ОБЩИЙ ВЗГЛЯД НА ПРОЦЕССЫ РЕВЕРС-ИНЖИНИРИНГА В ПРОМЫШЛЕННЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Номер секции: 1

Шведова Ольга Александровна
старший преподаватель кафедры ИСиТ Института информационных технологий Белорусского государственного университета информатики и радиоэлектроники
Orcid ID: 0009-0009-2422-8185; shvedova@bsuir.by

Аннотация. В статье рассмотрена технология реверс-инжиниринга как один из способов разработки документации, алгоритмов и программного обеспечения для автоматизированных систем управления технологическими процессами и производствами. Представлены этапы проведения реверс-инжиниринга со спецификой применения в промышленных системах управления. Приведен пример использования реверс-инжиниринга для управления установкой на молочном производстве.

Ключевые слова: промышленных системах управления, реверс-инжиниринг, алгоритм управления сепаратором.

Annotation. Annotation. The article considers the technology of reverse engineering as one of the ways to develop documentation, algorithms and software for automated control systems for technological processes and industries. The stages of reverse engineering with the specifics of application in industrial control systems are presented. An example of using reverse engineering to control a dairy plant.

Key words: industrial control systems, reverse engineering, separator control algorithm.

На белорусском рынке промышленной автоматизации большую часть технологического оборудования и компонентов систем управления составляет оборудование производства ЕС. В связи с введенными санкциями наблюдается уход компаний-поставщиков и специалистов, ограничение или блокирование поставок компонентов и программного обеспечения для автоматизации на различных уровнях и этапах. Таким образом в настоящее

время становятся очень актуальными проблемы, связанные с бесперебойным обслуживанием автоматизированных систем управления технологическими процессами и производствами (далее АСУТПиП) (замена на аналоги технологического оборудования или компонентов автоматики, устранение технологических ошибок, настройка параметров работы оборудования), а также связанные с их модернизацией или интеграцией в системы MES или ERP.

Одним из вариантов решения проблем может быть применение реверс-инжиниринга для восстановления полной технической документации и алгоритмов функционирования АСУТПиП на основании знаний о принципах ее работы, имеющейся документации, реального оборудования и опыте его эксплуатации.

Обратный инжиниринг, обратное проектирование или реверс-инжиниринг в промышленных системах управления — это комплекс технологий, аппаратных и программных средств, а также методик, необходимых для создания объекта с характеристиками аналогичными или более высокими по сравнению с исходной системой [1].

Особенностью промышленных систем управления является их комплексность. Предполагается, что, помимо высокотехнологичного оборудования, в их состав входит и программное обеспечение (далее ПО) контроллерной группы, панелей оператора, SCADA-систем и т.п. Таким образом, выделяют следующие *этапы проведения реверс-инжиниринга промышленных систем управления для восстановления документации и ПО*:

1. анализ существующих производственных процессов (технологическое оборудование, элементы системы управления, выполнение алгоритмов управления) с формированием списка замечаний и требований по доработке;
2. анализ и фиксирование параметров обмена данными интегрированного оборудования;
3. анализ алгоритмов и параметров технологического процесса с помощью проведения испытаний работы установки по разработанным методикам и

программам с учетом специфики технологического процесса с фото и видео фиксацией;

4. изучение и восстановление документации до актуального состояния (технологических, структурных схем системы управления, электрических принципиальных схем оборудования) с требуемой для решения задачи детализацией;

5. разработка ПО;

6. проведение испытаний с использованием моделей технологического процесса и симуляторов системы управления с итерационным приближением к существующей системе до достижения желаемых результатов управления технологическими процессами;

7. пуско-наладочные работы с доработкой и тестированием программного решения на технологическом оборудовании, а также подбором параметров. Итерационное приближение к функциональности существующей системы до достижения желаемых результатов управления технологическими процессами;

8. внесение корректировок в полученную систему управления в соответствии с замечаниями и требованиями;

9. доработка технической и эксплуатационной документации.

Для примера применения технологии реверс-инжиниринга рассмотрим разработку сегмента ПО для управления сепаратором Tetra Pak с внедрением его в работу пастеризационно-охладительной установки (далее ПОУ) Frau Impianti на молочном производстве. Основными сложностями для выполнения проекта были: использование редкой конфигурации системы управления (панель управления выполняла алгоритмы контроллера и панели оператора), доступ с использованием системы паролей к ПО сепаратора, отсутствие технической документации или недокументированные изменения в процессе эксплуатации оборудования, разнородная сетевая топология Profinet (подключение ПОУ со сложной структурой и алгоритмами обмена данными)

и Profibus DP (подключение частотных преобразователей с собственной конфигурацией и параметрами).

Основными этапами проекта были:

1. восстановление схемы электрической:

1.1. собеседование с заказчиком, осмотр объекта (с фотографированием);

1.2. первоначальное планирование работ, подготовка к обследованию объекта и поиск технической документации или ее фрагментов, формирование начального архива;

1.3. первичное обследование объекта: фотографирование общих планов со всех необходимых ракурсов; перепись номеров цепей с привязкой к номерам клемм элементов; фотографирование отдельных зон и отдельных элементов;

1.4. составление предварительных перечней элементов с номерами клемм и цепей, к ним присоединенным, предварительной электрической схемы, списка невыясненных вопросов;

1.5. повторное обследование объекта;

1.6. разработка схемы электрической принципиальной;

2. восстановление алгоритма работы:

2.1. первичное обследование объекта: пробные пуски (с изменениями режимов работы или активации отдельных элементов при необходимости); видеофиксация элементов индикации и экранов панелей операторов; запись таблиц мониторинга на программаторе, подключенных к ПЛК; фиксация пользовательских настроек параметров;

2.2. составление блок-схем 1-2 уровней и списка невыясненных вопросов;

2.3. повторное обследование объекта;

2.4. восстановление (описание и документирование) алгоритма - перечень активных элементов, сигналов АСУТП, параметров и уставок; аварийные ситуации, блокировки; аварийная и предупредительная сигнализация; режимы работы, отдельные алгоритмические последовательности; полная пошаговая таблица активации (активные элементы, сигнализация, параметры) с указанием условий перехода; корректировка блок-схемы 2-го уровня;

2.5. интегрирование программы управления сепаратором в программу управления ПОУ для контроллера и панели оператора;

2.6. обновление программ, первичные испытания с фиксацией полученных результатов;

2.7. доработка программного обеспечения, повторные испытания и т.д.;

2.8. ввод в эксплуатацию, доработка эксплуатационной документации.

Оперативно выполнить проект позволило знание технологии работы сепаратора и ПОУ, а также открытый программный код ПОУ. В ходе решения задачи дополнительно были обнаружены и исправлены некоторые технологические ошибки в работе ПОУ.

Таким образом, описанный в работе подход обладает рядом преимуществ:

1. формирование полного пакета технической и эксплуатационной документации, получение полного доступа к технологическому оборудованию и системам управления;

2. возможность изучить примененные технологии, на разработку которых могли быть затрачены большие временные и материальные ресурсы.

Можно отметить, что проведение реверс-инжиниринга для промышленных систем управления является непростой и специфической задачей со своими отличительными особенностями.

Список использованной литературы

[1] Обратное проектирование и реверс-инжиниринг [Электронный ресурс]. – Режим доступа: https://unicon-engineering.ru/services/design/section7/. Дата доступа: 04.05.23.

[2] Знание Основных Концепций Реверс-Инжиниринга [Электронный ресурс]. – Режим доступа: https://www.dz-techs.com/ru/reverse-engineering-concepts. Дата доступа: 04.05.23.

[3] Русакович В.Г., Техническая документация проекта: Восстановление структуры АСУТП. – ПлаваРБ, 2020. 48 с.