Towards a Detective Approach to Business Process-Centered Resilience

Thomas Koslowski and Christian Zimmermann

University of Freiburg, Germany
{koslowski,zimmermann}@iig.uni-freiburg.de

Abstract. Protection of today’s interconnected and complex information infrastructures is of high priority. Traditionally, protection means robustness: preventively identify the threats to business processes and propose countermeasures within the context of a risk analysis. This, however, only covers known risks having punctual effects upon the IT infrastructure. In contrast, the notion of resilience, as a refinement of trustworthiness, is getting attention both in academia and within organizations as a denominator to move beyond survival and even prosper in the face of adverse conditions. This paper reports on ongoing work towards the development of PREDEC, a detective framework to realize resilience in the context of business processes. Specifically, it firstly motivates the need for operational resilience and corresponding tool support at the level of processes. Secondly, it sketches the operation and building blocks of PREDEC, which currently employs process mining techniques to analyze process event logs to assess systems’ resilience. Finally, it describes the intended evaluation steps to be undertaken once PREDEC is completely implemented.

Keywords: Operational Resilience, Automated Detection, Process Intelligence, Resilient BPM.

1 Introduction

The intensive use of densely interconnected and complex IT-systems incurs risks with increasingly severe disruptive effects. Today, most decision makers, either public administrators or private organizations, have come to understand that protection of information systems is of high priority. But the expanding landscape of emerging risks illustrates the borderless and unpredictable nature of risk and uncovers the limits of traditional risk management practices and theories in the face of highly interconnected systems: new emerging risks or new surprises lack a priori indication of occurrence, they exhibit the potential to “cascade” through time and space at different speeds and their relation between origin, evolution and final consequence are frequently ill-understood. But just because some systems are complex does not mean they are unmanageable or impossible to govern. However, managing them requires different methods and rests on other assumptions than classical risk and security management.
Where we had come to expect predictability and consistency, we now must accept the necessity of dealing with the consequences of uncertainty [30].

Against this background, the notion of resilience is getting attention as a denominator to move beyond survival and even prosper in the face of challenging conditions [25, 29]. Resilience is an emergent property associated with an organization’s capacity to continue its mission despite disruption through mindfulness [41], resourceful agility and recoverability, e.g., [15, 25]. Therefore, resilience is a combination of technical design features, such as fault-tolerance and dependability [9], with organizational features such as mindfulness, training and decentralized decision making [8, 11].

Today, enterprise systems and information infrastructures increasingly build upon processes. Generally speaking, processes are structured specifications of personnel and business data usage that run (at least) semi-automated in a business process management (BPM) system. Examples of systems building upon processes can be found in very different domains and range from, e.g., organizations’ supply chains, banking backbone infrastructure to parts of critical infrastructure such as smart grids or nuclear power plants. The advantage of process-orientation is the decoupling of infrastructure and organizational workflows as a means to enhance enterprises’ overall performance and effectiveness.

The current state of the art at the intersection of business processes management and resilience approaches the high-level design of resilient information systems [8], the satisfiability of workflows [11, 39], change propagation [18] and incident response [23]. However, there are no approaches and technical frameworks that put processes in a “resilience loop” which also encompasses adaption.

In this paper, we report on ongoing work towards PREDEC, a detective framework to assert the resilience of business process-based information technology infrastructures. According to the BPM lifecycle, the analysis of processes can happen at design time (a priori), at runtime and offline (a posteriori) [2] (compare Figure 2). While the first two timepoints allow for preventive mechanisms to avoid violations, a posteriori methods based on the analysis of event logs are detective. Casting them into the context of resilience, preventive methods are in place to allow for robustness (resistance against incidents) whereas detective approaches serve as an input for business process redesign and, if in large scale, re-engineering. However, extensive literature review in the field of risk-aware BPM reveals that current approaches focus on the design-time phase, while concepts and artifacts with focus on runtime and offline analysis are rare [26, 36].

The ultimate goal of PREDEC is to enable organizations to automatically identify and assess the interdependence of assets and processes. In order to extract the interdependencies we employ process mining techniques developed by [2, 37]. Additionally, we employ techniques as developed by, e.g., [38] to elicit socio-metric data from event logs in order to build social networks of the subjects involved in process executions. In that, we aim at augmenting the assessment of interdependence of assets and processes with a social network perspective.