Remove wAste Before Automation (RABA) : the Graph-based Anomaly Detection (GAD) Model

Computer Engineering solutions for the Factory of the Future

Pierre Parrend
ECAM Strasbourg-Europe, 2, Rue de Madrid 67300 Schiltigheim
Laboratoire ICube, Université de Strasbourg
Complex System Digital Campus UNESCO Unitwin
pierre.parrend@ecam-strasbourg.eu

Julio Navarro
Laboratoire ICube, Université de Strasbourg
Complex System Digital Campus UNESCO Unitwin
jnavarrolara@etu.unistra.fr

Rémi Porcedda
ECAM Strasbourg-Europe, 2, Rue de Madrid 67300 Schiltigheim
remi porcedda (remi.porcedda@ecam-strasbourg.eu)

Aline Deruyver
Laboratoire ICube, Université de Strasbourg
Complex System Digital Campus UNESCO Unitwin
aline.deruyver@unistra.fr

Abstract* — A key principle of the digital transformation of industries is 'Remove wAste Before Automation' – what we call the RABA approach: in a digital factory, processes must first be optimized before they can be digitalised efficiently. In this paper, we define a graph-based model for detecting wastes in digital systems under the form of anomalies: the GAD (Graph-based Anomaly Detection) model. GAD defines a three-step process: extraction of system behaviour as graph from system logs, evaluation of anomalies, and user-driven investigation. It bases on a two-fold data model built of Concrete Anomaly Scenario Graphs (CASGs) and Abstract Anomaly Scenario Graphs (AASGs). CASGs represent the actual behaviour of the system. AASG represent known behaviours, being either acceptable of abnormal. The GAD model aims at addressing one key challenge of research on the Factory of the Future: the availability of versatile models that are able to cover a broad range of applicative domains and technologies. The applicability of GAD wrt. to representative issues in Factory of the Future: production monitoring, predictive maintenance, IT infrastructure, service monitoring; is therefore evaluated.

***Mots-clés*— Industry of the Future, Computing, Anomaly detection, graphs, Waste elimination**

I. Introduction

The massive ongoing digitalisation of the industry that started at the beginning of the 2010's [W12] embeds promises of radical breakthrough in quality and productivity for the industries. However, these promises come with a significant threat: that the growth in complexity of digital production processes hinders the very capacity to operate them in an efficient manner. It is therefore necessary to ensure the performance gain: in particular the interworking of industrial best practices, on one side, and of IT best practices, one the other side, is a key enable for successful digital factories. This is a strong requirement to support efficient Cyberphysical Production Systems (CPPS).

ECAM Strasbourg-Europe therefore set up a dedicated Collaborative Service Platform to address two key issues: A) the connected production line of the Factory of the Future, and B) the life cycle of the product. The connected production line entails a training factory for initial and professional training, a digital twin of this line for ERP binding and pick-to-light support, a secure network compliant with ANSSI recommendations for secure industries, and a training platform for IoT[1]. The product life cycle excellence centre provides resources for numerical simulation, 3D printing, electronics and embedded systems, mechanical characterization and material characterization. A shared innovation lab completes the platform resources.

The objective of the Collaborative Service Platform of the ECAM Strasbourg-Europe is to define and promote pragmatic solutions for a complex environment, to give the key to enterprise partners and students to quick off the digital transformation of their industries, and to connect production and R&D to foster innovation.

Training efforts focuses on three profiles of engineering professionals:

- Industrial engineers, who must leverage the benefits of digitalisation in the processes and products they develop and manage; these are typical students of the ECAM Arts-et-Métier diploma and professional trainees of *école du Lean*.
- IT engineers, who must lead the technological as well as business aspects of the digitalisation of production environments; these are typical students of the ECAM major *TNI 'Transformation Numérique de l' Industrie'.*
- Digital transformation experts, who must foster the productivity and flexibility of production environments by taking the best of the worlds of operational excellence, on the one side, and of IT services, on the other; these are typically the students of the *ETNO (Expert de la transition numérique opérationnelle)* Mastère Specialisé.

[1] https://github.com/pierrep67/IoTPlatform/

To address these challenges we propose the RABA Approach – Remove wAste Before Automation – and its implementation for industrial IT Systems GAD, the Graph-based Anomaly Detection Model. GAD extends previous work on anomaly analysis in time series [GCP17] and extracts fine-grained behaviour of systems and users to track wastes in software-intensive processes and help remove them.

The following of the paper is structured as follows. Section II identifies the requirements for the GAD model. Section III defines the model, and Section III.C specifies its process. Section IV evaluates the model through its two implementation: Logan and SimSC. Section V concludes this work.

II. Requirements

A. Industrial best practices

Best quality and performance practices are key for competitive production lines. We are strongly convinced that approaches such as the traditional Lean Manufacturing tools will keep providing critical insights, in particular approaches like *8 Mudas*, *Standard Processes* and *Continuous Improvement*. Mudas help to identify the waste to work on for the optimisation of processes. The main challenge here is the classification of wastes in 8 categories. Standard Processes help to identify the normal behaviour of the IT system. Continuous Improvement help to increase the knowledge of the system and the way to perform.

Thus, any technological solution for the Factory of the Future should consider these known best practices, be compliant with them, and provide significant support to enforce them. In previous work, we summarizes them in the Lean Organisation Framework (LOF)[2] [PMa17]. The nine LOF core concepts are:

- Customer first
- Stakeholder satisfaction
- Make people (hitozukuri)
- Stop in time (jidoka)
- Just in time
- Safety
- Continuous improvement (kaizen)
- Visualization (mieruka)
- Make things (monozukuri)

The implementation of these concepts in an industrial IT environment leads to following principles:

- Address emergence in the process
- Focus on the interactions rather than individual tasks
- Perform data-driven analysis from actual system and organisation behaviour
- Support domain independent analysis capability (IT, production)
- Provide Technology independent analysis capability
- Support learning from the expert.

However, these principles stay at a rather abstract level, and are improper as implementation guidelines. Their analysis therefore needs to be refined.

B. Summary of RABA requirements:

The implementation of the LOF principles for industrial IT environments can be reformulated as SMART (specific; measurable; actionable; realistic; timely) requirements:

- Remove waste before automation
- Extract knowledge from field behaviour
- Support the heterogeneous technologies of the Factory of the Future
- Support the variety of challenges of the connected factory: production, automation, IT infrastructure, intelligent services (data analytics, artificial intelligence), cybersecurity [SFS11,LET11,ANS12]
- Support continuous learning from the professional

C. Industrial IT infrastructure

The model of an industrial IT infrastructure is a hierarchical system with three main layer: field layer, field servers, core servers, as shown in Figure 1. The field layer entails production workshops, individual sensors and mobile devices. It can entail IoT 'things' in IoT environments. The field server layer entails distributed servers, *i.e.* so called gateways with limited computation and storage capability, and control the individual production lines. The core server layer entails the core computational and storage facilities, typically as private or external cloud infrastructures, with massive computational and storage resources.

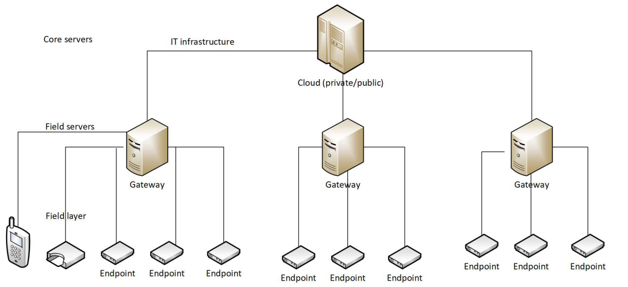


Figure 1 : Model of an industrial IT infrastructure

The device types to be monitored are therefore typically:

- The Cloud infrastructure
- The IT infrastructure
- Gateways
- Individual machines

Atop this infrastructure, a certain number of services and applications run to trigger and control the actual operations of the production lines, as shown in Figure 2. At the field layer, those are process trackers, RFID-based product trackers, machining systems. At the field server layer, the Manufacturing Execution System (MES) or similar distributed operation controllers operate. At the core server layer, the Entreprise Resource Planning (ERP) system centralises the management of operations.

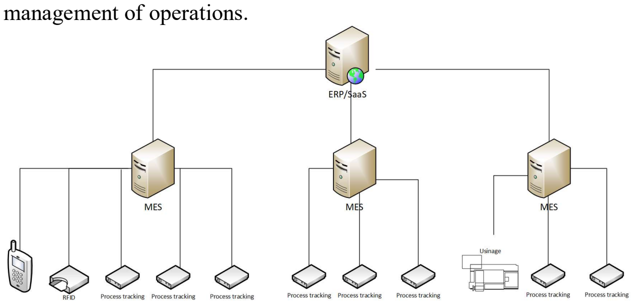


Figure 2 : Applications in an industrial IT infrastructure

The key applications to be monitored are therefore:

- The ERP
- The Production software (Manufacturing Execution System/MES)

[2] https://thecomplexlean.wordpress.com/

- Machine-specific control software.

In such an environment, the data sources available for tracking and analysing the system behaviour are:

- System logs
- Warning and error messages
- Functional logs.

III. The GAD Model

The GAD Model – Graph-based Anomaly Detection – aims at addressing one key challenge of research on the Factory of the Future: the availability of versatile models that are able to cover a broad range of applicative domains and technologies. It defines a three-step process as show in Figure 3: the *extraction* of system behaviour as graph from system logs, the *evaluation* of anomalies, and user-driven *investigation*.

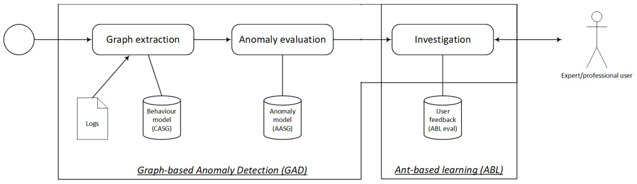


Figure 3 : The GAD process

A. The users

Investigation in GAD enables to provide the user with significant information related to the state of the system, and support to explore and analyse these pieces of information. It can also include a feedback mechanism to learn from the user expertise [GCP17], for instance through the ABL – Ant-based learning – approach [NDP16] [PMD17] which proves particularly efficient for rapid expert-based learning. The users can be of two types: an expert, or a professional user. Each of them provides a specific type of information of the ongoing production process.

1) Expert

The expert is proficient both in the industrial domain to be analysed, such as the optimisation processes of the production line, and of the digital support process. He/she can therefore make informed decisions about system configuration, process optimisation or algorithm parametrisation. He/she is therefore a reference so as to how the production line *could* behave, or to analyse complex defects outside the production flow.

2) Professional user

The professional user routinely uses the production lines and typically performs two kind of operations: production or control. He/she is highly skilled at operating the workshop in an efficient way and at identifying sensitive quality defects. He/she is therefore a reference so as to how the production line *should* behave, or to analyse product defects inside the production flow.

B. Data models

GAD bases on a two-fold data model built of Concrete Anomaly Scenario Graphs (CASGs) and Abstract Anomaly Scenario Graphs (AASGs). CASGs represent the actual behaviour of the system. AASG represent known behaviours, being either acceptable of abnormal.

1) CASG

A CASG is a directed graph modelling a multi-step process as observed from an IT system from its logs, events or errors. It is introduced in the literature as directed acyclic graphs (DAG) that are used historically to represent complex processes such as multistep cyberattacks [CM02, NCR02, VVK04, ZNX06, SLK13, HVV17]. A DAG is a directed graph without any directed circuit [Van Steen 2010]. In other words, if one chooses a node in a DAG one cannot find a path starting from one given node that brings back to the initial node. In the cybersecurity context, the term *attack scenario graph* is also used [EHN11, ST12, ZHS12, KA14] to depict these types of graphs. The reader should note that this concept is very different from the *attack graph* naming, which is an abstract representation of the network containing the vulnerabilities of the network assets as the graph nodes.

2) AASG

An AASG is a directed graph modelling known behaviours of an IT system. There behaviours can be either acceptable of abnormal. An AASG is a store model of a behaviour that serves as reference in the system; on the contrary to a CASG that represents the actual behaviour of such a system. When a CASG meets an AASG which codes for a known system defect, an anomaly is detected and a warning is raised. AASGs are defined as single-source directed acyclic graphs (DAG) represented by an ensemble of N nodes K and an ensemble of arcs A.

C. GAD process

1) Graph extraction

The first step of GAD consists in the extraction of behaviour graphs from the system logs, warning of errors. These graphs represent a partial scenario of action by a machine or by a user. Typically, two operations pertain to the same scenario when they are located on the same system, or relate to a single session between two distant machines, and stay close in time. The meaning of 'close' here is highly application-dependant: tracking manual operations or operations involving physical production steps implies far greater timespans than automated software-only processes. The *graph extraction* step provides *Concrete Anomaly Scenario Graphs* (CASGs) as output.

2) Anomaly evaluation

Once the CASGs are made available, *anomaly evaluation* can be performed. Two major approaches are defined: *behavioural anomalies*, *i.e.* the identification of behaviours that drift away from normal system condition, and *known anomalies*, i.e. the identification of behaviours that draw dangerously near known system defects. *Behavioural anomalies* detection can operate in unsupervised manner, basing uniquely on history, or in supervised manner, by comparing the actual system behaviour as CASG with expected system behaviour as AASG. *Known anomalies* detection is performed in supervised manner only by searching for patterns defined as AASG from previous analyses of the system.

3) Investigation

Investigation consists in a mainly manual step that involve the analysis of the system use scenarios, as a set of CASGs, to identify characteristic system behaviours. These behaviours are then specified as AASG and stored for latter analyses. The *investigation* step provides *Abstract Anomaly Scenario Graphs* (AASGs) as output.

IV. Experiments

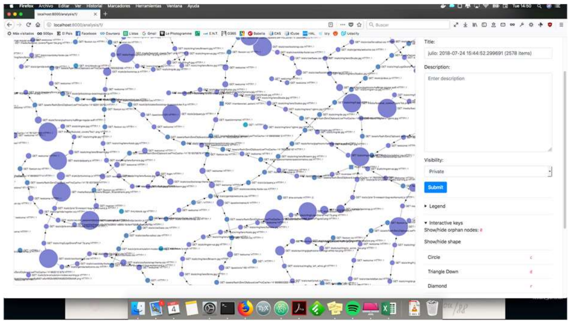
For the evaluation of the GAD model, we developed two user interfaces for investigation: Logan for web traffic analysis, and SimSC for system log analysis.

A. Use scenario analysis : Logan for Genida

Logan is the first GAD tool for extracting knowledge from field behaviour of users and systems as **Use scenario analysis**. It has been deployed on the Genida[3] project, which is a shared effort with IGBMC

[3] https://genida.unistra.fr/

to analyse genetic data bound with rare diseases. One key challenge of Genida is ensuring the security of the software: it is therefore crucial to efficiently identify regular user behaviour so as to track and prevent abnormal ones. Logan only supports bottom-up information extraction and visualisation, *i.e.* neither extensive analysis nor interaction with the user. Figure 4 shows an excerpt of Logan use scenario analysis interface.


Title: julio: 2018-07-24 15:44:52.299691 (2578 items)

Description: Enter description

Visibility: Private

Figure 4 : Overview of Logan Use Scenario Analysis interface

Erreur ! Source du renvoi introuvable. shows an example of a legitimate user behaviour, namely login and session start.

Logan is a Javascript module running on the web administration interface. It exploits IP addresses and timestamp of web server logs, which makes it suitable for a single analysis target but ready for broad extensions.

B. *Cybersecurity investigation: Genida, HuMa*

The second flavour of GAD tool is SimSC, which extends Logan with two key features: 1) it can extract graphs from any log type, and 2) it supports the investigation of massive logs by the expert. It is deployed on the HuMa project[4], which is a FUI-founded project for performing security investigation in massive system data. Feature 1) makes its very powerful to support the heterogeneous technologies of complex IT infrastructures, in particular the Factory of the Future. Feature 2) enforces GAD capability for manual expert-driven analysis of the system behaviour.

Figure 6 shows the SimSC interface and the investigation environment for complex, heterogeneous IT environment. Figure 7 shows the application of SimSC to cybersecurity analysis through the extraction of multi-step attacks in the Darpa2000 dataset, using the SimSC cytoscape module.

SimSC is a python server-based application that supports the full GAD process for graph extraction, anomaly analysis and investigation. It is a forked extension of Logan, which graphical interface is partly reused. It log-format-agnostic process enables to support a broad range of network devices and machine; moreover, it opens the way to more applications by enabling the support of non-system-specific behaviour analysis, and thus enabling to perform functional analyses beyond user and system technical sessions.

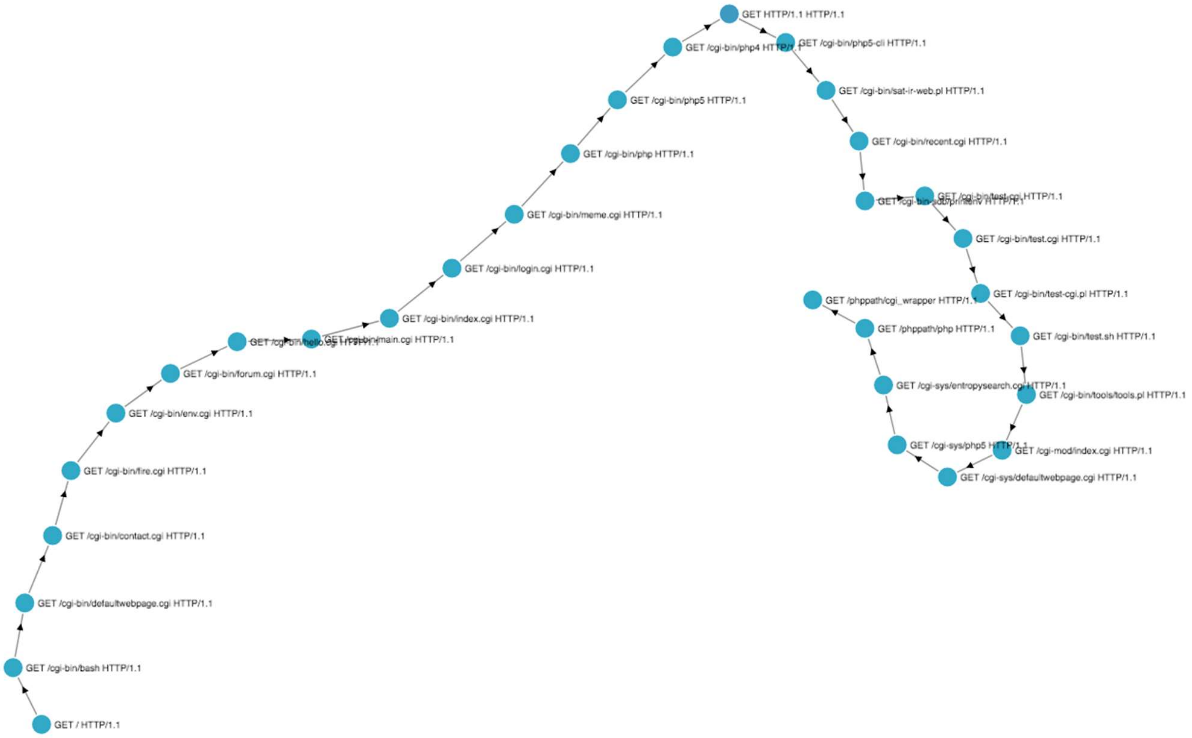

GET / HTTP/1.1
GET /cgi-bin/bash HTTP/1.1
GET /cgi-bin/defaultwebpage.cgi HTTP/1.1
GET /cgi-bin/contact.cgi HTTP/1.1
GET /cgi-bin/fire.cgi HTTP/1.1
GET /cgi-bin/env.cgi HTTP/1.1
GET /cgi-bin/forum.cgi HTTP/1.1
GET /cgi-bin/hello.cgi HTTP/1.1
GET /cgi-bin/main.cgi HTTP/1.1
GET /cgi-bin/index.cgi HTTP/1.1
GET /cgi-bin/login.cgi HTTP/1.1
GET /cgi-bin/meme.cgi HTTP/1.1
GET /cgi-bin/php HTTP/1.1
GET /cgi-bin/php5 HTTP/1.1
GET /cgi-bin/php4 HTTP/1.1
GET HTTP/1.1 HTTP/1.1
GET /cgi-bin/php5-cli HTTP/1.1
GET /cgi-bin/sat-ir-web.pl HTTP/1.1
GET /cgi-bin/recent.cgi HTTP/1.1
GET /cgi-bin-sdb/printenv HTTP/1.1
GET /cgi-bin/test-cgi HTTP/1.1
GET /cgi-bin/test.cgi HTTP/1.1
GET /cgi-bin/test-cgi.pl HTTP/1.1
GET /cgi-bin/test.sh HTTP/1.1
GET /cgi-bin/tools/tools.pl HTTP/1.1
GET /cgi-mod/index.cgi HTTP/1.1
GET /cgi-sys/defaultwebpage.cgi HTTP/1.1
GET /cgi-sys/php5 HTTP/1.1
GET /cgi-sys/entropysearch.cgi HTTP/1.1
GET /phppath/php HTTP/1.1
GET /phppath/cgi_wrapper HTTP/1.1

Figure 5: Legitimate user behaviour: login and session start

[4] http://www.huma-project.org/

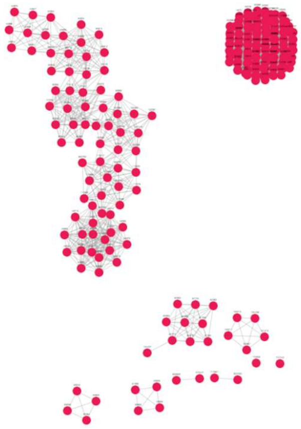


Figure 6 : Investigating use scenarios in a complex IT environment

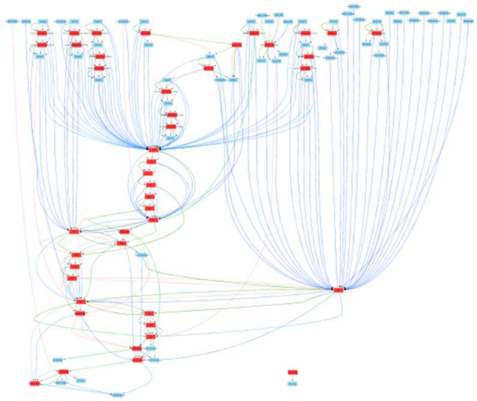


Figure 7 : Investigating multi-step attacks in Darp2000 dataset

C. Perspectives

The GAD model opens two main perspectives: cloud monitoring solutions, on the first hand, and tracking of production wastes ('digital mura') on the other.

1) Cloud monitoring

To evaluate the versatility, SimSC has been deployed for other goals. For instance, it provides promising results for the quality of service evaluation in the context of Cloud-based applications such as Enterprise Resource Planning. In this context, it exploits warning and error messages.

2) Production: Digital Mura

SimSC is currently under evaluation as a tracking tool for production process regularity and quality, for RFID-triggered intelligent workshops.

More applications are foreseen on predictive maintenance to identify early signs of irregularities or defects in connected machines.

V. Evaluation

Thanks to the various implementations of the GAD model in various environments relevant to the Factory of the Future: web applications; complex IT infrastructures; cloud-based applications; production tracking, we now have a significant experience to draw the first conclusion on the relevance and performance of the GAD – Graph-based Anomaly Detection – approach to solve the challenges of RABA – Remove wAste Before Automation – approach.

A. Adaptability

GAD is available in two flavours: the Logan tool, dedicated to web application management, and SimSC, which is a versatile tool enhanced with investigation capabilities.

	Use scenario analysis	**Cybersecurity investigation**	**Cloud monitoring**	**Digital Mura**	**Predictive maintenance**
Data type	Server logs	System logs	Warning and error messages	Functional logs	Machine logs
Location	IP	IP	IP	App-level label	Module-level label
Time	System timestamp	System timestamp	System timestamp	System timestamp	System timestamp
Technological target	SaaS	IT infrastructure	Cloud	Production/ MES	Machine
Graph extraction	Yes	Yes	Yes	Yes	Yes
Anomaly evaluation	-	Yes	-	-	Yes
Investigation	-	Yes	Yes	Yes	-

Through these two examples, GAD proves to handle server logs, system logs, warning and error messages, and functional logs. An extension to machine specific logs will be necessary for supporting predictive maintenance feature for machining devices. Location in the IT environment is mostly based on IP addresses, but can also rely of application- or module- specific labels. Time analyses consider that system timestamps are reliable, which can be questioned if synchronisation is broken between independent, remote network parts, but proves to be efficient is all considered use cases. Logan and SimSC cover a broad range of technologies: Web/SaaS, IT infrastructure, Cloud, Production/MES, Machines.

The SimSC tool currently covers the full GAD process: Graph extraction, Anomaly evaluation, Investigation. Actually, for several use cases, only a partial coverage of this process is sufficient to leverage the GAD model. Graph extraction itself is a powerful tool; investigation without refined graph analysis provides a great deal of support for the expert.

B. Requirement coverage

The experiments presented in this work show that GAD approach enforces RABA requirements in an extensive manner:

- Extract knowledge from field behaviour: log-based analysis ensures that the behaviour graphs represent a very accurate view of the environment behaviour and its current processes;
- Support the heterogeneous technologies of the Factory of the Future: the variety of technological domains for which Logan and SimSC are evaluated confirm the versatility of the approach;
- Support the variety of challenges of the connected factory: production, automation, IT infrastructure, intelligent services (data analytics, artificial intelligence), cybersecurity: the variety of application domains for which Logan and SimSC are evaluated confirm the versatility of the approach;

- Support continuous learning from the professional: the investigation interface of SimSC proves to be a powerful tool for user information and expert analysis. More learning implies further algorithmic solutions such as ant-based learning evaluated in previous works of the authors;
- Remove waste before automation: and lastly, by explicating the actual system behaviour, GAD enables to visualise and analyse the current setup of partly digitalised environments, thus enabling to solve misconceptions before going to the next integration step.

In particular, GAD distinguished itself from competing approaches (rule-based approaches, markov chain models) by mapping the actual behaviour of the system from system data, whereas most models are usually built in a top-down manner and thus far more difficult to adapt when the production environment evolves.

VI. Conclusion and Perspectives

In this work, we presented the RABA – Remove wAste Before Automation – requirements and the GAD – Graph-based Anomaly Detection – model which aims at providing a versatile, technology agnostic solution for monitoring and optimising the digital infrastructures of the Factory of the Future. The evaluation we performed on both implementations of GAD, Logan and SimSC, confirm that GAD is a very promising tool to leverage the promises of the Factory of the Future.

The next steps for the GAD model will be 1) to enhance it with numerical analysis capabilities to couple the behaviour models with quantitative prediction models, and 2) to further refine the graph model so as to support broad ranges of behaviour analysis algorithms from deviation detection to known pattern identification.

VII. References

[W12] Wahlster, W. (2012). From industry 1.0 to industry 4.0: Towards the 4th industrial revolution. In Forum Business meets Research.

[GCP17] F. Guigou, P. Collet, P. Parrend, The Artificial Immune Ecosystem: a bio-inspired meta-algorithm for boosting time series anomaly detection with expert input, EvoApplications, 20th European Conference on the Applications of Evolutionary Computation, Amsterdam, Netherlands, avril 2017

[CM02] Frédéric Cuppens and Alexandre Miège. Alert correlation in a cooperative intrusion detection framework. In Security and privacy, 2002. proceedings. 2002 IEEE symposium on, pages 202–215.

[NCR02] Peng Ning, Yun Cui and Douglas S. Reeves. Constructing attack scenarios through correlation of intrusion alerts. In Proceedings of the 9th ACM Conference on Computer and Communications

[VVK04] Fredrik Valeur, Giovanni Vigna, Christopher Kruegel and Richard A. Kemmerer. Comprehensive approach to intrusion detection alert correlation. IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 3, pages 146–169, 2004.

[ZNX06] Yan Zhai, Peng Ning and Jun Xu. Integrating IDS alert correlation and OS-level dependency tracking. In International Conference on Intelligence and Security Informatics, pages 272–284. Springer, 2006.

[SLK13] Seongjun Shin, Seungmin Lee, Hyunwoo Kim and Sehun Kim. Advanced probabilistic approach for network intrusion forecasting and detection. Expert Systems with Applications, vol. 40, no. 1, pages 315–322, 2013.

[HVV17] Pilar Holgado, Victor A. Villagra and Luis Vazquez. Real-time multistep attack prediction based on Hidden Markov Models. IEEE Transactions on Dependable and Secure Computing, 2017.

[EHN11] Ali Ebrahimi, Ahmad Habibi Zad Navin, Mir Kamal Mirnia, Hadi Bahrbegi and Amir Azimi Alasti Ahrabi. Automatic attack scenario discovering based on a new alert correlation method. In Systems Conference (SysCon), 2011 IEEE International, pages 52–58, 2011.

[ST12] Sherif Saad and Issa Traore. Extracting attack scenarios using intrusion semantics. In International Symposium on Foundations and Practice of Security, pages 278–292. Springer, 2012.

[ZHS12] Zeinab Zali, Massoud Reza Hashemi and Hossein Saidi. Real-Time Attack Scenario Detection via Intrusion Detection Alert Correlation. In 2012 9th International ISC Conference on Information Security and Cryptology (ISCISC), pages 95–102. IEEE, 2012.

[KA14] Fatemeh Kavousi and Behzad Akbari. A Bayesian network-based approach for learning attack strategies from intrusion alerts. Security and Communication Networks, vol. 7, pages 833–853, 2014.

[NDP16] J. Navarro, A. Deruyver, P. Parrend, Morwilog: an ACO-based System for Outlining Multi-Step Attacks, IEEE Symposium Series on Computational Intelligence (IEEE SSCI 2016), Athènes, Greece, décembre 2016

[LVM18] Latapy, M., Viard, T., & Magnien, C. (2018). Stream graphs and link streams for the modeling of interactions over time. Social Network Analysis and Mining, 8(1), 61.

[DA04] Van Dongen, B. F., & Van der Aalst, W. M. (2004, November). Multi-phase process mining: Building instance graphs. In International Conference on Conceptual Modeling (pp. 362-376). Springer, Berlin, Heidelberg.

[PMa17] P. Masai, Modeling the lean organization as a complex system, Thèse de doctorat, Université de Strasbourg, 29 septembre 2017

[SFS11] Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. NIST special publication, 800(82), 16-16.

[LET11] Rafał Leszczyna, Elyoenai Egozcue, Luis Tarrafeta, Victor Fidalgo Villar, Ricardo Estremera, Jairo Alonso, Protecting Industrial Control Systems - Recommendations for Europe and Member States, ENISA, 14th of December, 2011

[ANS12] Managing Cybersecurity for Industrial Control Systems - Anssi, June 2012

[PMD17] P. Parrend, C. Maller , E. Dietrich, The Ant Reconciliation Algorithm (ARA): Ant-hill learning for label matching, Artificial Evolution, Paris, France, octobre 2017.