Разработка метода имитационного компьютерного моделирования эталонного состояния и поведения SCADA-систем на основе модели акторов

Барчан Константин Андреевич

Научный руководитель: к.т.н., зам. директора ООО “СИБ”
Гончаров Сергей Анатольевич

АСУТП и SCADA

АСУ ТП

Верхний уровень
(HMI, станции оператора)

SCADA-система

Сетевой уровень
(сетевые элементы)

Нижний уровень
(PLC - контроллеры)

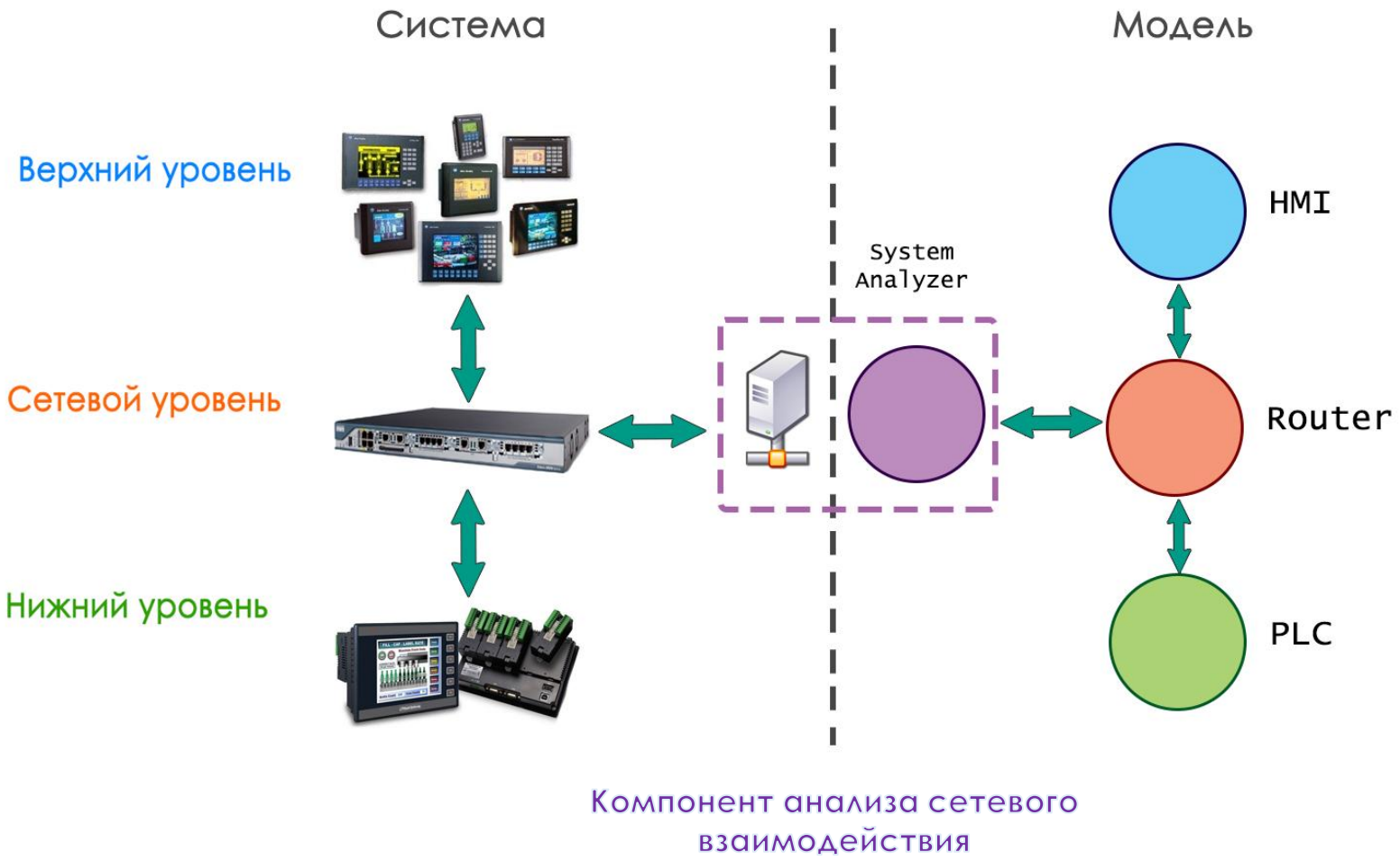
Полевой уровень
(датчики и механизмы)

Актуальные проблемы

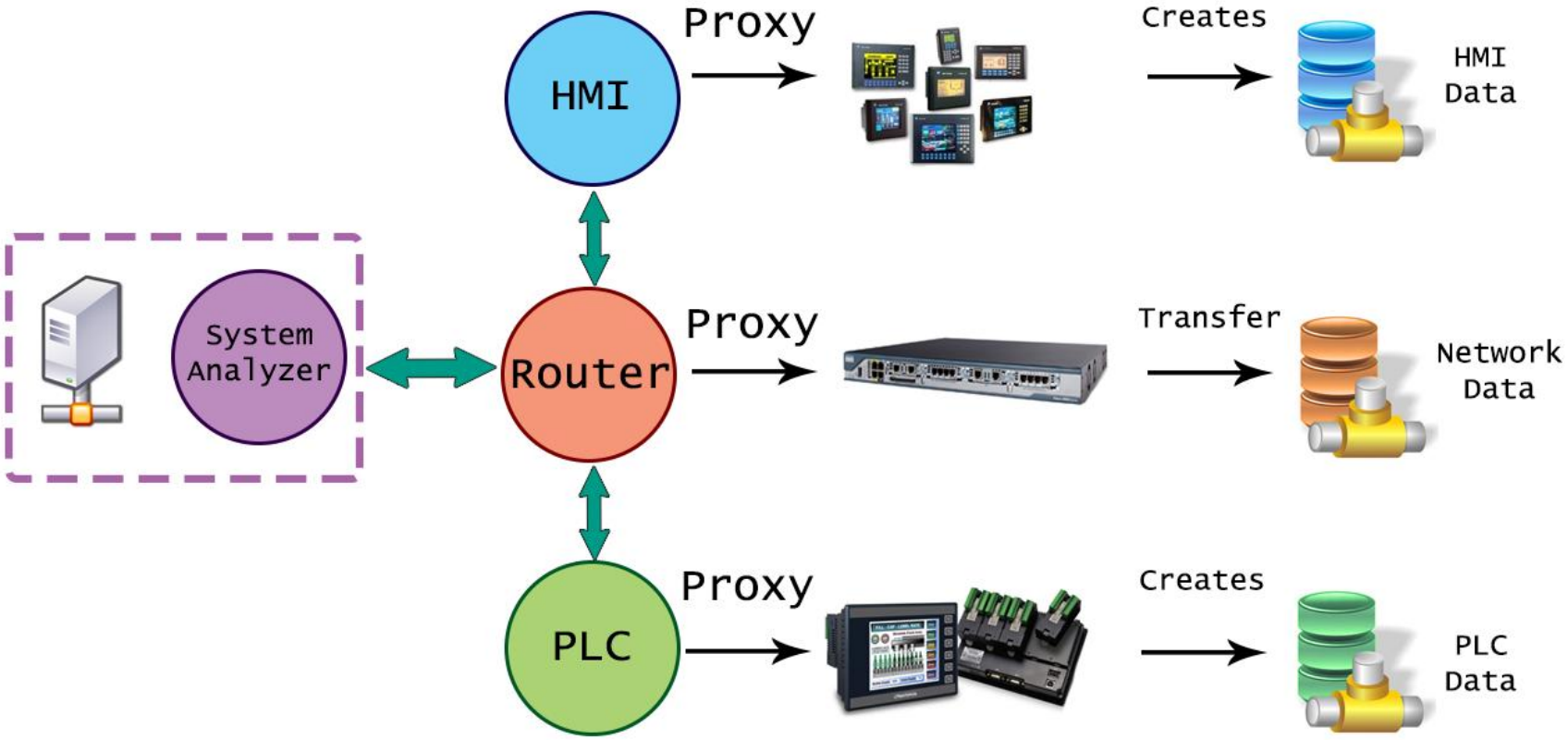
- Отсутствие возможности **оперативной** оценки компрометации системы.
- Создание **дополнительной вычислительной нагрузки** на технологические компоненты инфраструктуры систем управления.
- Невозможность **гарантировать работоспособность** СУ в ходе работы СЗИ.

Предлагаемый метод

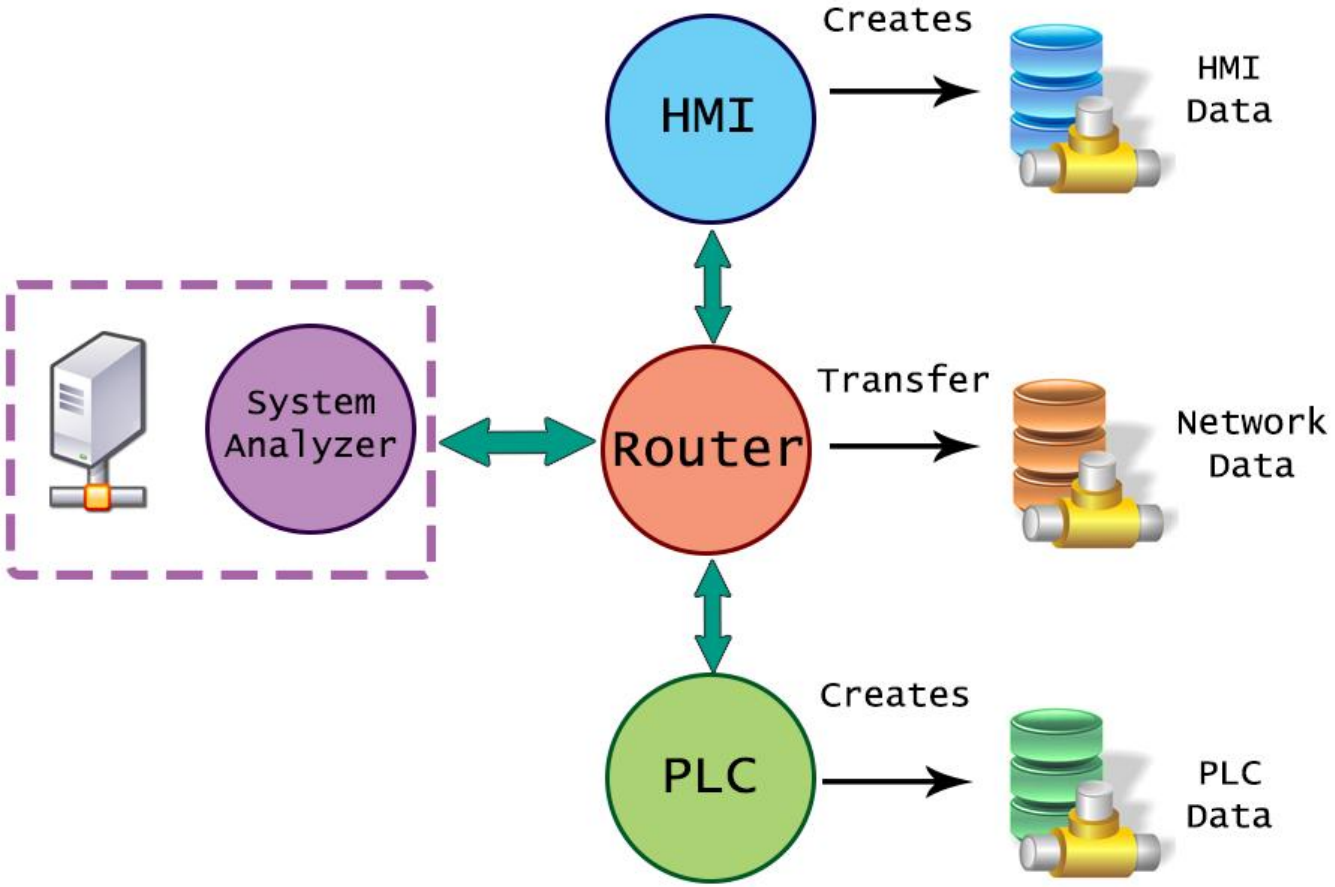
Архитектурное решение



Режим реальных данных



Режим имитации данных



Эталонная модель SCADA

- Общая функция безопасности системы:
  - $F(t) = \max(\varphi_i(t))$, где
- φ_i - частные функции безопасности:
  - $\boldsymbol{\varphi_1}$ – работоспособность каналов HMI – PLC;
  - $\boldsymbol{\varphi_2}$ – состояние сети;
  - $\boldsymbol{\varphi_3}$ – состояние настроек оборудования;
- t – начало времени сравнения модели и системы
- Dom $\boldsymbol{F(t)}$ = [0,1], Dom $\boldsymbol{\varphi_i}$ = [0,1].

Эталонная модель. Нечёткость

- X – уровень компрометации системы – Dom F(t)
- U = [0,1]
- T = {“низкая”, “средняя”, “высокая”}
- $\mu_{low}(x), \mu_{mid}(x), \mu_{high}(x)$ – функции принадлежности для $x \in X$

Спецификация модели акторов

- Оригинальная МА не гарантирует **срок доставки** сообщений.
- В работу актора введено понятие множества **проверок** (ассертов), которые необходимы для проверки временных (алгоритмических) ограничений.

Обнаруживаемые несанкционированные действия

- Оперативное обнаружение:
  - **Компрометации** инфраструктуры SCADA **вредоносным ПО**.
  - Действий **хакера**.
  - Скрытых **каналов**.
  - Нарушения процедуры управления **конфигурациями**.
- Упрощает процедуру расследования **инцидентов**.

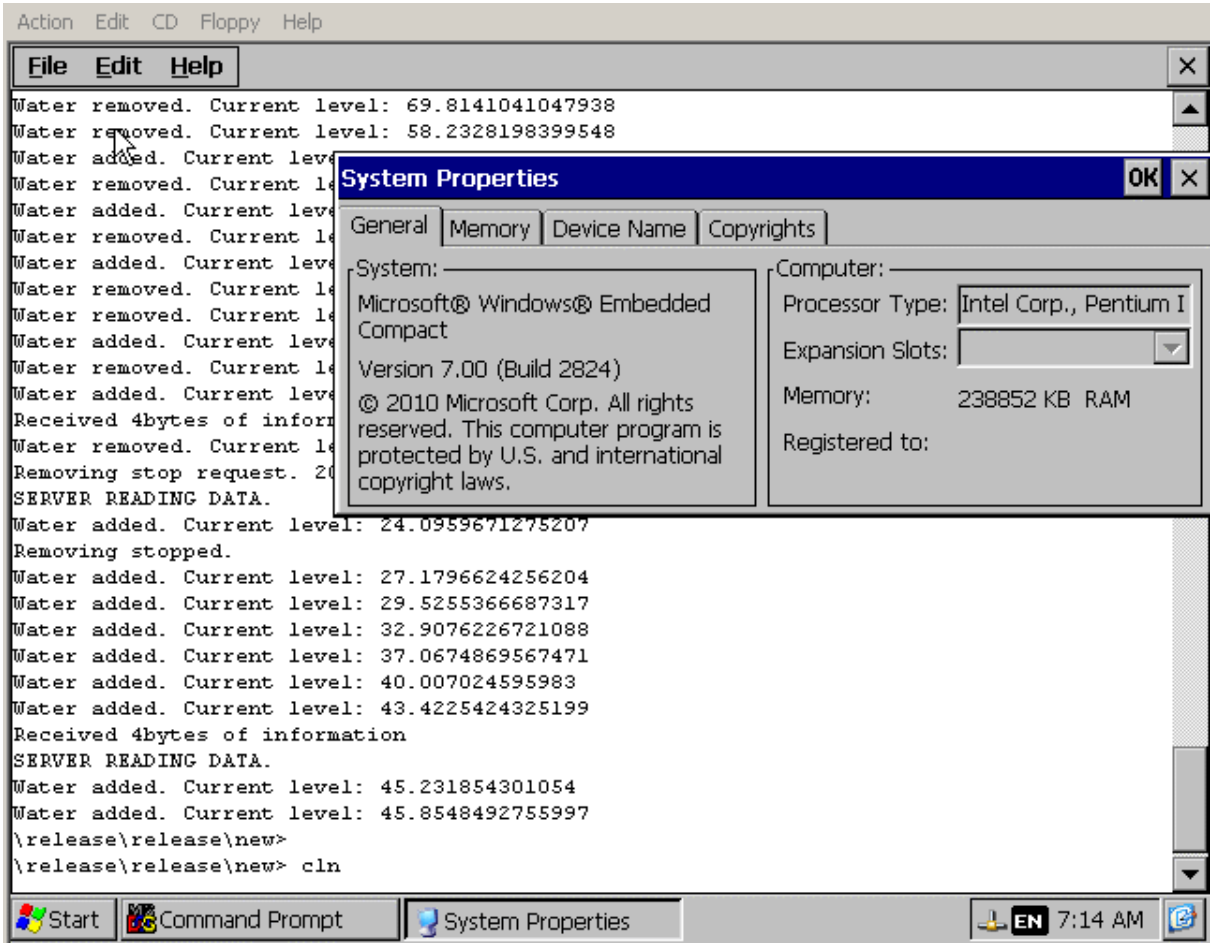
Апробация метода.

- Создан виртуальный **стенд** SCADA для АСУЗ на основе Windows Embedded Compact 7(PLC) (контроллеры Beckhoff CP62**)и Windows XP Embedded.

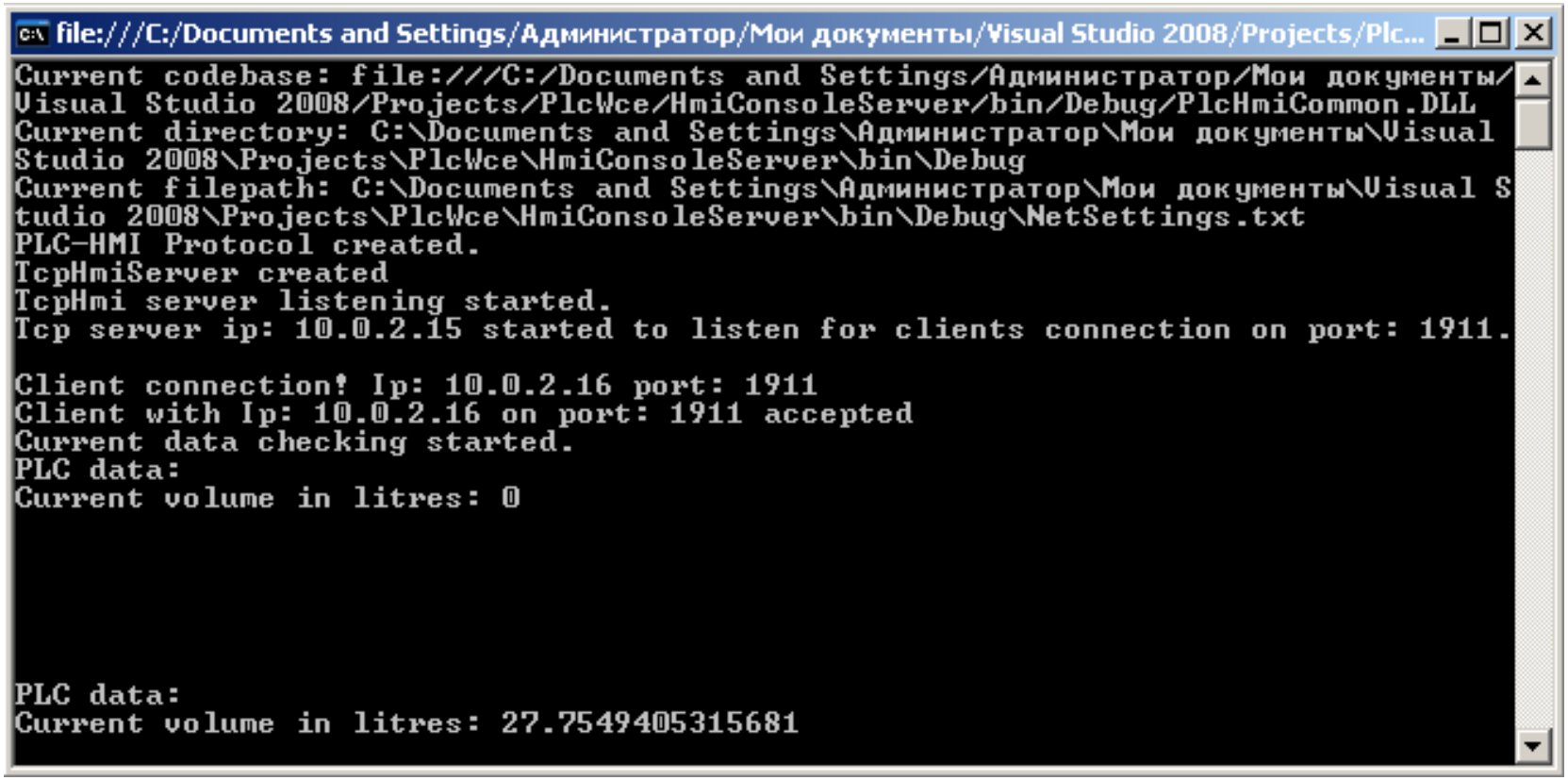
- Реализована **модель технологического процесса** аэрации жидкости в цистерне.

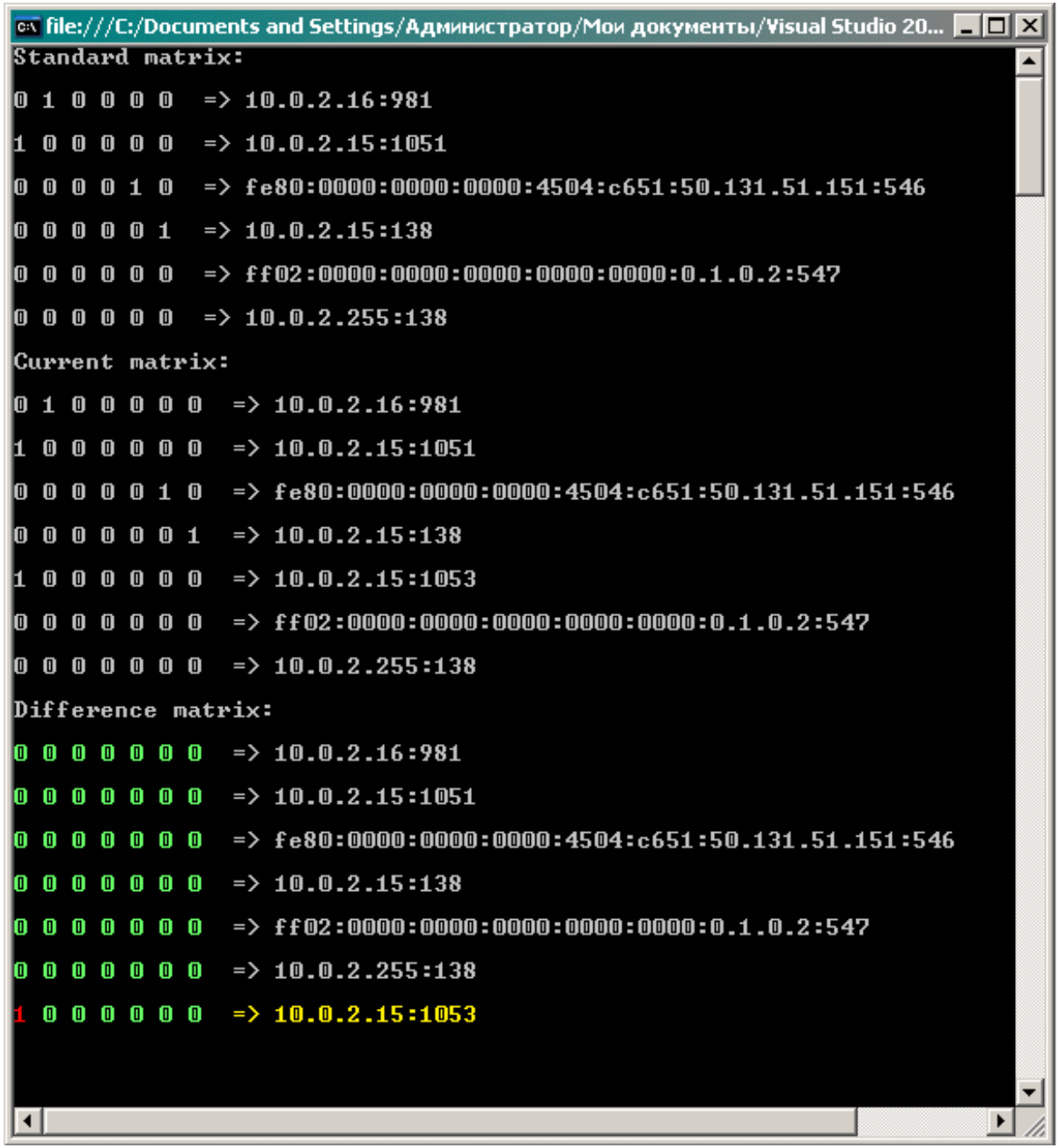
- **Выявлена** попытка несанкционированного **внедрения** злоумышленника в работу стенда.

Win EC PLC.


Action Edit CD Floppy Help
File Edit Help
Water removed. Current level: 69.8141041047938
Water removed. Current level: 58.2328198399548
Water added. Current leve
Water removed. Current le
Water added. Current leve
Water removed. Current le
Water added. Current leve
Water removed. Current le
Water removed. Current le
Water added. Current leve
Water removed. Current le
Water added. Current leve
Received 4bytes of infor
Water removed. Current le
Removing stop request. 2
SERVER READING DATA.
Water added. Current level: 24.0959671275207
Removing stopped.
Water added. Current level: 27.1796624256204
Water added. Current level: 29.5255366687317
Water added. Current level: 32.9076226721088
Water added. Current level: 37.0674869567471
Water added. Current level: 40.007024595983
Water added. Current level: 43.4225424325199
Received 4bytes of information
SERVER READING DATA.
Water added. Current level: 45.231854301054
Water added. Current level: 45.8548492755997
\release\release\new>
\release\release\new> cln
System Properties
OK
General
Memory
Device Name
Copyrights
System:
Microsoft® Windows® Embedded Compact
Version 7.00 (Build 2824)
© 2010 Microsoft Corp. All rights reserved. This computer program is protected by U.S. and international copyright laws.
Computer:
Processor Type: Intel Corp., Pentium I
Expansion Slots:
Memory: 238852 KB RAM
Registered to:
Start
Command Prompt
System Properties
EN 7:14 AM

Win XP Embedded HMI.





Вывод модуля сетевого анализа System Analyzer.

Результаты.

- **Специфицирована** структура **модели акторов** для работы в SCADA-системах (для обеспечения оперативной оценки состояния).
- На основе специфицированной модели акторов **разработана модель** SCADA-системы и её взаимодействия с системой обнаружения вторжений (СОВ).
- **Разработан метод** ИМ эталонного состояния и поведения SCADA-систем для СОВ и его математическая основа.
- **Реализована модель** сетевого взаимодействия PLC и HMI по протоколу TCP/IP.
- **Реализован модуль** сбора сетевой статистики.
- **Реализован модуль** анализа состояния сети.
- **Реализован модуль** анализа настроек оборудования.

Публикации.

- Барчан К. А. Разработка метода имитационного компьютерного моделирования эталонного состояния и поведения SCADA-систем на основе модели акторов // 52-я Международная научная студенческая конференция «Студент и научно-технический прогресс». – Новосибирск : НГУ, 2014.

- Барчан К. А. Разработка метода имитационного компьютерного моделирования эталонного состояния и поведения SCADA-систем на основе модели акторов // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2014. вып. 1. С. 11–18.

Спасибо за внимание!