УДК 004.94

Применение сетей Петри при моделировании атак на системы АСУ ТП

V.Yu. Shevtsov, D.I. Pravikov

The Application of Petri Nets for Modeling Attacks on ICS

Abstract. *. In this paper, we present a method of modeling attack on ICS that is based on extended Petri nets. This approach allows to describe object of automatisation. It's possible through changing positions. The model has been created for a pumping station. A typical control scheme of a pumping station and scenarios of its operation in case of various attacks are given. The CPN Tools software is being used for model realizing.*

Keywords: *Petri net, subclass of Petri net, industrial control system (ICS), pumping station, programmable logic controller (PLC), Supervisory Control And Data Acquisition (SCADA system), decision support system (DSS), functional safety.*

В.Ю. Шевцов[1]
Д.И. Правиков[2]
[1]Аспирант, инженер кафедры комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина.
E-mail: vadim94.d@mail.ru
[2]Кандидат технических наук, заведующий кафедрой комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина.
E-mail: dip@gubkin.pro

Аннотация. *В статье предлагается метод моделирования атак на системы АСУ ТП на базе расширенного аппарата сетей Петри. Данный подход позволяет подробно описать процесс объекта автоматизации, благодаря поддержке изменений состояний. Модель выполнена для нефтеперекачивающей станции. Описана типовая схема управления нефтеперекачивающей станции, сценарии ее работы в случае различных атак злоумышленника. Для реализации модели используется программное обеспечение CPN Tools.*

Ключевые слова: *сеть Петри, подкласс сети Петри, автоматизированная система управления технологическим процессом (АСУ ТП), нефтеперекачивающая станция (НПС), программируемый логический контроллер (ПЛК), единая система диспетчерского управления (SCADA-система), система поддержки принятия решений (СППР), функциональная безопасность.*

ВВЕДЕНИЕ

Информационная безопасность (ИБ) автоматизированных систем управления технологическими процессами (АСУ ТП) продолжает оставаться актуальной проблемой, ввиду высокого уровня значимости таких систем и интереса со стороны злоумышленников [1]. При этом, даже не смотря на наличие систем защиты отдельных подсистем, функциональная безопасность всей системы может оставаться под угрозой.

Для понимания того, каким образом необходимо обеспечивать безопасность АСУ ТП, важно проводить моделирование различных сценариев работы таких систем. Но текущие исследования обычно рассматривают типовые АСУ ТП без привязки к специфичным процессам конкретного производства [2-6].

В данной работе за основу моделирования взят аппарат сетей Петри, т.к. он позволяет показать изменение состояний системы, а благодаря расширениям базового метода (использованы функциональные, цветные, ингибиторные, иерархические подклассы сетей Петри) возможно подробное описание АСУ ТП.

Для реализации модели АСУ ТП нефтеперекачивающей станции используется свободно распространяемое программное обеспечение CPN Tools версии 4.0.1. Оно предоставляет широкие возможности и гибкость при построении сетей Петри.

Статья состоит из следующих частей. В первом разделе рассматривается типовая схема управления нефтеперекачивающей станции в разрезе АСУ ТП, для которой будет разработана модель. Во втором разделе дается описание сети Петри для целевой системы на основе программной реализации в CPN Tools. В третьем разделе представлены возможные сценарии работы нефтеперекачивающей станции в случае реализации угроз злоумышленником на основе разработанной модели.

ТИПОВАЯ СХЕМА УПРАВЛЕНИЯ НЕФТЕПЕРЕКАЧИВАЮЩЕЙ СТАНЦИИ

Нефтеперекачивающая станция – комплекс раз-

личного оборудования и сооружений, который позволяет производить эффективную транспортировку нефтепродуктов по нефтепроводам.

В общем виде схема управления нефтеперекачивающей станцией представлена на рисунке 1. Она состоит из следующих элементов:

• автоматизированное рабочее место оператора (АРМ);

• система поддержки принятия решений (СППР);

• единая система диспетчерского управления (SCADA-система);

• программируемый логический контроллер (ПЛК);

• узел регулирования давления (УРД);

• входной и выходной манометры (датчики входного и выходного давления).

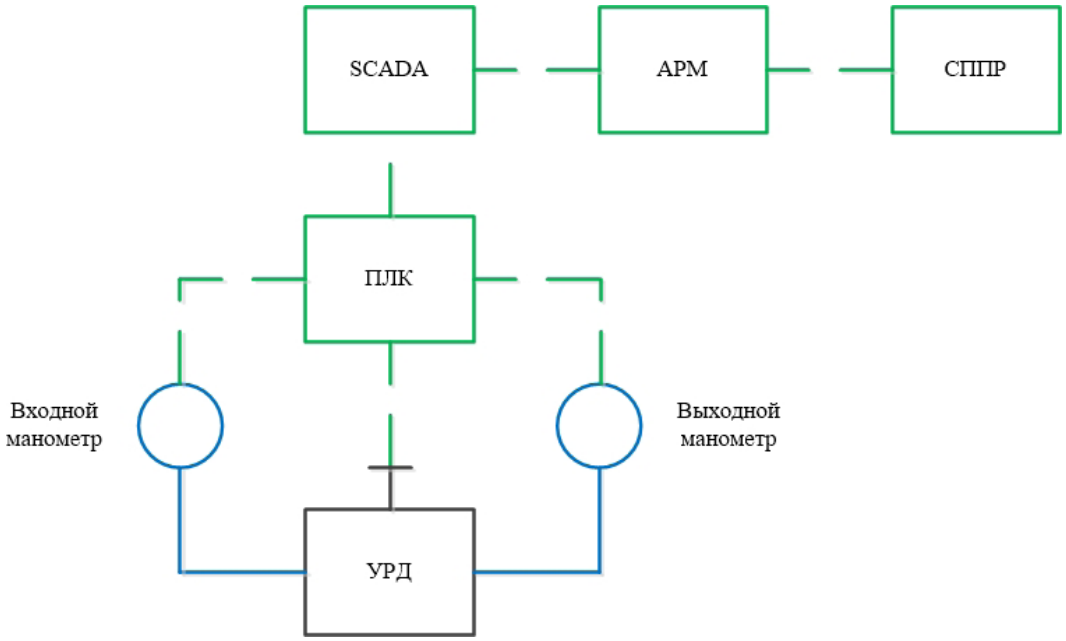

Рис. 1. Типовая схема управления нефтеперекачивающей станции

При нормальном режиме работы значения давления на манометрах находятся в определенном уровне допустимых значений, ручного изменения состояния УРД не требуется.

В случае выхода значений давления на датчиках за пределы допустимых оператор отправляет соответствующий сигнал на УРД, чтобы нормализовать давление в системе. Также может сработать система противоаварийной защиты и остановить НПС.

Для рассматриваемой НПС возможны следующие атаки:

• Атака на АРМ оператора;

• Атака на SCADA-систему;

• Атака на датчики (входного и выходного давления);

• Атака на ПЛК с заменой данных, поступивших от датчиков;

• Атака на ПЛК с отправкой данных на УРД.

При этом данные атаки направлены либо на открытие регулятора (в дальнейшем происходит остановка НПС или снижение надежности системы), либо на его закрытие (в дальнейшем происходит остановка НПС или снижение расхода).

МОДЕЛЬ НЕФТЕПЕРЕКАЧИВАЮЩЕЙ СТАНЦИИ НА ОСНОВЕ СЕТИ ПЕТРИ

Сеть Петри, выполняющая моделирование НПС, включает в себя 6 подсетей, соответствующих элементам схемы управления НПС (рисунок 2):

• ***2 подсети датчиков давления (Manometer1 и Manometer2):*** входные позиции атак на датчики (Attack Sensor1, Attack Sensor2); выходные позиции получения данных от датчиков (Get Sensor1 Data, Get Sensor2 Data).

• ***Подсеть ПЛК (PLC):*** входные позиции получения данных от датчиков (Get Sensor1 Data, Get Sensor2 Data), атака на ПЛК с заменой данных датчиков (Attack1 PLC, Attack2 PLC), атака с отправкой данных на УРД (Attack3 PLC); выходные позиции получения данных от PLC и получение сигнала управления (Get PLC data, Send rule signal).

• ***Подсеть SCADA (SCADA):*** входные позиции получения данных от ПЛК и отправки сигнала на SCADA-систему (Get PLC data, Send signal to SCADA); выходные позиции получения данных и отправки

данных на ПЛК (Get data, Send signal to SCADA).

• ***Подсеть АРМ оператора (Operator's PC):*** входные позиции получения данных и атаки на АРМ оператора (Get data, Attack operator's PC); выходная позиция отправки сигнала на SCADA (Send signal to SCADA).

• ***Подсеть УРД (Rule_Mechanism):*** входная позиция получения сигнала управления (Get rule signal); выходные позиции закрытия и открытия регулятора (Close regulator, Open regulator).

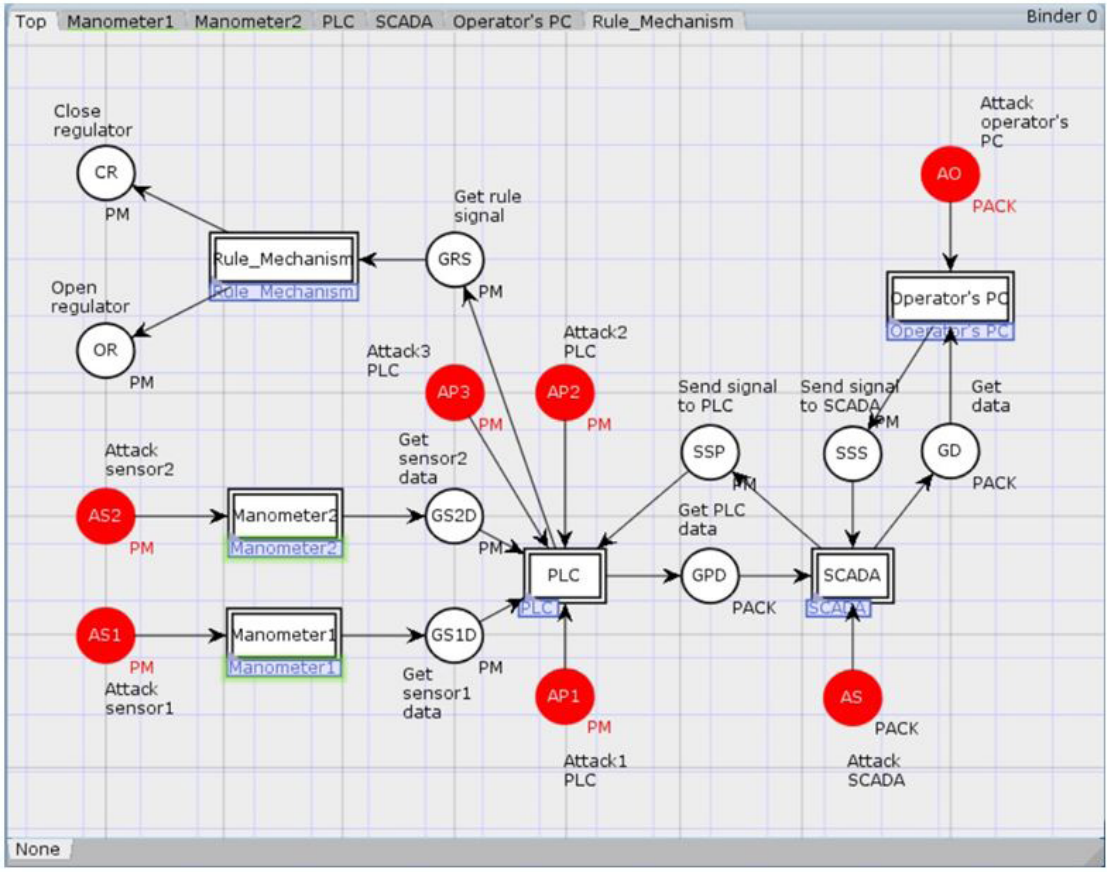

Рис. 2. Основная сеть Петри модели нефтеперекачивающей станции

Данная модель использует следующие объявления:

```
colset pm = with NP1 | LP1 | HP1 | NP2 | LP2 | HP2
| RP1 | RP2 | RP3 | PLC;
colset I = int;
colset PM = product pm * I;
var p1 : pm;
var i : I;
colset PACK = list PM;
var pack : PACK;
var pack1 : PACK;
var pack2 : PACK;
```

Позиции, имеющие цвет PM описываются двумя параметрами: pm – информация датчика/ПЛК, I – счетчик цикла. Для цвета PACK – список, содержащий несколько значений PM для последующей обработки.

Закрашенные позиции соответствуют атакам злоумышленника. В случае наличия фишки в одной из таких позиций произойдет вредоносное воздействие на систему, в результате чего сеть завершит свое выполнение в одной из конечных позиций: открытие регулятора (Open regulator) или закрытие регулятора (Close regulator).

СЦЕНАРИИ РАБОТЫ НПС ПРИ РЕАЛИЗАЦИИ УГРОЗ ЗЛОУМЫШЛЕННИКОМ

Рассмотрим подробнее сценарии проведения атак злоумышленником на НПС, озвученные в первой части.

• ***Атака на АРМ оператора*** (позиции внутри подсети: система поддержки и принятия решений: Decision support system; анализ данных – Analysis data), ***атака на SCADA-систему*** (позиции внутри подсети: отправка данных – Send data; получение сигнала оператора – Get operator's signal) представлены на рисунке 3.

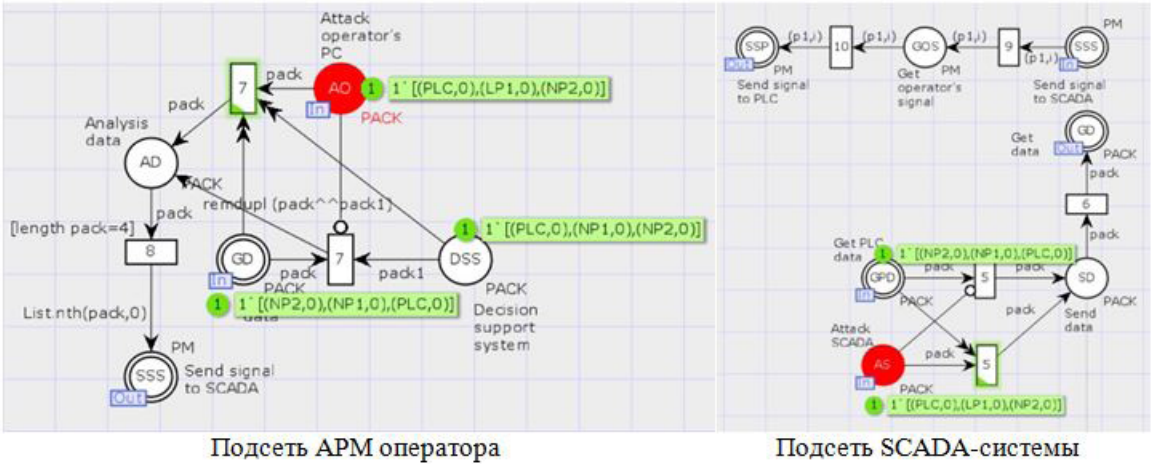

Рис. 3. Сети Петри, иллюстрирующие первую и вторую атаки

Особенность атак на автоматизированное рабочее место оператора и SCADA-систему в том, что эти объекты часто работают на базе операционных систем общего назначения и могут использовать распространенные программные решения (например СУБД). Поэтому для нарушения производственного процесса самым сложным для злоумышленника будет разобраться в специализированном ПО. В таком случае, как видно на рисунке 3, происходит блокирование передачи и сброс реальных данных из смежных объектов АСУ ТП (для этого в сети Петри использованы ингибиторные дуги и дуги сброса соответственно). Разрешенным переходом является переход из позиции атак со сбросом реальных данных (данный переход выделен на рисунке).

• ***Атака на датчики*** (позиции внутри подсети: считывание входного/выходного давления – Reading correct input/output pressure; отправка данных входного давления – Send manometer1 data) представлена на рисунке 4.

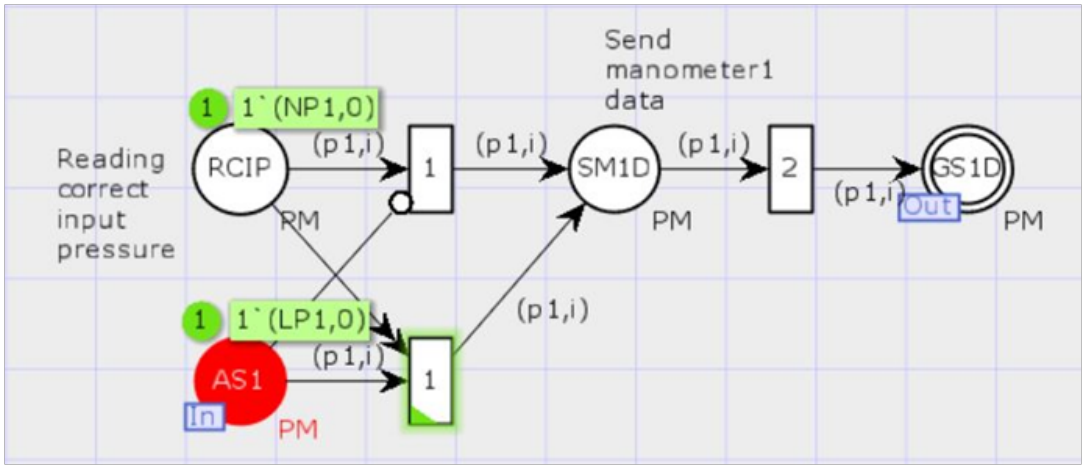

Рис. 4. Сеть Петри, иллюстрирующая третью атаку

Атака на датчики (входного и выходного давления) позволяет злоумышленнику точечным образом привести НПС в аварийное состояние, затратив минимум усилий. Оператор может не сразу понять, что датчик отправляет ложные значения, и в итоге отправит неправильные команды управления на УРД. Алгоритм атаки прост: реальные данные датчика блокируются и подменяются критическими.

• ***Атака на ПЛК с заменой данных, поступивших от датчиков, атака на ПЛК с отправкой данных на УРД*** (позиции внутри подсети: отправка полученных данных – Send getting data; получение сигнала от SCADA-системы – Get SCADA signal; отправка сигнала управления – Send rule signal) представлены на рисунке 5.

Данные атаки нацелены на программируемый логический контроллер, что требует от злоумышленника определенных знаний об атакуемом объекте. При этом в первом случае происходит атака, аналогичная третьей, при которой необходимо иметь

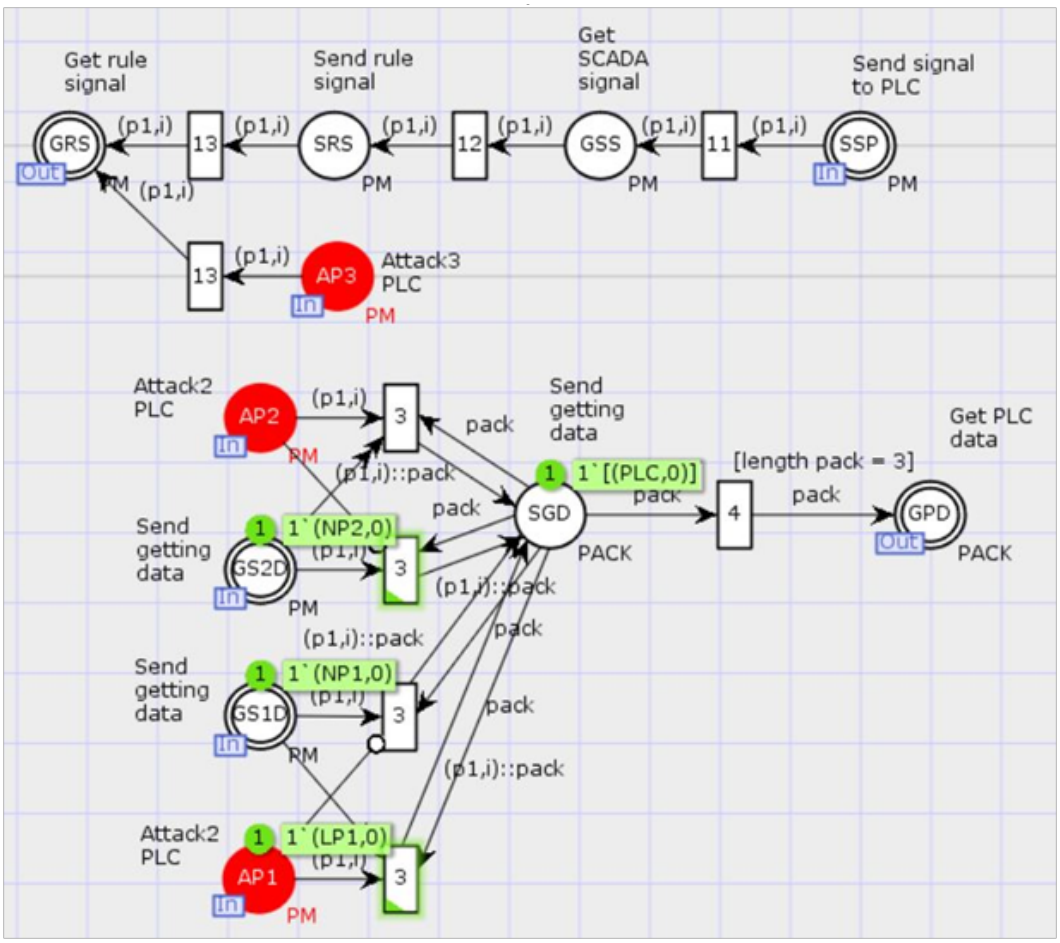

Рис. 5. Сеть Петри, иллюстрирующая четвертую и пятую атаки

представление о формате принимаемых и отправляемых данных уровня давления (на уровне устройств и сети). Во втором случае, злоумышленник должен обладать сведениями о самом технологическом процессе, чтобы успешно отправить управляющий сигнал с программируемого логического контроллера на узел регулирования давления.

ВЫВОДЫ

Моделирование атак на системы АСУ ТП с использованием различных подклассов сетей Петри позволяет алгоритмически описать входящие в их состав сложные объекты. При этом сценарии функционирования АСУ ТП легко проследить, что позволяет определить уязвимые места системы, а также предпочтительные цели для злоумышленника.

Построение имитационных моделей на основе сетей Петри дает не только подробное описание рассматриваемых систем, но и позволяет оценить анализируемый объект в целом при его нахождении в различных состояниях.

Приведенная модель нефтеперекачивающей станции является базовой, на основе которой планируется построить более сложную сеть, демонстрирующую реализацию более специфичных угроз и уязвимостей, а также использовать полученный опыт при создании других моделей АСУ ТП.

СПИСОК ЛИТЕРАТУРЫ

1. Реагирование на инциденты: аналитический отчет 2020 // securelist.ru : Блог Securelist – отчеты «Лаборатории Касперского» об угрозах информационной безопасности, анализ угроз, реверс-инжиниринг вирусов и статистика. 13.09.2021. URL: https://securelist.ru/incident-response-analyst-report-2020/103591/
2. Машкина И.В., Гарипов И.Р.. Разработка EPC-моделей угроз нарушения информационной безопасности автоматизированной системы управления технологическими процессами // Безопасность информационных

технологий. 2019. Т. 26. № 4. С. 6–20.

3. Васильев В.И., Вульфин А.М., Кириллова А.Д. Анализ и управление рисками информационной безопасности АСУ ТП на основе когнитивного моделирования. Моделирование, оптимизация и информационные технологии. 2022. №10(2).

4. Римша А.С. Метод и алгоритмы управления рисками информационной безопасности АСУ ТП критических инфраструктур. [Текст] : дис. … канд. техн. наук : 2.3.6 / Римша Андрей Сергеевич. – СПб., 2021. – 234 с.

5. Лившиц И.И. Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами. [Текст] : дис. … д-р техн. наук : 05.13.19 / Лившиц Илья Иосифович. – СПб., 2018. – 407 с.

6. Язов Ю.К., Анищенко А.В. Сети Петри-Маркова и их применение для моделирования процессов реализации угроз безопасности информации в информационных системах. Монография. – Воронеж, Кварта, 2020. – 173 с.