Формальный дедуктивный анализ автоматного алгоритма управления генератором эндогаза с помощью платформы Rodin

Часть 1. Определение требований надёжности и безопасности работы генератора эндогаза

Максим Нейзов (neyzov.max@gmail.com)

Формальный дедуктивный анализ представляет собой строгий математический подход к верификации алгоритмов: алгоритм описывается с помощью аксиом, а требуемые свойства доказываются как теоремы. Цель представленного анализа – доказать соответствие алгоритма управления предъявляемым требованиям надёжности и безопасности. В статье описывается технологический процесс генерации эндогаза и определяются предъявляемые к нему требования надёжности и безопасности.

Введение

К программному обеспечению ответственных систем управления предъявляются серьёзные требования по безопасности. Для гарантии соответствия программ требованиям применяются формальные методы верификации и специальные инструментальные средства. В статье представлен формальный дедуктивный анализ автоматного алгоритма управления на предмет его соответствия требованиям безопасности технологического процесса генерации эндогаза. Данный анализ представляет собой строгий математический подход к исследуемой проблеме: математическая модель алгоритма строится на базе системы аксиом, а свойства безопасности доказываются как теоремы. Платформа Rodin [1] используется как средство автоматизации доказательства теорем.

В первой части статьи определяются требования надёжности и безопасности технологического процесса. Во второй – представлена платформа Rodin и автоматный алгоритм управления генератором. В третьей – выполняется построение формальной теории для алгоритма управления: алгоритм описывается с помощью аксиом, формализуются требования, которые должны быть доказаны как теоремы, демонстрируется доказательство теоремы.

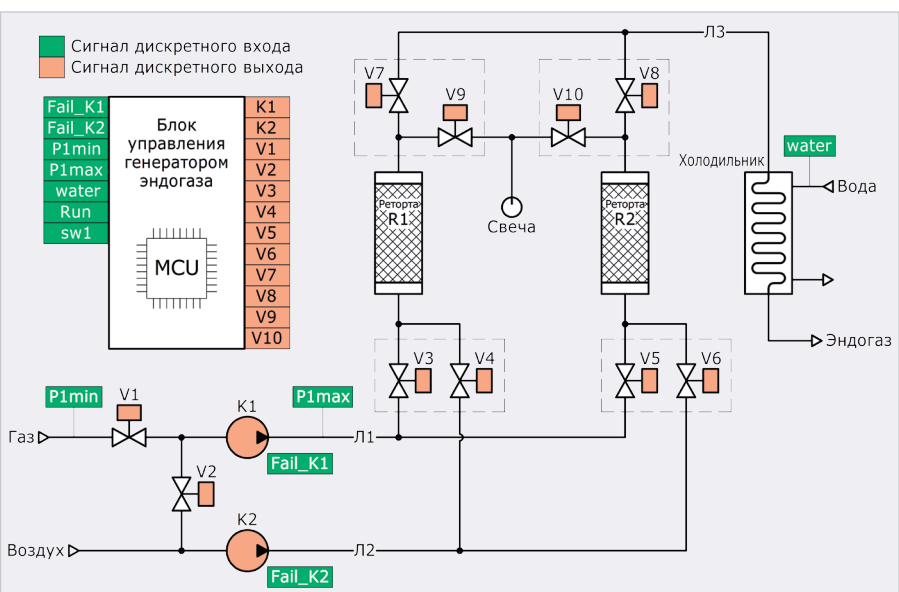

Рис. 1. Схема генератора эндогаза

Технологический процесс генерации эндогаза

Эндогаз используется в промышленной термообработке для насыщения стали углеродом. Эндогазовая установка предназначена для получения эндогаза. Химическая реакция приготовления эндогаза осуществляется в генераторе, который входит в состав установки. Схема генератора эндогаза изображена на рисунке 1. Генерация эндогаза имеет следующую технологию: исходная газовоздушная смесь (далее газ) проходит через катализатор реторты и под воздействием температуры +1050°C в результате химической реакции преобразуется в эндогаз. Далее происходит его охлаждение в холодильнике. Генератор имеет два канала: канал реторты R1 и канал реторты R2. В работе может находиться только один канал, второй канал – на восстановлении катализатора. Восстановление осуществляется чистым воздухом. Перед генерацией реторта должна продуваться газом в течении определённого времени.

В компрессорный блок входят компрессоры К1, К2 и клапаны V1, V2. Для подачи газа в реторты R1/R2 открывается клапан V1 и включается компрессор К1, создавая давление в линии Л1. Для подачи воздуха в реторты R1/R2 включается компрессор К2, создавая давление в линии Л2. При поломке компрессора К2 генерация эндогаза прекращается, и продувка реторт воздухом осуществляется с помощью компрессора К1. Для этого закрывается клапан V1 и открывается клапан V2.

Клапаны реторт V3...V10 предназначены для управления потоками через реторты R1/R2. Клапаны V4 и V6 предназначены для подачи воздуха в реторты. Клапаны V3 и V5 предназначены для подачи газа в реторты, а также воздуха в случае отказа компрессора К2. Клапаны V7 и V8 предназначены для подачи горячего эндогаза в линию Л3. Клапаны V9 и V10 предназначены для продувки реторт на свечу.

Система управления генератором эндогаза

Блок управления генератором эндогаза (см. рис. 1) построен на базе микроконтроллера (MCU), программируемого на языке C. Блок управления имеет дискретные входы и выходы. Сигналы Fail_K1/Fail_K2 – неполадка компрессоров K1/K2 – устанавливаются системой диагностики. Сигнал P1min – низкое давление газа на входе – и сигнал P1max – высокое давление в линии Л1, блок управления получает от реле давления. Сигнал water – наличие потока воды через холодильник – блок управления получает от реле потока. Сигнал Run – запустить генератор эндогаза – и сигнал sw1 – переключить на реторту R1 – блок управления получает от смежной системы эндогазовой установки. Блок управления выдает сигналы K1/K2 на электроприводы компрессоров, а также сигналы V1...V10 – электромагниты соответствующих клапанов. Оборудование генератора работает только при наличии сигнала Run. Если установлен сигнал sw1, то включается реторта R1, иначе включается реторта R2. Перед включением в работу реторта обязательно продувается газом. До включения реторты в работу противоположная реторта продолжает производить эндогаз. Отключённая реторта продувается воздухом. Компрессор K2 работает только при отсутствии неполадки Fail_K2. Компрессор K1 работает только при разрешении генерации эндогаза. Генерация эндогаза разрешена, если нет сигналов P1min, P1max, Fail_K1 и есть сигнал water. При отключении одного из компрессоров обе реторты продуваются воздухом.

Требования надёжности и безопасности

Генерация эндогаза сопровождается следующими опасными производственными факторами: высокой температурой, ядовитостью и взрывоопасностью эндогаза. В связи с этим к генератору и его программному обеспечению предъявляются повышенные требования (*REQ1...REQ16*) по надёжности и безопасности.

Первая группа требований относится к работе клапанов.

REQ1: Клапаны V1 и V2 никогда не открыты одновременно.

Одновременное открытие клапанов V1 и V2 приведёт к смешиванию газа и воздуха. Попадание воздуха в исходный газ негативно скажется на технологических параметрах эндогаза. Попадание газа в воздушный тракт сделает невозможным восстановление катализатора реторт.

REQ2: Клапаны V3 и V4 никогда не открыты одновременно.

Одновременное открытие клапанов V3 и V4 также приведет к смешиванию газа и воздуха при работающих компрессорах. При отключении одного из компрессоров может произойти переток, что приведет к снижению расхода через реторту. Аналогичное требование к работе клапанов V5 и V6.

REQ3: Клапаны V5 и V6 никогда не открыты одновременно.

REQ4: Клапаны V7 и V9 никогда не открыты одновременно.

Если реторта R1 производит эндогаз, то одновременное открытие клапанов V7 и V9 приведет к выбросу эндогаза на свечу и резкому снижению производительности генератора. Если реторта R1 продувается воздухом, то одновременное открытие клапанов может привести к попаданию воздуха в линию Л3 и **взрыву** эндогаза. Аналогичное требование к работе клапанов V8 и V10.

REQ5: Клапаны V8 и V10 никогда не открыты одновременно.

REQ6: Снятие сигнала Run закрывает все клапаны.

Несанкционированное открытие клапанов может привести к аварийной ситуации.

Вторая группа требований относится к работе компрессоров.

REQ7: Компрессор K1 работает только при наличии разрешения генерации эндогаза.

Несанкционированное включение газового компрессора может привести к аварийной ситуации. Аналогичное требование для компрессора K2.

REQ8: Компрессор K2 работает только при наличии разрешения его работы.

REQ9: Воздушный компрессор K2 перекачивает только воздух.

Попадание газа в линию Л2 приведёт к невозможности восстановления катализатора реторт.

REQ10: Компрессор K1 перекачивает или газ, или воздух, но не их вместе.

Одновременная перекачка газа и воздуха приведёт к невозможности восстановления катализатора реторт и генерации эндогаза с заданными параметрами.

REQ11: Компрессоры K1 и K2 никогда не перекачивают одно и то же вещество.

Одновременная подача в линии Л1 и Л2 одного и того же вещества приведёт к невозможности правильной работы одного из каналов генератора.

REQ12: Снятие сигнала Run отключает компрессоры.

Несанкционированное включение компрессоров может привести к аварийной ситуации.

Третья группа требований относится к потокам веществ.

REQ13: Эндогаз не может подаваться в холодильник из двух реторт одновременно.

Одновременная генерация эндогаза двумя ретортами приведёт к останову генератора после выработки ресурса катализаторов. Поэтому хотя бы одна реторта должна быть на восстановлении катализатора, чтобы заменить реторту, выработавшую свой ресурс. Таким образом обеспечивается бесперебойность работы генератора.

REQ14: В линии Л3 никогда нет воздуха.

Попадание воздуха в линию Л3 может привести к **взрыву** эндогаза.

REQ15: При подаче газа всегда открыт газовый тракт через реторту.

Отсутствие газового тракта через реторту приведёт к прекращению подачи газа, т.е. компрессор K1 будет работать в упор на закрытый клапан. Работа в данном режиме запрещена.

REQ16: Газ подаётся на две реторты и одна из них работает на холодильник тогда и только тогда, когда первая реторта находится в рабочем режиме, а вторая – в режиме продувки газом.

Данное требование устанавливает соответствие режимов работы фактическим действиям.

Для безаварийной работы генератора эндогаза требования *REQ1...REQ16* должны гарантированно соблюдаться. Тестирование не может гарантировать соблюдение данных требований – для этого необходимы формальные методы верификации. Для доказательства корректности алгоритма управления относительно данных требований выполняется формальный дедуктивный анализ.

Заключение

В статье рассмотрен технологический процесс генерации эндогаза и определены предъявляемые к нему требования надёжности и безопасности. Алгоритм управления технологическим процессом должен соответствовать этим требованиям. Для гарантии соответствия необходим формальный анализ алгоритма. Во второй части статьи будет рассмотрена платформа Rodin и автоматный алгоритм управления генератором.

Литература

1. Rodin Handbook. URL: www3.hhu.de/stups/handbook/rodin