

シーケンス制御回路の設計検証システム (1)
— システム構成 —

3U-9

松田 聖、武藤 昭一、吉澤 純一 (東京電力)
山田 直之、小林 康弘、元光 和夫、上田 至克、伊藤 順子 (日立製作所)

1. はじめに

各種の設計問題において、設計された結果が与えられた設計仕様を満たしているか否かの検証は不可欠である。現在、論理回路等の設計検証では、この検証法として数値シミュレーションによる方法が利用されている。しかしながら、高信頼性が要求される設計を中心として、数値シミュレーションによらない Formal Verification法が注目され始めている。

本研究では、対象として変電所の制御保護装置の設計検証を取り上げ、定理証明法を利用した検証システムを開発した。以下では、設計検証システムの構成を中心に報告する。

2. 問題の特徴

変電所の制御保護装置は、主に制御対象である主回路の電流、電圧、及び開閉器の動作状態により種々の論理判断を行うシーケンス制御回路により構成されている。設計対象であるこれらの制御保護装置は、設計検証上特に、(1)論理不具合、(2)廻り込み等回路構成上の不具合、(3)時間協調不具合、がないことを確認する必要がある。本研究で開発したシステムは、上記(1)(2)を対象としている。

さて、定理証明法による設計検証は、設計結果及び各種の公理の下で設計仕様が定理として証明できるか否かを検証する方法である。従って、設計検証システムは、シーケンス制御回路の以下に示す特徴を考慮した効率的なシステム構成とする必要がある。(a)設計仕様は、制御対象の動作として表現される、(b)制御回路の論理は、制御対象の動作として等価表現できる。

3. システム構成

開発したシーケンス制御回路の設計検証システムの構成を変電所の主回路と、その開閉器に対する操作インターロック回路の例を用いて図1に示す。図に示すように、本システムでは、シーケンス制御回路が実現する制御対象(主回路)の動作を制御論理として抽出(論理抽出プログラム)することにより、設計仕様と制御論理を制御対象の世界で統一的に表現し、それらに対して定理証明法を適用(定理証明プログラム)する方式を採用している。

この結果、本方式によれば、設計仕様からシーケンス制御回路の制御仕様を導く際に入り込む可能性のある誤りをも検証の対象範囲に含めることができる。

論理抽出プログラムは、シーケンス制御回路の構成要素の特性、及びそれらの結線関係から電氣的に実現される状況をリストアップすることにより制御論理を抽出する。

また、定理証明プログラムは、抽出された制御論理の下で、与えられた設計仕様が定理として証明されるか否かを一階述語論理体系での定理証明法を用いて検証する。この際、一階述語論理表現された制御対象の回路情報、及びその上での設計仕様の記述に関する公理を使用する。

4. むすび

以上、開発したシーケンス制御回路の設計検証システムについて、そのシステム構成を中心に説明した。検証手法の具体的説明、及び設計検証例については続報に記す。

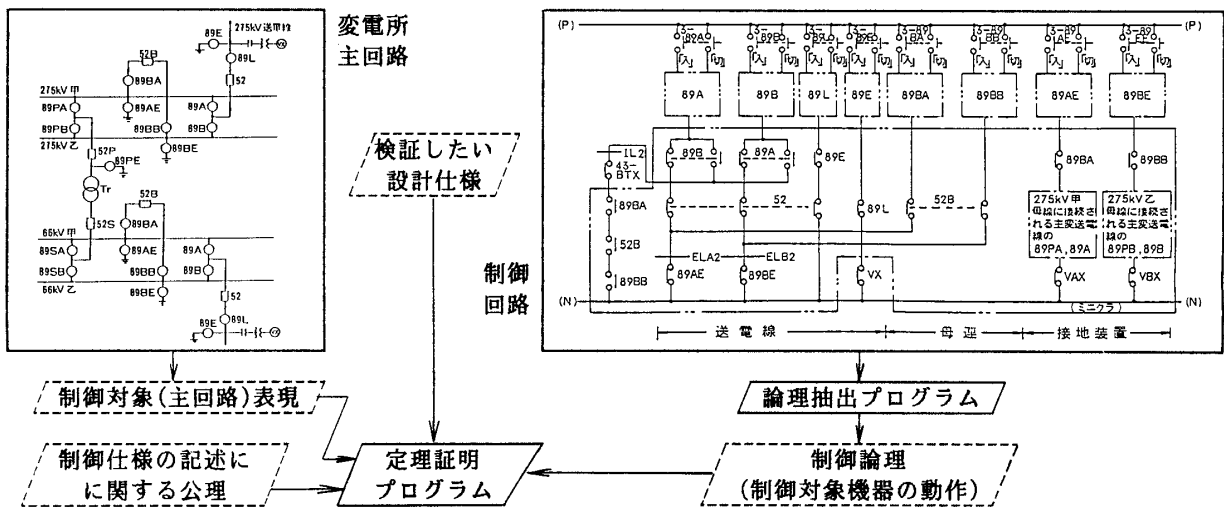


図1 設計検証システムの構成

A Design Verification System for Sequential Control Circuits No.1

Satoshi MATSUDA¹, Shoichi MUTO¹, Junichi YOSIZAWA¹, Naoyuki YAMADA², Yasuhiro KOBAYASHI²
Kazuo MOTOMITSU², Yosikatsu UEDA², Junko ITO² 1:TEPCO, 2:Hitachi Ltd.