SUMMARIES

G. Godena, T. Lukman, M. Heričko, S. Strmčnik. The Experience of Implementing Model-Driven Engineering Tools in the Process Control Domain. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 135–147.

Model-driven engineering (MDE) is a software-engineering paradigm that is being introduced into a growing number of domains. One of the most important success factors for a new MDE approach is the availability of the appropriate tool support for it. Although the literature discusses the development of support tools, only a few reports and analyses are available about the development of tool support for real-life modeling languages and MDE approaches. The goal of this paper is to fill this gap through an experience report about developing a tool-suite prototype for an MDE approach for the process control domain that is capable of supporting the development of real-life process control software. Before the work presented in this paper an initial prototype tool suite was already developed. However, it was not able to adequately support industry-scale projects. The paper starts with an analysis of the past development of this already-existing laboratory prototype and then moves on to a report about the development of the industrial prototype, which is influenced by the findings of the analysis. Then a comparison between the two prototypes is made and the lessons learned are described, which may be useful to practitioners who attempt to develop support tools for an MDE approach that are useful in practice. The most important lesson learned is that when developing tool support for complex modeling languages, the traditional development approach should not be easily rejected.

I. Belovas, V. Starikovičius. Parallel Computing for Mixed-Stable Modelling of Large Data Sets. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 148–154.

In this paper, we develop efficient parallel algorithms for the statistical processing of large data sets. Namely, we parallelize the maximum likelihood method for the estimation of parameters of the mixed-stable model. This method is known to be very computationally demanding. Financial German DAX stock index data are used as empirical data in this work. Several hierarchical levels of parallelism were distinguished, analyzed and implemented using OpenMP and MPI library. Parallel performance tests were conducted on the IBM SP6 supercomputer. Obtained performance results show that implemented parallel algorithms are very efficient and scalable on distributed and shared memory systems. Speedups up to 800 times were obtained for 1024 parallel processes. Noticeably, our parallel application is able to efficiently utilize the Simultaneous multithreading (Intel Hyper-Threading) technology in modern processors. This research demonstrates that the application of modern parallel technologies allows a fast and accurate estimation of mixed-stable parameters even for large amounts of data and promotes a wider use of stable modelling for the statistical data processing.

I. Markievicz, J. Kapočiūtė-Dzikienė, M. Tamošiūnaitė, D. Vitkutė-Adžgauskienė. Action Classification in Action Ontology Building Using Robot-Specific Texts. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 155–164.

Instructions written in human-language cause no perception problems for humans, but become a challenge when translating them into robot executable format. This complex translation process covers different phases, including instruction completion by adding obligatory information that is not explicitly given in human-oriented instructions. Robot action ontology is a common source of such additional information, and it is normally structured around a limited number of verbs, denoting robot specific action categories, each of them characterized by a certain action environment. Semi-manual action ontology building procedures are normally based on domain-specific human-language text mining, and one of the problems to be solved is the assignment of action categories for the obtained verbs. Verbs in English language are very polysemous, therefore action category, referring to different robot capabilities, can be determined only after comprehensive analysis of the verb's context. The task we solve is formulated as the text classification task, where action categories are treated as classes, and appropriate verb context – as classification instances. Since all classes are clearly defined, supervised machine learning paradigm is the best selection to tackle this problem.

We experimentally investigated different context window widths; directions (context on the right, left, both sides of analyzed verb); and feature types (symbolic, lexical, morphological, aggregated). All statements were proved after exploration of two different datasets. The fact that all obtained results are above random and majority baselines allow us to claim that the proposed method can be used for predicting action categories. The best obtained results were achieved with Support Vector Machine method using window width of only 25 symbols on the right and bag-of-words as features. This exceeded random and majority baselines by more than 37% reaching 60% of accuracy.

Y. Zhang, Y. Zhang, Y. Li, C. Wang. Strong Designated Verifier Signature Scheme Resisting Replay Attack. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 165–171.

Strong designated verifier signature shows that only designated user can verify the validity of the signature, others who have not signer's private key or verifier's private key cannot judge the signature's originator. Lee et al. presented a designated verifier signature scheme to realize signature's verification in the limited time. We demonstrate that Lee et al.'s scheme is insecure. Other

legal users can forge valid signatures which convince designated verifier. In this paper, we show a concrete forgery attack of Lee et al.'s scheme and propose a new strong designated verifier signature scheme with time limit. In our new scheme, message and time stamp don't need transmit in public, which are embedded in signature via the method of signcryption. Only signer and designated verifier can recover those secrete values. Based on the Bilinear Diffie-Hellman problem and Pre-Image Resistance assumption, it is proved that new strong designated verifier signature scheme can resist the ordinary forgery attack and replay attack, and enforce signature verification with time limit.

U. E. Kocamaz, A. Göksu, H. Taşkın, Y. Uyaroğlu. Synchronization of Chaos in Nonlinear Finance System by means of Sliding Mode and Passive Control Methods: A Comparative Study. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 172–181.

In this paper, two different control methods, namely sliding mode control and passive control, are investigated for the synchronization of two identical chaotic finance systems with different initial conditions. Based on the sliding mode control theory, a sliding surface is determined. A Lyapunov function is used to prove that the passive controller provides global asymptotic stability of the system. Numerical simulations validate the synchronization of chaotic finance systems with the proposed sliding mode and passive control methods. The synchronization performance of these two methods is compared and discussed.

R. Piotrowski, A. Skiba. Nonlinear Fuzzy Control System for Dissolved Oxygen with Aeration System in Sequencing Batch Reactor. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 182–194.

Biological processes at a wastewater treatment plant are complex, multivariable, time varying and nonlinear. Moreover, interactions between the components are very strong. Control of dissolved oxygen is one of most important task at the plant. The level of dissolved oxygen in aerobic tanks has significant influence on behaviour and activity of microorganisms at the plant. Air for aerated tanks is supplied by the aeration system (blowers, pipes, diffusers), which is a complicated nonlinear dynamical system. A fuzzy control system for tracking the dissolved oxygen reference trajectory in activated sludge processes was proposed and investigated. The sequencing batch reactor was considered. The nonlinear aeration system dynamic was included. Two systems (sequencing batch reactor, aeration system) were modelled and validated. Inverse model of an aeration system was used to control system design. Dissolved oxygen is the control input, while the rotational speed and blowers on/off are control outputs. The nonlinear fuzzy control system was tested by simulation based on real data records sourced from a case study plant located in Swarzewo, Northern Poland.

F. Wei, J. Ma, A. Ge, G. Li, C. Ma. A Provably Secure Three-Party Password Authenticated Key Exchange Protocol without Using Server's Public-Keys and Symmetric Cryptosystems. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 195–205.

Three-party password authenticated key exchange (3PAKE) protocols allow two clients to establish a common secure session key via the help of an authentication server, in which each client only needs to share a single password with the server. Many researchers pay attention to 3PAKE protocols since they are well suited for large-scale communication in mobile environments. Recently, Farash et al. proposed an enhanced 3PAKE protocol without using server's public-keys and symmetric cryptosystems. They claimed that their protocol is secure against various attacks. However, we found that Farash et al.'s protocol is vulnerable to partition attacks and off-line dictionary attacks. Moreover, their protocol needs 5 rounds to work, so it is inefficient in terms of communication. To overcome these shortcomings, we improve their protocol and propose a provably secure 3PAKE protocol, which is more efficient and secure than other related protocols.

K.-H. Yeh. An Anonymous and Lightweight Authentication Scheme for Mobile Devices. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 206–214.

In this paper, we present a lightweight authentication scheme designed to enable mobile devices to achieve robust client-anonymity and computation efficiency. Instead of the heavy encryption and decryption modules of Elliptic Curve Cryptography (ECC), we adopt the key agreement operation of ECC as the core technique in the proposed anonymous authentication scheme. This eliminates significant computation cost and thus does not exceed the inherent resource-limitations on mobile devices. Security analyses are conducted to guarantee the robustness of the proposed authentication scheme. Moreover, when we implement our proposed scheme, the demo-system we have named AuthDroid, into the Android system, the implementation results demonstrate a practical execution time, e.g. 149.7 microseconds, on an Android-based smartphone, i.e. HTC ONE X, to complete the whole authentication procedure of AuthDroid.

Y. Yang, R. Leipus, L. Dindienė. On the Max-Sum Equivalence in Presence of Negative Dependence and Heavy Tails. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 215–220.

In this paper, following [1], the equivalence of the tail probabilities for the maximum and the sum with heavy-tailed summands under the negative dependence structure is investigated. Applications to some risk models with financial and insurance risks are provided. The Monte-Carlo simulation study illustrates the results.

A. Dmuchovskis, R. Jasinevičius, V. Jukavičius, E. Kazanavičius, L. Kižauskienė, A. Liutkevičius. Solution of the Augmenting Sequence of Linear Programming Problems as a Tool for the Intellectual Home Environment's Self-Training. *Information Technology and Control, Kaunas, Technologija*, 2015, Vol. 44, No. 2, 221–233.

This work presents the solution based on the augmenting sequence of linear programming problems (LPP) as a tool for intellectualizing home environment. The proposed solution empowers the intelligent decision making procedure which can be applied to various intelligent control applications. The augmenting self-training procedure based on LPP approach is presented as

well, which allows making reasonable decisions having only limited data about the controlled environment. The method permits retraining the decision making system when new data is available. As a proof of concept, this solution is applied to intelligent light control application. The obtained simulation results show the method's capability in making reasonable decisions according to users preferences.