IEEE

# PROCEEDINGS

# 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies

# DESSERT




2020 Theme:
IoT, Big Data and AI for a Safe & Secure World and Industry 4.0

## ORGANIZED BY

**National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine**
**Banking University, Kyiv, Ukraine**
**Leeds Beckett University, Leeds, United Kingdom**
**IEEE United Kingdom and Ireland Section**
**IEEE Ukraine Section**

**Ukraine, Kyiv**
**May 14-18**
**2020**

# Table of Contents

*Anatoliy Gorbenko, Andrii Karpenko, Olga Tarasyuk.* ANALYSIS OF TRADE-OFFS IN FAULT-TOLERANT DISTRIBUTED COMPUTING AND REPLICATED DATABASES 1

*Oleg Bisikalo, Viacheslav Kovtun, Oksana Kovtun, Volodimir Romanenko.* RESEARCH OF SAFETY AND SURVIVABILITY MODELS OF THE INFORMATION SYSTEM FOR CRITICAL USE 7

*Oleg Ivanchenko, Yuriy Ponochovniy, Vyacheslav Kharchenko, Borys Moroz, Evgene Brezhnev, Leonid Kabak.* DEPENDABILITY ASSESSMENT FOR SCADA SYSTEM CONSIDERING USAGE OF CLOUD RESOURCES 13

*Viktoriia Merlak, Heorgii Kuchuk.* RESOURCE ALLOCATION FOR HIERARCHICAL WIDGET SYSTEM 18

*Oleksandr Lemeshko, Oleksandra Yeremenko, Maryna Yevdokymenko, Batoul Sleiman, Pavel Segec, Jozef Papan.* ADVANCED PERFORMANCE-BASED FAST REROUTING MODEL WITH PATH PROTECTION 23

*Lev Raskin, Oksana Sira, Yurii Parfeniuk.* RELIABILITY ASSESSMENT OF LARGE SYSTEMS THAT FAIL AS A RESULT OF DAMAGE ACCUMULATION 29

*Herman Fesenko, Ihor Kliushnikov, Vyacheslav Kharchenko, Serhii Rudakov, Elena Odarushchenko.* ROUTING AN UNMANNED AERIAL VEHICLE DURING NPP MONITORING IN THE PRESENCE OF AN AUTOMATIC BATTERY REPLACEMENT AERIAL SYSTEM 34

*Vladimir Sklyar, Vyacheslav Kharchenko.* STRUCTURED ARGUMENTATION FOR ASSURANCE CASE OF MONITORING SYSTEM BASED ON UAVS 40

*Anton Kamenskih, Yuri Stepchenkov, Yuri Diachenko, Yuri Rogdestvenski, Denis Diachenko.* IMPROVEMENT OF THE QUASI DELAY-INSENSITIVE PIPELINE NOISE IMMUNITY 47

*Sergey Tyurin.* REVERSIBLE MAJORITY VOTER BASED ON FREDKIN GATES 52

*Oleksandr Drozd, Vitaliy Romankevich, Mykola Kuznietsov, Myroslav Drozd, Oleksandr Martynyuk.* USING NATURAL VERSION REDUNDANCY OF FPGA PROJECTS IN AREA OF CRITICAL APPLICATIONS 58

*Vadym Puydenko, Vyacheslav Kharchenko.* THE MINIMIZATION OF HARDWARE FOR IMPLEMENTATION OF PSEUDO LRU ALGORITHM FOR CACHE MEMORY 65

*Oleksandr Gordieiev, Daria Gordieieva, Andrii Tryfonov, Vladyslav Dokukin, Elena Odarushchenko.* METHOD AND TOOL FOR SUPPORT OF SOFTWARE REQUIREMENTS PROFILE QUALITY ASSESSMENT 72

*Oleg Odarushchenko, Oleksiy Striuk, Elena Odarushchenko, Kostiantyn Leontiiev.* SOFTWARE FAULT INSERTION TESTING FOR SIL CERTIFICATION OF SAFETY PLC-BASED SYSTEM 80

*Maryna Miroshnyk, Oleksandr Shkil, Elvira Kulak, Dariia Rakhlis, Inna Filipenko, Anatolii Miroshnyk.* VERIFICATION OF FPGA CONTROL SYSTEMS BY ANALYZING THE CORRECTNESS OF STATE DIAGRAMS 85

*Kostiantyn Leontiiev, Ievgen Babeshko, Vyacheslav Kharchenko.* ASSUMPTION MODES AND EFFECT ANALYSIS OF XMECA: EXPERT BASED SAFETY ASSESSMENT 90

*Dmytro Progonov, Veronika Prokhorchuk, Andriy Oliynyk.* EVALUATION SYSTEM FOR USER AUTHENTICATION METHODS ON MOBILE DEVICES 95

*Dmytro Likhomanov, Vladyslav Poliukh.* PREDICTING MALICIOUS HOSTS BY BLACKLISTED IPV4 ADDRESS DENSITY ESTIMATION 102

*Anastasiia Poltorak, Nataliia Sirenko, Igor Atamanyuk, Yuriy Volosyuk, Olha Melnyk, Polina Fenenko.* PARADIGM CHANGES THAT STRENGTHEN THE FINANCIAL SECURITY OF THE STATE THROUGH FINTECH DEVELOPMENT 110

*Victoriia Turkina, Dmytro Ihnatiev.* APPROACH TO SUSTAINABLE TRUST AND REPUTATION EVALUATION IN DISTRIBUTED MOBILE NETWORKS OF THE INTERNET OF THINGS 117

*Vyacheslav Kharchenko, Yuriy Ponochovniy, Al-Khafaji Ahmed Waleed, Oleg Ivanchenko, Dmytro Uzun, Larysa Degtyareva.* AVAILABILITY MODEL OF TWO-ZONE PHYSICAL SECURITY SYSTEM CONSIDERING CYBER ATTACKS AND SOFTWARE UPDATE 122

*Sergii Lysenko, Kira Bobrovnikova, Oleg Savenko, Roman Shchuka.* A CYBERATTACKS DETECTION TECHNIQUE BASED ON EVOLUTIONARY ALGORITHMS 127

*Tamara Radivilova, Lyudmyla Kirichenko, Maxim Tawalbeh, Petro Zinchenko, Abed Saif Alghawli, Andrii Ilkov.* THE COMPLEX METHOD OF INTRUSION DETECTION BASED ON ANOMALY DETECTION AND MISUSE DETECTION 133

*Maryna Kolisnyk, Vyacheslav Kharchenko, Iryna Piskachova.* AVAILABILITY MODELS OF INDUSTRIAL INTERNET OF THINGS WIRED SYSTEM CONSIDERING CYBERATTACKS 138

*Victor Krasnobayev, Alexandr Kuznetsov, Irina Lokotkova, Anastasiia Kiian, Tetiana Kuznetsova.* TECHNIQUES FOR RAISING THE REMAINDER TO A POWER IN THE RESIDUAL CLASS SYSTEM 145

*Victor Krasnobayev, Alexandr Kuznetsov, Victoria Popenko, Anna Kononchenko, Tetiana Kuznetsova.* DETERMINATION OF POSITIONAL CHARACTERISTICS OF NUMBERS IN THE RESIDUAL CLASS SYSTEM 151

*Mariia Rodinko, Roman Oliynykov.* THE METHOD OF SEARCHING FOR DIFFERENTIAL TRAILS OF ARX-BASED BLOCK CIPHER CYPRESS 157

*Alexandr Kuznetsov, Alexey Smirnov, Alexander Onikiychuk, Tymur Makushenko, Olha Anisimova, Anna Arischenko.* ADAPTIVE PSEUDO-RANDOM SEQUENCE GENERATION FOR SPREAD SPECTRUM IMAGE STEGANOGRAPHY 161

*Alexandr Kuznetsov, Anastasiia Kiian, Vitalina Babenko, Iryna Perevozova, Iryna Chepurko, Oleksii Smirnov.* NEW APPROACH TO THE IMPLEMENTATION OF POST-QUANTUM DIGITAL SIGNATURE SCHEME 166

*Alexandr Kuznetsov, Anastasiia Kiian, Oleksii Smirnov, Alla Cherep, Meruert Kanabekova, Iryna Chepurko.* TESTING OF CODE-BASED PSEUDORANDOM NUMBER GENERATORS FOR POST-QUANTUM APPLICATION 172

*Valeriy Hlukhov.* FPGA BASED DIGITAL QUANTUM COMPUTER VERIFICATION 178

*Sergiy Gnatyuk, Tetyana Okhrimenko, Olena Azarenko, Andriy Fesenko, Rat Berdibayev.* EXPERIMENTAL STUDY OF SECURE PRNG FOR Q-TRITS QUANTUM CRYPTOGRAPHY PROTOCOLS 183

*Anatoly Shevchenko, Alexander Sosnitsky.* UNIVERSAL META-DEFINITION OF THE INTELLIGENCE 189

*Olga Morozova, Vyacheslav Kharchenko, Oleg Illiashenko, Sergii Sokolov.* COMBINATION OF DIGITAL TWIN AND ARTIFICIAL INTELLIGENCE IN MANUFACTURING USING INDUSTRIAL IOT 196

*Oleh Pihnastyi, Georgii Kozhevnikov, Tetiana Bondarenko.* AN ANALYTICAL METHOD FOR GENERATING A DATA SET FOR A NEURAL MODEL OF A CONVEYOR LINE 202

*Roman Leizerovych, Galyna Kondratenko, Ievgen Sidenko, Yuriy Kondratenko.* IoT-COMPLEX FOR MONITORING AND ANALYSIS OF MOTOR HIGHWAY CONDITION USING ARTIFICIAL NEURAL NETWORKS 207

*Olena Protsenko, Mykyta Myronenko, Taras Savchenko, Olesandr Prikhodchenko.* INFORMATIONAL AND EXTREME MACHINE LEARNING FOR ON-BOARD RECOGNITION SYSTEM OF GROUND OBJECTS 213

*Bo Jiang, Pengfei Liu, Jie Xu.* A DEEP LEARNING APPROACH TO LOCATE BUGGY FILES 219

*Valeriy Mygal, Galyna Mygal.* THE VIABILITY OF DYNAMIC SYSTEMS IN DIFFICULT CONDITIONS: COGNITIVE ASPECTS 224

*Petr Makarenko, Mikola Mogilat, Anton Neklesa, Olena Ponochovna, Yulia Makarenko.* COGNITIVE MODELING OF THE CONSUMER MARKET: SENSITIVITY AND SCENARIO ANALYSIS 230

*Maryna Derkach, Danylo Matiuk, Inna Skarga-Bandurova.* OBSTACLE AVOIDANCE ALGORITHM FOR SMALL AUTONOMOUS MOBILE ROBOT EQUIPPED WITH ULTRASONIC SENSORS 236

*Oleksandr Tymochko, Andrii Trystan, Andrii Berezhnyi, Olga Matiushchenko, Oleksandr Timochko.* METHOD OF AUTOMATED FLIGHT ROUTE PLANNING FOR UNMANNED AERIAL VEHICLES TO SEARCH FOR STATIONARY OBJECTS 242

*Kostiantyn Dergachov, Serhii Bahinskii, Iryna Piavka.* THE ALGORITHM OF UAV AUTOMATIC LANDING SYSTEM USING VISION SYSTEMS 247

*Oleh Pihnastyi, Georgii Kozhevnikov, Valery Khodusov.* CONVEYOR MODEL WITH INPUT AND OUTPUT ACCUMULATING BUNKER 253

*Igor Atamanyuk, Vyacheslav Shebanin, Valerii Havrysh, Vadim Lykhach, Sergey Kramarenko.* IDENTIFICATION OF THE OPTIMAL PARAMETERS FOR FORECASTING THE STATE OF TECHNICAL OBJECTS BASED ON THE CANONICAL RANDOM SEQUENCE DECOMPOSITION 259

*Vitaliy Tsyganok, Sergii Kadenko, Oleh Andriichuk.* HYBRID DECISION SUPPORT METHODOLOGY BASED ON OBJECTIVE AND EXPERT DATA 265

*Yaroslav Khortiuk, Galyna Kondratenko, Ievgen Sidenko, Yuriy Kondratenko.* INCREASING RELIABILITY OF PROGRAMMING INTERFACES BASED ON FUZZ TESTING 272

*Olena Golembovska, Vyacheslav Kharchenko, Igor Shostak, Mariia Danova, Olena Feoktystova.* ASSESSING THE PERCEPTION OF ABSTRACT PAINTINGS WITH ELEMENTS OF AUGMENTED REALITY 278

*Axel Sikora, Andreas Walz, Lukas Zimmermann.* RESEARCH ASPECTS FOR SECURE COMMUNICATION IN THE INDUSTRIAL INTERNET OF THINGS 284

*Maksim Pavlenko, Oleksandr Tymochko, Volodymyr Larin, Maksym Kolmykov, Serhii Khmelevskiy.* CONCEPTUAL BASIS OF CASCADING DIFFERENTIAL MASKING TECHNOLOGY 290

*Mykhailo Babii, Andrii Dikhtiarov.* IDENTIFICATION OF A PERSON BY GAIT ON THE BASIS OF WAVELET TECHNOLOGY 295

*Viktor Makarichev, Vladimir Lukin, Iryna Brysina.* DISCRETE ATOMIC COMPRESSION WITH DIFFERENT STRUCTURES OF DISCRETE ATOMIC TRANSFORM: EFFICIENCY COMPARISON AND PERSPECTIVES OF APPLICATION TO DIGITAL IMAGES PRIVACY PROTECTION 301

*Fangfang Li, Sergey Krivenko, Vladimir Lukin.* A TWO-STEP PROCEDURE FOR IMAGE LOSSY COMPRESSION BY ADCTC WITH A DESIRED QUALITY 307

*Igor Shostak, Mariia Danova, Olga Morozova, Tamara Kliuieva.* USING INTERNET OF THINGS TECHNOLOGIES TO ENSURE CARGO TRANSPORTATION SAFETY 313

*Oksana Luchsheva, Ihor Turkin, Pavlo Luchshev.* NAVIGATION ASSISTIVE APPLICATION FOR THE VISUALLY IMPAIRED PEOPLE 320

*Anatoliy Sachenko, Oleksandr Osolinskyi, Maciej Dobrowolski, Pavlo Bykovyy, Volodymyr Kochan.* DEVELOPMENT OF THE FLEXIBLE TRAFFIC CONTROL SYSTEM USING THE LABVIEW AND THINGSPEAK 326

*Igor Zhukov, Nickolay Pechurin, Lyudmila Kondratova.* IoT'S PRIMARY INFORMATION LOAD ESTIMATION 331

*Iryna Svyd, Ivan Obod, Oleksandr Maltsev, Ganna Zavolodko.* FUSION METHOD OF PRIMARY SURVEILLANCE RADAR DATA AND IFF SYSTEMS DATA 336

*Iryna Svyd, Ivan Obod, Oleksandr Maltsev, Artem Hlushchenko.* SECONDARY SURVEILLANCE RADAR RESPONSE CHANNEL INFORMATION SECURITY IMPROVEMENT METHOD 341

*Nataliia Kussul, Andrii Shelestov, Bohdan Yailymov, Hanna Yailymova, Mykola Lavreniuk, Leonid Shumilo, Yuliia Bilokonska.* CROP MONITORING TECHNOLOGY BASED ON TIME SERIES OF SATELLITE IMAGERY 346

*Yaroslav Klyatchenko, Lev Yasenko, Oksana Tarasenko-Klyatchenko.* IMAGE NOISE REDUCTION BY DENOISING AUTOENCODER 351

*Valerii Zhabin, Valentina Zhabina.* METHODS OF ON-LINE COMPUTATION ACCELERATION IN SYSTEMS WITH DIRECT CONNECTION BETWEEN UNITS 356

*Sergii Saukh.* REGULARIZATION METHOD FOR THE CLARKE'S GENERALIZED JACOBIAN TO ENSURE THE FORMATION OF NONSINGULAR SYSTEMS FOR INEXACT NEWTON METHODS 363

*Vadym Shkarupylo, Oleksandr Chemerys, Valentyna Dusheba, Ravil Kudermetov, Andrii Oliinyk.* ON HOARE TRIPLES APPLICABILITY TO DEPENDABLE SYSTEM SPECIFICATION SYNTHESIS 371

*Artem Perepelitsyn, Inna Zarizenko, Vitaliy Kulanov.* FPGA AS A SERVICE SOLUTIONS DEVELOPMENT STRATEGY 376

*Zlatogor Minchev.* DIGITAL SOCIETY FUTURE TRANSFORMATION PERSPECTIVES IN THE INFORMATIONAL AGE 381

*Oleksandr Potii.* METHODS OF CLASSIFICATION AND ASSESSMENT OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS 389

*Halyna Chmeruk, Tetiana Bludova.* PROBABILISTIC APPROACH FOR EVALUATION OF ORGANIZATION OF ENTERPRISE REENGINEERING 394

*Tamara Lozinska, Oleksandr Dorofyeyev, Yurij Ponochovniy, Tetiana Vlasenko.* LINEAR REGRESSION MODEL FOR SUBSTANTIATION OF SUSTAINABLE STATE POLICY IN A DIGITAL ECONOMY 399

*Olena Kopishynska, Yurii Utkin, Oleksandr Galych, Mykola Marenych, Ihor Sliusar.* MAIN ASPECTS OF THE CREATION OF MANAGING INFORMATION SYSTEM AT THE IMPLEMENTATION OF PRECISE FARMING 404

*Tetiana Hovorushchenko, Alla Herts, Yelyzaveta Hnatchuk.* MODELLING THE DECISION MAKING PROCESS ON LEGAL CONDUCTING THE SURROGATE MOTHERHOOD 411

*Viktoriya Saravas, Evgenii Pahalchuk, Andrii Molchan, Yuriy Kampov.* THE DEVELOPMENT OF EDUCATIONAL APPLICATION WITH VIRTUAL REALITY PLACING OBJECTS SYSTEM USING SNAP ZONE TECHNOLOGY 416

*Iryna Yakymenko, Volodymyr Kazymyr, Svitlana Lytvyn.* WEBOMETRICS RANKING ANALYSIS AND POSSIBLE WAYS TO IMPROVE THE POSITION OF THE UNIVERSITY 422

*Artyom Shamyna, Aleksey Ardyako, Alexandr Labokha.* MODELING THE DISTRIBUTION OF RADIONUCLIDES IN THE ENVIRONMENT AS A RESULT OF RADIATION ACCIDENTS 427

*Todor Tagarev, Yantsislav Yanakiev.* BUSINESS MODELS OF COLLABORATIVE NETWORKED ORGANISATIONS: IMPLICATIONS FOR CYBERSECURITY COLLABORATION 431

*Todor Tagarev.* GOVERNANCE OF COLLABORATIVE NETWORKED ORGANISATIONS: STAKEHOLDER REQUIREMENTS 439

*Kateryna Isirova, Oleksandr Potii.* DEVELOPMENT PRINCIPLES FOR ELECTRONIC VOTING SYSTEM USING DISTRIBUTED LEDGER TECHNOLOGY 446

*Lyudmila Vasylieva, Olga Procenko, Svitlana Chmykhun.* PROBLEMS AND SOLUTIONS FOR AN IT-DEPENDENT INFORMATION SOCIETY: ESSENCE, DEVELOPMENT AND PROSPECTS 451

*Sergiy Kryvyi, Olena Grinenko, Volodymyr Opanasenko.* LOGICAL APPROACH TO THE RESEARCH OF PROPERTIES OF SOFTWARE ENGINEERING ECOSYSTEM 456

*Tetiana Hovorushchenko, Ivan Lopatto, Olga Pavlova.* CONCEPT OF ACTIVITY OF INTELLIGENT AGENT OF VERIFICATION OF CONSIDERING THE SUBJECT AREA INFORMATION IN THE PROCESS OF SOFTWARE SYSTEMS DEVELOPMENT 465

*Sergii Dotsenko, Herman Fesenko, Oleg Illiashenko, Vyacheslav Kharchenko, Valentin Moiseenko, Liudmyla Yermolenko.* INTEGRATION OF SECURITY, FUNCTIONAL AND ECOLOGY SAFETY MANAGEMENT SYSTEMS: CONCEPT AND INDUSTRIAL CASE 470

*Yannick Fourastier, Claude Baron, Carsten Thomas, Philippe Esteban.* ASSURANCE LEVELS FOR DECISION MAKING IN AUTONOMOUS INTELLIGENT SYSTEMS AND THEIR SAFETY 475

The 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2020
14-18 May, 2020, Kyiv, Ukraine

# Dependability Assessment for SCADA System Considering Usage of Cloud Resources

Oleg Ivanchenko
*Department of Trnasport Systems and Technologies*
*University of Customs and Finance*
Dnipro, Ukraine
vmsu12@gmail.com

Vyacheslav Kharchenko
*Department of Computer Systems, Networks and Cybersecurity*
*National Aerospace University*
Kharkiv, Ukraine
V.Kharchenko@csn.khai.edu

Eugene Brezhnev
*Department of Computer Systems, Networks and Cybersecurity*
*National Aerospace University*
Kharkiv, Ukraine
e.brezhnev@csn.khai.edu

Yuriy Ponochovnyi
*Department of Information Systems and Technologies*
*Poltava State Agrarian Academy*
Poltava, Ukraine
yuriy.ponch@gmail.com

Borys Moroz
*Department of Computer Systems' Software*
*Dnipro Polytechnic National Technical University*
Dnipro, Ukraine
moroz.boris.1948@gmail.com

Leonid Kabak
*Department of Computer Systems' Software*
*Dnipro Polytechnic National Technical University*
Dnipro, Ukraine
kabak.leo@gmail.com

***Abstract*—Supervisory Control and Data Acquisition (SCADA) system is one the most significant cyber-oriented components of management circuit for any complex hierarchical infrastructure. The effectiveness and performance of the SCADA system depends on a number of relevant factors including a possibility to utilize additional cloud resources. Of particular note, the cloud services can apply in order to create concurrent redundant system for implementation of disaster recovery feature of SCADA information resources during different deliberate malicious impacts and intrusions. However, in spite of the fact that usage of the cloud services allow to enhance functionality of SCADA system, there are dependability and cybersecurity aspects for their joint utilization hat keep to remain a serious challenge for service personnel and users. In this paper, authors propose to employ analytical and stochastic modelling in order to get a numerical dependability assessment for SCADA system with realization of the cloud resourcing support considering influence of diverse negative factors. Furthermore, developers can utilize these modelling results in order to perform justification of overall functional requirements of the SCADA system.**

***Keywords—SCADA architecture; systemic failure diagram; reliability block diagram; Semi-Markov Modelling Process; dependability assessment***

## I. INTRODUCTION

The contemporary management modules for critical infrastructures usually build based on the use of Supervisory Control and Data Acquisition (SCADA) system. In fact, SCADA contains hardware equipment, software applications, different remote devices and relevant networks layers of server implementations [1]. In this, to create quite effective functioning SCADA system, developers should keep up with different achievements in the area of contemporary infocommunication technologies. In particular, utilization of power cloud computing resources and technologies. At the same time, manufacturers may apply cloud resources in order to improve dependability of SCADA system taking into account diverse malicious deliberate impacts and intrusions. It is noticeable, that different deliberate malicious impacts will eventually lead to descending availability level of SCADA. This important circumstance should be taken into account by developers. They should always remember that the dependability aspect is significant since SCADA system interacts directly with critical infrastructure and other complex critical systems.

Developers should also try to create effective functioning SCADA system, which can simultaneously perform great numbers of processing operations for input information data streams. This complex task can be solved by usage of much-needed additional cloud resources. From this point of view, researchers should remember that the cyber physical nature of SCADA and cloud computing systems gives more possibilities for different intruders to implement negative impact using malicious traffic and other incriminating actions [2].

In this regard, threats and vulnerabilities can eventually lead to various negative events for SCADA system. Therefore, in order to compline necessary requirements and to ensure effective functioning of SCADA, service personnel has to create effective response system to malicious deliberate impacts and invasions, considering as well other negative events namely, sudden and hidden failures, accidents and incidents, etc. Moreover, according to study conducted by different groups of scientists, most of all parts of SCADA failures are occurred due to negative events such as data breaches of computer systems and hacker attacks on cyber assets of great network providers.

In the proposed paper, authors consider a concrete issue pertaining to additional cloud resources provisioning to improve dependability and cybersecurity of SCADA system.

## II. RELATED WORKS

Let us try to perform analysis of related works pertaining to dependability and cybersecurity requirements for SCADA system. In that connection, significance of some control and monitoring provisions for technical and information states of the SCADA components should be noted. In particular, nowadays researchers and service personnel cannot neglect a possibility to improve dynamic features to management and control systems for different critical infrastructures based on the use of field-programmable gate array (FPGA) devices. Through implementation of energy consumption, throughput and trustworthiness principles, the checkable FPGA design [3], which allows to improve the SCADA performance, can be

978-1-7281-9957-3/20/$31.00 ©2020 IEEE

formed. A mix of cloud computing and micro services can also be used in order to create a SCADA platform architecture that will operational in real time mode [4]. As a result, some important characteristics of life cycle of the SCADA will improve, too.

Nowadays due to hidden faults caused by the extended utilization of digital virtual devices in critical applications, including software applications, the SCADA system has quite high downtime. The given circumstance can lead to great losses for users and major providers. Analysis of this problem was submitted in [5].

Considering the relevant above issues, authors as well propose to use cloud resources. Since utilization of the cloud resources as an additional service can help to provision necessary dependability level for SCADA system by creation the concurrent redundant close-loop, which implements significant features such as, disaster recovery and backup [6]. In addition, cloud infrastructure components have more extended capabilities for cybersecurity maintaining of the SCADA resources. It can be implemented on the basis of scientific studies, using the corresponding techniques of analytical and stochastic modelling. For instance, one such technique, which is based on Semi-Markov Modelling Processes (SMMP) of deliberate malicious impact on cyber and information resources of quite great IT companies of Ukraine in 2017 have been described by researchers in [7]. Therefore, the issues pertaining to different negative events for cloud systems, when they may be used as one of the most important components of management systems of critical infrastructures, need additional study.

It is worth to point out investigation results of some scientists to employ multiple pools of physical and virtual machines in order to improve the overall availability level and performance for a cloud infrastructure. These researches were conducting using toolkit of stochastic reward nets and homogeneous continuous time Markov chains (CTMC) [8]. More details about these models and sub-models can be uncovered in [9]. Possibilities for joint utilization of reliability block diagrams (RBD) method and CTMCs to estimate availability of a mobile cloud have been demonstrated by authors in [10]. In [11] researchers have looked a technique of availability estimation for large-scalable cloud infrastructure using a special model based on stochastic process algebra.

In the next section, authors propose to consider an analytical and stochastic method to dependability assessment of SCADA system considering its resources supporting based on the use of cloud services and an alleged variant of deliberate malicious impact on cyber assets of the system.

## III. Analytical and Stochastic Method to Determine Dependability Assessment of SCADA

The proposed method is based on consistent application of analytical and stochastic techniques and models considering influence of factors of diverse origin. According to this method, researchers should use the following steps in order to determine the dependability assessment of SCADA, which contents cyber and cloud assets.

### *A. Building of Structural Diagram of SCADA Assets*

The researchers should take into consideration architectural implementation of the cyber and cloud assets SCADA in design of the diagram, simultaneously considering network levels of data processing into the system. Figure 1 shows the simplified architectural implementation of the SCADA cyber and cloud assets [1].

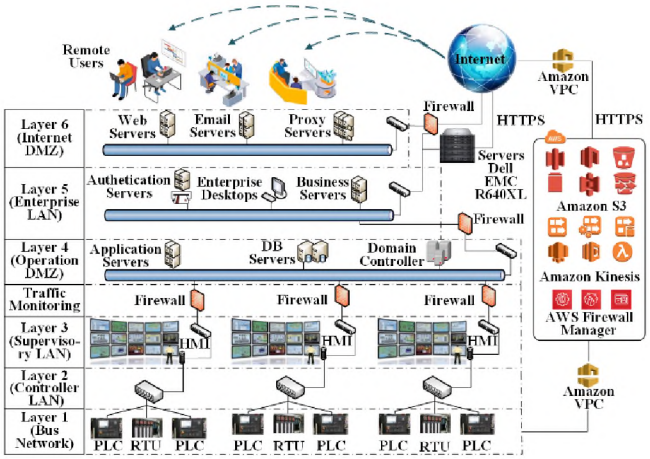



Figure 1. Simplified architectural implementation of the SCADA [1] cyber and cloud assets.

In according with Fig. 1, relevant Amazon Web services (AWS) form the additional redundant circuit for the SCADA assets.

Notable that the services AWS improve functionality properties of the SCADA, therefore these services contribute simplifying to some extent the assess procedure of dependability level for the system. At least, considering overall dependability requirements for SCADA the authors can claim that as follows:

1) service AWS Firewall Manager contributes flexible management of traffic filtration processes and improves SCADA cyber asset resiliency analysis;

2) service Amazon Kinesis contributes assess and ensuring of SCADA dependability by performing diverse processing procedures of information data streams;

3) service Amazon S3 contributes creation of storage units with immense amount of the data and ensuring of diverse processing operations in the context of the evolutionary development factors of SCADA cyber assets;

4) service Amazon VPC contributes creation of the private networks with high level of cybersecurity and ensuring of receiving and transmitting data for SCADA assets.

### *B. Building of Functional Diagram for a Deliberate Malicious Impact on SCADA Assets*

At this implementation stage of the proposed method, the researchers should build the functional scheme for the deliberate malicious impact (DMI) on SCADA cyber and cloud assets considering influence of negative factors such as, component's faults, vulnerabilities and threats for cyber and cloud components, their sudden and hidden failures, including different types of hacker attacks and even fake senders.

Figure 2 shows a functional diagram for DMI on cyber and cloud assets of the SCADA system. Assume that attackers aim to create and employ a harmful traffic (HMT), which negatively affects the SCADA cyber and cloud assets. At the same time, before begin the attack they usually previously conduct a wide phishing activity in order to get more information, pertaining to the attack object. In other words, a target phishing operation will be implemented by them. Therefore, researchers can apply this diagram in order to estimate negative impact on cloud, cyber and physical assets of the SCADA system in according with a concrete attack scenario.

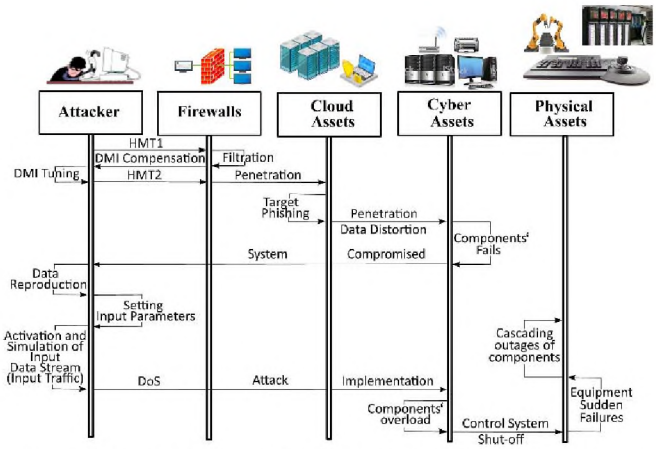



Figure 2. Functional diagram for DMI on assets of the SCADA system.

The attackers, acting in accordance with the presented functional diagram (Fig. 2), seek to achieve the following goals:

1) to create conditions for intrusion of the HMT through firewalls (FWs) by excluding performing the functions of filtering incoming information data streams;

2) to penetrate into the system in order to compromise it and as well to distort and replace the useful information with falsified;

3) to implement DMI, for example, to launch a denial of service (DoS) attack or to create additional conditions for deployment of the bot-Net.

### C. *Comprehensive Dependability Assess for SCADA Assets*

Taking into account the above cited, researchers can determine the comprehensive dependability assess for the SCADA assets. This assessment is determined as a probability of random events on the operational intervals of time for firewalls and SCADA assets. Figure 3 depicts an example for overall operational cycle of the firewalls and SCADA assets. Hence, according to Fig. 3 and considering theorems of multiplication and addition of probabilities [8] for two random events, the comprehensive dependability assessment can be written as

$$W_{SCADA} = \rho A_{SCADA} + [1-\rho] A_{SCADA}, \qquad (1)$$

where $\rho$ – event probability that firewalls successfully performing the functions of filtering of input information data streams (input traffic); $A_{SCADA}$ – steady- state availability for the SCADA assets.

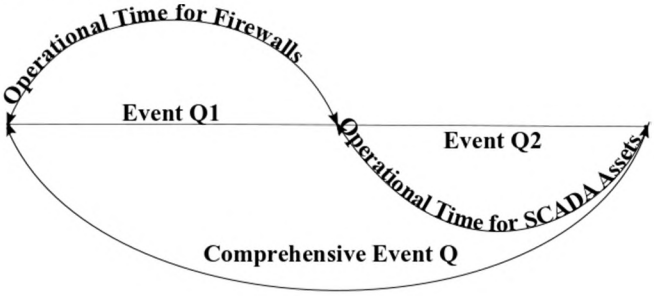



Figure 3. Overall operational cycle of the firewalls and SCADA assets.

### D. *Building of Systemic Failure Diagram of SCADA Assets*

Figure 4 provides a systemic failure diagram of the SCADA assets, which has been received by authors in according with the described architectural implementation that presents on Fig. 2. The crucial feature of the proposed method is that, in the diagram researchers can depict both different failures and deliberate malicious impacts on the SCADA assets. This circumstance provides an opportunity to obtain a complex probabilistic assessment of the dependability for the SCADA assets, taking into account the nature of the occurrence and mechanisms of DMI action. Negative events models for the SCADA assets including DMI models based on SMMP are promising in terms of further researches. The clusters, which depict in the diagram (Fig. 4) are formed by joining of elements of the network layers 1,2,3 with programmable logical controllers (PLCs), remote terminal units (RTUs) and human-machine interfaces (HMIs).

### E. *Building of Reliability Block Diagram of SCADA Assets*

Figure 5 shows reliability block diagram (RBD) for the SCADA assets considering proposals and requirements considered in [10].

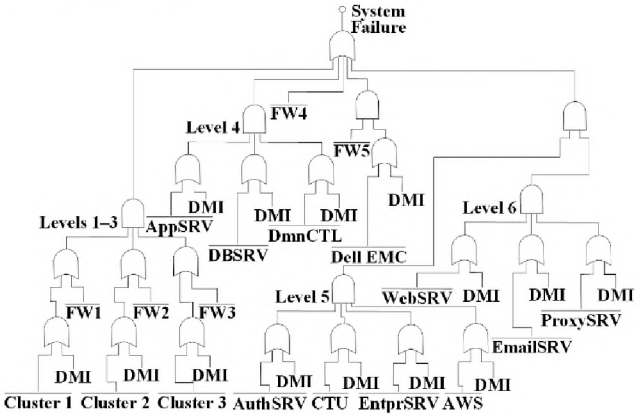



Figure 4. Systemic failure diagram of the SCADA assets.

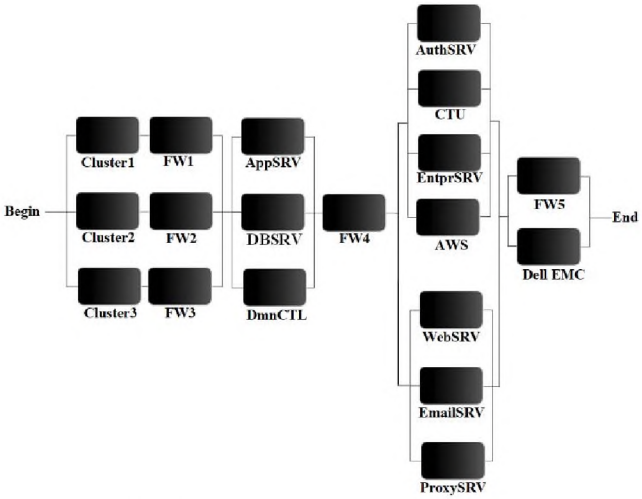



Figure 5. Reliability Block Diagram for the SCADA assets.

The development process of RBD is based on implementation of the previous steps and to take into consideration the factor of provisioning the reliable operation of the SCADA assets.

*F. Availability Assess of SCADA Assets*

Using the obtained RBD (Fig. 5) and the modeling results that have been noted in [10], the availability assessment for SCADA assets could be determined as:

$$A_{SCADA} = A_{SCADA1} A_{SCADA2} A_{SCADA3} A_{FW4} A_{FW5}, \quad (2)$$

where

$$A_{SCADA1} = 1-[1-A_{Cluster1}A_{FW1}]\times[1-A_{Cluster2}A_{FW2}]\times$$
$$\times[1-A_{Cluster3}A_{FW3}],$$
$$A_{SCADA2} = 1-\left[1-A_{AppSRV}\right]\times[1-A_{DBSRV}]\times$$
$$\times[1-A_{DmnCTL}],$$
$$A_{SCADA3} = 1-[1-A_{AuthSRV}]\times[1-A_{CTU}]\times$$
$$\times\left[1-A_{EntprSRV}\right]\times[1-A_{WebSRV}]\times$$
$$\times[1-A_{EmailSRV}]\times\left[1-A_{ProxySRV}\right].$$

*G. Semi-Markov DMI Model of SCADA Assets*

Let us utilize an opportunity to model behavior of the SCADA assets based on SMMPs. The supposed solution may be got based on the use of SMMPs with special deterministic and stochastic states [7]. There are indeed unlike typically employed stochastic models described in [8,9,10], the models based on SMMPs make it possible to address various stages of backstory time of the usage system, which to be studied. Suppose that the attack will implement according to functional diagram for a concrete DMI (Fig. 2), when attacker tries to penetrate through firewalls, using results of the previously realized phishing activity. Figure 6 shows a finite graph for Semi-Markov (SMM) DMI model of the SCADA assets.

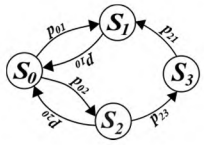



Figure 6. Semi-Markov DMI model of the SCADA assets.

In Fig. 6, authors depicted four states that can be characterized as follows: $S_0$ is state, when firewalls operational in normal mode and success conduct corresponding filter operations of both incoming and outgoing traffics; $S_1$ is state, when due to code keys change procedure (CKCP), the SCADA service personnel can perform DMI compensation for own cyber assets and cloud service provider (CSP) personnel can as well perform the similar operation; $S_2$ is state, when attacker performs target phishing; $S_3$ is state, when system is compromised and further it can't utilize to solve functional and operational tasks, that is, SCADA cyber and cloud assets are not available. The depicted SMMP (Fig. 6) can be interpreted as follows. As the conducted researches show, the CKCP may be held with periodicity $T_{ck}$ and with the duration $\tau_{ck}$. A further solution of this task is based on the apply transformation procedure of the SMMP model into embedded Markov chains.

Therefore, transition functions from states $S_i$ to state $S_j$ are given by:

$$Q_{01}(t) = \begin{cases} 0, & t < T_{ck}; \\ 1, & t \geq T_{ck}, \end{cases}$$

$$Q_{10}(t) = \begin{cases} 0, & t < \tau_{ck}; \\ 1, & t \geq \tau_{ck}, \end{cases}$$

$$Q_{02}(t) = \begin{cases} 1-e^{-\gamma_{tp}t}, & t < T_{ck}; \\ 1, & t \geq T_{ck}, \end{cases}$$

$$Q_{20}(t) = \begin{cases} 1-\left[1+\gamma_{pr}t+\left(\gamma_{pr}t\right)^2/2\right]e^{-\gamma_{pr}t}, & t < T_{ck}; \\ 1, & t \geq T_{ck}, \end{cases}$$

$$Q_{23}(t) = \begin{cases} 1-e^{-\gamma_{cm}t}, & t < T_{ck}; \\ 1, & t \geq T_{ck}, \end{cases}$$

where $\gamma_{tp}$ – events' rate, when target phishing is conducted; $\gamma_{pr}$ – events' rate, when cyberprotection of SCADA assets is provided, that is, target phishing is not succeed; $\gamma_{cm}$ – events' rate, when target phishing is succeed and SCADA assets are compromised.

Taking the total probability relation $\sum_{i=0}^{n}\pi_i = 1$, where $n=3$, and considering that $\forall\ \pi_i \in \Pi$, $\Pi = \{\pi_0, \pi_1, \pi_2, \pi_3\} \exists \left\{p_{ij} : \pi\left(p_{ij}\right)\right\}$, researchers can get the required result as

$$F_{ij}(t) = 1 \rightarrow P_{ij}(\infty), \quad (3)$$

$$P_{ij}(\infty) = p_{ij} = \int_0^{\infty} \prod_{k \neq j} \left[1-Q_{ik}(\tau)\right] dQ_{ij}(\tau), \quad (4)$$

$$\pi_0 = \frac{1}{1+p_{01}+p_{02}\left(1+2p_{23}\right)}, \quad (5)$$

$$\pi_1 = \left[p_{01}+p_{02}p_{23}\right]\pi_0, \quad (6)$$

$$\pi_2 = p_{02}\pi_0,\ \pi_3 = 1-\left[\pi_0+\pi_1+\pi_2\right], \quad (7)$$

$$\rho = \pi_0+\pi_2. \quad (8)$$

At the same time, researchers should remember and consider that scalability issue is a significant restriction to leverage of the proposed model. Since, computing complexity of the proposed model is growing significantly with the increasing number of information and technical states of the SCADA system. In order to address this issue, the researchers must carefully plane investigations

considering a complexity factor of the carry out analytical calculations.

## IV. Numerical Modeling Results

In order to get modeling results using above equations, researchers can take advantage of data, which have received in [12]. All numerical modeling results were received with condition that duration of the target phishing $T_{tp}$ equals $T_{ck}$. Figure 7 is illustrated results of Semi-Markov modeling for case of the deliberate malicious impact to SCADA assets considering different characteristics of the target phishing. At the same time, Fig. 8 shows numerical modeling results for the comprehensive dependability assessment $W_{SCADA}$ that have been got by authors considering value of $\gamma_{cm}$ parameter and duration of the target phishing $T_{tp}$. Overall modeling results considering maximum values of $\gamma_{tp}$ are shown in Fig. 9.

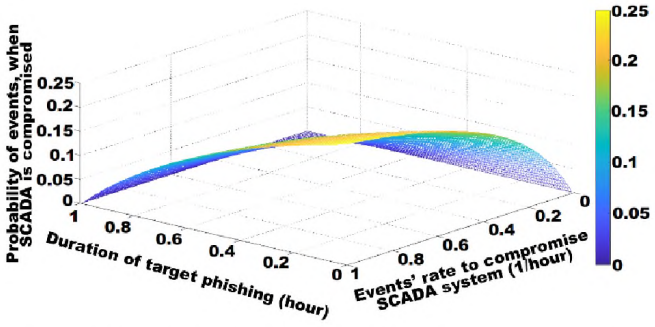



Figure 7. Numerical SMMP results for the SCADA system considering target phishing and DMI.

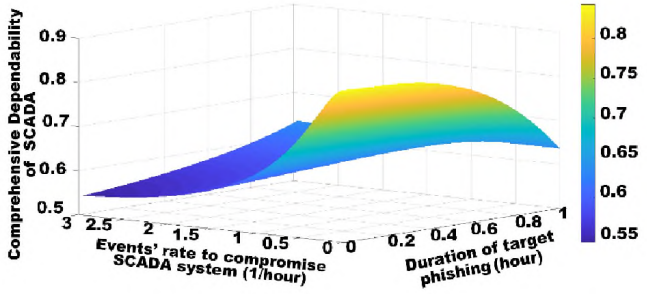



Figure 8. Comprehensive dependability assessment for SCADA.

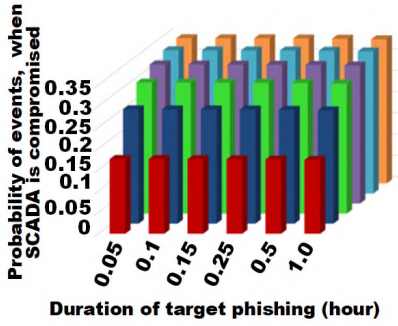



Figure 9. Overall modeling results for SCADA.

The modeling results indicated that overall dependability level of the SCADA system considering DMI with target phishing depends heavily on the characteristics of utilized firewalls, parameters of negative impact on cyber and cloud assets.

## V. Conclusion and Future Work

In this paper, authors tried to investigate aspects of ensuring SCADA dependability considering possibility of the joint use of cloud and cyber assets. The important dependability, cybersecurity aspects have been analyzed based on the use of analytical and stochastic approach including application of both new and known methods and models. Behavior of SCADA system has been modeled using SMMPs. The modeling has been also conducted according to the concrete scenario of development attack. Overall modeling results confirm that DMI with implementation of the target phishing procedure can significantly reduce SCADA dependability level, if probability of event, when the HMT penetrates through the firewalls equals about 35%.

In future works, researchers are planning to keep working in a field of dependability ensuring of the SCADA considering implementation of set of various negative events development scenarios. These modeling results may be employed in order to perform justification of dependability and cybersecurity requirements for looking-forward SCADA systems.

## References


[1] I. Ahmed, S. Obermeier, M. Naedele and G. Richard III, "SCADA systems: challenges for forensic investigators," *Computer*, vol. 45, no. 12, pp. 44-51, 2012.

[2] P. Fairley, "Cybersecurity at U.S. utilities due for an upgrade: Tech to detect intrusions into industrial control systems will be mandatory," *IEEE Spectrum*, vol. 53, no. 5, pp. 11-13, 2016.

[3] A. Drozd, S. Antoshchuk, J. Drozd, K. Zashcholkin, M. Drozd, N. Kuznietsov, M. Al-Dhabi, V. Nikul, "Checkable FPGA Design: Energy Consumption, Throughput and Trust-worthiness," *Green IT Engineering: Social, Business and Industrial Applications, Studies in Systems, Decision and Control*, vol. 171, pp. 73-94, 2018.

[4] S. Liang, C. He, W. Fang, Z. Zhou, Y. Li, and Y. Wang, "A SCADA platform architecture for cloud-based micro-service system with real time data process," in *IOP Conference Series: Materials Science and Engineering*, 2019.

[5] O. Drozd, V. Kharchenko, A. Rucinski, T. Kochanski, R. Garbos, D. Maevsky, "Development of Models in Resilient Computing," in *10th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT'2019)*, 2019.

[6] J. Mendonça, R. Lima, E. Queiroz, E. Andrade and D. S. Kim, "Evaluation of a Backup-as-a-Service Environment for Disaster Recovery," in *2019 IEEE Symposium on Computers and Communications (ISCC)*, 2019.

[7] O. Ivanchenko, V. Kharchenko, B. Moroz, L. Kabak, K. Smoktii. "Semi-Markov availability model considering deliberate malicious impacts on an Infrastructure-as-a-Service Cloud," in *14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET 2018)*, 2018.

[8] G. Bolch, S. Greiner, H. De Meer, and K.S. Trivedi, Queueing networks and Markov chains: modeling and performance evaluation with computer science applications. 2nd ed., John Wiley & Sons, 2006.

[9] R. Ghosh, F. Longo, F. Frattini, S. Russo and K. S. Trivedi, "Scalable Analytics for IaaS Cloud Availability," *IEEE Transactions on Cloud Computing*, vol. 2, no. 1, pp. 57-70, 2014.

[10] R. Matos, J. Araujo, D. Oliveira, P. Maciel and K.S. Trivedi, "Sensitivity analysis of a hierarchical model of mobile cloud computing", *Simulation Modelling Practice and Theory*, vol. 50, pp. 151-164, 2015.

[11] H. Lv, J. Hillston, P. Piho and H. Wang, "An Attribute-Based Availability Model for Large Scale IaaS Clouds with CARMA," in *IEEE Transactions on Parallel and Distributed Systems*, 2020.

[12] R. Bhardwaj, R. Singh, "A Cold-Standby System with Server Failure and Delayed Treatment", *International Journal of Computer Applications*, vol. 124, no. 17, pp. 31-36, 2015.