Process-Oriented Approach for Role-Finding to Implement Role-Based Security Administration in a Large Industrial Organization

Haio Roeckle
Dr. H. Roeckle IT-Sicherheit GmbH

Universitaetsstr. 142
D-44795 Bochum, Germany
0049 – 234 – 971 979 0
roeckle@roeckle.de

Gerhard Schimpf
Schumann
Unternehmensberatung AG
Hermann-Heinrich-Gossen-Str. 3
D-50858 Koeln, Germany
0049 – 2234 – 108 1263
Gerhard.Schimpf@schumann-ag.de

Rupert Weidinger
Siemens AG Information and
Communication Networks
Hofmannstr. 51
D-81379 Muenchen, Germany
0049 – 89 – 722 41018
Rupert.Weidinger@icn.siemens.de

ABSTRACT

In this paper we describe the work in progress with a process-oriented approach for role-finding to implement Role-Based Security Administration. Our results stem from using a recently proposed role model and procedural model at Siemens AG ICN, a large industrial organization.

The core of this paper presents the data model, which integrates business processes, role based security administration and access control. Moreover, a structured top-down approach is outlined which is the basis for derivation of suitable business roles from enterprise process models.

A brief description is given on how these results may be used to first build the Role Catalog and then support the implementation of RBAC and a single point of administration and control, using a cross-platform administration tool.

Keywords

Access Control, Authorizations, Business Processes, Enterprise Process Modeling, Heterogeneous Systems, Role Based Access Control, Security Administration, Security Data Models, Security Management, Security Models, Single Point of Administration and Control

Computing Review Classification

D.4.6, H.2.0, K.6.5

RBAC 2000, Berlin, Germany
© ACM 2000 1-58113-259-x/00/07 ...$5.00

1. INTRODUCTION

In recent years the research on Role-Based Access Control (RBAC) provided consistent and well-defined data models for representation, administration and activation of roles ([Bar], [FCK], [JGIL], [San], [SCFY]). However, little research was done on practical ways of finding business roles ([JGIL], [ES]), particularly to implement cross-platform Role-Based Security Administration. The previously published concepts of role engineering suggest ways to design roles manually ([ES], [TBB]) or in single environments ([FH]). In real life there is a need to find roles for cross-platform administration ideally automated, using existing organizational information in the company.

From a practical point of view we propose the concept of role-finding in diverse environments based on process-oriented approaches ([Roe]). For a contribution to this discussion, this paper provides a case study and reports on work in process concerning the role-finding activities at Siemens AG Information and Communication Networks (ICN). The concept of role finding is related to role engineering addressing the business needs of designing cross-platform roles. More details on the presented approach will be published in a forthcoming paper by Roeckle et al.

To solve typical problems of security administration in such a diverse environment, Siemens ICN initiated a number of strategic and innovative projects. One project investigated the suitability of the Role-Based Security Administration concept combined with a single point of administration and control. This concept was also required to be integrated into an overall trusted network architecture.

The integration of the project into the trusted network concept and the design of a single point of administration appeared to be straightforward. The identification of the roles, however, turned out to be a highly complex and non-trivial issue. To find business roles for cross-platform authorization the project team needed both, a sound knowledge about the administration of the included platforms and detailed knowledge of business processes for the organizational units. A formal role-finding procedure had to be defined, which could be extended from the pilot organization outward to the whole company. This procedure had to include role descriptions, initial role-finding, implementing of roles and changing of roles. The approach for role-finding chosen by Siemens ICN was the process-oriented approach from [Roe] adapted to their particular environment and requirements.

The remainder of this paper is organized as follows: Section 2 describes the initial situation and goals of the project. Section 3 describes the project outline. Section 4 provides an introduction to the abstract approach for process-oriented role-finding presented for the first time in literature. Section 5 reports on the implementation of the roles. Section 6 reports on the gained experiences at Siemens ICN with the tools "RoleFinder" for process-oriented role-finding and "SAM" resp. "SAM/RM" for Role-Based Security Administration ([RoFi], [SAM], [SRM]). The paper concludes with suggestions for scientific work on the subject of role-finding.

2. Business and IT-Security Background

2.1 Company Profile

Siemens Information and Communication Networks (ICN), a worldwide supplier for telecommunication products, is the leader in many major telecommunication sectors. It provides sales, services and solutions for more than 600.000 customers in over 160 countries.

The convergence of voice and data, as well as operating in the global market, presents many business challenges. Solutions provided by Siemens ICN help to protect customers' investments in traditional telecommunication products. Siemens ICN employs 60.000 people of which 15.000 engineers work in R&D with an annual budget of 2 billion Euro ([Mah]).

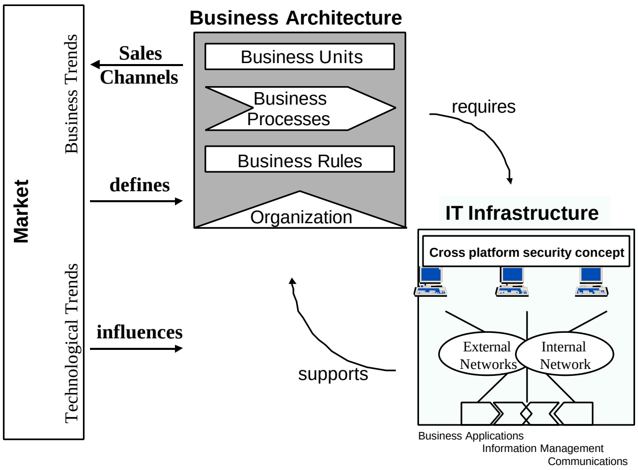

Figure 1 : IT supports Business

As seen in Figure 1 Siemens ICN is both a customer oriented and business driven company. Market forces require frequent realignment of business units and business processes. Business induced strategic partnerships, mergers and acquisitions and open communication with business partners result in a highly diverse user population on the IT systems of Siemens ICN.

Corporate management has initiated a number of so called "Roadmap Projects". The objectives of these are explicitly stated and comprise keeping pace with technology and restructure IT-services for a comprehensive coverage of all business processes. An explicit objective is "protection of corporate knowledge and support of a knowledge based enterprise".

It is obvious that IT security plays a major role in such an environment where knowledge is an asset which makes a difference in a competitive world. For this reason the Roadmap Project "Trusted Information Processing" was defined to realize the vision of "Trusted Network".

2.2 Trusted Network Projects

The vision of a trusted net at Siemens ICN covers all aspects for fast secure and binding information processing. The basis for a trusted net is given by a Public Key Infrastructure (PKI), which enables a unique process of identification and authentication, confidentiality and binding information processing. Single Sign On (SSO) is another component of the vision; it provides the authorization to use assigned applications after single authentication.

The issue of access control is examined in parallel to the already named components. It is assumed that Role-Based Access Control (RBAC) will provide a feasible solution for the ICN computing environment. Examples have been published by [Fly], [HDLG]. In addition, for the network infrastructure, parallel projects exist within the ICN Roadmap Projects. These projects will be driven by network engineers.

3. The RBAC-Project

The starting point for this project was the analysis of administrative procedures of access rights, in comparison to the vision of a trusted net, briefly introduced in the previous chapter. Like many large organizations, Siemens ICN has a wide range of diverse platforms and applications installed to serve its 60,000 end users. Both platforms and user population have grown over time in size and diversity with the evolution of business and information technology. Some of the applications serve global requirements, others support only local services. Just a few years ago, networking was restricted to support only local regions. Now, cross border electronic transactions must be processed without regard to geographic constraints. Mobile net-computing and integration of world-wide business partners have further increased IT complexity.

The focus of a trusted net is to keep net-computing secure, manageable and efficient, despite its complexity. This implies, that a controlled resource management with a single user and authorization administration must be implemented. It should always be possible (in shortest time) to have an overview about the current situation of assigned authorizations to specific users in all systems.

To make the authorization model manageable, the process for assigning and revoking authorizations should be easy, well defined and fast. Information technologies supports primarily business architecture, not the user community. To emphasize this important fact and to make it transparent, assigned authorizations should be derived from the business processes. Not that the user should select necessary resources for his work, his job function defines the needed authorizations; all should be predefined.

These objectives led to investigate cross-platform security administration and the feasibility of RBAC models in this dynamic environment of Siemens ICN.

3.1 Current Administration of Access Rights

The problems and needs to improve the administration in developed environments have already been described by [FBK] and [SMF]. The descriptions in these papers correspond to the situation at ICN, where the assignment of permissions to users takes place through established approval processes on a per platform basis. Access rights are directly associated with individual users. This method results in significant administrative cost and complexity. Additionally, it is often error prone and usually not up to date, because separate security administrators are being employed for each type of security system. They are required for maintaining, coordinating and tracking access rights on each of the involved computing platforms (e.g. through access control lists). Security audits need to be performed (if at all) in an isolated fashion. Each platform has its own reporting tools (some homegrown). The production of consolidated user access pattern reports is next to impossible.

The current ICN security policy is available only in paper form. The criteria concerning access rights for new or transferred users, and the deletion of users were all formulated for particular hardware platforms. Due to the absence of automated tool support, the quality of adherence is dependent on the skills and work load of the administrators. As a result of this manual control, long-term users might (through changing work assignments) accumulate access rights, and in some cases accounts, which they no longer need. This potential violation of the "need to know" policy requires tighter control, decreases the level of security and leads to a low level of security awareness when handling sensitive data.

3.2 Objectives for Future Administration

In the first phase of this RBAC project, objectives for enhanced security administration were defined:

- Integration with the technology employed by other Roadmap Projects. The major influence comes from the “Directory Information for a Global Organization” (DINGO) where a centralized repository for all attributes pertaining to users is maintained. DINGO is being considered as the guiding tool to supply user specific information
- Users should be administered from one place in the enterprise even if they have access rights on more than one system platform. The overall principle of Single Point of Control and Administration has to be realized
- Access rights are assigned according to job functions. No personal or “negotiated” rights shall be assigned
- For these job functions appropriate roles need to be defined. Roles should be robust enough to be stable against business restructuring. A comprehensive role catalog for the enterprise should be developed
- Cross-platform administration using roles is required to make sure that access rights given to a person are consistently withdrawn if a user changes a job assignment or leaves the company
- Wherever possible the burden of administration should be reduced ,e.g. through automated handling of bulk data
- Future administrative procedures, including the involved tools, should support the concept of least privilege. Here users receive the minimum set of access rights through roles needed to perform their work.

3.3 Future Administration Architecture

Figure 2 shown below gives a schematic diagram on the future security administration architecture:

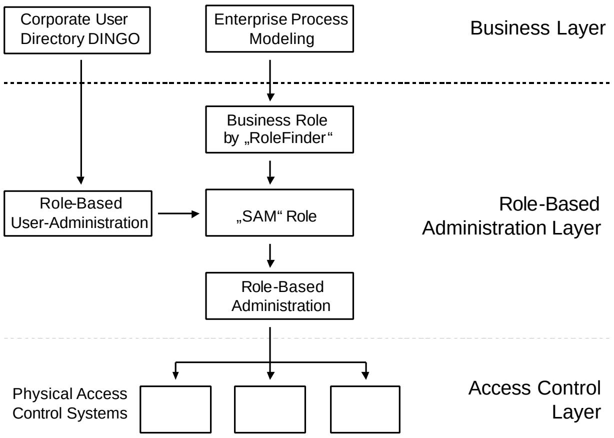
Corporate User Directory DINGO
Enterprise Process Modeling
Business Layer
Business Role by „RoleFinder“
Role-Based User-Administration
„SAM“ Role
Role-Based Administration Layer
Role-Based Administration
Physical Access Control Systems
Access Control Layer

Figure 2: Top down approach for Role-Based Security Administration

The planned architecture integrates 3 layers. The top layer is the business layer providing guidance through strategic business processes to the subordinate IT-infrastructure. In this context, DINGO represents the entire user population and the IT-infrastructure is conceived to be business-enabler.

The middle layer represents the IT security administration infrastructure from tool-based role-finding to role-based user administration. Roles are derived in a top down fashion from business processes and attributes in DINGO. They are maintained in a role catalog and implemented in a tool capable to perform Role-Based Security Administration. Control information representing access rights of users on one or several target systems are stored on this meta level. From this point forward, access control systems are automatically administered.

The bottom layer is the access control layer where physical access control takes place.

The layered architecture provides well-defined interfaces between the different administrative tasks and enables the use of tools implementing the tasks pertaining to each layer.

3.4 Deploying RBAC

In respect of this diverse landscape, implementing role-based access control is a complex task. Therefore, this project was divided into several implementation phases according to the architecture shown above. Some of the most important phases are:

- Role Catalog (requirements, role-finding process, examples)
- Processes (assigning roles, changing roles)
- Pilot (technical design, infrastructure, test)

The tasks of role-finding and role-implementing can be supported by tools which are commercially available. These tools must be deployed and their interfaces customized so they work together. The procedures of role-finding and role-implementing are described in the next two sections. The remainder of this section describes how roles are structured and integrated into the enterprise context at Siemens ICN.

In an industrial company, there are obvious roles like salesman, developer, buyer etc.; quite similar to the roles in RBAC literature. However, these roles do not address all of the requirements. For instance, there are a few authorizations that do not belong to functional roles. In addition obvious roles may lack granularity. To overcome the first problem Siemens ICN has agreed on a few non-functional role-classes to be introduced to the RBAC concept.

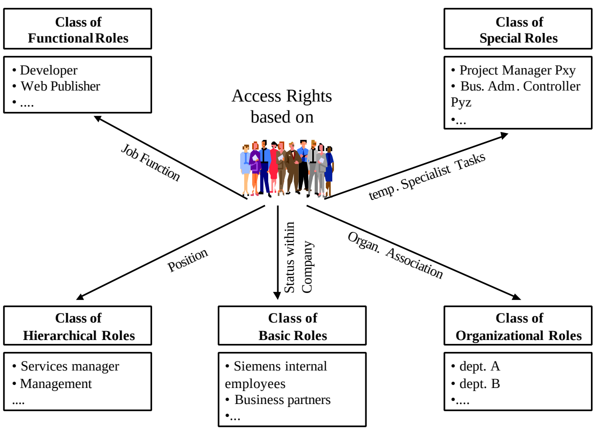

Figure 3: Classification of Roles

As shown in Figure 3 the roles are organized within different role classes. With this understanding roles can be semantically structured to reflect different kinds of authorizations. Role classes at Siemens ICN are

- Functional Roles
- Organizational Roles
- Basic Roles
- Hierarchical Roles
- Special Roles

This classification reduces the complexity of role management since the role class affects the design and administration of the respective roles. Changes in the business environment can thereby often be reduced to roles of only one role class. Moreover, the mass business of finding functional roles can be separated from the design of more technical roles. To handle the roles in a unified manner they are put together into the common structure of the role catalog.

Appropriate roles in the classes “basic roles”, “hierarchical roles” and “organizational roles” could be found quickly. Special interest was given to roles in the class “special roles” which will be defined temporarily. Mostly, it is not suitable to define them with a high degree of abstraction.

For the class “functional roles”, an investigation into the requirements and definition of a role-finding process was required. Objectives for role-finding, among others, were both a reduction in the number of roles and a strengthening in the robustness of roles in an organizational restructuring. A promising approach is the process-oriented role-finding.

4. Role-Finding

In this section the process-oriented approach for role-finding [Roe] is presented in some detail for the first time in the literature. However, this presentation is to be viewed as preliminary and a mathematically strong foundation is still to be published.

It is shown how this method integrates into the Siemens ICN RBAC project to cover the practical aspects of role-finding. To automate this technique, the software-tool “RoleFinder” has been implemented ([RoFi]).

4.1 The Process-Oriented Approach for Role-Finding

4.1.1 Introduction

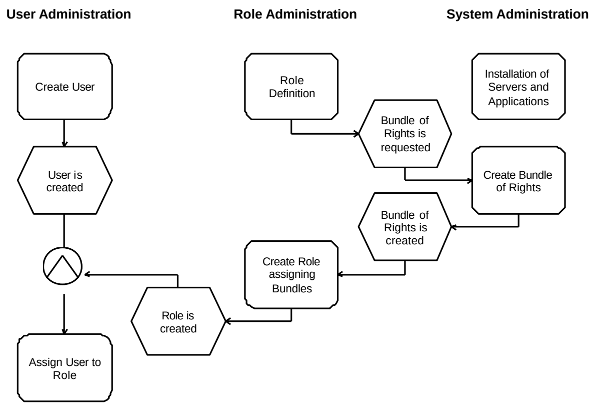

Figure 4 : The Process of Security Administration

The process-oriented approach is tightly coupled to the interpretation of the overall security administration process outlined in Figure 4. Security administration here is divided into the three subprocesses

- *User administration*: Bulk processing performed for numerous users per week. This process should be simplified, accelerated and exhibit improved quality as much as possible. This is the main reason for implementing RBAC.
- *Role administration*: This process consists of finding and implementing roles. While role-implementing is technical (if the roles to be implemented are clearly defined) role-finding is a most complex task requiring extensive business knowledge.

- *System administration*: Technical tasks consisting of cumbersome work. Objectives are work simplification and reduced complexity.

These processes should be separated in a way that user administration can be managed by medium skilled employees and automated where possible. System administration and role implementation should be supported with clear definitions and instructions. These definitions should be the results of role-finding, where a considerable amount of know-how must be incorporated.

Finally, the process-oriented approach is designed to meet the needs of all people involved in the process of implementing RBAC. These include the RBAC project team, role administrators, user administrators, system administrators and auditors.

4.1.2 Structure

The process-oriented approach is a formal approach for cross-platform RBAC which combines an RBAC meta model with a corresponding procedural model. The well-known RBAC models from [SBM], [SCFY] are utilized, but while role activation is not included into the meta model, there are three separate but related views within the meta model supporting the steps of finding and defining the roles.

These data views are the *process layer* providing the interface to business process models, the *role layer* providing the central repository for the cross-platform business roles and the *access rights layer* describing the structure of the corresponding system specific entities implementing the business roles in the different security systems.

The essential paradigm of the process-oriented approach is the possibility to automatically derive the role layer from the process layer, if the process layer contains security relevant information. Moreover, the access rights layer can be automatically derived from the role layer. The feasibility-proof was given by development of the software tool *RoleFinder*. RoleFinder performs these derivations such that the contents of the complete meta model are generated from the contents of the process layer.

4.1.3 The Meta model

The process layer consists of the basic entities "job function", "job position", "organizational unit", "information system", "security system" and "attribute" which can be seen as arbitrary sets F, J, O, I, S, P in a mathematically strong sense. A simplified presentation of the meta model is shown in Figure 5. For better readability, the organizational aspects, i.e. the set O is not included in the figure. Moreover, the process layer contains (n x m-) relations within the cartesian products J x F, F x F, F x I, F x S, F x P, O x I, O x S, O x P. Using these entities and relations, the structure of job functions and their assignment to job positions can be described. Moreover, it can be described which information systems support, which security systems protect and which attributes separate job functions and organizational units.

The role layer consists of "Roles", "Subroles" and "Bundles of Rights" represented in sets R, T, B together with the sets I, S, P from above. The allowed relations are within R x T, T x T, T x B, O x B, B x I, B x S, B x P.

The access rights layer consists of "assignable groups" and "subgroups" represented in A and G with relations within A x G and G x G.

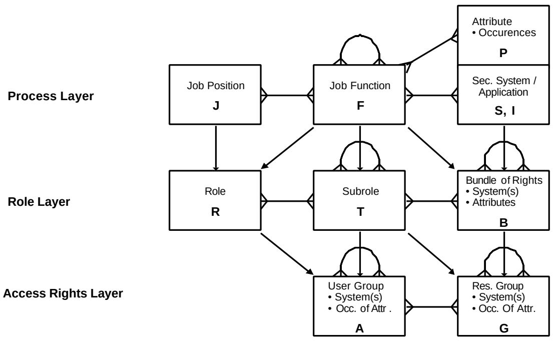

Figure 5: Meta model for Process-Oriented Role-Finding

Additionally the separate layers are connected by different relations. The role layer is completed by relations within R x J, R x F, R x O, T x F, B x F. The access rights layer is completed by relations within A x R, A x T, G x T.

4.1.4 The procedural Model

The procedural model accompanies the meta model, yielding practical steps and procedures for the contents of the process layer. Moreover, procedures for deriving the role layer from the process layer, and then the access right layer from the role layer are designed to produce the contents of the complete meta model

Steps for creating the process layer include:

- finding suitable organizational units and persons therein and assign role-finding responsibilities to them
- Provide training to these persons
- Find the complete set of job functions performed in this organization as far as they are supported by information systems
- Find job positions building bundles of job functions which coincide with the work performed by individual employees in the company
- Assign the information systems, security systems and attributes suitably to the job functions and to the organizational unit itself.

In the best case, this information can be extracted from existing business process models, at minimum the job functions, and hopefully up to the information and security systems. Assignment of attributes can be omitted if they are not needed to increase the granularity of the administration concurrent to minimizing the number of business roles. When the process layer is complete, both the role layer and the access rights layer are derived using a parameterized algorithm.

By following this procedural model, the role administrator can concentrate on the business cases modeled in the process layer and need not focus too much on implementation tasks.

Since this paper contains only an overview on the process-oriented approach for role-finding, the detailed algorithms and parameters for deriving the role layer and access rights layer are not presented here.

The algorithms and the constraints on the relations between the entities in the metamodel will be detailed in a forthcoming paper by Roeckle et al. The core of the algorithms is to decide which process entities are candidates for roles from the viewpoint of security administration. This takes into account the separation and combination of access rights from an administrative view and also the different security systems' capabilities to support role structures. The main principle is to keep track of the relations between the different layers in order to keep the system consistent and manageable.

4.1.5 Benefits

One of the benefits of this approach is the *formal approach* which leads to the process layer supporting the role-finding people giving business related semantics and clarity on the procedures.

The role layer supports the user administrators providing a *comprehensive role catalog* for their daily work of assigning users to roles.

The access rights view supports the system administrators and role administrators by *describing the implementation* of the roles in the different systems. Support for the internal revision can be seen in the fact that all this information is presented in one consistent model. This improves the *overview and manageability* of the overall security administration.

From the above description of the overall process of security administration, all subprocesses of security administration are supported using the meta model. Furthermore, by restricting the role administrators to this presented procedural model, both standardized documentation and presentation of identified roles are generated. The use of affiliations ([PS], [Bez]) and other user attributes for the separation of access rights is supported by the meta model.

4.2 Role-Finding at Siemens ICN

As described above the central notions of RBAC at Siemens ICN are the comprehensive role catalog organized in role classes. The software tool RoleFinder is build on an SQL database implementing the metamodel and providing reporting features able to generate the role catalog. Role classes are not explicitly mentioned in the process-oriented approach. However, the approach keeps track of the connection between roles and the process entities where the roles are defined for. Since the technical details of RoleFinder are beyond the scope of this business case study, see [RoFi] for further information on RoleFinder.

From this connection, roles resulting from business processes can be associated to the classes of Functional Roles, Organizational Roles and Basic Roles. Hierarchical Roles can usually be mapped to functions related to the hierarchical position. Special Roles usually are special or temporary cases of Functional Roles, (i.e. like *Member of Project P).*

During the deployment phase, several representative roles were designed and implemented to test the entire process from role-finding via role-implementation to role-based administration and access control. During this phase the process-oriented approach was found to be feasible.

5. Role-Implementation

In a heterogeneous computing environment, a role description virtually always includes privileges across several platforms with numerous applications. In our view, roles are not limited to a single operating system or platform. They are used on a meta level above the computing platforms to perform tool-based cross platform administration. For the Siemens ICN project, Schumann's Security Administration Manager (SAM) and SAM Request Manager (SAM/RM) were chosen. SAM is an IBM OS/390 based cross-platform role-based security administration tool performing online actions in the target security systems via agent technology. SAM/RM is a client/server based security administration workflow which, using predefined roles based upon the company structure, automates and standardizes the process of issuing authorization requests. Technical details about role concept and architecture of these modules can be found in [Awi], [SAM], [SMF], [SRM]

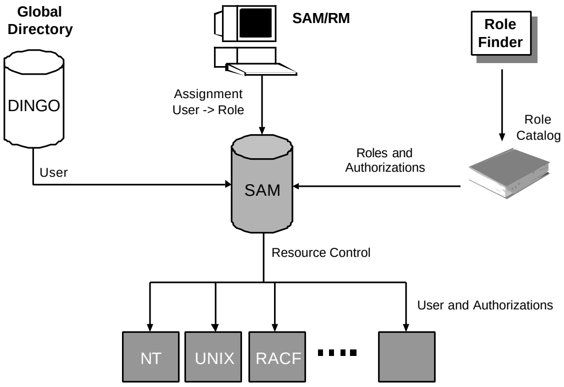

Figure 6 : System Architecture

The model architecture shown in Figure 2 has been implemented using SAM as the core integration element. The resulting overall system architecture is shown in Figure 6.

For the creation of a role catalog with a limited number of roles, different role-finding approaches have been evaluated. An intuitive approach did not lead to a comprehensive result for the pilot organization. Therefore the process-oriented approach was pursued based on existing business process models. Another reason was the tight integration of business processes and IT infrastructure required by the overall objectives of the Roadmap Projects.

A separate procedure was used for basic roles. Basic roles in the notion of Siemens ICN are related to user types such as “internal Siemens ICN employee” or “external Siemens ICN employee”. These user types are derived from user attributes maintained in the central Siemens ICN user directory (DINGO). At initial loading time (and subsequent updates) of the users from DINGO into SAM, an automatic assignment of the basic role to the user can be performed. The advantage is that bulk processing occurs automatically and does not need to be initiated by an administrator.

In SAM, roles were implemented using the so-called Master Models, i.e. templates controlling properties and access rights of the assigned users, see [Awi], [SAM] for details. In cases where the role-finding led to the use of affiliations (see [PS]) or other user attributes SAM's "Joker Group" constructs were used. At ICN this feature was needed to separate access rights of users performing the same job functions at different geographical sites.

The organization of administrative duties and inherent approval processes are important tasks within the total RBAC concept. This is supported by SAM and SAM Request Manager (SAM/RM), the SAM-tool for local administrators [SRM]. SAM/RM supports the security administration workflow where local administrators request user rights in a formal approval procedure which lead to role assignments via the SAM-kernel. The central security administrator creates, provides and maintains roles, while the local administrator uses the roles for assignments.

6. Conclusion and Outlook

6.1 Proof of Concept

The work at Siemens ICN was performed under a thorough and continuous reflection of all influencing factors. The feasibility of this RBAC concept was proven several times, each from a different point of view. For internal communication it was important to have a detailed procedural model defining precisely this role finding process. Without this model, management support for the RBAC project could not have been guaranteed.

From the beginning, it was clear that most of the roles had to be based on corporate functional structures. Organizational structures typically do not produce stable roles. The business functions however, are expected to remain essentially the same regardless to which organizational structure they belong. Therefore, role definitions were closely related to the identification of core business functions.

Defining roles using existing job descriptions as an input was infeasible, since these descriptions lacked sufficient meaning to deal with concrete access rights. Furthermore, intuitive role-finding does not lead to a comprehensive role-catalog. The ongoing business process documentation project was designed to provide process models for the entire company. These models proved usable as input for the role-catalog's creation.

6.2 Outcome of Project

The major outcome of the project was the demonstration of a fully integrated working model of Business Process Models and Role-Based Security Administration. We could build a running demo system using an initial role catalog to study and proof the concepts. This demo system provides the basis for rollout into productive security administration.

The following conclusions turned out to be the main success factors:

- Security policies must be tied to the business processes supported by the IT-systems since security criteria are inherent to business processes and cannot be derived from a technical context only. Using business processes allows to understand and revise decisions concerning access rights.
- In a large enterprise it is imperative to apply tools to find and maintain roles for reasons of workload, change management, documentation and business integration.

Business process models typically used for business reengineering do not contain all security aspects. However they provide a comprehensive set of functions with their structures that can be used for role modeling. For the purpose of role finding they can be enhanced by the entities shown in Figure 5.

6.3 Further Comments and Experiences

Obviously there is a strong correlation between the quality of the information within business functions and the resulting roles. Moreover, the usual process models, defined by event-process-chains, contain no more security relevant details than the business functions themselves. Therefore expert knowledge is necessary to enhance the process models with additional security relevant information such as attribute types, security systems or applications involved.

This security relevant information can be incorporated into the process view to obtain models for tool-based generation of the role-catalog. This results in consistent models integrating all three layers; process, role and access rights.

Following our process-oriented approach, the resources-side of the access rights layer provides descriptions for the bundles of access rights needed in the different security systems. While such bundles must be available in any system, if administered via RBAC or not, the description generated by our approach enhances support of these administration tasks.

6.4 Future Work

6.4.1 Practical Work

During this RBAC project the procedure to initially identify and implement the roles was defined in detail. The next step will require the analysis of influencing factors which influence changes in established roles. A supporting change management process and feedback to the role-finding process is also required.

The data generated from tool-based role-finding is collected in a database which implements the meta model. From this database, contents of the meta model are available for further processing. An interface program to convert and import the role definitions into the centralized administration tool should be developed.

6.4.2 Research Proposals

At the present time, the process-oriented approach for role-finding is not founded in a scientifically sufficient manner. We propose that this foundation could be researched by the scientific community to provide further clarity on the detailed procedures.

Interesting research topics might pursue the connection between different business process models and role structures when the requirements for the resulting roles vary. Additionally, the concept of role activation is not yet included into the process-oriented framework of role-finding.

Another promising topic for future research might be an analysis of the key factors for obtaining stable role structures from business process models. Such an analysis could investigate different modeling techniques or target systems. Another interesting research topic might be the identification of correct granularity for the business process models. The objective would be to define a stable role structure which reflects access rights within a large company.

The implementation of the role structure in some special systems has been researched [JGIL]. It would be interesting to develop the connections between ERP-systems automating business processes and the role structures derived from the same business processes using this process-oriented approach.

7. REFERENCES

[Awi] Awischus, R.; Role-Based Access Control with the Security Administration Manager (SAM); Proc. 2nd ACM Workshop on Role-Based Access Control, Fairfax, Virginia, USA (1997)

[Bar] Barkley, J. F.; Implementing Role-Based Access Control Using Object Technology; 1st ACM Workshop on Role-Based Access Control, Gaithersburg, Maryland (1995)

[Bez] Beznosov, K.; Requirements for Access Control: US Healthcare Domain; Proc. 3rd ACM Workshop on Role-Based Access Control, Fairfax, Virginia, USA (1998)

[ES] Epstein, P., Sandhu, R.; Towards a UML Based Approach to Role Engineering; Proc. 4th ACM Workshop on Role-Based Access Control, Fairfax, Virginia, USA (1999)

[FBK] Ferraiolo, D.F., Barkley, J.F., Kuhn, D.R.; A Role-Based Access Control Model and Reference Implementation Within a Corporate Intranet; ACM Transactions on Information and System Security, Vol. 2, No. 1, P. 34-64 (1999)

[FCK] Ferraiolo, D.F., Cugini, J.A., Kuhn, R.D.; Role-Based Access Control (RBAC): Features and Motivations; Proc. 11th Annual Computer Security Applications, New Orleans, Louisiana (1995)

[FH] Fernandez, E.B., Hawkins, J.C.; Determining Role Rights from Use Cases; Proc. 2nd ACM Workshop on Role-Based Access Control, Fairfax, Virginia, USA (1997)

[Fly] Flynn, H.; „Real-Life“ Use of Roles for Access Control; Gartner Advisory, Monthly Research Review August 1998 (1998)

[HDLG] Hummel, A.A., Deinhart, K., Lorenz, S., Gligor, V.D.; Role-Based Security Administration; Proc. Sicherheit in Informationssystemen (SIS '96), Vienna, Editors: K. Bauknecht, D. Karagiannis, S. Teufel (1996)

[JGIL] Jaeger, T., Giraud, F., Islam, N., Liedtke, J.; A Role-Based Access Control Model for Protection Domain Derivation and Management; Proc. 2nd ACM Workshop on Role-Based Access Control, Fairfax, Virginia, USA (1997)

[Mah] Maher, A.; A Universe of One™; Siemens AG Information and Communication Networks, press conference February 7th, 2000 (2000)

[PS] Parker, T., Sundt, C.; Role-Based Access Control in Real Systems; Information Systems Security, Spring (1996)

[Roe] Roeckle, H.; Rollenbasierter Zugriffsschutz, Automatisierte Bildung der Rollen im Unternehmen auf der Basis eines prozessorientierten Vorgehensmodells; IT-Sicherheit 2/99, datacontext fachverlag, Frechen (1999)

[RoFi] Roeckle IT-Sicherheit GmbH; RollenFinder Benutzer Dokumentation; RoFi-Handbücher, Rel. 1.0, Bochum (2000)

[SAM] Schumann Unternehmensberatung AG; Security Administration Manager (SAM), Concepts and Facilities; SAM-Manuals, Rel. 2.4, Koeln (1999)

[San] Sandhu, R.; Role Activation Hierarchies; Proc. 3rd ACM Workshop on Role-Based Access Control, Fairfax, Virginia, USA (1998)

[SBM] Sandhu, R., Bhamidipati, V., Munawer, Q.; The ARBAC97 Model for Role-Based Administration of Roles; ACM Transactions on Information and System Security, Vol. 2, No. 1, P. 105-135 (1999)

[SCFY] Sandhu, R., Coyne, E.J.; Feinstein, H.L., Youman, C.E.; Role-Based Access Control Models; IEEE Computer, 29(2) (1996)

[SMF] Schimpf, G.; Security Management for Administration and Control of Corporate-Wide Diverse Systems; ACM SIGSAC Review 15(1) (1997)

[SRM] Schumann Unternehmensberatung AG; SAM Request Manager (SAM/RM), User Manual; SAM/RM-Manuals, Rel. 2.1, Koeln (1999)

[TBB] Thomsen, D., O'Brien, R., Payne, C.; Napoleon Network Application Policy Environment; Proc. 4th ACM Workshop on Role-Based Access Control, Fairfax, Virginia, USA (1999)