УДК 681.5

В.Н. НЕМОВ, студент гр. ЭТа-211 (КузГТУ)
г. Кемерово

ТЕОРЕТИЧЕСКИЕ ВОЗМОЖНОСТИ ВОССТАНОВЛЕНИЯ ПРОГРАММНОГО КОДА ПРОГРАММИРУЕМОГО ЛОГИЧЕСКОГО КОНТРОЛЛЕРА ПО АНАЛИЗУ ЕГО РАБОТЫ.

Программируемые логические контроллеры уже долгие годы находят широкое применение в системах автоматического управления техническими процессами в различных областях промышленности, сельского хозяйства и электро- и теплоэнергетики[1]. На данный момент на рынке существует большое количество компаний, предоставляющих готовые проектные решения для создания систем автоматизации. При этом некоторые из них предоставляют продукт с закрытым программным обеспечением. Это усложняет ремонт, требует времени на ожидания визита авторизированного сервисного специалиста.

В текущей ситуации, когда многие иностранные компании перестали осуществлять свою деятельность на территории Российской Федерации, выполнение ремонта зачастую становиться просто невозможным. Из этого следует, что по мере выхода из строя систем автоматизации иностранного производства, и в частности входящих в их состав ПЛК, будет не только востребованная замена на отечественные системы, но и любые методы сокращения времени на эту операцию. А любая замена ПЛК на ПЛК другого типа или производителя потребует написание программного кода управления. При этом у разработчика не будет доступа с оригинальному коду, к его алгоритмам, параметрам регуляторов и временным интервалам, что, как минимум, усложнить и затянет разработку и наладку.

Для того, чтобы по возможности избежать ситуации написания кода программ «с нуля», выявить критические значения настроек, и тем самым сократить сроки разработки, предлагается использовать методы реинжиниринг, позволяющие восстановить хотя бы часть алгоритмов оригинального управлявшего программного кода.

Реализация этого предполагается через создание аппаратного и программного комплекса.

Аппаратный комплекс должен представлять собой переносное устройство, способное подключаться параллельно входам и выходам исследуемого ПЛК для выполнения регистрации его действия при различных комбинациях «естественных», идущих от оборудования, входных сигналах. Такое устройство может быть выполнено в виде металлического кейса с дополнительным комплектом проводников. При работе устройство может размещаться либо возле шкафа управления, либо, при наличии места или специальной, компакт-

ной, реализаций устройства, непосредственно в самом шкафу. Запись захватываемой информации может ввестись на внешний или встроенный носитель. Либо на оба сразу, а также передаваться по сети.

Сразу очевиден недостаток такого решения - возможна записи только «нормального» режима работы системы управления. Запись действий исследуемого ПЛК или системы при «аварийных» или любых иных, не регулярных, ситуациях становиться возможна только при установке ПЛК или системы управления в стенд-имитатор сигналов технологического процесса. Создание такого стенда не представляет большой сложности, но, в то же время, для его корректной работы требуется определенный уровень исследования технологического процесса, который способен привести на тот уровень понимания процесса, когда разработка собственной системы управления «с нуля» уже не будет являться проблемой. И тем самым задача обратной разработки просто перестанет существовать. Однако, некоторые алгоритмы реакции могут представлять интерес, как информация, позволяющая лучше понять специфику управления или реализации аварийных защит объекта автоматизации.

С другой стороны, существует фундаментальный вопрос самой возможности восстановления алгоритмов работы управляющей программы хотя бы и в «нормальном» режиме. Даже поверхностный анализ примеров [2] программного кода простых систем управления выявляет наличие возможность многообразие ветвлении и временных интервалов. Несомненно, все они могут быть записаны и представленные в виде графиков сигналов во времени, но само по себе это не решает задачу автоматизации анализа и восстановление оригинального алгоритма.

Для решения этой задачи стоит обратиться к опыту автоматического синтеза программ[3]. Существующие методики способны ускорить синтез линейных или параллельных программных процессов. Но не способны реализовать в полной мере синтез сложных алгоритмов. А также требуют точных входных данных для успешной реализации синтеза.

Другой, более интересный метод, появившейся в последнее время – «чат боты» на основе искусственных нейронных сетей. Они уже сейчас позволяют решать задачи по написанию программного кода на основе текстового описания желаемого алгоритма или функционала. Однако уровень таких решений не высок, само решение состоит из набора типовых решений, найденных нейронной сетью в сети интернет, и не всегда сразу способно к корректной работе. В то же время, нейронная сеть демонстрирует возможности синтеза приемлемого решения даже на основе не полного описания.

В то же время есть ещё одна задача, автоматизация которой тоже возможна и даже допускает не участие в этом человека. Это задача перехвата и декодировании протоколов обменная различной информацией. С одной стороны, в случай промышленных решений, все протоколы, их состав, структура, временные интервалы, либо уже полностью открыты, либо широко известны, несмотря на закрытость.

При этом «секретом» могут быть содержимое кодов управления, и назначений регистров. И в особенности – внутренние настройки, такие как адрес,

время ответа/запроса и т.д. Поэтому при восстановлении системы управления в целом эта информация тоже представляет значительный интерес при своей исходной недоступности.

В конечном итоге все существующие методы могут быть сложно применимы из-за очевидных пробелов в исходных данных. Поэтому участие компетентного специалиста необходимо на всех этапах процесса. Из предлагаемых в итоге программных решений наиболее перспективным видеться создание систем автоматического синтеза на основе нейронных сетей. Такие решения будут полезны не только в процессах обратного инжиниринга, но в практике любого проектирования программного кода систем автоматизации. А для проверки полученных решений допустимо реализовать нейронные сети с возможностью реконфигурации, имитирующие работу реальных объектов автоматизации.

Список литературы:

1. О.И. Максимычев, А.В. Либенко, В.А. Виноградов Программирование Логических контроллеров (plc). Учебное пособие. – М.: «МАДИ», 2006
2. М.П. Кульчавеня. Основы программирования ПЛК – М.: «Нобель Пресс», 2012. – 128 с.
3. Воеводин В.В., Воеводин Вл.В. Параллельные вычисления. – СПб.: БХВ-Петербург, 2004. – 608 с.

Информация об авторах:
Немов Владислав Николаевич, студент гр. ЭТа-211, КузГТУ, 650000, г. Кемерово, ул. Весенняя, д. 28, nemovvn@kuzstu.ru