Chapter 3
Awareness-Based Security Management for Complex and Internet-Based Operations Management Systems

Udo Inden
Cologne University of Applied Sciences, Research Centre for Applications of Intelligent Systems, Cologne, Germany

Georgios Lioudakis
National Technical University of Athens, Institute of Communication and Computer Systems, Greece

Claus-Peter Rückemann
Westfälische Wilhelms-Universität (WWU) & Leibniz Universität Hannover & North-German Supercomputing Alliance (HLRN), Germany,

ABSTRACT

Grounded on two use-cases from different domains of operations – aviation network management and service-bundling of small enterprises – the authors develop a management concept for increasingly complex business operations' systems. These cases exemplify the convergence of new technologies and with this the arising of new organisational and managerial challenges representing both, risk and chance. Soon so-called "Things-that-Think," profiting from future multi-core chip architectures and autonomously acting in the Internet, will become drivers of massive distribution and parallelisation of stationary and mobile operations' architectures and lead to hybrid networks of humans, things and systems. These developments require elaborating and implementing new principles and mechanisms of operations' management – not at least in order to manage holistic operations' properties raising with the complexity like criticality, resource footprints, or, pars pro toto addressed here, security. The core of the authors' argumentation is that the increase of operations' complexity emerging from this combination of massive heterogeneity, distribution and parallelism, on the other side offers new chances

DOI: 10.4018/978-1-4666-2190-9.ch003

of mastering complexity. For taking this change two concepts are paramount: intelligent peer-to-peer systems and self-aware system behaviour e.g. with regard to performance and for sure: security. Rather than struggling with the finally unavailing undertaking of controlling complexity, this chapter suggests implementing self-awareness as added-value service into complex operations' systems with the goal of managing their "holistic properties" like external effects, criticality, as well as issues of security and trust.

INTRODUCTION

"The machine is the problem: the solution is in the machine" (Poullet, 2006). Since man invented technology it is two-faced: a source of risk and of chance. Fuelled by competition, a race for better technology developed. The sheer complexity of technology grew and now, fuelled by Information and Communication Technology (ICT), it runs at an unprecedented speed. As co-decision-makers in hybrid architectures of widely parallel operations artificial objects (things) to a considerable degree are expected reaching eyes level of its inventors. For basic concepts see Maturana (1984/92) and Kauffman (1995). On examples from commercial and non-commercial service industries we want to illustrate that these features may also become tools of maintaining operations' integrity. Concepts and methodology of implementing principles of technologically enabled self-awareness will be shown in this chapter on the example of security management including considerations regarding the vulnerability of operations' systems which may be organised in the internet.

At this point some basic definitions may be useful: "Operations" comprise the whole network of processes and resources for realising business models which enable subsistence and growth in competitive environments. "Autonomous" means that a system (actor) is able of effectively subsisting on exchanges with its environment, pursuing own objectives and relying on own resources (means to an end).

"Adaptive" systems are able of maintaining their existence under conditions of unexpected, thus unplanned changes in the environment. "Environments" are formed by interactions of systems i.e. are equal to the volume and variety of systems interacting. "Contexts" are relevant backgrounds to acting and interacting, e.g., in terms of different values which derive from the variety of systems. Examples of contradictions may be costs versus quality, or short-term speculative profit versus long-term investor interests. Thus interacting with different systems requires capabilities of standing frictions and balancing conflicts.

Complexity, respectively the uncertainty it produces in terms of lacking information about the operations' scene and of unexpected and thus unplanned events, is the "intimate enemy" of operations' management. Very pragmatically ICT is needed for augmenting awareness and adaptive decision making. But by solving one concern another appears: future technology may even exacerbate the problem:

- Things-that-Think (TtT) are digitally augmented objects like future cars, aircrafts, containers, buildings, refrigerators (Ishi et al., 2010; Günther & Hompel, 2010; Scherer, 2011; C2C-CC Manifesto, 2007; Europe's Information Society, 2011) which – comparable to intelligent software agents (Rzevski, 2011; Koestler, 1967; Chevaleyre et al., 2005; Luck et al., 2005; Sandholm, 1993). I.e. like software agents, things may also have objectives and access to knowledge, may become context- and self-aware and finally able of autonomous decision making.
- Things collect, compute and collaborate in the Internet of Things and Services (IoT/S). IPv6 with 2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456 (Zivadinovic, 2007) addresses is the backbone for integrating things and ser-