The Challenge of Dynamic Services in Business Process Management

Tom Kirkham and Sandra Winfield
Information Services
University of Nottingham
United Kingdom

Thorsten Haberecht and Jens Müller
University of Karlsruhe (KIT)
Germany

Guglielmo De Angelis
Istituto di Scienza e Tecnologie della Informazione “Alessandro Faedo” Consiglio Nazionale delle Ricerche Pisa, Italy

Abstract
Advances in mobile and embedded computing have led to a computing environment that embraces personalisation, mobility and real-time computing. As a result Service-Oriented Architectures (SOA) has to adopt new methods of service security, service management and service execution. For business processes these adaptations yield challenges in terms of process modeling, delivery and execution. In order to make Business Process Management (BPM) work in practice in these new environments, what changes are needed in order to support increasingly dynamic and decentralised services in BPM?

Keywords: Business Process Management, Dynamic Web Services, User Centricity, Factory Automation, Mobile Web Services.

1. Introduction
Research into emerging Web Service architectures is increasingly placing business process management as a key component to the delivery of next generation web applications. The use of business process engines and business process templates allow application designers and business analysts a key focus for system functionality without the need to focus on the wider technical architectures. The use of Web Services to create loosely coupled business processes relies on orchestration to achieve the desired distributed application functionality. Typically this is done by the coupling together of stable services in a static workflow. However in dynamic environments the services are often non static and often change state and characteristics. Or the environment can be unstable and as a result the workflow has to adapt dynamically to changing execution conditions.

Emerging Web Service environments are increasingly embracing mobile devices, personal data and embedded low level functions. These service types stretch the current limits of BPM. The emerging needs of these computing environments place complex demands on the business process. In a typical business process application change can be managed by adding loops to the process or switching between templates. In more dynamic environments services have to be renegotiated and workflows altered during execution.

Changing the process model on runtime (e.g. inserting a loop or a fork) is a common research aspect (without major implications on real-world BPM systems). Whilst runtime adaptation of business processes depending on dynamically changing environments and resources (or service demands, etc.) is a rather un-investigated topic.

This paper explores challenges facing BPM as a key function in future Service Oriented architectures by citing experience gained in three EU research projects. These projects present challenges to BPM in different domains and explore adapting BPM to real time environments, mobile computing applications and frameworks that support user centric security.

2. Emerging Challenges to BPM.
Business Process Management and Service Oriented Architectures can be seen as a perfect match. The goal of BPM is to allow process designers the ability to create an application without concern for the underlying technical architecture. This has been made easier by a drive toward service representation of computing resources [1].
Services in SOA present common interfaces and support communication standards for data exchange to aid specific processes such as ebxml [2].

Within the domain of integrating companies’ enterprise and other office systems along with internet front ends, the application of BPM using process engines to execute process templates in formats such as BPEL is a clear design process and one that presents scalability and common technology for an organisation [3]. However as the BPM process to systems integration movement expands it will be exposed to more challenging computing environments where things are not as static as office based systems.

2.1 Mobile Services

In recent years the mainstream adoption of positioning technology in consumer electronics in particularly mobile phones is leading to the development of a new generation of mobile web applications. For organisations these applications yield a new possibility for improving business process. A good example can be seen as the management of transport resources and the ability to adapt to location information in terms of supply chain workflows [4].

Challenges to the business process designer can be seen when the workflow is present on a mobile device or has make critical decisions based on mobile services in an emerging environment. A good example here can be seen in the eHealth domain and has been explored in the Akogrimo project [5].

Here workflows are present to manage the response to an emergency from a centralised perspective. However the challenge facing the central workflow is compounded by local factors. For example the workflow may have to react to contextual information linked to location of Ambulances and specialist Doctors in the location of the emergency. Here the location of the devices is constantly changing and context in which they are present may differ (for example some Ambulances maybe responding to other calls).

Such unpredictability cannot be modeled into a traditionally static workflow [6]. Here the BPM has to adapt to the state of a number of services related to the context in which they are present. This has to be done relation to the execution of the wider response workflow.

2.2 Real Time Services

Organisations such as large scale manufacturers have adopted BPM to control elements of their organisation such as supply chain management. As discussed the workflows around stable office system require minimal maintenance and allow rapid integration with similar systems.

In the domain of manufacturing factory down time are a serious concern and a major factor in increasing production costs [7]. Typical causes of downtime relate to problems on the production line. These are typically caused by machine failure or failure in the supply of correct components.

The execution of production lines is typically controlled by closed circuit systems using technology such as Programmable Logic Controllers (PLC). The PLC’s are vendor specific and have their own control units for the execution of the line. Integration of these systems into the wider office and enterprise systems can improve the monitoring and maintenance of the line. But due to the nature of the control systems the integration is not seamless.

Work by partners including Schneider Electric in the EU SOCRADES project [8] has developed controllers that support Web Services. These services have been enabled by advances in embedded computing and can be integrated to form a real time reporting mechanism from the line to the enterprise. The Web Service enablement of the line has presented each line component as separate entity [9]. This has the potential to allow line orchestration using Business Process Management (BPM).

Controlling and integrating with live production lines using a BPM mechanism has its advantages in terms of line reconfiguration and standardisation. But real issues exist in terms of safety and reliability of BPM in the execution of live production lines. In order to support this modifications have to be made to both the way the workflow is designed and executed in standard BPM terms.

2.3 User Centric Services

Service providers rely on BPM to handle different customer paths through online systems. By using standardised workflows user experience can be better controlled and managed using a standardised approach that links through to the Web Services. Security in such frameworks is handled by set mechanisms of service provider authentication either locally or via a federation of linked service providers [10].

Federated identity management architectures rely on a trust and policy framework in order to establish the authentication and authorisation rules between service providers. These rules and mechanisms can be supported by centralised workflows. However, user centric models are emerging where the user’s data is protected by policy as it travels through the federation.

For the BPM designer user centric security places extra demands on the workflow. As users can define specific policies on their data negotiations and management of data and service provider access becomes more fine grained and subject to change. The BPM designer no longer has to support the
needs of service providers that tend to be fixed over time, but large numbers of users have to use the Business Processes with large variations in relation to data security policy.

User-centric approaches may require additional interactions with users, depending on the security context. Requiring application developers to model these interactions explicitly would put too much of a burden on them. Rather, more intuitive solutions are required. One such solution is modeling security-specific user interactions through annotations [14] and automatically performing the interactions using an approach based on a transformation of the process model and special components of the BPM system [15].

The management of applications using multiple data sets with user defined policies is a focus of the EU project TAS3 [11]. The project is focused on providing user centric security and envisages the Business Process playing a key role in the support of user and service provider interaction. This interaction is often dynamic and involved negotiation between parties. Figure 1 illustrates the position of the business process (Workflow) and how it is linked to trust and reputation services along with service discovery and authorization (Auth) and policy services.

**Figure 1. TAS3 Workflow and User Centric Security Model**

Within the model in Figure 1 the links to the two main sources of dynamicity (service discovery and trust services) is significant. As the trust measurements of services change new services are often discovered and added to the workflow during execution. Thus these services interface directly with the business process.

The more static policy and user interfaces link the user to the business process in order to control and monitor the progress distributed application execution. The graphical models usually created for the implementation of workflows include the interactions with web services. They are thus particularly fit to visualize the execution of the workflow, the data transfer, and features of chosen services, such as their trust levels.

### 3. Implementations

The implementations of the Business Processes in each project shed different insights into the challenge that BPM faces in supporting more dynamic Web Services.

#### 3.1 Mobile Dynamic Business Process.

The Akogrimo project developed Mobile Dynamic Virtual Organisations (MDVO) to support mobile workflow execution [12]. The MDVO were formed based on the specific application environment. For example services can be selected for execution based on location.

An alternative to the use of a business process is the peer-to-peer communication of services in a location based context. Such examples can include automated vehicle management systems. Here rules in each vehicle and the sensor data interact in order to complete a wider goal of traffic management. However this mechanism of peer-to-peer control removes the centralised authority needed in applications that need a service provider.

Service provider control allows the development of location based services along existing models of service provision. For example the logistics company would still take responsibility for the management of the supply chain routing based on location data rather than leave it to peer-to-peer determination between agents.

The Akogrimo project focused this approach in the eHealth emergency response scenario. In order to provide a centralised response to an emergency BPM provides the best standardised way of conducting and monitoring a response operation. The innovation in the business process application was to bind service endpoints to the process at runtime. As the exact service instances for use in the BP were linked to location and are unknown at the design phase of the BP. The business process templates had to be populated with endpoints of actual services based on the negotiation and reservation of services in real time.

Renegotiation was possible if service moved out of context by changing factors such as their location. This service selection and renegotiation was supported by the Akogrimo MDVO. Figure 2 illustrates the relationship between the MDVO and the Akogrimo Business Process / Workflow (WF) Management infrastructure.
The Akogrimo MDVO is created by a static and permanent Base VO. The Akogrimo Base VO manages the WF repository and can create multiple MDVO per application instance. The WF repository stores the workflows specific to each application and these are instantiated by the workflow instance and populated with live services (represented by Service Agents (SA)). The user or service for who the MDVO is executing an application is represented by the User Agent (UA). The UA starts the workflow instance and is a member of the MDVO the same way as the SA and WF components.

The Akogrimo Virtual Organisations were implemented using Java Web Services using the Globus Toolkit version 4 (GT4). The GT4 toolkit included the provision for the use of the standard WS-Resource. This enabled the individual instances of the MDVO to contain state identifiers. This enabled the splitting of resources between identifiable service instance belonging to specific MDVOs. The workflow engine and design tools were implemented using Active Endpoints using the BPEL standard.

3.2 Knowledge Based Line Management

To date opinion is still open as to whether BPM is needed on production lines. However if a seamless factor from floor to enterprise level is to be realised the communication between the IP layer has to be the same as the machine level on the production line. The SOCRADES project achieved this by implementing Web Services using Device Profile for Web Services (DPWS) [13] set of standards on Arm 9 controllers that operated individual line elements.

The inclusion of the business process linked to the line consisting of services controlling the execution of components with services linked to enterprise management. The aim being the knowledge from enterprise services can aid the execution of the line.

The services were deployed on a Ford test rig which is shown in figure 3.

![Figure 2. Akogrimo MDVO and related components.](image)

**Figure 2. Akogrimo MDVO and related components.**

The service level of communication enabled the BP to be designed in order to ensure the line is monitored and operated in real time by services linked to the enterprise computing layer. However the performance of this approach was proven to be lacking. Real-time execution of services could only be achieved using binary xml. It is likely that a similar binary form of processing will be needed for BPM to control line orchestration.

In addition to the performance challenge for BPM to work on production lines the safety issue is another major factor worth considering. In order to ensure operator and machine safety the process of BPM design on production lines has to ensure that the process is fail safe. Thus any integration with Enterprise systems has to ensure a clear flow of data.

Due to the complexity of a production line (many consist of 1000’s of elements each of which could be a Web Service) the BP design and execution phase is put under increased pressure in terms of knowledge management.

In the SOCRADES project the Business Process was complemented with ontology design which explored the relationship of the components in more detail. This aided the correct decision making when the BP encountered problems or forks in the business process. Because of the merger of ontology and business process a specific execution engine has been developed for the project at Loughborough University. This engine uses the knowledge in the ontology and supports existing line based standards for line workflow description and execution.

3.2.1 Production Line Ontology

The line Ontology provides in depth knowledge to the line business process allowing greater automation in recovery from line errors or machine
reconfiguration. The Ontology is also used outside of the line execution environment for data mediation, wider process management and has inference capabilities with the help of a developed inference engine.

Figure 4. Ontology model relation to line data, rules and business process.

The ontology has been applied specifically in a car production environment. Here a business process is the set of all formally coordinated tasks and activities, conducted by both people and equipment, which leads to accomplishing a specific organizational objective. An example of a business process is order fulfilment. The act of a customer placing an order initiates a process to record the order, approve their credit, and trigger the production and delivery.

As the Business Process Management (BPM) is a process-centric way of doing business and it requires adjusting the enterprise frameworks and the enterprise architecture accordingly. It is natural therefore to link the business process to the production line. Integration with the production line adds to the business processes collection of complex assemblies of models, rules, data, logic and services.

BPM linked to the line facilitates holistic car manufacturing and will enhance the rapid design, assembly, and deployment of complete enterprise to line business processes. The vision is that a developer attaches IT systems and services to the same process model designed by the business analyst. A complete set of connectors and codeless tools makes the development of solutions even faster.

The ontology supporting BPM describes the composition of elements that make up a machine. On a production line multiple machines exist and work together in the production process. Within these machines elements make up specific parts that perform tasks. Any changes to neighbouring machines or the part as it is passed down the line requires often specific elements to be also reconfigured.

The ontology represents the machines in a finer way than the business process. The business process is largely concerned with what machines work on the part. The ontology represents how the machines operate and this operation can be analysed against any changes in part or integrated machinery.

Thus the integration of BPM with semantics will enable the business process such as reconfiguration of the line to be linked directly to the appropriate domain knowledge.

Figure 5. Business processes routed in domain knowledge

Implementation started from validated and approved models of engine assembly business processes. Ontology development has been hindered by data that is stored in independent silos where integration to create ontologies is a time consuming and often manual process. On top of the ontology development a need also exists to integrate this new approach to process support among all the stakeholders during new machine design or reconfiguration of the line.

3.3 User Centric Security

TAS\(^3\) [1], stands for "Trusted Architecture for Securely Shared Services". Specifically TAS\(^3\) is a European FP7 funded project (2008-2011) that aims to create a solid foundation for ecosystem of consumer-citizens, service providers, and eGov providers.

3.3.1 Sticky Policies

The project is an ambitious synthesis of existing technologies and standards in Identity Management and Web Services. Furthermore, it also focuses on the management of policies in distributed frameworks of services in order to form a trusted environment for user and service provider co-operation.

The measurement and management of trust is therefore vital for the execution of services and
sharing of data in the framework. The awareness of trust gives users the opportunity to express their needs in the network better and to find appropriate services. The TAS³ project harnesses trust in order to present a method to provide user-centric control over security and privacy in distributed web service based applications.

The authentication and authorisation infrastructure in TAS³ has been implemented using ZXID [16] and XACML policies. The network operates by checking messages as they are sent out from TAS³ endpoints and checked as they are received. The position of the Policy Enforcement Points (PEPs) in a TAS³ data exchange can be seen in Figure 1.

Typically BPM operations are executed from centralised servers using services with pre-defined access clearance. In a user centric security environment this execution becomes more complex. Complexity increases due to each data object being associated with user defined ‘sticky’ policies. Therefore large amounts of individual authentication and authorisation (AA) are needed for access to groups of distributed data objects. Such AA calls reduce the performance of the business process and can cause application failure. For example, most online service providers in the social network domain operate by the expectation that personal data between linked individuals can be aggregated. This is because policy is assumed on the level of the individual. In a user centric world envisaged by TAS3 the policy will be present on the data layer and defined by the user at different levels for separate data objects. The finer grained policy management will offer the user more security.

To adapt to this each business processes instance has to cut through large swaths of data with separate user defined policies in order to function. Thus to achieve this in a practical way it is envisaged that each business process instance will have its own profile. This profile corresponds directly to the common policy format used by users in the system. The profile will be determined on contextual factors such as time of day, number of users involved and privacy settings. In theory it can be negotiated between user privacy settings around specific applications.

As a result of such negotiations the profile can be granted appropriate privileges over specific data when executing in specific contexts. This will allow the process to operate efficiently as it can cut through the AA. As in the mobile services scenario the appropriate pre-execution priming of the workflow allows it to operate at a more finely grained level.

Within TAS3 the workflow infrastructure was implemented using Intalio software. The policy infrastructure was created using ZXID (www.zxid.org) using XACML policies and policy enforcement points using PERMIS (www.permis.org).

### 3.3.2 Online Compliance Testing

User centric security in TAS3 is based upon notifications of access attempts to data. The management of these notifications by the user places increased demands on the workflow and has led to the need for specific policy profiles. These policies can override specific user policies in order to maintain system critical business process. In order to ensure service providers do not manipulate this measure automated online compliance testing has been introduced into TAS3.

The OCT component is a conceptual framework supporting on-line testing of deployed systems. Specifically, for each service under test the OCT component continuously verifies that it does not violate any of the declared access control policies running a set of test cases. The OCT component uses realistic credentials and dummy data to see if the proper results are achieved. If the appropriate results are achieved, they pass; if they are not, they fail. Figure 7 depicts the general pilot for the OCT component.
Specifically, a tester designs the test cases and formats them so they can be used during the on-line testing sessions. The tester also configures the tool in order to activate the on-line testing sessions either periodically or driven by events. During each on-line testing session, the OCT component loads all the test cases and executes those toward a specified service under test (SUT).

In the TAS³ architecture we require secure communication between the OCT component and the Identity Provider (IdP) (e.g. SOAP over an https channel). Once the OCT component has collected all credentials specified for a test case, it securely sends a SOAP request to the SUT. Specifically, the OCT component first includes in the header of the SOAP message the IdP-signed assertion testifying the role that the tester is playing, and then it signs the whole message.

As a test, a correct credential can be transported by an envelope with security errors (e.g. broken signature of the envelope) or an incorrect credential can be transported in an otherwise good envelope. The OCT component also includes features that are able to perform such “negative” tests.

When the SUT replies, the OCT component validates the response according to security aspects. Specifically, it not only checks whether the response message is properly signed, but also its integrity, and the acceptability of both the obligations and any sticky policy. Also, the response from the interaction with the SUT is compared with the result expected for each test case. Thus the result for each test case execution can be stored as a log and sent to the workflow.

Use of checking by the workflow engine alongside the user of failed tests ensures that user centric security is supported by machine defined testing. The workflow link enables that services what provide rogue results can be excluded from the user application or renegotiated in the workflow without user input.

4. Future work

Using enterprise linked business processes to control production lines is an area of future work where security needs to be further investigated. Recent hacking of industrial systems by the Stuxnet virus has proved the vulnerability of non-integrated, but somehow connected systems. This is particularly important when integrating the production line control system into enterprise systems. Here it such integration could make it easier to hack it and stop the whole facility (or nuclear power plan or whatever).

Security is also an issue for workflow use in personal data and mobile environments where the dynamic needs of the workflow could expose the ability to intercept or manipulate the service selection or workflow decision making phases of execution. Online compliance testing is a method to counter this threat, but the work needs to be expanded into the mobile domain and a wider range of applications.

Performance of dynamic workflows is another area of future investigation. The negotiation of services to add dynamic nature of BP or the decision points needed to react to unstable application environments will reduce execution time. A possible way around this is to further encode the service environment from XML based services to the use of binary. This is being research particularly in production environments.

Logging and error recovery and detection is made more complex by dynamic workflows. As the execution does not follow as set patterns as traditional workflows, error detection mechanisms and monitoring mechanisms are harder to apply. This a new generation of tools is needed in order to maintain reliable workflow execution in these emerging environments.

5. Conclusion

Services are become more context specific, real time and the policy surrounding them is becoming finer grained. With this in mind the need to support greater flexibility in BPM and execution increases. This shifts the focus from one-time modelling of static business processes to a more flexible but thereby complex management of - only partially defined in advance - business process instances and associated resources.

Thus, BPM can continue to work in practice when faced with a world of dynamic services. However in order to do this the method by which business processes are designed, populated, executed and supported will need to change. Using online compliance testing, user notifications and service renegotiation based on virtual organisations of trust are some methods to address this problem.

6. Acknowledgements

This paper describes work undertaken partly in the context of the ‘Trusted Architecture for Securely Shared Services’ (TAS3) project (www.tas3.eu). TAS3 is a collaborative project supported by the 7th European Framework Programme, with contract number 216287.

7. References

Services and Ecommerce, Volume 41, Number 2, 2002.
[16] ZXID homepage www.zxid.org