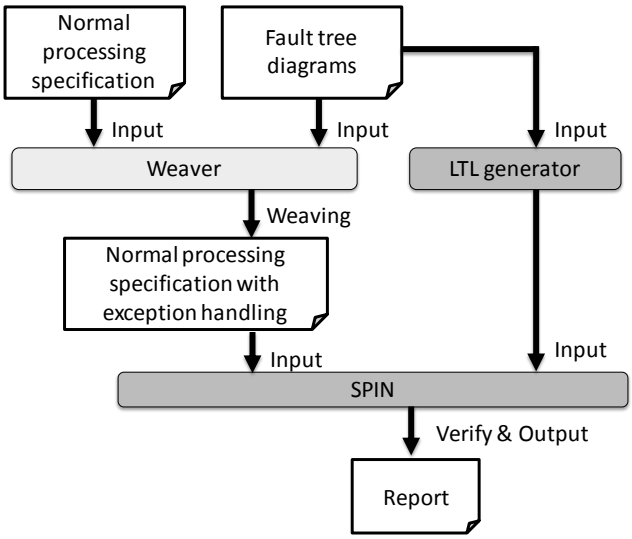

図 1 提案手法

† 三菱電機 Mitsubishi Electric Corporation

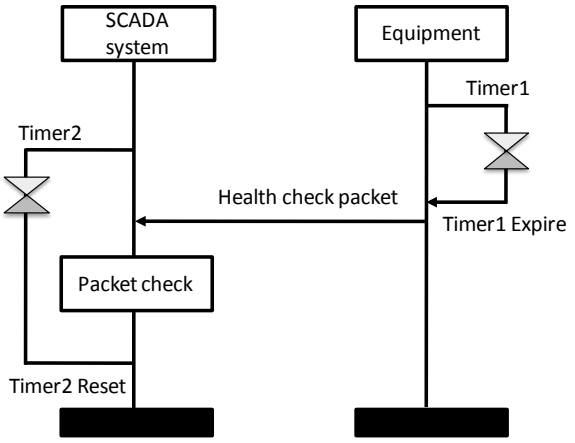

図 2 ヘルスチェックシーケンス

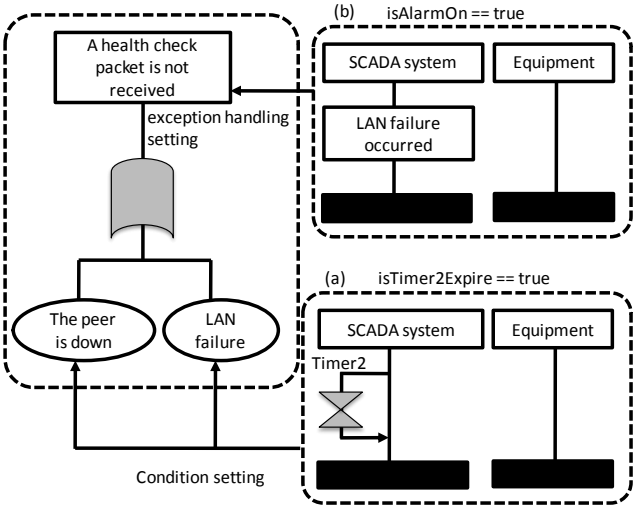

図 3 故障木図

手不応答と LAN 断が発生する条件は，監視制御システムのタイマ 2 が発火した時で，ヘルスチェックパケット未着が発生した時の例外処理は，アラーム発生であることを示す．

本アルゴリズムは，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故障木図の特性を利用する．

基本事象で示されるトップ事象の発生原因が生じた場合，中間事象やトップ事象の例外処理によって，望ましい状態に遷移している必要がある．これを確認するためには，発生原因が生じたならば，中間事象やトップ事象の例外処理を実行した後に満たすべき条件が必ず成立しているかどうかを調べればよい．この条件は，「□(<基本条件の発生条件>) ⇒◇(<中間事象の例外処理実行後の条件>∪…∪<トップ事象の例外処理実行後の条件>))」という LTL 式のテンプレートで表現される．

LTL 式では，命題 P に対して□P は「常に命題 P が成り立つ」，◇P は「いつか命題 P が成り立つ」ことを意味する．上述の LTL 式テンプレートは，<基本条件の発生条件> が発生した場合，いつか中間事象及びトップ事象の例外処理実行後の条件が必ず成り立つことを示す．

本アルゴリズムは，以下のステップから構成される．

- Step1. 故障木図の各基本事象に，基本事象が発生する条件を設定する．
- Step2. 故障木図の各中間事象とトップ事象に，当該事象の例外処理実行後に成立する条件を設定し，Step3 へ移動する．当該事象に例外処理が設定されていない場合は，本 Step を省略して Step3 へ移動する．
- Step3. 基本事象を一つ取得しカレント事象とする．全ての基本事象が取得済みの場合は，終了する．また，カレント事象の例外発生条件を取得して，Step4 へ移動する．
- Step4. カレント事象の上位事象が存在する場合，上位事象の例外処理後の成立条件を取得し，カレント事象の上位事象をカレント事象として，再度 Step4 を実行する．上位事象が存在しない場合は，Step5 へ移動する．
- Step5. LTL 式テンプレートに対して，Step3 で取得した基本条件の発生条件と，中間事象及びトップ事象の例外処理実行後の条件を適用し，LTL 式を生成する．その後，Step3 へ移動する．

本アルゴリズムの Step1 において，故障木図の基本事象「通信相手不応答」と「LAN 断」の発生条件を isTimer2Expire == true と設定する．これは，機器からヘルスチェックパケットが一定時間内に届かなかったことを示す．また，Step2 において，トップ事象「ヘルスチェックパケット未着」における例外処理「アラーム発生を行う」が実施された後に成立すべき条件を，isAlarmOn == true とする．これは，アラームが発生しているかを表すフラグが ON になっていることを示す．

図 3 の故障木図に対して本アルゴリズムを適用すると，□((isTimer2Expire == true)⇒◇(isAlarmOn == true))で示される LTL 式が導出される．これは，通信相手不応答か LAN 断が発生してタイマ 2 が発火したならば，必ずアラームが発生することを示す．

5. おわりに

本稿では，故障木図から導出した例外処理が適切かどうかを確認するための LTL 式を導出する手法について提案した．提案手法を用いることで，例外処理が実行された後に成立すべき条件を記述した LTL 式を導出することができる．検査対象となる例外処理が付加された通信シーケンスの Promela 記述を作成し，導出した LTL 式を満たすかどうかモデル検査ツールが網羅的に検査する．これにより，例外処理が適切に付加されたかどうかを確認することができる．

参考文献

[1] 長田知之，原内聡，北村操代，山地勉，上野泰秀:「故障木図からの例外処理導出による通信プログラム構築手法」，第 11 回情報科学技術フォーラム，No.11，pp.45-48 (2012)

[2] G.J. Holzmann : “The SPIN Model Checker“, Addison-Wsley (2004)