Large Scale Integrating Project

Grant Agreement no.: 257899

D11.1 – SMART VORTEX Classification model for streams and interactions and description of the rules acquisition

SMART VORTEX –WP11-D11.1

Project Number	FP7-ICT-257899
Due Date	2012-09-30
Actual Date	2012-09-30
Document Author/s:	Hans-Ulrich Heidbrink, Felix Engel, Jens Grabarske, Tore Risch, John Lindström, Magnus Löfstrand, Lennart Karlsson, Mathias Johanson, Holger Brocks, Jörg Brunsmann, Jordan Janeiro Lopes Da Silva, Daniel Wedlund, Jonas Larsson, Arne Byström and Jens Harder
Version:	1.2
Dissemination level	CONFIDENTIAL
Status	Final
Contributing Sub-project and Workpackage	WP11
Document approved by	RTDC

Co-funded by the European Union

Document Version Control			
Version	**Date**	**Change Made (and if appropriate reason for change)**	**Initials of Commentator(s) or Author(s)**
0.1	120626	First version	JL
0.2	120628	Updated after work meeting	JL
0.3	120807	Additions from several partners	JL, JoL, HUH, FE, JG, JB
0.4	120809	Small additions	JL, ML
0.5	120906	Re-structuring and additions	JL, ML, LK, MJ, JoL, AB, JH, HUH, HB, JJ
0.6	120912	Requirements, Survey and Appendixes 1, 2	HUH
0.7	120920	Integration of additions	JL, TR, MM, JG, FE, JB, DW, HUH, JJ
0.8	120924	Summary,requrements, conclusions	HUH, FE, TR, JG, JH, MM
0.9	120925	Finalization of deliverable	HUH, JG, FE, JL, JoL, AB, JH
1.0	120926	Final version	JL, FE, HUH, DW
1.1	120927	Additions/changes after internal review	JL
1.2	120930	Finalization	JL, JG

Document Change Commentator or Author		
Author Initials	**Name of Author**	**Institution**
HUH	Hans-Ulrich Heidbrink	InConTec
FE	Felix Engel	FernUni Hagen
JG	Jens Grabarske	FTK
TR	Tore Risch	UU
JL	John Lindström	Luleå University of Technology
LK	Lennart Karlsson	Luleå University of Technology
ML	Magnus Löfstrand	Luleå University of Technology
MJ	Mathias Johanson	Alkit Communications
HB	Holger Brocks	InConTec
JoL	Jonas Larsson	Volvo CE
JB	Jörg Brunsmann	FUH
DW	Daniel Wedlund	Sandvik
JoL	Jonas Larsson	VCE
AB	Arne Byström	Hägglunds Drives

JH	Jens Harder	FE-Design
MM	Massimo Mecella	Sapienza
JJ	Jordan Janeiro Lopes Da Silva	Delft

Document Quality Control			
Version QA	**Date**	**Comments (and if appropriate reason for change)**	**Initials of QA Person**
1.0	120926	Internal review	TR
1.2	120930		IK

Catalogue Entry

Title	D11.1 - Classification model for streams and interactions and description of the rules acquisition
Creators	JL et al.
Subject	Software architecture requirements analysis and description
Description	The WP11 runs from M7 to M36, and this is the final version of the D11.1 unless further important discoveries necessitate an updated version of the D11.1 at M36. Describes the classification model for streams and interactions and description of the rules engine. Based mainly on tasks T11.1 and T11.2, but also to a certain extent T11.3. WP11 roadmap Until 2nd review: investigation of useful policy and framework technologies (XACML) and establishment of trial technology to sort out the best fitting solution. For the 2nd review: comparison of two open source technologies OpenAM and HERA^{AF} and presentation of the trial set-ups during the review. Year 3: Decision which system/technology best fulfilling the requirements of the SmartVortex research and development teams. Implementation of the rule and policy framework as a service to be working with the collaboration and decision solution and the user dashboard in tight integration with the federated DSDM system. Generation of loose coupled prototype Year 4: The work continues in the ISP1-3 (i.e. WP13-15) regarding the extension of the collaboration and decision room implementation with access to documents and artifacts stored in persistent repositories outside the FDSDM kernel system; Full implementation of the ISP1-3 use cases in the related demonstrators and documentation of the added functionality.
Publisher	Smart Vortex Project
Contributor	
Date	2012-09-30
ISBN	
Type	
Format	
Language	English
Rights	

Citation Guidelines

EXECUTIVE SUMMARY

This document describes the requirement generation process for the rules and policy framework to be implemented in the SmartVortex tool suite and proposes an architectural approach for the following detailed functional specification and prototypical implementation in the D11.2 delivery.

The intention of this report is to describe **WHAT** the rules and policy framework will provide as well as how to implement that. The following deliverable D11.2, which is a prototype, will be able to demonstrate **HOW** the rules and policy framework operates (together with other components in the SmartVortex suite).

The document will be the starting point for detailed technical specifications and implementations of the management of rules and policy framework of the Smart Vortex suite.

Following the recommendation of the SmartVortex reviewing team the eXtensible Access Control Markup Language (XACML) has been reviewed and to check the applicability in the SmartVortex system a survey about the access control requirements has been conducted at the participating industrial partners. The XACML is an OASIS approved standard for access control. XACML specifies access control requests, responses and policies, and there are several XACML implementations available. Thus, the most important XACML implementations have been reviewed. **Axiomatics** provides a widely used Attribute Based Access Control (ABAC) solution. Due to legal and licensing reason this commercial solution has been excluded even if the features would have fulfilled most of the requirements. It would have been also in contradiction with the FP7 regulations to make the solution unlimited public available. Therefor the concentration went to open source solutions. Two of the available open source systems/implementations have been analyzed in detail:

- **OpenAM –** which was originally developed at SUN Microsystems (Oracle today) and was given to the open source community after SUN decided that the maturity gradient was sufficient and further investments would not be made. Today ForgeRock is the development organization supporting OpenAM. The system is very powerful and provides beside access control also authentication up to digital signature functionality and single sign on. The user interface is powerful and allows generation of rules and conditions in an easy menu guided manner to be used as well from administration personal with limited programming skills. To test the system a test installation with some own grown use cases have been performed.
- **HERA**$^{\mathbf{AF}}$ (Holistic Enterprise-Ready Application Security $^{\text{Architecture Framework}}$) – which has been developed at the HRS (University of Applied Science), Rapperswil, Switzerland, and provides a strong research oriented solution only for authorization. The authentication functionality, especially the single sign-on feature, is missing. The solution is not built as "Out Of the Box" ready to use system but gives the researcher high flexibility in the implementation supported by a powerful Java API. HERA^{AF} is addressing in that case more developer than users or administrators. The missing user interface does not limit its usability in a project like SmartVortex where the solution will be a serve to the entire DSDM and collaboration system.

Regardless which system/implementation we give the preference, both systems are fully OAIS and XACML standard 2.0 compliant and the XACML code can be interpreted by both systems. The final decision will be made during the implementation of the rules and policy framework. XACML will be the basis for the implementation and extensions required to support access control in collaborations applying social graph and semantic information will be developed during the implementation phase.
The architecture of the rules and policy framework has been designed to make it flexible in terms of usage by the existing SmartVortex suite software components as well as if adding additional components.

KPI fulfillment and Milestone

Regarding the KPIs, the first KPI can be measured by one defended master thesis [6] reaching 33% of the target. In addition, the work on another master thesis addressing "policies and their management" is ongoing at FTK.

The second KPI has not yet reached written acceptances by the industrial partners, however we have investigated how they look upon the matter of collaboration and sharing of information during development of Functional Products. Thus, we measure the second KPI to 33% having made a large part of the investigative work to understand the requirements for a written acceptance.

Title of KPI	Management of access / Usage
Defined	Management of access, usage rules, and policies to be able to correctly share data streams and artifacts in terms of information security and intellectual property rights (IPR)
Measured	% of fulfillment described by master thesis (defended during 2011) and two issued papers
Target	100%

Title of KPI	Establishment of best practices for building secure cross-organizational collaboration environments
Defined	Create clear understanding on various levels and non-disclosure/disclosure at different stages on collaborating partners documented in papers. Certified by the industrial partners. The process description determines the key factors for IPR protection and how typical IPR problems can be solved and implemented by the authorized users
Measured	% Written acceptance by all (4) industrial partners
Target	100%

The milestone MS11 has been moved to M36 as the deliverable D11.2 was moved to M36.

Abbreviations used
XACML - eXtensible Access Control Markup Language
SAML - Security Assertion Markup Language

TABLE OF CONTENTS

1 INTRODUCTION

In the Smart Vortex project, a number of software components will be developed and integrated with existing software components to form a suite of software tools known as the Smart Vortex Suite. The key software components include a Federated Data Stream Management System (FDSMS), data capture and telematics components, visual query and data visualization components, collaboration and decision-making components and social networking components. Data interchange with external systems, such as Product Lifecycle Management (PLM) systems, will also be required. To get all this to work together in industrial (realistic) scenarios, a rules and policy framework is needed to provide basic **access control** to for instance **information or system resources**. This is especially important in collaborative scenarios involving actors or stakeholders from different organizations, where all involved should not have full access to the other parties' intellectual property (IP) in terms of information or system resources etc. Thus, the access needs to be possible to restrict in an adequate manner with large volumes of "users" originating from different organizations.

This document focuses on describing the rules and policy framework of the Smart Vortex from a software engineering perspective. However, there are also other aspects that are important to consider in the design of such framework. Strategically, one important aspect is the business service dimension, which from a process perspective adds value. This aspect of framework design involves crossing organizational boundaries. The strategic aspect must consider the fact that large parts of industry will/may to a larger extent in the future transition to a service-based business model. These services will often be delivered by a cluster of several cooperating organizations. Therefore, the framework must be designed so that it is possible to provide access control to information resources, well-defined services based on the software components or other system resources.

2 RULES AND POLICY FRAMEWORK OVERVIEW

This section comprises an overview of the functional requirements for the rules and policy framework. The functional requirements collected in the D1.1 and D1.2 deliverables are complemented with additions from the industrial partners.
Further, this section provides an overview of different access right classification models, the criteria for selection of such, as well as the selection and its rationale. In addition, a selection approach for selection of access rights classification model implementation is discussed.

2.1. Functional requirements ISP-1-3

In the requirement analysis D1.2 it got obvious that in a FDSMS several level of access control is needed. While some calculated results of derived data stream might be accessible from several users in a company or at their customers other defined stream shall be only accessible to specific roles in a project team or members of established or ad hoc collaboration sessions.
The access to formulas which are the base for the FDSDM calculation has in many cases additional stronger restrictions. These formulas are representing trade secrets and specific IP of the industrial partners and are mostly subject of long lasting research activities.
During collaboration sessions initiated by dedicated events in the trend analysis or at threshold violations of data streams, background knowledge in terms of document access or specialist contributions are required to take the right decision as reaction to the given alert.
The documents which need to be referred to or which need to be shared will contain also company IP and cannot be made accessible to everyone in a collaboration session and in some cases approvals of higher management levels or prior sharing established "Non-Disclosure Agreements" are required.

Thus, the workgroup has conducted a survey about the specific needs of access control related to existing rules, roles and policies

2.1.1. Methodology for role and responsibility definition

FDSDM technology is used at all involved industrial partners as an instrument to verify the run-time behaviour of a technical system in a customer or development project regardless if software or hardware based. Therefore similar organization structures appear in the responsibility model of such projects. JISC[1] has proposed a role/responsibility model that can be found in a majority of industrial projects, and it is possible adopt or refine it to the specific hierarchy structure of a company respective its project organization. This model has been explained to the industry partners and adopted to those kinds of projects which are typical for the usage of FDSDM technology representing the deep or flat organizational structure of each partner. The model which includes adopted responsibilities has been extended with a section that defines the access rights for specific document types used in projects.

2.1.2. Proposed roles following the JISC model

The following roles have been reviewed with the project partners and have been subject for the rules and policy investigation regarding access control:

- Project Manager
- Project Sponsor
- Steering Group/Board
- Senior Consultant or Supplier-side Project Manager
- Project Team Members
- Project Administrator or Co-ordinator
- Systems Developer

[1] www.jisc.ac.uk

- System Service Manager
- System Service Member
- System Administrator
- Observation and Monitoring Centre Member
- Programme Manager
- External Partner R&D
- Customer (service and user)

The assigned responsibilities can be seen in Appendix 1.

2.1.3. Data streams, metadata, skill information and document types with access control

The discussion with the perspective users in the industry resulted in a list of information sources which are in general subject of access control. In many cases simple role based access control was not applicable. To verify that a questionnaire has been generated to give detailed information for the following elements:

- System history tracks (recorded data streams)
- Sensor definition data
- Meta data that operate on the sensors
- Formulas that calculate the derived sensor streams
- Stream query editor
- Collaboration invitation
- Collaboration participation
- Project deliverables in line with the project plan.
- Project progress, status and performance reports
- Project problem reports
- Cost calculation related to the project
- Project member definition
- Change requests documentation related to the project.
- Training Material
- Marketing material for promotion and dissemination activities.
- Consultancy input if involved and related to the project
- Design specification and functional requirements.
- Design documents
- Drawings or models
- Maintenance and repair documentation
- Skill and responsibility information within the project frame
- Documents describing the User Acceptance Testing program.

All these items can be subject for FDSDM initiated collaborations and requiring access of the users acting on events or alerts in the data stream to verify the behaviour or to identify the source and the reason of a failure and to take the right action to resolve the problem. There are elements which directly deal with the data stream its self and elements which might be stored in different systems like PLM, CAD, DMS or similar systems to give background information during collaboration sessions.

2.1.4. Results of the Survey about access control and conclusions

Due to the different organizational structures in the projects that have been provided as use cases for the ISPs in SmartVortex the team established a survey about access control requirements starting from the role and responsibility description and using the access to items list. Each partner that provided use cases in the project gave feedback about its own access control, rules and policy model where different kind of control features have been requested. The aggregated survey results are not disclosed in this deliverable due to confidentiality reasons. However, those results will be used as input guiding the development of the rules and policy framework.

The access rights models that are used in several systems like in PDM/PLM or DMS at our industrial partners are mostly role oriented. In collaborative environments the document type gets an additional weight especially if customer, external consultants or development or outsourcing partners are involved in any kind of development or service projects. The survey has shown that the access rights have a multitier character.

First tier is given by the project structure and the roles which are assigned to the project member levels representing their responsibilities. Nevertheless there is no direct relation between role and document type. The detail deepness level of the document defines the possible IP contents and requires more attention while sharing those documents during collaboration. This can only be performed introducing as additional level an attribute and rule based access control mechanism. As example might be used the following graphic extracted out of the survey representing one of the industrial partners. This is a typical situation while the shown percentage varies from partner to partner.

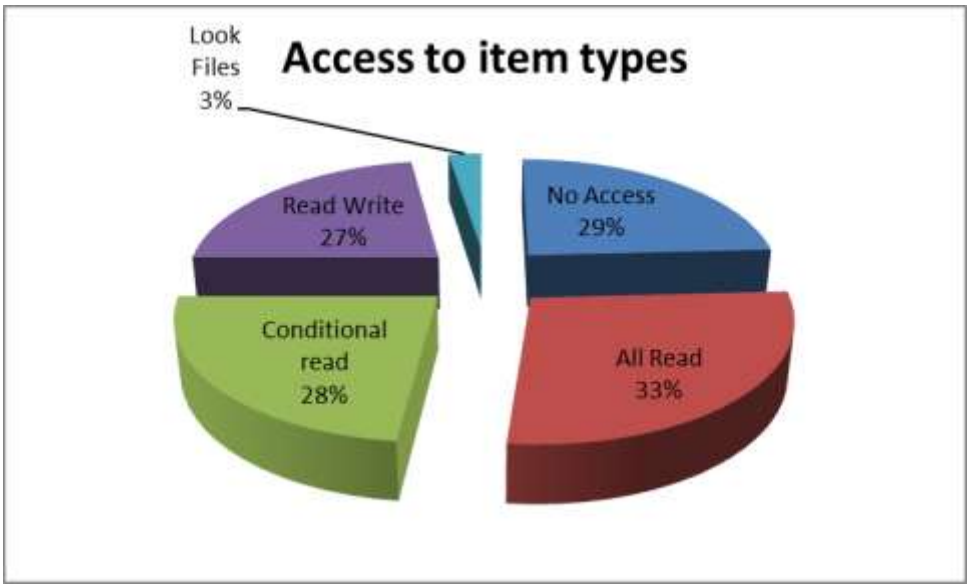

Figure 1 – example of survey result graphics

The comparison is made about all document types and roles. There have been 14 different project member roles defined and the result shows the all over all access distribution including each active role.

Specific conditional attributes that have been requested are the following:

- Give sequential access rights: check with person A on permission if the document can be shared permanently
- Check if a valid service contract exists to give access rights

- Give access right only if non-disclosure agreements exist
- Limit access rights outside working hours
- Vary access rights for on-site or off site access
- Limit access rights related to locations (different IP regulations)
- Give permission only in a sequence: Document A must be access first before document B can be accessed
- Limit access to specific layers in a CAD model document for defined project members or roles (exclude drawing or measurement layer, exclude tolerances
- Exclude information from the social graph following the legal and workers units obligations

These specific access control mechanism need to be implemented when establishing the rule and policy framework. The XACML technology allows such mechanism. Nevertheless this needs extension of the current applications and their configuration tailored to the specific case as multi-tier model where role, rule and policy interact and gives therefore a fine grained solution for the SmartVortex access control engine.

2.1.5. Access Control Models

In the literature different access control can be found. These are summarized as follows in Wikipedia: *Access control models are sometimes categorized as either discretionary or non-discretionary. The three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC). MAC is non-discretionary.* The essentials of these models are described as follows:

2.1.5.1. Attribute based Access Control (ABAC)

In attribute-based access control (ABAC), access is granted not based on the rights of the subject associated with a user after authentication, but based on attributes of the user. Several attributes can be combined or be used to exclude.

2.1.5.2. Role Based Access Control (RBAC)

Role-based access control (RBAC) is an access policy determined by the system, not the owner. RBAC differs from DAC in that DAC allows users to control access to their resources, while in RBAC, access is controlled at the system level, outside of the user's control.

2.1.5.3. Discretionary Access Control (DAC)

Discretionary access control (DAC) is a policy determined by the owner of an object. The owner decides who is allowed to access the object and what privileges they have.
Two important concepts in DAC are:

- *File and data ownership: Every object in the system has an owner. In most DAC systems, each object's initial owner is the subject that caused it to be created. The access policy for an object is determined by its owner.*
- *Access rights and permissions: These are the controls that an owner can assign to other subjects for specific resources.*

2.1.5.4. Mandatory Access Control (MAC)

Mandatory access control refers to allowing access to a resource if and only if rules exist that allows a given user to access the resource. One specific case in the MAC is the Rule- or Label-based access control. This type of control further defines specific conditions for access to a requested object.

Based on the survey response the full variety of access control requirements can be distinguished in the RBAC and ABAC model categories which belong to the discretionary access models. Nevertheless for some rules a MAC model might be applicable protecting specific sensitive IP information. The selected models to be implemented in the rules and policy framework of the SmartVortex project will be determined in sub-sections 2.5 and 2.6.

2.1.6. Performance

Access control must be implemented in many components of the entire SmartVortex software suite. The access control needs to be implemented to not cause unnecessary delays, and the rules and policy framework further needs to be scalable to not become a bottleneck itself. Performance issues are further discussed in section 3.

2.2. Industrial partner requirements and limitations

To complement the functional requirements collected in the D1.1 and D1.2 requirement engineering deliverables, the industrial partners below describe the different scenarios and requirements related to those.

2.2.1. Sandvik Coromant

The main stakeholders can be divided into the ones within Sandvik Coromant and those from the customer side. Note that a customer can be an external as well as an internal customer. Within a project with its aim to deliver a particular solution to a customer many different roles come into play.

When developing the solution, may it be new methods and/or tools, data in a broader context is generated both from test sites within Sandvik Coromant and from the customer. This data can be static type such as files and dynamic type as in live data measured.
Most often all data is available to project team members and the customer only has access to data that they generate. All data generated from tests are analysed and then different methods are applied to generate new strategies and/or tool to satisfy the customer needs.
When the strategy with all its incorporated tools have been developed a testing phase occurs in multiple steps starting with dry-runs at the Sandvik Coromant side and ending with live test at the customer side. Same restrictions on data generated and streamed is in this phase as in the development phase.

With a strategy with all its tools deployed at the customer site the project has most often ended. Still problems can occur e.g. due to changed conditions, machine aging etc. and the need for troubleshooting introduces the criteria for streaming support-data to Sandvik Coromant for analysis. Since this can be some time after the project ended, it is important for the contacted person at Sandvik Coromant to be able to find the persons that where involved in the project and/or persons with similar skills, all this to ensure good troubleshooting practice.

When the strategy works well and only requires the operators and managers at customer side to monitor the process and act accordingly to the service plan set up. In this case the operators get a detailed view on their machine and all the data, raw and derived, from the process for instance power levels. The manager at customer side has a broader view of all machines but generally in less detail. They have access to summarized numbers on uptime and downtime of each machine.

In general the customer can only see the result of derived streams and some/all of the data from raw streams. They can formulate own queries, for instance they could sum all the uptime for the whole shop floor, but they cannot change or see queries/formulas provided by Sandvik Coromant. In this scenario Sandvik Coromant has access to data related to the process depending on the type of project, customer agreement and roles/permissions set up during the project.

2.2.2. Volvo CE

From a Volvo CE perspective, the stakeholders are: the operator utilizing the Volvo CE machine, the site owner, the machine owner, the dealer or other third party that provides services to the end customer, Volvo CE back office users and development partners.

The operator would in the machine have access to a set of data streams where the available data streams is given by a table stored onboard the machine linking operator ID to stream ID. Example of streams could be loaded tons/consumed fuel in liters, cycle time.

The machine owner and site owner would have access by wireless communication to most streams of the operator but would also have access to information on total cost of ownership, on accumulated loaded tons per material type, operator efficiency in tons/hour, machine uptime and comparison of operator to operators having same type of machine and applications at other Volvo CE customers and more. The access rights for the machine and site owner are stored at the Volvo CE back office.

The dealers and third party service vendors have access to machine deviation detection streams in order to trigger these service providers to take a closer look at the machine in question. They also receive error codes. They receive the data streams from servers run by the site owners.

Volvo CE has complete access to the data streams available from servers run by the site owners. This includes on top of previously mentioned machine usage characterization in terms of types of operations performed and component usage in 1D and 2D histograms displaying e.g. time spent at a certain speed/torque range or the amount of times a certain gear shift has occurred.

The Volvo CE development partners have access to data streams through Volvo CE and can have restricted access to selected machine usage streams to evaluate the usage of their supplied machine components. The external service providers can have the same setup to evaluate their services.

The roles Volvo CE is interested in are: operator, machine owner, site owner, service provider, back office, development partner.

2.2.3. Hägglunds Drives

The stakeholders for streamed and calculated data from Hägglunds Drives hydraulic systems are End customers, Machine manufacturers (OEMs), Hägglunds Drives development, Hägglunds Drives internal users and External development partners.

At the End customers (users of our delivered equipment) the main users are the maintenance personnel. The need is to have a tool to get an overview of rising problems and system usage for planning of their maintenance activities. The access will be limited to selected signals needed for their activities and to some selected KPIs (Key Performance Indicators). Examples are speed, pressure, temperature, error lists, usage counters, and health indicators. Some signals can be also be used for production performance purpose. The signal access will also be limited depending on the level of service agreement with a Hägglunds Drives country unit.

OEMs have a need to follow the usage of their delivered fleet of machines. They need to have an overview of how the machines are utilized for future dimensioning and design. The data can also be used to examine if the machine has been used in proper way in a warranty process. The access will be limited to selected signals and KPIs depending on the level of service agreement with the Hägglunds Drives country unit.

Hägglunds Drives development is the owner of the data and KPI model calculations. All data are accessible within the development organisation.

Hägglunds Drives internal users are Country unit service stations, Country unit sales, Aftermarket development, System engineering and Quality department. Country unit service

stations need is to have a tool to get an overview of rising problems and system usage for planning of maintenance activities and troubleshooting within the country. They will have access to all measured signals and calculated KPIs. Country unit sales engineering have a need to follow the usage of the country unit fleet of delivered equipment. They need to have an overview of how the equipment is utilized for future dimensioning and design. The data can also be used to examine if the machine has been used in proper way during a warranty process. The aftermarket development's role is to improve the service station activities and to help in the troubleshooting process if needed. They need to have a tool to get an overview of problems and system usage for the troubleshooting help. They will have access to all measured signals and calculated KPIs. System engineering handles bigger installations. They need to have an overview of how the machines are utilized for future dimensioning and design. The quality department needs to use data to examine if the equipment has been used in proper way if a failure occurs during the warranty period. They will have access to selected signals and KPIs.

External development partners will have access to data and calculation limited to the need for their part of the work and according to the contract.

The knowledge and the models behind the KPIs are not accessible for end customers or OEMs, but can be needed to share working together with external development partners.

2.2.4. FE-Design

Described below are three possible access right scenarios for FE-Design: internal, with customer, and mix of involvement.

Internal scenario: The optimizations are all done in the engineering department of a single company. There can be multiple people working on one project. The work is organized by a team leader. Additional persons from other departments can be involved if needed (development, support or sales department)
By default everyone should be able to see his own optimizations, but gets restricted access with project defined limitations to everything conducted by his colleagues. (Thus, this is more like filter rules.) Team leaders have full access to be able to monitor and redistribute work.

With customer: In this scenario a customer is doing the optimization inside his own company. Help can be requested from the support or engineering department at FE-Design.
Data confidentially is critical in this case. When accessing optimizations running at the customers company, only the basic logging information should be visible for the support or engineering people at FE-Design (and sometimes even this will not be allowed!). If more information is needed to support a customer or to discuss some optimization progress/result, the access to the data streams must be requested. It will depend on the customers and the kind of their contracts to what of the following they allow access to:
(1) log files
(2) optimization monitoring data (optimization variables)
(3) the visualization data (screenshots or 3D intermediate results) or
(4) everything including the optimization setup, input files.

As soon as the collaboration gets finished or terminated access to the previous shared documents is no longer allowed or possible.

Mix of involvement: A mix of everything should be possible. So a large customer could have teams with limited access to their own data streams, and maybe only a team leader is allowed to grant access to the streams for external people (for example the support at FE-Design).

2.3. Access rights classification models – overview and criteria for selection

To save time and resources, we decided to use an existing access rights classification model and not develop our own. This sub-sections comprises an overview of concepts required to provide access control, different access rights classification models, criteria for selection and the model selected based on what rationale.

To provide access control, there are a couple of things that are required. Firstly, in order to authenticate a user or object – it needs to firstly identify itself and then prove that it is who it claims to be by for instance providing a password which then is validated. Depending on the strength of the credential provided, i.e. password, one-time password, password + certificate or biometric data etc. the level of authentication can be set in case a system has more than one such level due to holding open, internal or confidential information or resources. To provide access control, commonly information or system resources are classified according to an organizational classification standard combined with an on-a-need-to-know-basis. Using this classification, an authorization schema can be set up for users or objects that need to access information or system resources. Thus, access control requires a combination of authentication and authorization working together. Below, there are further descriptions of the concepts mentioned above as well as an overview of an access right classification models, such as XACML and SAML, together with which criteria that are will be used for the selection of such a model.

2.3.1. Authentication and Authorization

2.3.1.1. *Authentication*

Authentication does answer the question about who someone is. This is not restricted to humans only but includes also resources as for instance electronic documents. In case of a computer program authentication is managed by the provision of a password.

2.3.1.2. *Authorization*

Authorization is what someone is allowed to do. Hence, authorization follows an authentication, investigating if access to a given resource is allowed or not. In this sense authorization is the granting of specific rights.

2.3.2. Access Control Characteristics

Four characteristics of access control could be distinguished, that are *Attribute Based Access Control* (ABAC), *Discretionary Access Control* (DAC), *Mandatory Access Control* (MAC) and *Role Based Access Control* (RBAC). Since DAC and MAC are not further considered in this work just the rationales behind ABAC and RBAC will be described in more detail in the following sub sections.

2.3.2.1. *Attribute Based Access Control (ABAC)*

Attribute Based Access Control realizes access control not by evaluating access rights that are granted to a subject after its successful authentication, but on base of attributes that are assigned to the subject. Practically a subject (e.g. user) must fulfill several criteria's to get access to a protected resource. Such criteria's could be for instance that the user must be older than 20 years or the user must be a member of a specific organization. Generally the idea behind ABAC is to not define static properties, but make use of somehow more dynamic concepts grounding for granting access.

2.3.2.2. *Role Based Access Control (RBAC)*

Within organization the concept of roles are used for various tasks. For example roles to implement read only access, read and write access or access limited to specific documents.
Within a *Role Based Access Control* system each user is assigned to one or more roles. On base of assigned roles (and associated group belonging) the system denies or allow access to protected resources. Mostly RBAC is used in order to control read, write and execution permissions and hence is often applied in multi user systems.

Here, for instance the XACML provides three basic rules:

1. **Role Assignment:** a subject (e.g. person) must be member of a specific role in order to get access to a specific resource.
2. **Role Authorization:** the role (a subject is member of) must be authorized for the action to be taken on a specific subject. Together with rule 1 this rule ensures that a subject could be just member of roles it is authorized to be part of.
3. **Permission authorization:** a subject could enforce the permission to access a specific resource only if the permission for the active role is authorized. Together with rule 1 and 2 this rule ensures that a user could only access resources he is authorized to.

In conclusion it could be observed that RBAC is a specification of the ABAC approach. ABAC represents a more general view concerning access requested to a given resource by the evaluation of all attributes linked with the requesting user. While in contrary RBAC just evaluates only those attributes about a user role or group belonging.

2.3.3. Further specifications

Several frameworks for managing access control besides XACML exists, and another famous one for instance is the Security Assertion Markup Language (SAML)[2]. SAML is, as XACML likewise another XML based specification but managed by the OASIS group. An important aspect of SAML is that it provides several options to make statements about users that in terms of SAML are called assertions. Such Assertions hence are managed by the SAML system. Three distinct types of SAML assertion could be differentiated, that are[3]:

- Authentication: authentication by a particular means at a specified time of a subject
- Attribute: the subject associated attributes
- Authorization Decision: the decision if access to a specified resource is allowed or not

SAML likewise provides interfaces for usage with an XACML implementations, for instance an XACML policy could assert what a provider is allowed to do in case he receives an SAML assertion[4]. The Authentication and Authorization Service (JAAS)[5] is a third authentication and authorization implementation, hosted and developed at Oracle distributed as a module within the recent Java (J2SDK) distribution. Actually JAAS is a Java based implementation of PAM. PAM hence, is an acronym for Pluggable Authentication Module and has been originally developed at SUN as an authentication module for the SUN Solaris operation system. Currently, PAM is frequently applied within UNIX based operation systems.

2.3.4. Classification models, criteria for selection and selection of classification model

There are many different models for access rights, and as it was clear that an existing model should be used if possible. Furthermore, a solution was sought that could also help with other aspects dealing with rules and policies. The most important aspect here was the cross-organizational communication. A model that is easily communicable to another party should be preferred, to allow for better integration between partners. On the other hand the system should be as flexible as possible to allow other modes of use in the future.

[2] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
[3] http://saml.xml.org/assertions
[4] https://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf
[5] http://docs.oracle.com/javase/6/docs/technotes/guides/security/jaas/JAASRefGuide.html

XACML is the current de facto industry standard on access rights exchange which also contains a flexible process model. Competing formats like SAML usually include XACML bindings and recommend using it directly for advanced features [1].
Studies have shown XACML to be best suited for sophisticated access control both on the enterprise and the user level [2] compared to competing formats like SAML, XACL, P3P, APPEL, XPref, CPExchange, PRML, E-P3P, EPAL, DPAL, Geo-Priv and Rei.

2.4. The XACML classification model

The eXtensible Access Control Markup Language (XACML) is an XML based language to manage access control. The XACML standard defines a process model for the management of authorization requests, formalized through rules. Rules are parts of policies that have to be evaluated by the XACML system. By this approach, digital resources like websites, files or applications could be protected against unauthorized access. Preliminary, XACML provides an attribute based access control that uses attributes assigned to specific users, resources or actions. Even though role based access control could also be realized as a specification of an attribute based implementation approach.

2.4.1. XACML Components

An XACML compliant system consists of four modules as depicted in Figure 2. The following subsection describes the four parts of an XACML system in more detail.

2.4.2. Policy Administration Point (PAP)

The *Policy Administration Point* is the component of the access control system that is used to define and store access rules. As such a PAP could be e.g. a data base.

2.4.3. Policy Decision Point (PDP)

The *Policy Decision Point* is the central component of each XACML system. This component implements the decision whether access to a resource is allowed or not. PDP accepts queries from the *Policy Enforcement Component Point* and evaluates it against various rules. The result of this evaluation (*allowed, forbidden, not applicable, error*) is send back to the PEP, in addition the PDP could impose the PEP specific obligations to adhere. Such obligations could be for instance logging of allowed and not allowed resource access. In case a PDP does not have sufficient information in order to take a decision PDP could query the *Policy Information Point.*

2.4.4. Policy Enforcement Point (PEP)

The *Policy Enforcement Point* receives access requests for a specific resource for a specific user. This request is forward by PEP to the PDP. The PDP proves if the requested access is permitted or not. PEP, hence enforces the decision made by PDP.

2.4.5. Policy Information Point (PIP)

The *Policy Information Point* is only used in case that PDP should make a decision but do not have enough information to do so. In such a case PDP contact PIP that provides him the missing attributes from various information sources (e.g. databases or LDAP). This could for instance help if an access request contains only the subject, action and object but not the actual role. The role hence could be provided by PIP.

2.4.6. Component interplay

The four above described XACML system components are interlinked as partially described above. A further, more detailed description is given in the following list and Figure 2:

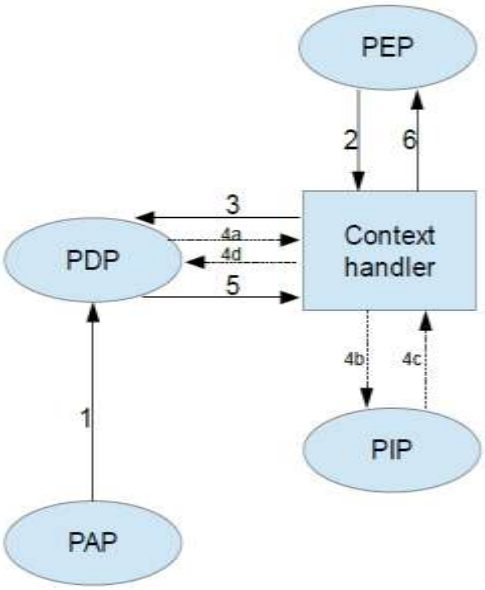

Figure 2: XACML component interplay

1. PAP creates policies or sets of policies and provides them for PDP usage
2. PEP forwarded the access request from the user to the context handler. The context handler is responsible for the conversion between various used formats to XACML specification.
3. The *Context Handler* creates an valid XACML request context sending it to PDP for evaluation
4. Steps 4a – d are optional. They are executed in case PDP does not have sufficient information available. In this case PDP the *Context Handler* queries PIP concerning missing attributes.
5. PDP sends decision (response context) to context handler.
6. Context handler converts response to format used by user and sends it back to PEP.

2.4.7. XACML Policy-Model

The following subsections describe the three elements of the XACML Policy Model.

2.4.7.1. *Rule*

A rule is a fine granular part of a policy for access control. A rule consists of the following parts:

- Target (application area)
- Effect (consequence)
- Condition (optional condition)

The value of *Effect*-attributes is either *Permit* (access allowed) or *Deny* (access denied). *Target* is used to test if a rule could answer specific queries or not. In case the rule is applicable the *Conditions* will be further evaluated.

2.4.7.2. *Policy*

A policy contains one or more rules. Hence, rules could not be evaluated directly but have to be part of a policy. Policies are restricted to a specified application area (*Target*). In contrast to *Targets* for rules, *Targets* for policies are mandatory. Furthermore *Rule-Combining-Algorithm-Identifier* und *Obligations* are part of a policy:

- The *Rule-Combining-Algorithm-Identifier* ensures in case that multiple rules exist (possible with contrary behavior) no error behavior results. Several algorithms exits,

like *Deny-Overrides* (a *Deny* rule is superordinate to a *Permit* rule), *Permit-Overrides, First-Applicable* (use first applicable rule) *or Only-One-Applicable*. If none of these algorithms is applicable the result is *NotApplicable*.

- *Obligations* are optional for a policy.

2.4.7.3. *PolicySet*

PolicySets are sets of Policies or sets of *PolicySets* itself. PolicySets uses a *Rule-Combining-Algorithm-Identifier* as well as optional *Obligations* as described above.

2.5. XACML implementations

Some XACML implementations exists, in order to give a brief overview about such existing software solutions the Projects OpenAM [3] and HERAS^{AF} [4] will be introduced in this subsection.

OpenAM

The OpenAM implementation is the successor of SUNs Open Web Single Sign-On project (OpenSSO). Since Oracle acquired SUN, the OpenSSO project has not been further developed. Existing software modules are recently further implemented within the OpenAM project. Actually, OpenAM offers the four core functionalities [5]: Authentication, Authorization, Single Sign-On and Federated Identity. The authentication module is used for user to system login (assessment who the user is). The authorization module in turn affects after the successful authentication procedure and checks if the user has valid access rights to a given resource. The Single Sign-On module provides the ability to login once with authentication of that user for all accessible interlinked resources as for instances local computers or services. Federated Identity or Cross Domain Single Sign-On extends Single Sign-On implementation by the ability to work even in use cases where user and application resides in different domains (for instance on two sides of a firewall).

The XACML components specified in section 2.4.1 could be mapped to OpenAM as follows:

- PAP: by offering services to define, store and manage policies
- PDP: by evaluation of policies and its enforcement
- PIP: by provision of further information required for complete decision about granting resource access
- PEP: OpenAM Policy Agents serves as PEP (receiving decisions from PDPs and secure resources)

A direct depiction from OpenAM- to XACML-Components is as follows:

- PDP to OpenAM Policy Evaluation Engine
- PIP to OpenAM Identity Store
- PEP to OpenAM Agent
- PAP to OpenAM Admin Console

HERAS^{AF}

HERAS^{AF} is developed and hosted at the University of Applied Sciences, Rapperswil, Switzerland. HERAS^{AF} was founded in 2005 and is an Open Source project since 2006. Mainly three main objectives are part of the implementation [4]

1. Offer an XACML implementation, to be maintained and extended
2. Publication of best practices, trends, know-how and experiences concerning the software engineering
3. To make research within the area of application security. Actually, the HERAS^{AF} implementation is a comprehensive reference implementation of the XACML 2.0 specification.

2.6. Selection approach for classification model implementation and justification

From the number of XACML implementations made available on the market three have been taken in account to provide the best base solution, to build the SmartVortex specific requirements on top of it.

a) **Axiomatics**: The Axiomatics implementation was excluded due to licensing and legal/IP problems that could not be solved by the consortium
b) **OpenAM**: The recent version of OpenAM provides wide user interface functionality for users that are not used to work in programming languages. Even if the libraries of OpenAM could be used the implementation generates limitations to be stuck in the functionality of the user interface provided by OpenAM. Additionally lacks in user support based on the fact that SUN has terminated all development activities on the current console in version 10. Nevertheless the libraries are useful, well documented and can be considered as base for an own grown solution
c) **HERA^{AF}**: The HERA^{AF} supports the research and development activities strongly and provides a good documentation as well as a backing development team at the university of Rapperswil. The solution is code based which makes it easier to add additional functionality on top of the existing one. Authentication is a missing functionality but if such functionality is required while the documents are fully stored in systems that have their own authentic solution is currently under investigation. Dashboard that is the central user interface for all activities requires an authentication solution which exists in all of the partners IT environment based on LDAP technology. This might be a possible base to fill the missing gap in HERA^{AF} and to extend this system with the requirements for the social policies and the semantic driven access rights.

Due to the facts above, we do not yet want to make a final recommendation or take a decision based on the given requirements. The research and development teams will conduct additional tests using the two existing test installations, i.e. OpenAM and HERA^{AF}, to decide what to use during the implementation of the D11.2 deliverable due M36.

3 SMART VORTEX RULES AND POLICY FRAMEWORK IN RELATION TO THE TIERED ARCHITECTURE

In Figure 2, the main rules and policy framework software components are presented. In Figure 3, all SmartVortex software components that need an authentication/authorization decision prior executing a request will send a request to the PEP in Figure 2.

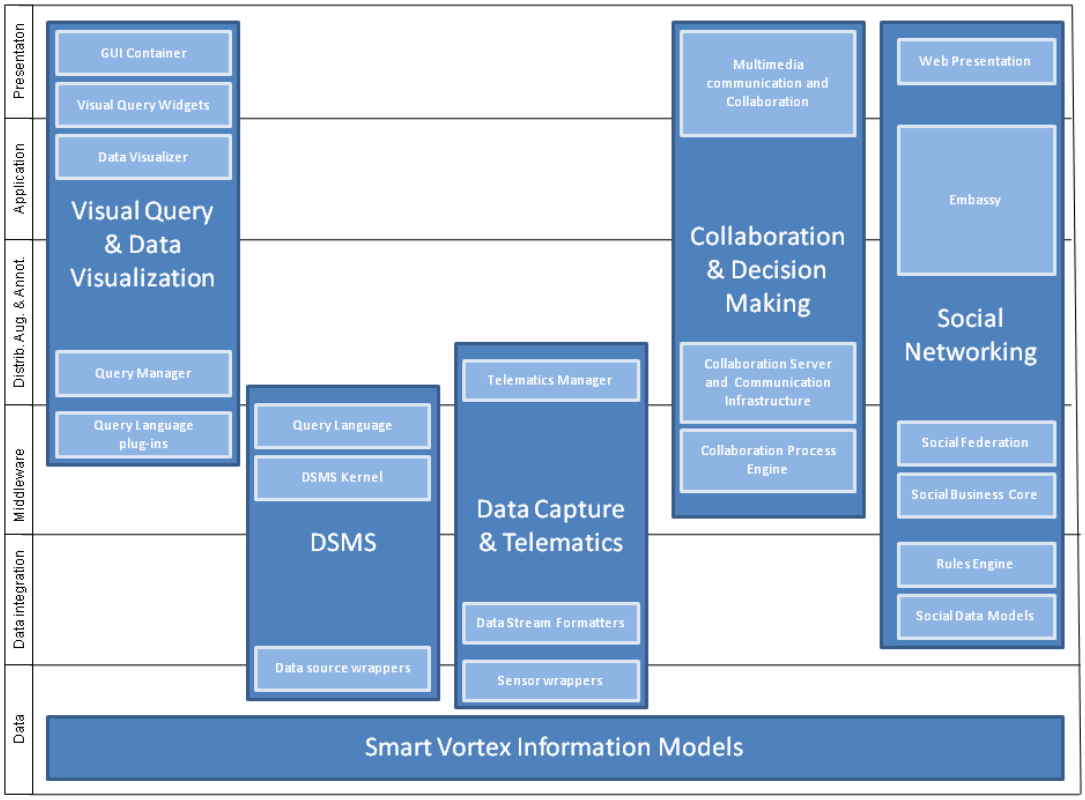

Figure 3: The main functional components of the SmartVortex suite.

On the right you can see the social networking components of which the social business core (SBC) is the most important. The SBC coordinates the creation, management and destruction of social constructs and the membership of other agents. Cross-organizational aspects are handled by the Social Federation Module, which annotates data by the SBC according to the rules of the federation.

The Embassy is the main router for handling requests within the system. As connections between organizations is seen as social in nature, it is counted as part of the social networking components, but it can be used by any part of the system to send requests to other parties.

1.1. Architectural dependencies

The architectural dependencies for each of the main SmartVortex software components are briefly described in this sub-section.

Any time-outs, i.e. if a user is connected longer than a certain duration of time, are described in the respective components following.

1.1.1. Known limitations

There are different options for how to device the architecture for the rules and policy implementation. One way would be to make all authentication/authorization requests via a

graphical user interface and its underlying code, but that opens up security issues in terms of possibilities to bypass. Another worst case scenario opened up is also that the developers forget to add the request, and consequently no authentication/authorization request is made prior using a components and accessing any data streams etc. via that component. Thus, to avoid the above, each component needs to call the rules and policy implementation when necessary.

1.1.2. Social/collaboration

The collaboration suite is part of the Smart vortex suite, as collaboration components interact with components that handle data streams of equipment, for example. The collaboration suite is a software platform that supports real-time collaboration across a multi-organization environment. The platform supports its users through many types of (synchronous) collaboration components, such as: video-conferencing, discussion and data analysers.
The social collaboration component supports these components by providing expert finding functionalities. Through this component, a group can search and invite experts according to their skills and expertise.

The core of the social collaboration suite is used for routing requests between organizations. This can be used by other components of the SMART VORTEX suite. For this mechanism to work, the partners need to specify whether the data needs to be mapped between instances.

Synchronous collaboration services and access control

Initiation of synchronous collaboration session is typically done by the Session Initiation Protocol (SIP). When access control is required (e.g. inter-organizational collaborative work), access control based on a challenge/response security mechanisms is supported in the SIP INVITE process. The SIP-based authentication / authorization can be regarded as a PEP in the XACML based access control architecture. The PDP will be in the SIP proxy server.

In the overall framework, a mapping will be necessary from the credentials used to identify a Smart Vortex user to a SIP address used in the set-up of synchronous sessions. This could for instance be done in an LDAP directory service, or, more generally, be represented in the collaboration ontology. The SIP proxy servers must be able to access the credentials of all Smart Vortex users that be allowed to set up a (secure) collaboration session.

1.1.3. Data capture and telematics

The data capture and telematics subsystem of the Smart Vortex architecture is where data from sensors in industrial equipment enters into the Smart Vortex system. Since the data can be sensitive, access control must be applied, securing who can access the captured data and ensuring that illicit data is not maliciously injected into the system. Since data capture devices can be in customer premises equipment outside of physical control from the operator of the Smart Vortex system, the access control mechanisms must be capable of revoking access previously granted to a particular device, in case for instance a data capture device is found to be subverted or stolen. Such access restrictions could be accomplished by using certificates that are installed on the data capture devices, and certificate management framework whereby revocations of certificated can be handled.

1.1.4. FDSMS – Federated Data Stream Management System

A central component in the Smart Vortex project is the distributed Federated Data Stream Management System (FDSMS), which processes queries and computations over data streaming from equipment and other stream data sources and produces data streams sent to other Smart Vortex components. A data stream can be seen as a continuously growing sequence of tuples or events. An event can be a sensor reading or some action by a human operator. The result of processing a query over streams (a continuous query, CQ) is also one

or several *derived* streams of tuples. The FDSMS engine furthermore contains a local semantic database where data is stored that is continuously matched against incoming streams queried by CQs.

For example, sensors deployed in vehicles generate data regarding environment and vehicle status (e.g. engine temperature) that can be accessed by CQs through the FDSMS from a manufacturer or a service provider. Having access to such streaming data often includes the wish to analyse the data in order to generate new knowledge. The result of such an analysis, which even can be executed in real-time, could be used to inform other actors about identified complex event and trigger further actions.

Both incoming and outgoing data streams need some access control mechanisms to prevent illegal access to data. Also the local data stored inside the FDSMS engine needs access control. A particular issue is that the processing of CQs over streams often requires very high performance in order to keep up with the stream flow and to execute more or less costly algorithms on streaming data. For high performance the semantic database built into the FDSMS is therefore stored in main memory. The semantic database can periodically be saved on disk for backup purposes.

The requirement for high performance over massive data streams also becomes an issue when handling access control mechanisms. Since access control will involve accessing the SmartVortex rules and access policy framework (where rules and policies are stored), the communication time for this becomes an issue. There are two alternatives for handling access control:

1. If access control rules concern access to an entire stream, the communication performance with an authorization server is less on an issue. Essentially there is an added delay to contact an authorization server only when a CQ is started. Since a CQ runs for a long period of time this delay will be insignificant. This is chosen as the initial approach to access control for the FDSMS in Smart Vortex because of its simplicity.
2. However, CQs in Smart Vortex usually add meta-data as semantic annotations being parts events in derived streams. Such annotations can also describe access policies which have to be observed and enforced by a policy engine. Because of this, Smart Vortex requires more fine grained access control mechanisms than entire data streams. One would like to have semantic rules that are continuously matched against individual incoming tuples (events). It will then be infeasible to access an access control server for every event. Therefore a mechanism will have to be developed where semantic rules are converted from the access control server to the local database, e.g. when a CQ is started. After that the performance of the semantic access control rules will be sufficient for matches against individual tuples. Depending on application requirements in SmartVortex this approach will also be investigated.

1.1.5. PLM-systems, persistent databases external database sources

PLM systems and DMBSs have their own frameworks for access control (i.e. authentication and authorization). For example, many modern relational databases' authorization mechanisms are based on a very rich set of roles. For the integration in the SmartVortex rule and policy framework, the access control including authorization is not the problem that needs to be solved. The main protection mechanisms need to be integrated in the collaboration suite along questions alike "can this document be shared during a collaboration with all or a selected limited group of participants?". Another question is if "is there a need for a filtering mechanism related to some members that would get information out of e.g. a CAD model or drawing and if they should have access to all information in the document, such as tolerances, dimensioning, simulation model parameters or data stream sensor parameters or mathematical functions embedded in the meta data of the sensors as well as controlling the used formats

while sharing document like PDF vs. Word file extensions?". SmartVortex will add this level of sharing authorization in its rule and policy framework.

1.1.6. Visualization

Exploiting data streams of product service systems and the generation of complex events is useless if it is not possible to explore the identified complex events. The visualization of detected complex events and their provenance enable to gain further knowledge that support human decisions in collaboration processes. Monitoring complex events in real time is required.

From the access control point of view, the Visual Query Widget executes using the log-in identity of the user currently interacting with it, and restrictions on data required by the visually generated query are checked by the underlying policy framework. Additionally a definable time-out function in the dashboard prevents unauthorized use of the application if the dashboard is used on mobile devices where loss or loan can be an issue. As an example, if creating a query the user requires access to a data stream source which she is not allowed to access, this would result in an empty visualization output. The same is true for event visualizations, etc. Conversely, the Data Visualizer component shows whatever it receives back from the underlying components, as it assumes by-design that data items to be visualized have been filtered by the underlying layers before returning to it.

4 RULES AND POLICY FRAMEWORK

The work on the Rules and Policy Framework will continue during year 3, and be presented as part of the D11.2 deliverable. Below are initial decisions on how user access rights and the acquisition platform are/will be implemented and used.

.

4.1. User access rights

The authorisation of policies within the social semantic suite will be integrated with the XACML implementation to be discussed in D11.2. This way all services using the system described in [6] will be able to use the XACML subsystem with no further adaptation required, if the policies are described in XACML.

4.2. Acquisition platform - how to enter rules/policies related to users and artefacts

Currently there is no acquisition platform for rules and policies that is specific to SmartVortex. This is currently worked on and a first version will be shown in year 3. For now, the OpenAM console for version 9 is being used.

5 SUMMARY AND CONCLUSIONS

The basis for the rules and policy framework design are the existing SmartVortex requirement engineering deliverables D1.1 and D1.2, additional input from the industrial partners as well as a survey based on the JISC-model for project management responsibilities with adoptions by our industrial partners.

The SmartVortex project will base its rules and policy framework implementation on extended XACML technology, to get such a flexible and agile implementation as possible. The selection of which implementation to use will be made until M36.

For performance reasons, the rule and policy engine will be implemented as a service, which can be called from several applications/components within the SmartVortex tool suite.

The existent authorization systems used in the pilots' technical IT environment remain unchanged and will work with the SmartVortex authorization framework in a synergetic manner. There is no plan to substitute those existing systems, especially as the migration and sourcing cost combined with possible transfer failures would never justify the change or substitution.

APPENDIX 1: ROLES AND RESPOSIBILITIES

Title	Role
Project Manager	The person responsible for developing, in conjunction with the Project Sponsor, a definition of the project. The Project Manager then ensures that the project is delivered on time, to budget and to the required quality standard (within agreed specifications). He/she ensures the project is effectively resourced and manages relationships with a wide range of groups (including all project contributors). The Project Manager is also responsible for managing the work of consultants, allocating and utilising resources in an efficient manner and maintaining a co-operative, motivated and successful team.
Responsibilities	
• Managing and leading the project team. • Recruiting project staff and consultants. • Managing co-ordination of the partners and working groups engaged in project work. • Detailed project planning and control including: • Developing and maintaining a detailed project plan. • Managing project deliverables in line with the project plan. • Recording and managing project issues and escalating where necessary. • Resolving cross-functional issues at project level. • Managing project scope and change control and escalating issues where necessary. • Monitoring project progress and performance. • Providing status reports to the project sponsor. • Managing project training within the defined budget. • Liaison with, and updates progress to, project steering board/senior management. • Managing project evaluation and dissemination activities. • Managing consultancy input within the defined budget. • Final approval of the design specification. • Working closely with users to ensure the project meets business needs. • Definition and management of the User Acceptance Testing programme. • Identifying user training needs and devising and managing user training programmes.	

Title	Role
Project Sponsor	The person who commissions others to deliver the project and champions the cause throughout the project. They will normally be a senior member of staff with a relevant area of responsibility that will be affected by the outcome of the project. They are involved from the start of the project, including defining the project in conjunction with the Project Manager. Once the project has been launched they should ensure that it is actively reviewed. The Project Sponsor is usually the one who has to negotiate a path through the tricky diplomatic areas of the project!

Responsibilities	
• Acts as champion of the project. • Is accountable for the delivery of planned benefits associated with the project. • Ensures resolution of issues escalated by the Project Manager or the Project Board. • Sponsors the communications programme; communicates the programme's goals to the organization as a whole. • Makes key organisation/commercial decisions for the project. • Assures availability of essential project resources. • Approves the budget and decides tolerances. • Leads the Project Steering Board. • Ultimate authority and responsibility for the project.	

Title	Role
Steering Group/Board	This group, normally containing management grade personnel, is responsible for overseeing the progress of the project and reacting to any strategic problems. The group is optional, as the Sponsor-Manager relationship may be seen as the best means of control, but is usually required in large projects which cross functional boundaries.
Responsibilities	
• Championing the project and raising awareness at senior level. • Approving strategies, implementation plan, project scope and milestones. • Resolving strategic and policy issues. • Driving and managing change through the organization. • Prioritizing project goals with other on-going projects. • Communicating with other key organizational representatives.	

Senior Consultant or Supplier-side Project Manager	The person responsible for managing supplier-side input to the project.
Responsibilities	
• Ensures that mandatory supplier requirements are met. • Manages the production and approval of the supplier side of the budget. • Makes effective use of supplier resources within the approved budget. • Tracks performance of consultants and takes appropriate action. • Proactively develops a collaborative relationship with the organisation to Project Steering Board level. • Ensures that there are clear communication paths within the project team and the organisation and supplier. • Acts as main point of contact between the supplier and the organisation. • Produces and monitors financial reports including entry and maintenance of all actual time and	

expense against the master plan.
- Day to day management of supplier staff assigned to the project.
- Quality Assures the work of supplier staff assigned to the project.
- Encourages the transfer of product knowledge and skills to the appropriate staff within the organisation.

.

Title	Role
Project Team Members	The staff who actively work on the project, at some stage, during the lifetime of the project. Some may have a specific role – for example, the Team might include a Project Administrator (see below).

Responsibilities

Team member roles will vary depending on the type of project. Typically they might be to:

- Provide functional expertise in an administrative process
- Work with users to ensure the project meets business needs
- Documentation and analysis of current and future processes/systems
- Identification and mapping of information needs
- Defining requirements for reporting and interfacing
- User training

Title	Role
Project Administrator or Co-ordinator	Responsible for maintenance of the project plan, maintenance and updating of a project website (if appropriate). Provides administrative support to the Project Manager.

Responsibilities

- Sets up and manages support functions covering planning, tracking, reporting, quality management and internal communication.
- Produces consolidated reporting to the Project Steering Board, including milestone summary, key issues, risks, benefits, summary of costs incurred.
- Establishes standards, tools and procedures for use on the project, including Issue, Risk, Change and Information Management.
- Manages the Project Library.
- Reviews project activities for compliance with procedures and standards.
- Manages the support and provision of project tools and equipment.
- Manages data security, software and license control.
- Assists with the production of user documentation.
- Assists with testing.

Title	Role

Systems Developer	To work with the Project Manager on defining and executing development requirements.
Responsibilities	
• Working with the Project Manager on definition of development requirements and priorities. • Data Migration. • Interfaces with other systems. • Reporting configuration and deployment. • Set up and maintenance of security rights and access permissions. • Contributing to technical strategy, policy and procedure. • Development and operation of technical testing programmes. • Production of technical documentation to agreed quality standards. • Reporting on progress/issues to management and users.	

Title	Role
System Service Manager	Supervising Service Members and defining repair and maintenance requirements.
Responsibilities	
• Working with the Service Manager on definition of preventive maintenance requirements and priorities. • Repair activities of defect systems and parts • Scheduling and planning of preventive or established maintenance activities • Maintenance activities preventive and adhoc • Reporting about service activities • Feedback to R&D departments and Project management • Set up and maintenance of security rights and access permissions for the service organization • Contributing to technical strategy, policy and procedure. • Execution of technical testing programs onsite. • Review and test of applicability of technical documentation. • Reporting on problems and issues to management and users.	

Title	Role
System Service Member	To work with the Service Manager on defining and executing repair and maintenance requirements.
Responsibilities	
• Working with the Service Manager on planning of preventive maintenance requirements and priorities. • Repair activities of systems defects and exchange parts • Preparation and execution of preventive or established maintenance activities • Maintenance activities preventive and adhoc	

- Reporting about operative service activities, time, parts, remaining problem areas
- Feedback to R&D departments and Service management
- Contributing to technical strategy, policy and procedure.
- Execution of technical testing programs onsite.
- Feedback of applicability of technical documentation.
- Reporting on problems and issues to service management and users
- Feedback about user satisfaction

Title	Role
System Administrator	Management and support of the IT system environments
Responsibilities	

- Management and support of the various environments.
- Network operating systems management and support.
- Database management and support.
- Back-up and disaster recovery measures.
- Contributing to technical strategy, policy and procedure.
- Development and operation of technical testing programs.
- Production of technical documentation to agreed quality standards.

Title	Role
Observation and Monitoring Centre Member	Surveillance of System Behaviour using Data Streams generated by calculations of the DSMS
Responsibilities	

- Surveillance of performance and well-being of the monitored systems
- Analysis of calculated trends and cumulative values against given thresholds
- Immediate reaction if threshold are violated
- Information and reporting generation to the service and commercial management
- Back-up and disaster recovery initiation .
- Fine grain watch on risky data stream items
- Definition of queries to focus the data stream engine on problem areas
- Generate statistics about fleet or system behaviour
- Control and monitor machinery usage against given contractual conditions
- Initiate collaboration and decision processes with service, R&D or controlling if required

Title	Role
Programme Manager	This role is relevant if there are several related projects.
Responsibilities	

- Overall management and co-ordination of the program of projects.

- Contributing to strategy, policy and procedure.
- Management of supplier/contractual relationships.
- Budgetary control of the program of projects.
- Monitoring of, and responding to, issues at the program level.

Title	Role
External Partner R&D	This role is relevant if there the company collaborates with external partners in R&D or manufacturing projects (outsourcing case).
Responsibilities	
• Development and design of subparts or parts of the entire system. • Service operations on behalf of the product vendor • Management of supplier/OEM/contractual relationships. • Budgetary control of the subprojects. • Monitoring of, and responding to, issues at the subprogram level. • Quality control of the subparts • Collaboration with the OEM to meat time lines and development goals	

Title	Role
Customer (service and user)	The customer is the user of the delivered system and might have local maintenance, surveillance failure inspection and repair obligations
Responsibilities vs. the vendor	
• Reporting of bugs and failures to the vendor • Initial test and inspection activities • Acceptance tests • Requirement and improvement proposer • Monitoring of the wellbeing behaviour of the system • Active participation in the planning process of preventive maintenance • Stocking repair elements and parts for immediate use • Executing required and/or contractual agreed maintenance inspections/activities	

APPENDIX 2: ACCESS REQUIRED TO

In the survey the following questionnaire has been attached on each project role with the following items that might have access control during the DSDM and combined collaboration system:

Access required to	No Access	All Read Access	Selective Read Access*	Read and Write	Ability to Lock files
• System history tracks (recorded data streams) • Sensor definition data • Meta data that operate on the sensors • Formulas that calculate the derived sensor streams • Stream query editor • Collaboration invitation • Collaboration participation • Project deliverables in line with the project plan. • Project progress, status and performance reports • Project problem reports • Cost calculation related to the project • Project member definition • Change requests documentation related to the project. • Training Material • Marketing material for promotion and dissemination activities. • Consultancy input if involved and related to the project • Design specification. • Design documents • Maintenance and repair documentation • Skill and responsibility information within the project frame • Documents describing the User Acceptance Testing program.					

*	In the row marked with selective read access conditional rules should be marked and explained in detail in separate referencing footnotes

REFERENCES

[1] OASIS, “Assertions and Protocols for the OASIS Security Assertion Mark-up Language (SAML) V2.0”, March 2005

[2] Kumaraguru et al., “A Survey of Privacy Policy Languages”, Workshop on Usable IT Security Management (USM 07). In SOUPS ‘07

[3] OpenAM, http://openam.forgerock.org/, visited 2012.09.24

[4] HERAS^{AF}, http://www.herasaf.org/, visited 2012.09.24

[5] OpenAM Product Sheet, http://www.forgerock.com/sites/default/files/file/ProductSheet-OpenAM-A4.pdf visited 2012.09.24

[6] J. Grabarske, “Use cases and security requirements for data exchange between corporate social networks,” master thesis, Fernuniversität Hagen, April 2011.