HU DUAAL SYSTEEMBEHEER

ANALYZING AND DESIGING SECURITY FOR SHARED DATA

EMERSON™

Process Management

Emerson Process Management Flow BV

Author	M. Nijland
Student nr	1538010
1st examiner	H. Karssenberg
Coach	G. Bouw
Document	Analyzing and Designing Security for Shared Data
Revision	1.1
Revision Date	26 May 2010
Print Date	27 May 2010

PREFACE

Twenty years ago, after finishing Dutch high school HAVO, I wanted to achieve a degree in electronics and started studying electronics at the Windesheim University of Applied Sciences in Zwolle. Unfortunately I failed to pass the propaeduetic exam and continued to study electronics at a technical school. After I completed this successfully, I started my professional career, first in electronics and after four years in ICT. I always regretted however, not to have achieved my bachelor degree.

Much later, spring 2007, while reading an ICT professional magazine, my attention was drawn to an advertisement of Hogeschool Utrecht (Utrecht University of Applied Sciences). They offered a three year course to achieve a bachelor degree in ICT, specialism: Systems Management. This three year course was especially designed for students with a few years experience in System Management, who are currently working in a System Management related job. I considered this course as an opportunity to achieve a bachelor degree and applied for the course.

The first year of the course started very well, I had a stable private life and at work everything was OK. In 2008 however, things started to change rapidly. Within two years time, I met my wife, moved house and got married. Meanwhile at work, due to a split-up of the company, workload increased. This combination made it very hard for me to focus on my study. The unconditional support of my wife however, made it possible for me to continue.

Therefore I want to thank you, Barendine. Without your support, I would not have made it.

(*Daarom wil ik jou, Barendine bedanken. Zonder jouw ondersteuning, zou ik het niet hebben gered.)*

Apeldoorn, May 2, 2010

Marco Nijland

MANAGEMENT SUMMARY

For a long time, I was suspected that the security of our file server was inadequate, difficult to manage and time consuming to audit. Therefore I decided to make analysis and improvement of the file server security, subject of my thesis for my Bachelor in ICT course. I have set the following goals:

1. Make the file server security structure more secure.
2. Make the file server security structure better auditable.
3. Make the file sever security structure manageable in such a way that it can be outsourced.

Analysis of the security (See chapter 5) revealed the following security threats:

1. Users with permissions directly on a folder. This is a security risk because it hard to find out which folder a user has permissions to.
    - 19% of the users do have permissions set directly on one or more folders.
    - 44% of the folders do have permission set directly for one or more users.
2. Folders with permissions assigned to 'Domain Users' groups. This is a security risk because the 'Domain Users' group contains all Emerson employees with an Active Directory user ID.
    - 14% of the folders have permissions set for 'Domain Users'
3. Groups with permissions assigned to more than one folder. This is a security risk because when a user is added to the group to give him permission to folder A, he also gets access to folder B, which might be unwanted.
    - 55% of the identified groups are used to give permissions to more than one folder.

To eliminate these threats, I propose to implement Role Based Access Control (RBAC). With RBAC all permissions to files and folders are granted to user roles instead of to users directly. When a user changes job internally or a new employee is hired, simply changing or adding roles the user belongs to changes his access to files and folders.

At the same time, reorganizing the folders on the file server to match the organizations hierarchy will make it much easier to manage. To further improve manageability and auditability, a SharePoint list will be created, containing necessary information about the folders and roles.

Creating an entry in a SharePoint list for each folder with unique permissions makes security visible and allows for additional metadata to be added, such as the folder owner or approver.

Having the file server security setup as described, allows management tasks to be described in procedures and work instructions, which can be published to the Service Desk. This makes it possible to outsource file server security management to the Service Desk.

Summarizing, the following actions must be completed in order to accomplish the defined goals:

- Implement Role Based Access Control.
- Have a SharePoint list figuring as a management database set up.
- Have a management procedure be written and distributed to all administrators.

It is important that all three parts will be implemented. Only the three of them together will bring the security to an acceptable level.

Implementation of all parts will take about 16 weeks, based on 25% FTE IT resource availability. Apart from the IT resource, approximately 20 hours will be needed from the business. See chapter 8 for a detailed planning.

After implementation, the effectiveness of the security model will be evaluated by me, the IT & Business Systems Manager (Gerhard Bouw) and an independent person, which will be determined at a later time. This evaluation will be communicated back to the business.

If the model appears to be effective, it will be shared with Emerson Process Management's European clients and server teams.

TABLE OF CONTENTS

TABLE OF FIGURES

INTRODUCTION

Emerson Process Management Flow BV, from now on to be called: ‘Emerson Flow’, is one of many subsidiaries of Emerson Electric co, from now on to be called: ‘Emerson’.

Emerson is a global multidivisional organization with approximately 130.000 employees. Emerson’s headquarters are located in St. Louis, USA.

Emerson Flow is part of the division Emerson Process Management, which is a collection of companies, all manufacturing process management instrumentation. Think of valves, sensors, actuators and control systems. Emerson Flow assembles and distributes flow sensors for the European and Middle-Eastern market. Emerson Flow serves two divisions with these services: MicroMotion and Rosemount Flow Division (RFD).

Currently Emerson Flow employs about 185 people, of which about 160 in the Ede Netherlands facility and another 25 in Manila (Philippines) and Cluj (Romania). Also, Emerson Flow shares its data on the file server with employees in other sites like European sales offices and divisional manufacturing and engineering sites.

Emerson’s IT organization is fragmented, originally each facility had its own IT organization and functioned fairly autonomous. A couple of years ago, Emerson started consolidating IT services, of which the implementation of the Manila (Philippines) based ITSS Service Desk is one of the achievements in 2009. The ultimate goal is to have all routine tasks described in procedures and outsourced to the ITSS Service Desk.

Within this organization, I have been employed as a network and systems administrator for over ten years. This is an all-round job with responsibilities varying from end user support and system administration to project management.

Key initiative number one of Emerson’s corporate IT is security. All corporate initiated security related projects are mandatory and should be given precedence over other projects. Examples are: laptop encryption, centralized patch management and centralized antivirus management.

With this strategy in mind and in my role as a systems administrator, I have performed a quick scan of the folder structure of the fileserver and had to conclude that the folder and security setup is unstructured in such an extent that it very likely to be a serious security risk.

Emerson Flow is frequently being audited by both internal and external auditors like DNV (ISO 9001) and KPMG (Financial). With the current situation it is very hard, if not impossible, to show the auditors where a specific employee has access to.

The possible security risk, audit limitations and the opportunity to outsource tasks to the service desk lead to the idea to have these be the subject of my thesis.

1 PROBLEM DESCRIPTION

As already mentioned in the introductory, this thesis had three goals:

1. Make the file server security structure more secure.
2. Make the file server security structure better auditable.
3. Make the file sever security structure manageable in such a way that it can be outsourced.

The inability to match these goals currently is due to the following core problems:

- Hardly any structure in the folder layout.
- No 1 to 1 match between folders on the server and security groups in Active Directory.
- Permissions on folders granted to individual users instead of groups.
- Folder layout is not a reflection of the organizational structure.
- Group names are often not related to the folder they apply to.
- No approval workflow defined.
- Folder owner often unknown.

All these core problems together make it difficult and time consuming to reveal all folders a specific user has access to. Also because it is often unclear who the owner of a folder is, it is difficult, if not impossible, to check whether a user is authorized before granting access to a folder. This makes the risk that a user has access to data which he should not have very plausible.

There is another drawback to the current unstructured folder layout and permissions setup. Managing it requires a lot of knowledge of the local organization, making it impossible to outsource folder and security management to the Service Desk, which is one of the strategic initiatives of Emerson IT.

Emerson being a matrix organization adds a lot of complexity to the task of aligning the folder structure with the organization. Emerson has both a divisional and regional organizational structure, where regional sales managers have to access data for their regions across all divisions and where divisional marketing directors have to access their divisional data for all regions. This complexity of the organization makes it hard to align the folder and security structure with it. Currently the fileserver contains about 90 folders on the 1st level and 1250 folders on the 2nd level of the share “SHAREDF” which is presented to the users as drive Q: and W:. Both drive mappings refer to the same share for historical reasons. Active Directory includes about 200 security groups used to apply security to folders on the fileserver.

2 DELIVERABLES

The primary deliverable of this project is to deliver an advisory report to the management of Emerson Flow. This report will contain a restructuring plan for improvement of the security of the fileserver. Partial implementation of the new structure will be part of the project to demonstrate the proposal and proof its effectiveness.

This thesis will act as advisory report to the management of Emerson Flow and will be presented at the first management team meeting in June 2010.

The advisory report will contain the following components:

- Proposal for restructuring the folder layout on the fileserver
- Proposal for restructuring the security groups in Active Directory
- Proposal for an approval workflow
- Procedure for management of the proposed new structure

The proposal must match the three earlier defined goals:

1. Make the file server security structure more secure.
2. Make the file server security structure better auditable.
3. Make the file sever security structure manageable in such a way that it can be outsourced.

The following is considered to be out of scope:

- Creating the new folder structure according to the proposal
- Creating the new Active Directory groups structure according to the proposal
- Active Directory managed access to systems other than the fileserver of Emerson Flow
- Security and structure of the user's personal 'home' shares on the fileserver
- Searching for alternatives for document storage
- Full implementation of the proposed new structure

4 APPROACH

In order to get to a structured folder layout and permissions assignment, the following project tasks have to be completed:

Tasks for restructuring and assigning permissions:

- Perform research of NTFS permissions management tools
- Analysis of the folder structure
    - Which shares exist
    - Which folders exist
    - Who has access to each folder
    - Who is the owner of each folder
    - What is the audience of the data in the folder
- Analysis of the organization
    - Which departments exist
    - Which roles and positions exist
    - What are the qualifications of each role/position
- Design a new folder layout
    - Align folder layout with organization
- Design a security structure
    - Align Active Directory security group structure with organization
- Write a proposal containing the new folder and security structure.

Tasks for outsourcing folder and security management to the Service Desk:

- Design an approval workflow
- Design an access request form
- Write a procedure for assigning permissions to folders

5 CURRENT SITUATION

The current situation of the way data on the file server is organized and secured is the inheritance of over fifteen years of system management without a decent set of rules to which data structure and security must comply. This resulted in an uncontrolled growth of root level folders. At the same time different visions of the system administrators lead to different ways of applying permissions: sometimes a user has been granted permissions directly on the folder, sometimes departmental groups were used and sometimes a dedicated group for the folder in question.

The uncontrolled folder organization, combined with several methods of assigning permissions, makes it very disorderly.

The following sections describe the current situation of these three subjects:

- Security
- Management
- Audits

5.1 SECURITY

Emerson Flow uses two types of security on the file server for 'normal' users.

1. Protect files from reading. This is to obtain confidentiality
2. Protect files from modifying. This is to obtain integrity.

Apart from these two, administrator and systems accounts can have 'Full Control' permissions, allowing them to change permissions on files or folders. Administrative and system permissions are considered to be out of scope for this project, although with the implementation these permissions also have to be applied to the new folder structure.

During the quick scan, the security properties of a random set of folders have been looked at, which identified the following security threats:

1. Users with permissions directly on a folder
    - These permissions are very difficult to trace. Result: When a user changes role, it is very likely these permissions are not removed.
2. Folders with permissions assigned to 'Domain Users' groups
    - Since Emerson recently migrated to a single domain model, the 'Domain Users' group includes all 57.000 regular user accounts within Emerson.
3. Groups with permissions assigned to more than one folder
    - Granting a user access to one folder may result in also granting access to another folder, which can be unwanted.

These threats apply both to confidentiality and integrity, so from a security standpoint we can treat these two security types equal.

Next step is to analyze to what extent these threats apply. If there are only a few folders to which these threats apply, we might not need to change the security model. Therefore, I have performed a thorough analysis of the current applied security.

5.1.1 ANALYSIS TOOL AND METHOD

As analyzing over 1300 folder manually is impossible within the timeframe of this project, I searched for tools to help me in performing my tasks. I had no budget for this project, so I limited my search to free tools and functioning demo versions.

For the analysis of the permissions currently set on the folders of the file server, I downloaded the tool "SecReport Enterprise" from SmartX software (www.smart-x.com), a company specialized in developing software tools for (Windows) system administrators.

Due to the budget restraints, I used the demo version. The limitation of the SecReport Enterprise demo version is as follows:

- The program works only for 30 days.
- The program analyses a maximum of 100 security objects per scan.

The consequence of this last limitation was that I had to analyze each 1st level folder individually and for some folder trees also each 2nd level folder.

SecReport has been configured to only report Domain accounts and not to show permissions on folders which are identical to its parent. The reason for only showing Domain accounts is that each folder has permissions set for the "SYSTEM" and "CREATOR-OWNER" built-in groups and most folders also for the local "Administrators" group. These groups are however only used by the internal server processes or for administrative purposes and are considered to be out of scope for this project.

For most folders, SecReport will generate one or more errors like:

```
emrsn.org: An error occured while resolving sid 'S-1-5-21-1004336348-1454471165-725345543-18150'.;Error resolving SID 'S-1-5-21-1004336348-1454471165-725345543-18150' to name on machine 'Error resolving SID 'S-1-5-21-1004336348-1454471165-725345543-18150' to name'.;No mapping between account names and security IDs was done;
```

These errors are due to 'orphaned' security identifiers (SID). These SIDs do not exist anymore on the domain controller, hence they cannot be translated to a group- or username.

The output of the SecReport tool is saved as a comma separated text file (.CSV). These .CSV files have been imported into Microsoft Excel and redundant data has been removed. The redundant data consists of column labels, report title and generation date being repeated before each data row. After this redundant data has been removed, the files are saved in Excel format (.XLSX)

An Excel add-in called RDB Merge, created by Excel specialist Ron de Bruijn (www.rondebruijn.nl) is used to combine all the individual .XLSX files into one.

Now with all the data in one Excel sheet, pivot tables have been used to analyze the data, which lead to the following:

5.1.2 ANALYSIS RESULTS

Generic Data:

1. Total 224 folders have 1355 unique permissions assigned.
2. Total 145 groups have permissions assigned to 222 folders.
3. Total 69 users have direct permissions assigned to 97 folders.
4. Total 356 users have access to the file server. Either by group membership or by direct permissions.

Analysis of the threats, described in chapter 5.1:

1. Users with permissions directly on a folder
   - 69 out of 356 users have been identified to have permissions applied to folders directly, which is 19% of the identified users.
     97 out of 224 folders are affected by this threat, which is 44% of the folders with unique permissions applied.
2. Folders with permissions assigned to 'Domain Users' groups
   - 32 out of 224 folders have permissions set to 'Domain Users', which is 14% of the folders with unique permissions applied.
3. Groups with permissions assigned to more than one folder
   - 80 out of 145 groups have permissions assigned to 2 or more folders, which is 55% of the identified groups.

Apart from this statistic data, the Excel files also contain detailed information about which folders have unique permissions configured and who has access to it. This information is needed later during the actual implementation to determine which roles need to have access.

In the original approach plan, also the audience for a folder and the owner were part of the analysis plan. Due to time restrictions (analyzing the data was much more time consuming than budgeted) I decided to defer that part to the implementation phase.

5.2 MANAGEMENT

Currently, there is no structural management of the file server folder structure or the way permissions are applied.

When a user needs access to a folder, in general the following happens:

- The user logs a service call with the Service Desk asking for access to a folder. The Service Desk routes the service call to workgroup 'Emerson Netherlands Deskside Support'. Next, the system administrator opens the service call and analyzes the request.
- The system administrator checks which groups currently have permissions applied to the concerned folder. Next he needs to decide into which of the groups to put the user. The names of these groups are not always clearly related to their purpose, making it difficult to decide if the user should be added to the group. If none of the groups are suitable, he might decide to grant the user directly permission to the folder.

There is no approval workflow or folder owner defined, so it is up to the system administrator's best guess as who to contact for approval.

There is no central place where permissions or the purpose of groups are recorded, resulting in the system administrator having no idea who has access to what, unless he checks each and every folder individually.

5.3 AUDITS

When an audit takes place and the system administrator receives a request to show where a particular user has access to, he has to perform the following tasks:

- Make a list of all groups the user is a member of, including group memberships inherited by group nesting.
- Manually check each folder's permissions and check whether one of the groups the user is a member of has permissions to the folder.

With 224 folders with permissions applied, this is very time consuming

Emerson's current audit requirements require periodical review of access to resources, which is in the current setup practically impossible.

Apart from these formal audits, also periodical 'Self Audits' need to be performed, where a list of questions has to be filled out to good conscience.

5.4 USERS AND ROLES

To identify user roles I received a function description list from the HR manager. This list contains the 153 currently in Ede employed users.

356 unique user ID's have been identified as being a member of one or more groups, granting them permissions to the data stored on the file server in Ede. Grouping these ID's into the following categories, leads to the following numbers:

- Internal users: 156
- Best Cost Country users: 32
- External users: 150
- Special: 31

The 'Special' users are disabled accounts, service accounts, administrative accounts and generic accounts for conference rooms and manufacturing.

External users are users from other offices, mostly European sales offices and the divisional headquarters in the USA.

Best Cost Country users are users located in India, Philippines or Romania, working dedicated for Emerson Flow. Currently Emerson Flow has documentation handlers in the Philippines, project engineers in India and order entry employees in Romania.

The difference in users supplied by HR and the count based on group membership can be explained by the fact that there are a few accounts of people working for Emerson Flow, receiving their IT support from the Ede IT, but are physically located elsewhere. These people are probably also elsewhere on the payroll, thus not on the list HR supplied me.

Of the internal users, not all are part of the local Emerson Flow business. Emerson Flow is hosting for 7 users with jobs on European level. Also some people are dedicated to one of the two major divisions located in Ede: 6 for Micro Motion (MMI) and 4 for Rosemount Flow Division (RFD). This leaves 136 users who work either for both divisions, or for a non-divisional part of the business.

6 DESIRED SITUATION / FUTURE STATE

To determine a desired situation we have to look at three perspectives:

1st from a security standpoint
2nd from a management standpoint
3rd from an audit standpoint

From a security standpoint it is important to eliminate the threats I identified earlier:

1. Users with permissions directly on a folder
   - Add users to a group with permissions to the folder
2. Folders with permissions assigned to ‘Domain Users’ groups
   - Narrow down to PM_Users, PMEMA_Users or NLEDE-All Users.
3. Groups with permissions assigned to more than one folder
   - Use dedicated group for each folder and each permission type.

From a management and audit standpoint we want to achieve the following:

1. Quickly identify all folders where a user has access to.
2. Quickly identify all users who have access to a folder.
3. Quickly identify to which group a user has to be added in order to gain access to a folder.
4. Quickly identify the owner or approver for the folder.

7 DESIGN

Before making the design for the proposed new security structure I performed a literature research about access models. My primary source for this was the book used for the course DU6-SECU1: (Harris, 2008). Secondary I consulted a few European Emerson colleagues, specialized in Active Directory. I also checked within Emerson IT if there are technical or legal issued to be considered.

7.1 ACCESS MODELS

A key element in securing a company's data is controlling access to it. The way access is controlled is depending on the type of data and required protection. Do you need to protect the data to being read by unauthorized persons, or do you need to protect the data to be modified or deleted?

This section describes methods used to control access to system resources after the user's identity has been verified and the user has been granted access to the system.

There are three commonly used access models:

1. Mandatory Access Control
2. Discretionary Access Control
3. Role Based Access Control

These access models are frameworks that dictate how users access resources.

7.1.1 MANDATORY ACCESS CONTROL

With Mandatory Access Control (MAC) all security is centrally defined by a security officer. All objects are labeled with a security level and category. All users will also have security and category labels. Users can only access objects when their labels match the object's labels. The structure of MAC is hierarchical: users of a certain security level can access objects of their own and lower level.

MAC was defined by and is primarily used by the US government and is not supported by the common file server operating systems without adding third party components.

Within MAC there are two common security models: Bell-LaPadula and Biba. These models provide in protecting information in flowing the wrong direction.

Bell-LaPadula

The Bell-LaPadula model is designed for protecting confidential information. A user with a certain security level, cannot read documents of a higher security level, and cannot write documents of a lower security level. With this model, confidential information cannot 'leak' either deliberately or accidentally. Bell-LaPadula has been designed for and used by the US government to protect its classified information.

Biba

The Biba model is designed to protect the integrity of information. Its design is opposite to Bell-LaPadula, a certain user cannot write documents of a higher integrity level, and cannot read documents of a lower integrity level. This prevents information of a lower integrity level being mixed with information with a higher integrity level. The Biba model is common for financial institutes.

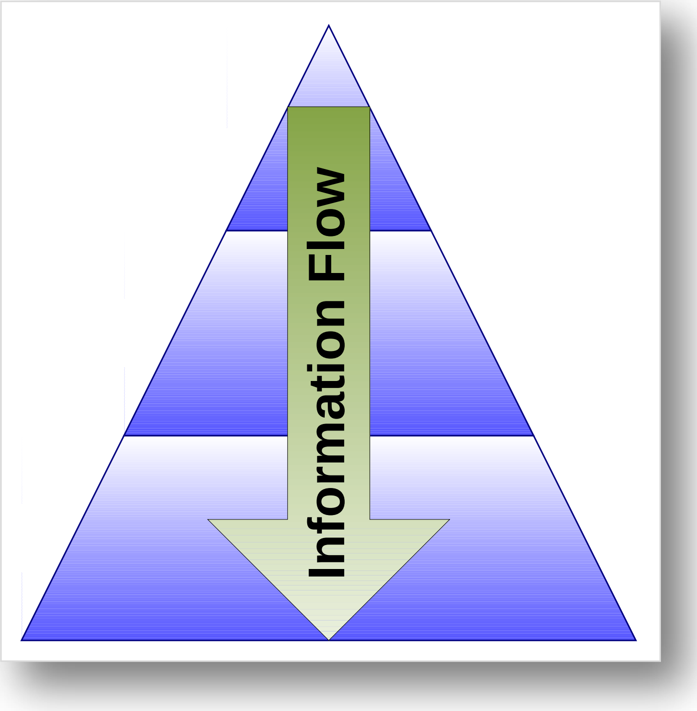


Figure 1: Information flow with MAC

Because the Bell-LaPadula and Biba models enforce a hierarchical information flow, they are less useful in commercial business, which organization is often a matrix style rather than hierarchical. These models can be applied to parts of the organization however. For example: Bell-LaPadula for Research and Development, to protect confidential new product information to leak out to sales persons and Biba for Finance departments to make sure financial data cannot be modified by unauthorized persons.

7.1.2 DISCRETIONARY ACCESS CONTROL

The most commonly used access model in commercial business is the Discretionary Access model (DAC). With this model, each resource (folder or file) has an owner assigned to it. The owner of the resource is free to assign access permissions to the resource to other users. In daily practice, permissions are most times assigned by system administrators on behalf of the owner of the resource. The owner might not even have the technical permissions to change permissions of the resource he owns.

DAC is highly flexible, because the owner of the data is able to assign permissions himself. This flexibility however, makes it difficult to maintain and audit.

Most common file server operating systems, including Microsoft Windows, Linux and Apple OS use this model by default.

7.1.3 ROLE BASED ACCESS CONTROL

More controllable and auditable than DAC and more flexible than MAC, is Role Based Access Control (RBAC). With RBAC, functional roles will be defined, such as Sales Manager, Director Operations, Works Council Member, etc. There is a many to many relation between users and roles. A user can have multiple roles and a role can be assigned to multiple users. See figure 1 for an example of a RBAC structure.

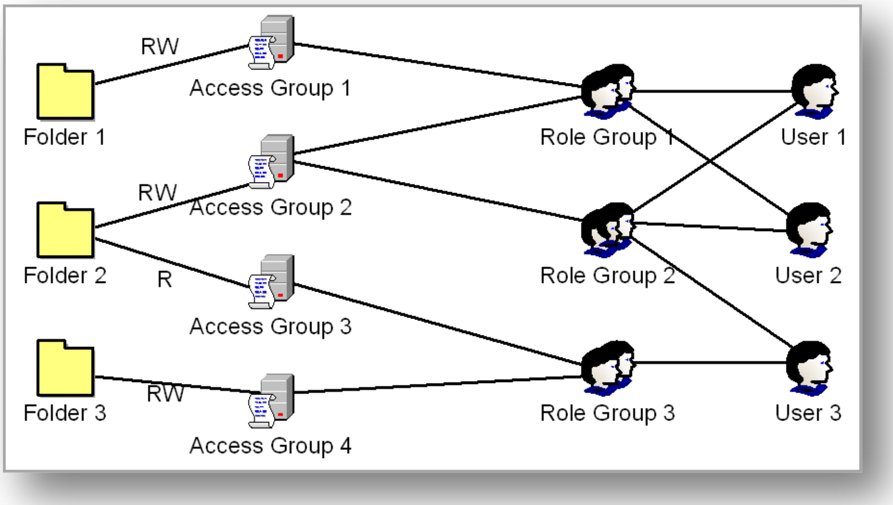


Figure 2: Graphical presentation of the RBAC model

Of these three access models, Role Based Access Control most closely matches Emerson's requirements. It is more controllable than DAC and more flexible than MAC. Basically it combines the best of both worlds.

There is however a downside to RBAC: it is not possible to enforce it within Microsoft Window's NTFS file system. This means that periodically checks are needed to check whether the file server security still complies with the RBAC setup.

7.2 LIMITATIONS TO GROUP NESTING

Separating groups defining permissions and groups describing roles has one major downside in a large Microsoft Active Directory domain like Emerson is using. Every group a user is a member of, whether it is directly or by nesting one group into another, adds that group's SID to the user's Kerberos token. This Kerberos token is limited in size to 12 kilobytes, which is equivalent to approximately 70 to 120 SIDs.

Especially when common groups like 'Domain Users' are made member of other groups, the limit of 70-120 groups can be reached easily. This results in users being member of groups they don't need to.

For this reason, it is not recommended to make such a group member of a group describing permissions, but to grant such a group direct permissions on the resource.

7.3 GOVERNMENTAL REGULATIONS

Emerson, being an American company, has to comply with the United States Federal laws. One of these Federal laws is the Sarbanes-Oxley (SOX) act. This act, a result of some large financial fraud cases, like the Enron and WorldCom cases, requires companies to take measures that make it impossible for an individual to practice fraud. It contains a lot of articles, mainly targeted at financial processes and upper management of the company. Some articles however do touch IT. For example: an individual must not be able to enter a purchase order, book the goods as received and approve the invoice. One could practice fraud by ordering goods for their own benefit. This system of separating task capabilities is within Emerson known as 'Segregation of Duties'

At this moment Segregation of Duties seems not applicable for the file server security, but needs to be kept in mind when applying permissions to folders.

7.4 CONVERGING PERMISSIONS

Another aspect of dealing with folder permissions is permission convergence. This aspect is not found during analysis, but is something I frequently run into in daily management of the file server.

Converging permissions are situations where more people need access to lower-level folders than to the root-level folder.

Especially for read permissions this is something to plan carefully. If not carefully planned for, there is the risk a user has read access to a specific folder, but not to its parent folder. If that is the case, the user is unable to browse through the folder structure to the desired folder. See for example figure 2, where in the left folder tree, a user has read access to folder A, Read & Modify access to folder D and is denied access to folder C. Without having read access to folder C however, the user is not able to browse from folder A to D. A better solution would have been to create another sub folder of C, i.e. folder E. This folder E should contain the data which is restricted for the user. Next, the user could be granted Read access to folder C. The right folder tree in figure 2 shows this.

One option to eliminate this is to create a folder tree which acts like a corridor with doors accessing rooms. All users can traverse this corridor. Next to the corridor are rooms, some accessible, some not. Goods are stored in the rooms, not in the corridors.

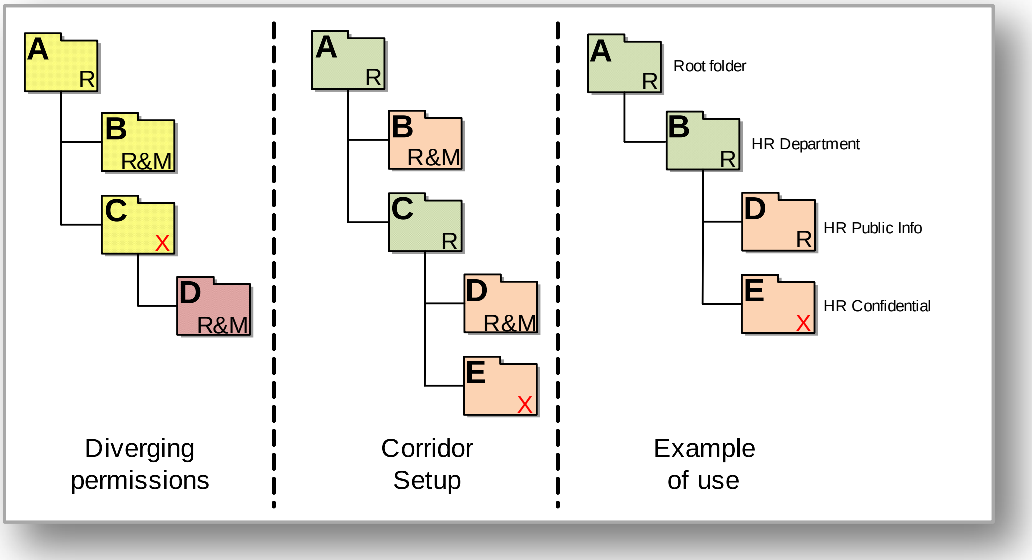


Figure 3: diverging permissions

Equivalent to this is the second folder structure in figure 2. Folders A and C are the corridors, folders B, D and E are the rooms. Being corridors, folders A and C should not contain data, only subfolders.

This setup makes it easy for users to browse the file server, and for departments to share some of their data with users outside their department. For example: in the third folder structure in figure 2, folder B is the HR department folder and folder D the public information of HR. When the structure is properly setup, any user can browse to the HR folder and access the HR public information. Only authorized users can however access the HR confidential data. By granting only read permissions to the corridor folder, one avoids sensitive data being accidentally stored there. This is a very important part of the design, since users are not aware which permissions other users have to their folders.

7.5 NEW SECURITY DESIGN

The access structure for the future state will be as follows:

- Each folder which requires specific permissions to be assigned will have dedicated security groups, one for each required permission type. I.e. Read and Read & Modify.
- Each of these security groups will contain role groups.
- No individual users will have permissions on folders directly.
- No role groups will have permissions on folders directly.
- The use of the '*Domain Users*' group must be eliminated because it contains all Emerson users. For generic access, the groups '*NLEDE-All Users'* (all Emerson Flow users), '*PMEMA_Users'* (all Emerson Process Management Europe users) or '*PM_Users'* (all Emerson Process Management users) are available. To avoid 'token bloat' (see chapter 7.1) these groups must be assigned permissions to folders directly instead of nesting them into permission groups.
- Each folder with specific permissions set, must be documented with the following attributes:
    - Group for read access
    - Group for modify access
    - Owner / approver
- Each role must be documented with the following attributes:
    - Role group
    - Approver
    - Users assigned to the role

7.6 RESTRUCTURING FOLDER STRUCTURE

To make the folder structure more orderly, the number of root level folders has to be reduced. The folder hierarchy for subsequent folders should follow the organization's structure. As input for this, I used the organizational charts, which have been created by the human resources department.

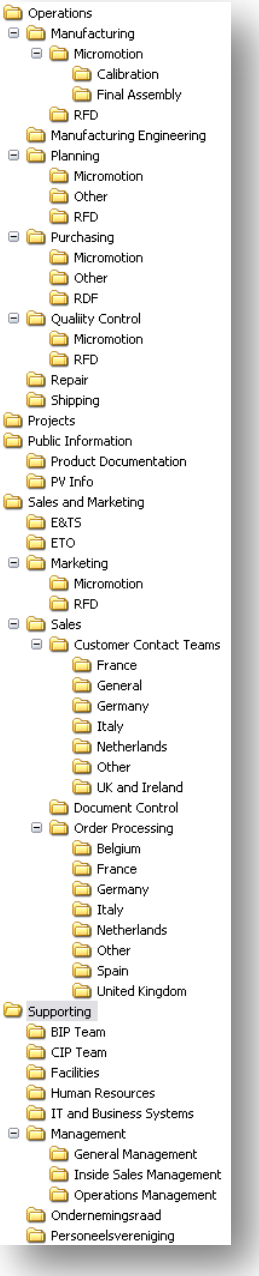
My proposal is to limit it to the following:

- Operations\
- Projects\
- Public Information\
- Sales and Marketing\
- Supporting\

Below these root-level folders subfolders for the departments will be created. Figure 4shows an example how the future folder structure can look.

As Emerson Flow does works in departments, and secondary has divisional or regional responsibilities, I decided to place the divisional or regional separation below the department level.

Restructuring the actual data into this new structure requires close collaboration between the systems administrator and the owners / users of the data. This is out of scope for this project and will be done when a new file server is deployed. Deployment of this new file server is scheduled for August 2010. The data will be migrated to the new server one department at a time.



```
Operations
    Manufacturing
        Micromotion
            Calibration
            Final Assembly
        RFD
    Manufacturing Engineering
    Planning
        Micromotion
        Other
        RFD
    Purchasing
        Micromotion
        Other
        RDF
    Qualiity Control
        Micromotion
        RFD
    Repair
    Shipping
Projects
Public Information
    Product Documentation
    PV Info
Sales and Marketing
    E&TS
    ETO
    Marketing
        Micromotion
        RFD
    Sales
        Customer Contact Teams
            France
            General
            Germany
            Italy
            Netherlands
            Other
            UK and Ireland
        Document Control
        Order Processing
            Belgium
            France
            Germany
            Italy
            Netherlands
            Other
            Spain
            United Kingdom
Supporting
    BIP Team
    CIP Team
    Facilities
    Human Resources
    IT and Business Systems
    Management
        General Management
        Inside Sales Management
        Operations Management
    Ondernemingsraad
    Personeelsvereniging
```

Figure 4: Proposed folder structure

7.7 MANAGEMENT

In order to keep the new structure structured, it must be properly managed.

Microsoft's NTFS file system does not provide metadata fields for files and folders. This is needed however to record approvers for each folder with unique permissions defined.

Microsoft Active Directory groups do have some additional fields available. The 'Managed By' field for example, can be used to identify an approver. It is however not possible to view those in a list view, or to search based on those fields.

These limitations made me conclude that we need some kind of database to record all permissions.

Within Emerson Flow, there are two database servers available, one running Microsoft SQL Server 2005 and one Running Oracle 10g. Using one of these two databases however, requires an application to be developed. Since I do not have application development skills and our developer already has a large workload, it is not very likely a custom application can be developed within the timeframe of this project.

Another available system with (limited) database capabilities is Microsoft Office SharePoint Server 2007 (MOSS). MOSS is Microsoft's document management and collaboration system. One of the features it offers it to create 'Lists' these lists are presented in a table form and can contain user definable fields. These fields can contain text, numbers, dates and others. One of the nice features of these lists is that a field can be configured to lookup values in another list, giving it some database functionality. It is also possible to attach files to an entry in a list. Apart from this MOSS provides an index based search function, making it easy to find documents or records.

Because MOSS is totally web-based, it is also easy to access by people all over the world (for example: Service Desk agents in Manila)

For these reasons and because the use of MOSS is encouraged within Emerson, I decided to use MOSS for management of the file server security structure.

7.7.1 SHAREPOINT LIST SETUP

For management of the permissions and roles, I have created two SharePoint lists:

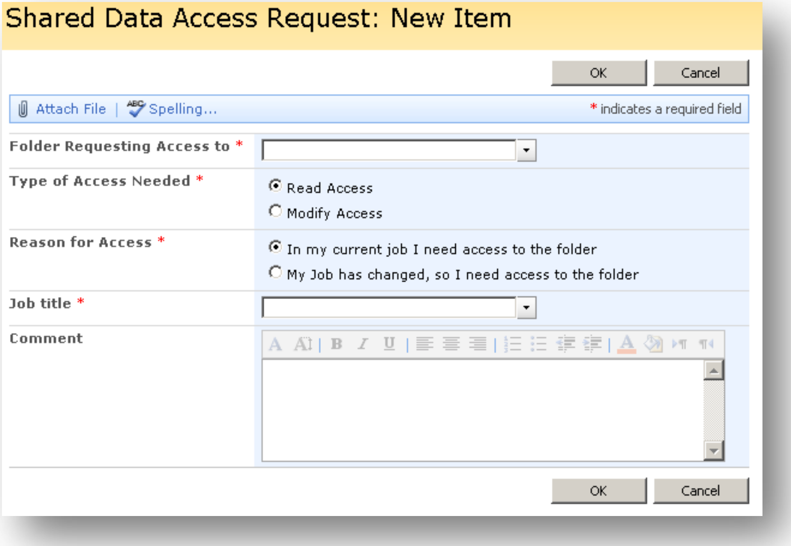
1. Folder Permission Assignment
   In this list, each folder with unique permissions will have a record. Each record will contain the folder location, name of the read and modify groups, name(s) of the approver(s) and the assigned roles. Appendix B shows an example of how the list and the form for entering Folder Permission Assignment data will look like.
2. Role Assignment
   In this list, each role will have a record. Each record will contain the role name, associated Active Directory group, associated users and the name(s) of the approver(s). Appendix C shows an example of how the list and the form for entering Role Assignment data will look like.

The assignment of roles to folder permissions is based on a link between the two lists.

When someone needs to know which users have access to a specific folder, he can just click the role(s) assigned to the folder and the members of this/these role(s) are displayed.

7.7.2 SERVICE DESK PROCEDURE

To make it possible for the Service Desk, it is necessary that they receive requests in a consistent form. To accomplish this I have designed a SharePoint form as shown in Figure 5.



Shared Data Access Request: New Item

* indicates a required field

Folder Requesting Access to *	
Type of Access Needed *	● Read Access ○ Modify Access
Reason for Access *	● In my current job I need access to the folder ○ My Job has changed, so I need access to the folder
Job title *	
Comment	

Figure 5: Example of how the access request form will look.

When this form is filled out by a user, an email is sent to the Service Desk. The Service Desk will refer to their standard procedure for change requests. This standard procedure will refer to a new procedure, which is based on the flowchart shown in Appendix A.

This flowchart tells the Service Desk agent which steps to take and finally refers to the general Active Directory management procedure.

8 IMPLEMENTATION

The Implementation can be split in the following steps:

1. Creation of an empty folder structure.
2. Creation of permission and role groups.
3. Creation of the SharePoint lists.
4. Assigning permissions to roles and roles to users.
5. Updating assignments in the SharePoint lists.
6. Communicate data migration process to all users.
7. Copying existing data into the new folder structure.
8. Make old data unavailable.
9. Clean old, unused groups.

Steps 1, 2 and 3 have been completed within this project.

Steps 4 and 5 have been completed partially within this project, and take approximately another 40 hours to complete.

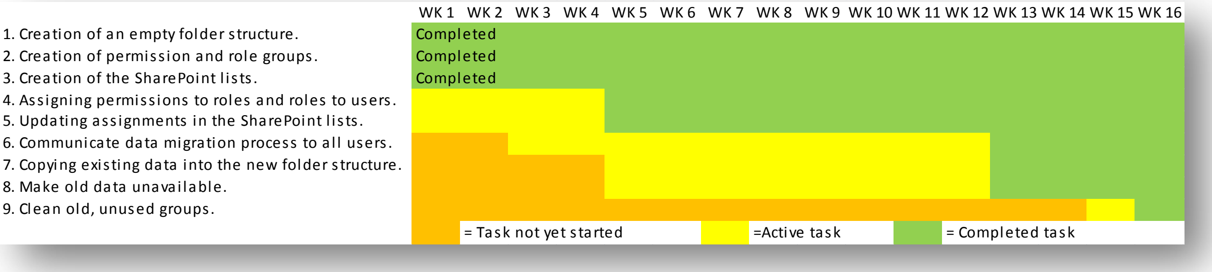
Step 6, communication will take about 2 hours, and needs to be completed at least 5 working days before step 7 starts. Also after each folder in step 7 users must be informed about the new location of the data.

Step 7, copying data will take 1 to 10 hours preparation time per root-level folder, depending on the complexity of the current security. Estimated total needed preparation time is 80 hours. The preparation needs to be done in close coordination with the data owner or department manager. Currently I estimate the time the data owner or department manager has to spend at 25% of the time I have to spend for a folder.

Step 8 will take about 15 minutes per root-level folder and needs to be completed per folder immediately after copying.

Step 9 must not be started before all others have been completed and a grace period of 2 weeks has past.

Assuming the maximum available project time is 25% per full workweek, the planning for the execution will be as shown in figure 5:



	WK 1	WK 2	WK 3	WK 4	WK 5	WK 6	WK 7	WK 8	WK 9	WK 10	WK 11	WK 12	WK 13	WK 14	WK 15	WK 16
1. Creation of an empty folder structure.	Completed	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
2. Creation of permission and role groups.	Completed	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
3. Creation of the SharePoint lists.	Completed	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
4. Assigning permissions to roles and roles to users.	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
5. Updating assignments in the SharePoint lists.	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
6. Communicate data migration process to all users.	🟧	🟧	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟩
7. Copying existing data into the new folder structure.	🟧	🟧	🟧	🟧	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟩
8. Make old data unavailable.	🟧	🟧	🟧	🟧	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟩
9. Clean old, unused groups.	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟨	🟩

🟧 = Task not yet started 🟨 =Active task 🟩 = Completed task

Figure 6: Implementation planning

The actual start date is depending on the availability of a new fileserver and storage infrastructure. This is planned for July 2010. Summer holidays have not been considered in this planning and may affect the finish date.

About 1 or 2 months after the implementation is completed, the new security model will be evaluated for effectiveness. This evaluation will be performed by me, the Manager IT & Business Systems and a third person from the business (non IT). This third person preferably will be the Compliance Manager.

If the security model appears to be effective I will share and promote it with the Emerson Process Management European standards teams, the clients and server teams in particular.

9 RECOMMENDATION / CONCLUSION

Analysis of the current file server security revealed several security threats and showed it is currently hard to manage.

To make it more secure, better manageable and compliant with Emerson's audit requirements, my recommendation is to implement the following:

- On the new fileserver, to be installed July 2010, create the new hierarchical folder structure.
- Create all the required permission groups and record them in the SharePoint list.
- Create all the required role groups, assign the roles to users and record it in the SharePoint list.
- Setup two SharePoint lists: one with folder permissions and one with role assignments.
- One department at a time, in coordination with the manager and employees of the department, identify how their data will fit into the new structure. If required additional folders and permission groups can be created. Then copy the data from the old to the new server, and make it inaccessible on the old server.
- Make the procedure for assigning permissions available for the Service Desk, and authorize them to change group memberships.

Finally, I can conclude that my suspicions about security threats and manageability were valid. I am confident however that when my recommendations are complied with, the file server security will meet Emerson's requirements and will be much better manageable.

BIBLIOGRAPHY

Books:

Harris, S. (2008). *All-In-One CISSP Exam Guide.* New York, USA: McGraw-Hill.

Internet resources:

de Clerq, J. (2003, May 12). *Role Based Access Control*. Retrieved April 11, 2010, from Windows IT Pro: http://www.windowsitpro.com/article/security/rolo-based-access-control.aspx

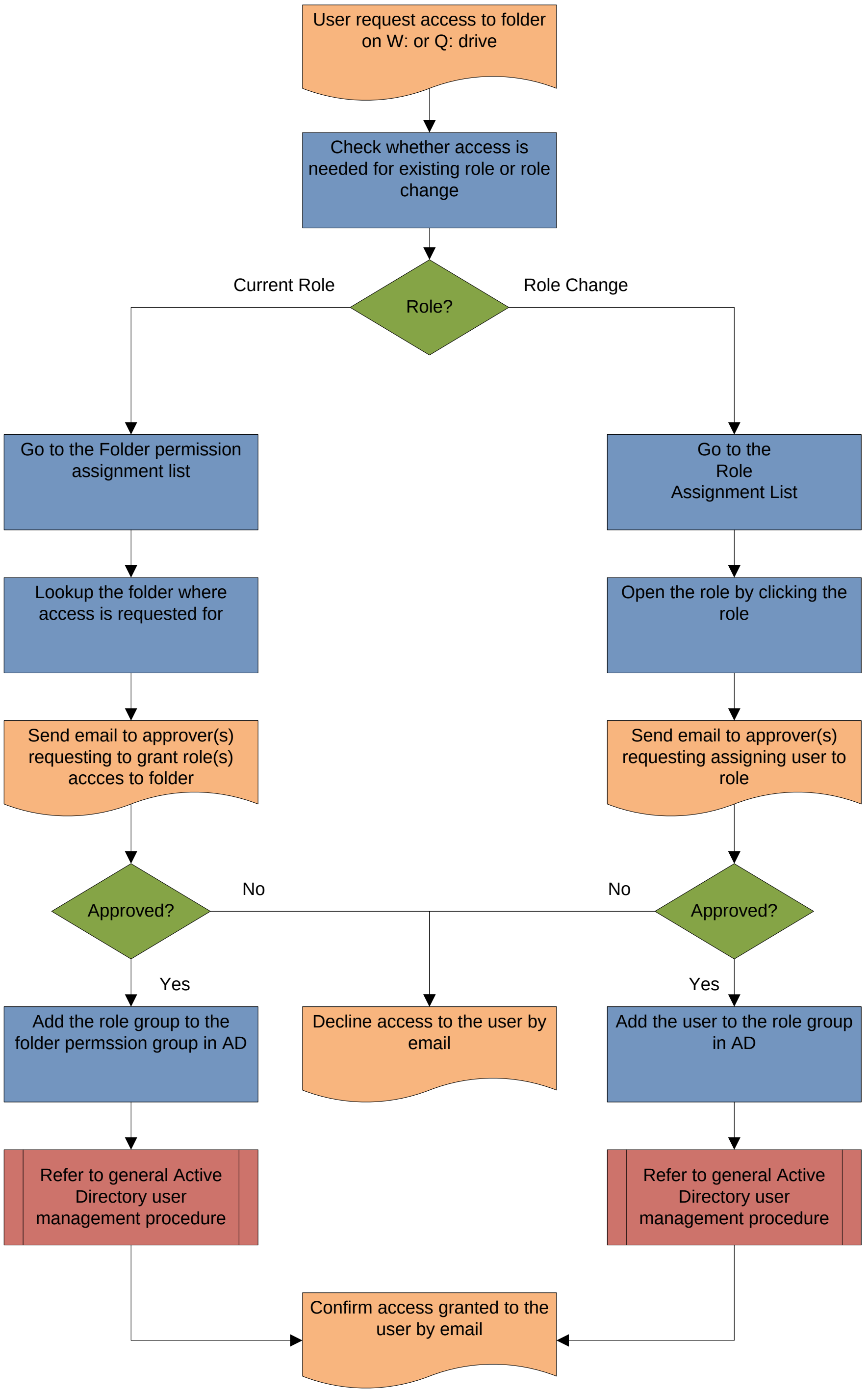
Role based Access Control (RBAC) and Role Based Security. (n.d.). Retrieved April 11, 2010, from NIST: http://csrc.nist.gov/groups/SNS/rbac

APPENDICES

APPENDIX A: SERVICE DESK PROCEDURE

User to Folder permission assignment procedure with approval workflow

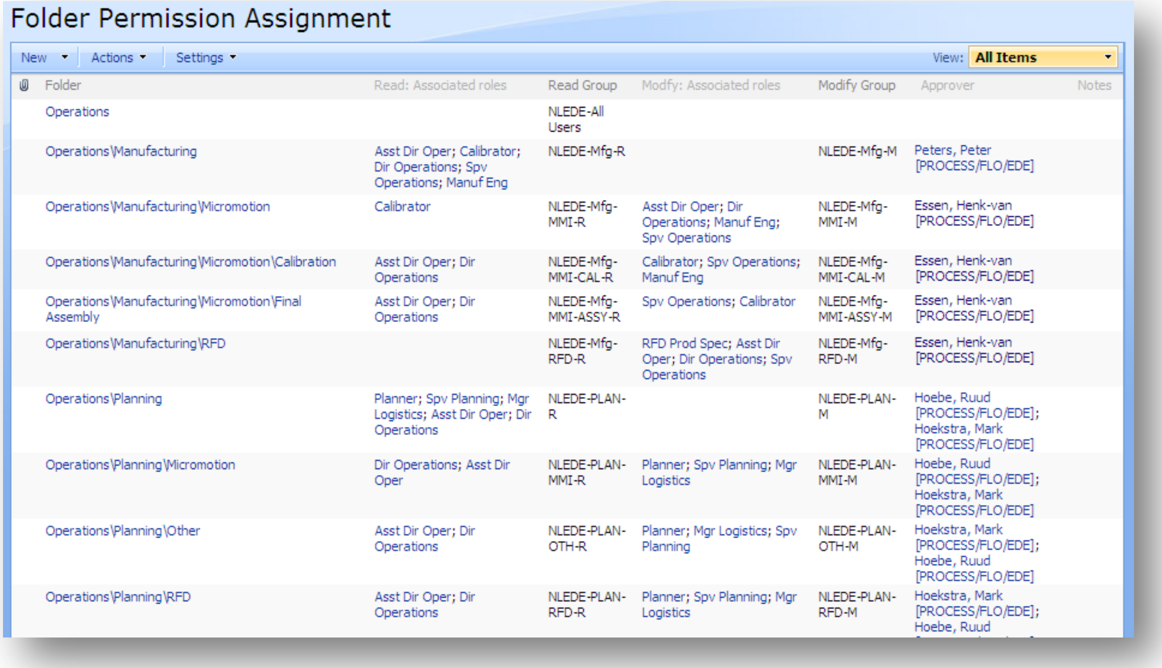
Follow this flowchart step-by-step to grant a user access to a folder.
Only accept request by SharePoint form. If a user request access by email, please redirect them to the SharePoint form.


User request access to folder on W: or Q: drive
Check whether access is needed for existing role or role change
Role?
Current Role
Role Change
Go to the Folder permission assignment list
Lookup the folder where access is requested for
Send email to approver(s) requesting to grant role(s) accces to folder
Approved?
No
Yes
Add the role group to the folder permssion group in AD
Refer to general Active Directory user management procedure
Go to the Role Assignment List
Open the role by clicking the role
Send email to approver(s) requesting assigning user to role
Approved?
No
Yes
Add the user to the role group in AD
Refer to general Active Directory user management procedure
Decline access to the user by email
Confirm access granted to the user by email

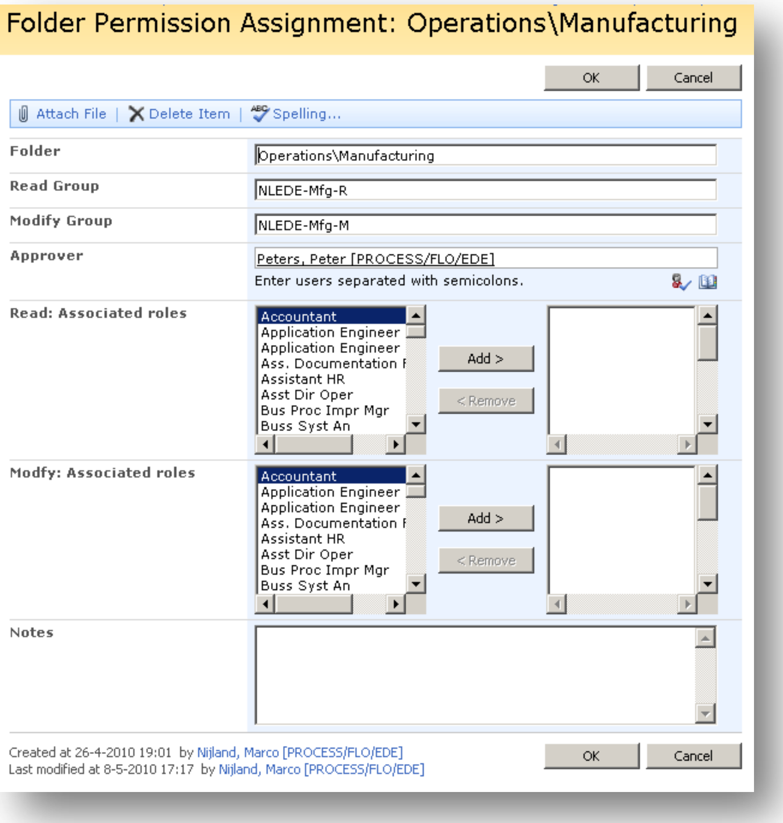
Links to locations listed in the chart:

Folder Permissions List
Role Assignment List

APPENDIX B: SHAREPOINT FOLDER PERMISSIONS ASSIGNMENT LIST



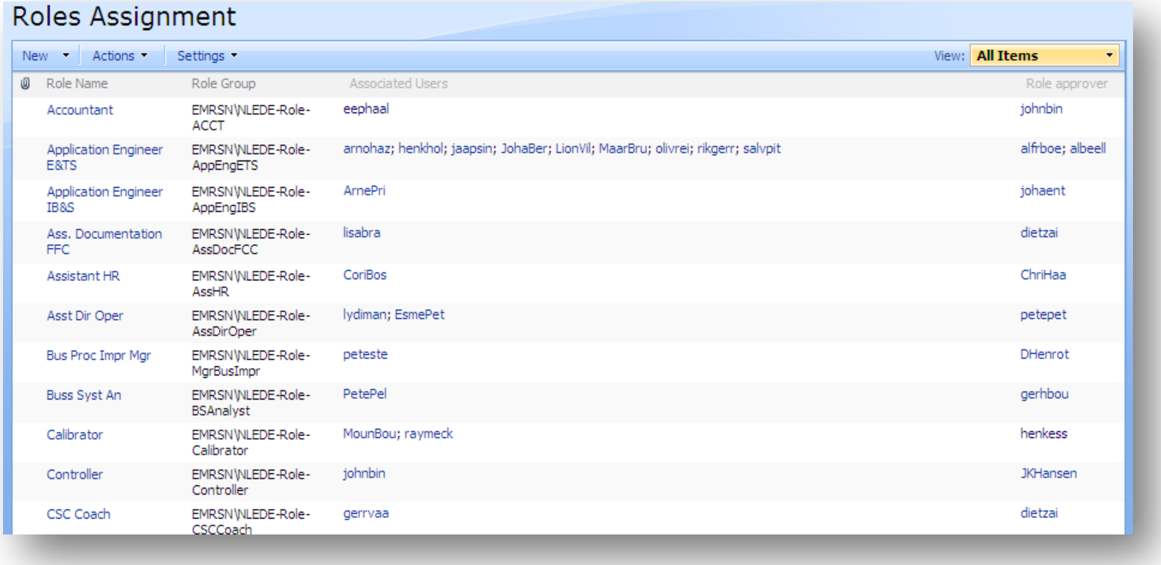
Folder	Read: Associated roles	Read Group	Modfy: Associated roles	Modify Group	Approver	Notes
Operations		NLEDE-All Users				
Operations\Manufacturing	Asst Dir Oper; Calibrator; Dir Operations; Spv Operations; Manuf Eng	NLEDE-Mfg-R		NLEDE-Mfg-M	Peters, Peter [PROCESS/FLO/EDE]	
Operations\Manufacturing\Micromotion	Calibrator	NLEDE-Mfg-MMI-R	Asst Dir Oper; Dir Operations; Manuf Eng; Spv Operations	NLEDE-Mfg-MMI-M	Essen, Henk-van [PROCESS/FLO/EDE]	
Operations\Manufacturing\Micromotion\Calibration	Asst Dir Oper; Dir Operations	NLEDE-Mfg-MMI-CAL-R	Calibrator; Spv Operations; Manuf Eng	NLEDE-Mfg-MMI-CAL-M	Essen, Henk-van [PROCESS/FLO/EDE]	
Operations\Manufacturing\Micromotion\Final Assembly	Asst Dir Oper; Dir Operations	NLEDE-Mfg-MMI-ASSY-R	Spv Operations; Calibrator	NLEDE-Mfg-MMI-ASSY-M	Essen, Henk-van [PROCESS/FLO/EDE]	
Operations\Manufacturing\RFD		NLEDE-Mfg-RFD-R	RFD Prod Spec; Asst Dir Oper; Dir Operations; Spv Operations	NLEDE-Mfg-RFD-M	Essen, Henk-van [PROCESS/FLO/EDE]	
Operations\Planning	Planner; Spv Planning; Mgr Logistics; Asst Dir Oper; Dir Operations	NLEDE-PLAN-R		NLEDE-PLAN-M	Hoebe, Ruud [PROCESS/FLO/EDE]; Hoekstra, Mark [PROCESS/FLO/EDE]	
Operations\Planning\Micromotion	Dir Operations; Asst Dir Oper	NLEDE-PLAN-MMI-R	Planner; Spv Planning; Mgr Logistics	NLEDE-PLAN-MMI-M	Hoebe, Ruud [PROCESS/FLO/EDE]; Hoekstra, Mark [PROCESS/FLO/EDE]	
Operations\Planning\Other	Asst Dir Oper; Dir Operations	NLEDE-PLAN-OTH-R	Planner; Mgr Logistics; Spv Planning	NLEDE-PLAN-OTH-M	Hoekstra, Mark [PROCESS/FLO/EDE]; Hoebe, Ruud [PROCESS/FLO/EDE]	
Operations\Planning\RFD	Asst Dir Oper; Dir Operations	NLEDE-PLAN-RFD-R	Planner; Spv Planning; Mgr Logistics	NLEDE-PLAN-RFD-M	Hoekstra, Mark [PROCESS/FLO/EDE]; Hoebe, Ruud	



Folder	Operations\Manufacturing
Read Group	NLEDE-Mfg-R
Modify Group	NLEDE-Mfg-M
Approver	Peters, Peter [PROCESS/FLO/EDE] Enter users separated with semicolons.
Read: Associated roles	
Modfy: Associated roles	
Notes	

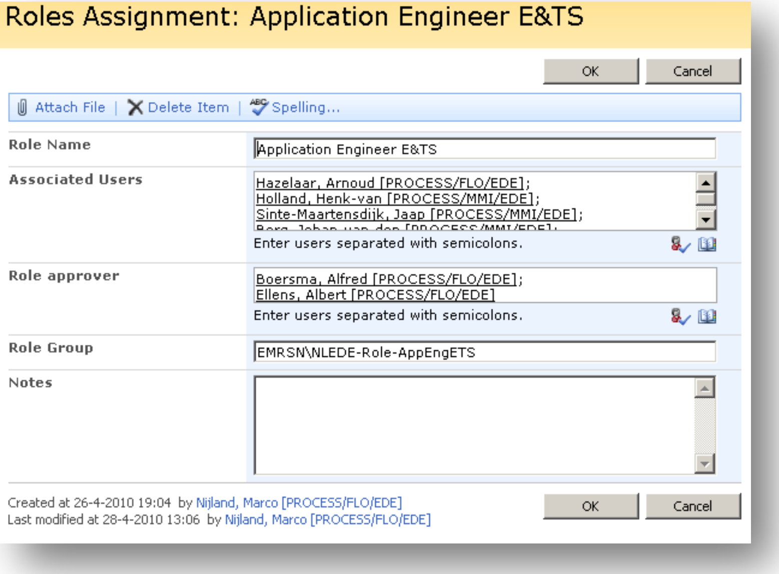
Created at 26-4-2010 19:01 by Nijland, Marco [PROCESS/FLO/EDE]
Last modified at 8-5-2010 17:17 by Nijland, Marco [PROCESS/FLO/EDE]

APPENDIX C: SHAREPOINT ROLES ASSIGNMENT LIST



Roles Assignment

Role Name	Role Group	Associated Users	Role approver
Accountant	EMRSN\NLEDE-Role-ACCT	eephaal	johnbin
Application Engineer E&TS	EMRSN\NLEDE-Role-AppEngETS	arnohaz; henkhol; jaapsin; JohaBer; LionVil; MaarBru; olivrei; rikgerr; salvpit	alfrboe; albeell
Application Engineer IB&S	EMRSN\NLEDE-Role-AppEngIBS	ArnePri	johaent
Ass. Documentation FFC	EMRSN\NLEDE-Role-AssDocFCC	lisabra	dietzai
Assistant HR	EMRSN\NLEDE-Role-AssHR	CoriBos	ChriHaa
Asst Dir Oper	EMRSN\NLEDE-Role-AssDirOper	lydiman; EsmePet	petepet
Bus Proc Impr Mgr	EMRSN\NLEDE-Role-MgrBusImpr	peteste	DHenrot
Buss Syst An	EMRSN\NLEDE-Role-BSAnalyst	PetePel	gerhbou
Calibrator	EMRSN\NLEDE-Role-Calibrator	MounBou; raymeck	henkess
Controller	EMRSN\NLEDE-Role-Controller	johnbin	JKHansen
CSC Coach	EMRSN\NLEDE-Role-CSCCoach	gerrvaa	dietzai



Roles Assignment: Application Engineer E&TS

Role Name	Application Engineer E&TS

Associated Users	Hazelaar, Arnoud [PROCESS/FLO/EDE];
	Holland, Henk-van [PROCESS/MMI/EDE];
	Sinte-Maartensdijk, Jaap [PROCESS/MMI/EDE];
	Borg, Johan van den [PROCESS/MMI/EDE];
	Enter users separated with semicolons.

Role approver	Boersma, Alfred [PROCESS/FLO/EDE]; Ellens, Albert [PROCESS/FLO/EDE] Enter users separated with semicolons.
Role Group	EMRSN\NLEDE-Role-AppEngETS
Notes	

Created at 26-4-2010 19:04 by Nijland, Marco [PROCESS/FLO/EDE]
Last modified at 28-4-2010 13:06 by Nijland, Marco [PROCESS/FLO/EDE]

APPENDIX D: ACRONYMS AND DEFINITIONS

AD	Active Directory, Microsoft's hierarchical structure to manage users, groups and other security objects.
Bell-LaPadula	A data integrity protection model
Biba	A data confidentiality protection model
DAC	Discretionary Access Control, an access control model
File Server	A Microsoft Windows 2003 server configured to be used as a central storage location for documents.
MAC	Mandatory Access Control, an access control model
MMI	MicroMotion Inc, one of Emerson's divisions with presence in the Ede Netherlands site.
NTFS	New Technology File System. A technology, proprietary to Microsoft, to store files on a hard disk, first introduced with Microsoft Windows NT 3.1
RBAC	Role Based Access Control, an access control model
RFD	Rosemount Flow Division, one of Emerson's divisions with presence in the Ede Netherlands site.
SOX	Sarbanes and Oxley, an American act to separate responsibilities within companies.