Predictive Analytics and Communication Diagnostic Tool for Modbus-TCP Components of Automation System

FEHIS Project
Student: Olena Primachova
Supervisor: Dr. Piotr Czekalski

22.05.2017

The Topic

Predictive Analytics and Communication Diagnostic Tool for Modbus-TCP components of automation system is a software, which has following purposes:

- Simulate a Modbus-TCP client or server basing on the common information provided by the producer, such as number of registers, number of digital inputs/outputs, memory capacity etc.

- Test connection and compatibility of a certain Modbus-TCP device type to the existing automation system of the enterprise, without having a physical device.

- Determine the optimal configuration parameters (size of transaction and connection pools) for a certain device type to enhance its performance.

Main Terms

- **Industrial Automation System** - several types of control systems and associated instrumentation used in industrial production, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations such as programmable logic controllers (PLC) often found in the industrial sectors and critical infrastructures

- **OSI** - Open Systems Interconnection model (OSI model) is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. Contains 7 layers: Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer, Application Layer.

- **Modbus** - application layer messaging protocol, positioned at level 7 of the OSI model, that provides client/server communication between devices connected on different types of buses or networks.
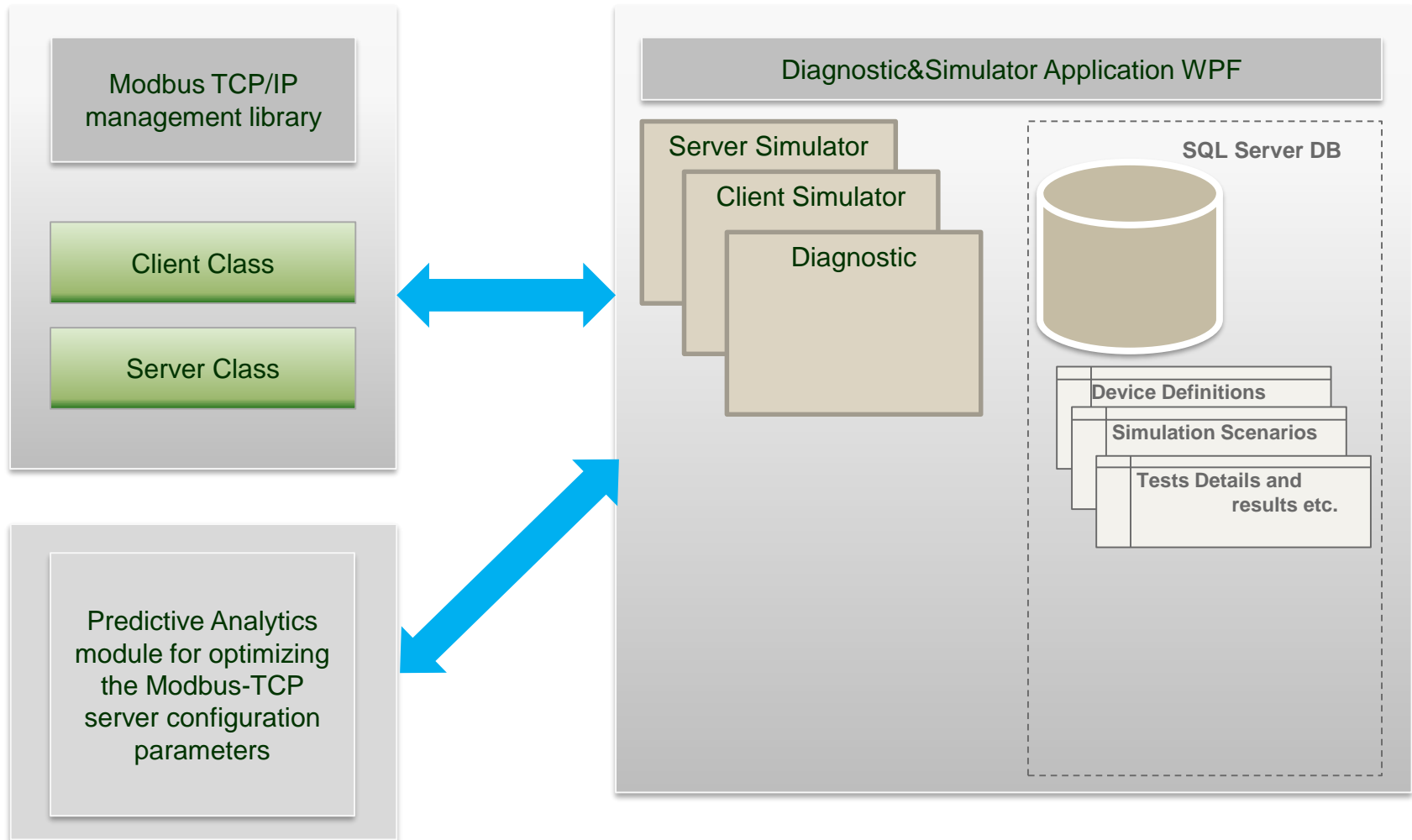
Main Terms

- **TCP/IP** - conceptual model and set of communications protocols used on the Internet and similar computer networks.

- **Modbus-TCP** - protocol which implements the MODBUS messaging service over TCP/IP networks.

- **Client** - Modbus Master device, sending requests.

- **Server** - Modbus Slave device, providing responses.

- **Transaction pool** - Maximum number of requests/responses, which a Modbus-TCP device can process simultaneously. Has a critical influence on a device's performance, especially for Server.

- **Connection pool** - Maximum number of open connections over TCP/IP network, which a Modbus-TCP device can keep at the same moment.

- **Predictive analysis** – set of statistical techniques, such as predictive modeling, machine learning, and data mining that analyze current and historical facts to make predictions about future or otherwise unknown events.

Solution Model

Modbus TCP/IP management library

Client Class

Server Class

Predictive Analytics module for optimizing the Modbus-TCP server configuration parameters

Diagnostic&Simulator Application WPF

Server Simulator

Client Simulator

Diagnostic

SQL Server DB

Device Definitions

Simulation Scenarios

Tests Details and results etc.

Considered methods of predictive analytics

№	Method	Advantages	Disadvantages
1	Artificial intelligence	Powerful method, allows effective evaluating of parameter sets with respect to many rules and factors	High implementation complexity and computation cost aren't reasonable for given task
2	Statistical data analysis	Exact determination of optimal parameters for this specific system basing on historical data	Gathering the sufficient amount of statistics is extremely time-consuming process
3	Queueing theory	Analytical method with efficiency proven by majority of telecommunication systems	Necessity to calculate performance measures for all possible parameter combinations to find the best solution => high computation complexity

Selected solution

Combination of Queueing theory and Genetic algorithms.

Applying Genetic algorithm allows to significantly reduce the number of parameter combinations for calculating the performance parameters, which leads to decreasing the computation time and complexity.

Modbus-TCP device parameters to optimize:

- Maximum number of server transactions;
- Maximum number of connections to server.

Both parameters can take integer values from 1 to 16.

Genetic Algorithm

Phenotype:

- in nature – set of traits and features of a species;
- in genetic algorithm – solution of the problem (i.e. $N_{trans.max} = 8$)

Genotype:

- in nature – genetic code of chromosomes;
- in genetic algorithm – binary coding of the phenotype (8 => 0100)

Genetic algorithm chromosome: [$N_{trans.max}$; $N_{con.max}$]
Example: [1100 0110]

  [$N_{trans.max}$=12 ; $N_{con.max}$=6]

Genetic Algorithm Stages

1) **Population initialization**
2) **Fitness function evaluation**
3) **Parent selection**
4) **Crossover**
5) **Mutation**

The cycle is repeated until stop condition is met. Possible variants:

- Number of generations;
- Appropriate fitness function value;
- Small difference between the results of neighboring iterations.

Fitness function
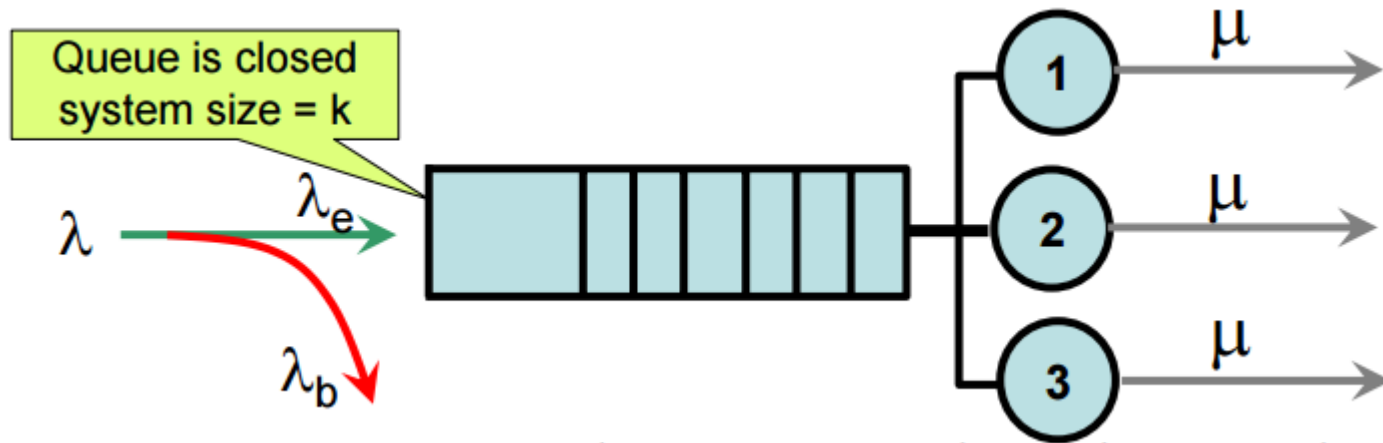
M/M/s/k Markov model

- k – max number of connections;
- s – max number of transactions;
- λ – request intensity;
- μ – response intensity;
- ρ – utilization;
- p(n) – loss probability.

Fitness function

$$P_0 = \left[\sum_{n=0}^{s-1} \frac{\rho^n}{n!} + \sum_{n=s}^{k} \frac{\rho^n}{s!\,s^{n-s}} \right]^{-1}$$

$$P_n = \frac{\rho^n}{n!} P_0 \qquad n < s$$

$$P_n = \frac{\rho^n}{s!\,s^{n-s}} P_0 \qquad s \leq n \leq k$$

P_k – loss probability

Performance Measures to minimize:

1. Loss probability.

2. Average time spent in the system.

Average Time Spent in System W_s:

$$W_s = \frac{L_s}{\lambda_e}$$

User's Manual

1) Execute AIM Modbus/TCP Simulator
2) Select "Client" role and connect to the server
3) Perform simulation and memorize the measured mean service time
4) Execute Genetic Algorithm Optimization tool
5) Enter the mean service time, number of clients and average frequency of requests from one client per second
6) Perform simulation step by step or go directly to final result.

Implementation

Literature

- NIST SP 800-82 standard
- ISO/IEC 7498-1 standard
- Modbus IDA. Modbus application protocol specification V1.1a.
- Comer, D. E. Internetworking with TCP/IP - Principles, Protocols and Architecture.
- Modbus IDA. Modbus messaging on TCP/IP implementation guide V1.0a.
- Nyce, C. Predictive Analytics White Paper.
- Giurgiu, I.; Bogojeska, J. Predictive analytics for server incident reduction. Machine learning for IT services.