B-008

非機能要件を考慮した制御ロジック部品推薦手法
A Method to Recommend Control Logic Component using Non-functional Requirement

長田 知之†
NAGATA Tomoyuki

1. はじめに

変電所や上下水処理場などのプラントには、適切にプラントを運転するために必要な様々な機器が存在する。これらの機器の操作は、事故を発生させないための安全機構(インターロック)や遠隔制御機能などが含まれ、複雑な制御ロジックになる場合がある。プラントに含まれるコントローラは、制御ロジックに従い適切に機器を制御する(1)。

機器の制御ロジックは、機器や処理の入出力のつながりを接続線と論理演算素子(論理和、論理積など)で示した制御ロジック図で記述されることが多い。プラントには数百台の機器が含まれる場合があるため、システムエンジニアが作成する制御ロジック図も数百枚になる場合がある。このため、制御ロジック図の効率的な作成が求められている。

制御ロジック図作成の生産性を向上させるために、制御ロジック処理を部品化する手法が提案されている(2)(3)(4)。再利用可能な制御ロジック部品を用いることで、効率的に高品質な制御ロジック図を作成することができる。

本稿は、制御ロジック図の機能要件や非機能要件の仕様を基に、制御ロジック部品を推薦する手法について述べる。本手法を用いることで、適切な制御ロジック部品を用いて効率的に制御ロジック図を作成することができる。

2. 従来手法と課題

制御ロジック部品の提供によるシステム構築コスト低減手法には、以下の二つの課題がある。

課題の一点目は、開発を重ねると蓄積された部品の数が多くなり、システムエンジニアが目的の部品を探し出すことが困難になることである。適切な部品を短時間で検索できなければ、システムエンジニアは部品を探すよりも部品を使わずに制御ロジック図を作成するようになる。

課題の二点目は、システムエンジニアにとって未知の部品を検索することが困難なことである。汎用性は低いが特定の用途にのみ使用する部品は、システムエンジニアがその存在を知らないことが多い。このような場合、制御ロジック部品を探し出すことは難しい。

3. 提案手法

本稿では、制御ロジック部品の機能要件や非機能要件などの仕様から、適切な制御ロジック部品を推薦する手法について提案する(図 1)。提案手法では、制御ロジック部品の仕様を線形時相論理式(LTL 式; Linear Temporal Logic)で記述する。LTL 式は時間を取り扱える論理式で、対象のシステムの性質の記述に用いられることが多い。制御ロジック部品推薦ツールは、システムエンジニアが入力した仕様をキーに、仕様実現に必要な制御ロジック部品を推薦する。このとき、各部品の仕様は人手で全て記述する必要は無く、制御ロジック部品仕様生成ツールが部品仕様を自動生成する。

† 三菱電機　Mitsubishi Electric Corporation

制御ロジック部品の提供によるシステム構築コスト低減手法の課題の一点目「蓄積された部品の数が多くなると目的の部品を探し出すことが困難」と、二点目「システムエンジニアにとって未知の部品を検索することが困難」を、提案手法が適切な制御ロジック部品を入力された仕様から検索し推薦することで解決する。

提案手法では、「どのように制御するか」などの機能要件だけでなく、安全性質やセキュリティなどの非機能要件も LTL 式で記述する。これらの仕様をキーに部品を検索するため、システムエンジニアは非機能要件を考慮して部品を検索することができる。

4. 実現方式

本章では、制御ロジック部品仕様生成ツールによる制御ロジック部品仕様生成アルゴリズムと、制御ロジック部品推薦ツールによる制御ロジック部品推薦処理について具体例を述べる。

図2は基本制御ロジック部品の例で、図3は複合制御ロジック部品の例である。基本制御ロジック部品は、多くの制御ロジック図に繰返し現れる処理を部品化したものである。基本制御ロジック部品中に他の制御ロジック部品は含まないとする。

図2中左の制御ロジック部品は、「制御権取得中でかつエラーが発生していないとき、制御可能である」ことを示し、右の制御ロジック部品は値の上下限値逸脱判定を示している。このような入出力の関係を示す機能仕様だけでなく、「本制御ロジック部品ではアラームが発生することは無い」などの安全性質などの非機能要件も、LTL式で定義する。図2中の二つの部品とも、非機能要件「アラームは発生しない」を、LTL式「□(Alarm==false)」(常にAlarm変数はfalseである)で記述している。

複合制御ロジック部品は、複数の基本制御ロジック部品を組み合わせたものである。図3は、図2の二つの基本制御ロジック部品を組み合わせたもので、「上下限値判定で逸脱していないとき、制御する」ことを示す複合制御ロジック部品である。

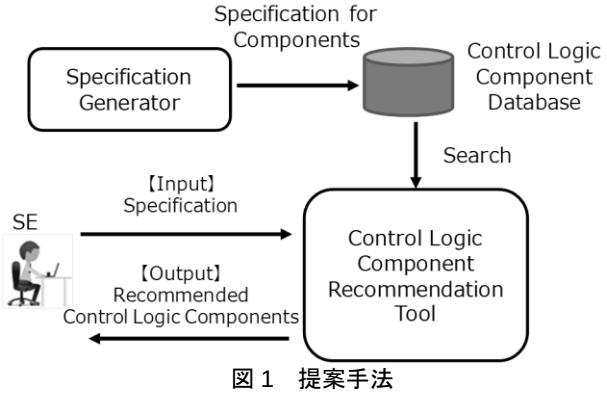

図 1　提案手法

4.1 複合制御ロジック部品仕様の導出

LTL 式の記述には数理論理の知識が必要なため、一般的なシステムエンジニアには難しい。提案手法では、基本制御ロジック部品の仕様の記述は、システムと数理論理の知識を有している熟練システムエンジニアが行うとし、複合制御ロジック部品の仕様は制御ロジック部品仕様導出ツールが生成する。

基本制御ロジック部品仕様からの複合制御ロジック部品仕様の導出は、以下のステップにより構成される。

- **Step1.** 複合制御ロジック部品の入力から、ロジック線の分岐が現れるまで、制御ロジック図の構成要素(基本制御ロジック部品や、論理演算部品などの演算部品)を取得し、Step2 へ移動する。出力まで到達した場合は、Step4 へ移動する。ロジック線の分岐が現れた場合は、Step3 へ移動する。
- **Step2.** 構成要素が基本制御ロジック部品の場合、事前に定義された部品仕様を取得し、Step1 へ移動する。構成要素が演算部品の場合、これまで取得した LTL 式の命題を演算部品に適用して新たな LTL 式を取得し、Step1 へ移動する。
- **Step3.** ロジック線の分岐が現れた場合、分岐以降のそれぞれのロジックに対して、Step1 の処理を実行する。
- **Step4.** 分岐ごとの LTL 式を論理積で結合し、簡略化して複合制御ロジック部品の部品仕様とする。

本処理により、図 3 の複合制御ロジック部品の仕様は、((LowerBound<Input2 ∧ Input2<UpperBound)∧(Input1==true) ⇒(Outpu1==true ∧ □(Alarm==false))となる。

4.2 LTL 式の仕様を基にした制御ロジック部品の検索

制御ロジック部品推薦ツールは、システムエンジニアが記述したい処理の仕様(自然言語または LTL 式)をキーに、仕様が定義された各部品の中から、必要な制御ロジック部品を検索して推薦する。

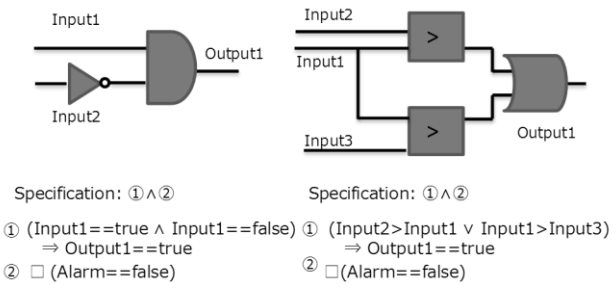

図 2　基本制御ロジック部品

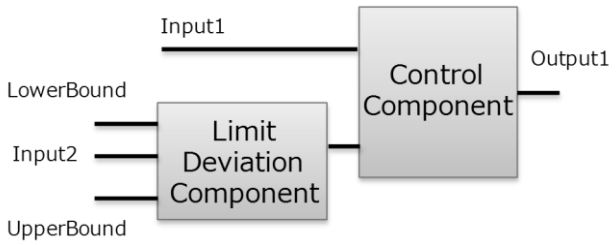

図 3　複合制御ロジック部品

システムエンジニアが入力した記述したい処理の仕様(機能要件と非機能要件)と、各部品の仕様とを比較し、以下のように検索を行う。

(ア) 機能要件と非機能要件が一致する部品が見つかった場合

- 入力されたシステムエンジニアの仕様と一致した制御ロジック部品が見つかったため、本部品を推薦する。

(イ) 機能要件は一致しているが、非機能要件が一部一致しない部品が見つかった場合

- 本部品を推薦すると共に、システムエンジニアに一致しない非機能要件を提示する。これにより、基本制御ロジック部品の非機能要件記述漏れか、部品が非機能要件を満たしていないかのチェックをシステムエンジニアに促す。

(ウ) 機能要件が一部一致している部品が見つかった場合(非機能要件の一致・不一致は問わず)

- 一致箇所と非一致箇所が論理和で結合されているならば、本部品の中の一致箇所をシステムエンジニアに通知する。作成対象処理の記述に本部品を直接利用することはできないが、本部品の一部をコピー&ペーストして利用することができる。また、本部品の一部では実現できない仕様をシステムエンジニアに通知する。

5. おわりに

本稿では、制御ロジック図の機能要件や非機能要件の仕様を基に、制御ロジック部品を推薦する手法について提案した。本手法を用いることで、非機能要件を考慮した制御ロジック部品を推薦することができる。

今後の課題としては、導出した複合制御ロジック部品の非機能要件の検証である。SCADE Suite Design Verifier[5]や MATLAB/Simulink Design Verifier[6]などのモデル検査ツールでは、制御ロジック図が LTL 式などで定義された性質を満たすかどうか、網羅的に検査する。導出された制御ロジック部品の仕様が成り立つかをモデル検査ツールで確認することで、提案手法の有効性を確かめることができる。

参考文献

[1] NAGATA Tomoyuki, NAKAGAWA Koichi, TSUDAKA Shinichiro, “A Method to Search Plant Control Systems as a Basis for Customization Using Plant Information", IIAI-AAI (2016).
[2] 長田 知之, 中川 晃一, 津高 新一郎 “解析ルールの階層化による制御ロジック図解析手法の提案”, 電気学会情報システム研究会 IS-15 pp.53-57 (2015).
[3] 脇本 浩司, 島 光秀, 田中 聡, 前田 アキラ, "グラフ表現を利用した図面の類似検索方式", 電子情報通信学会論文誌 D-II Vol.J77-D-II No.7 pp.1302-1310 (1994)
[4] 鷲崎 弘宜, 村上 真一, 深澤 良彰, " Simulink モデルにおけるグラフに基づく非完全一致モデルクローン検出", 電子情報通信学会技術研究報告, 知能ソフトウェア工学 112(165), pp.7-12 (2012)
[5] Esterel Technologies 社, "SCADE Design Verifier" (2017)
[6] MathWorks 社, "MATLAB Simulink Design Verifier" (2017)