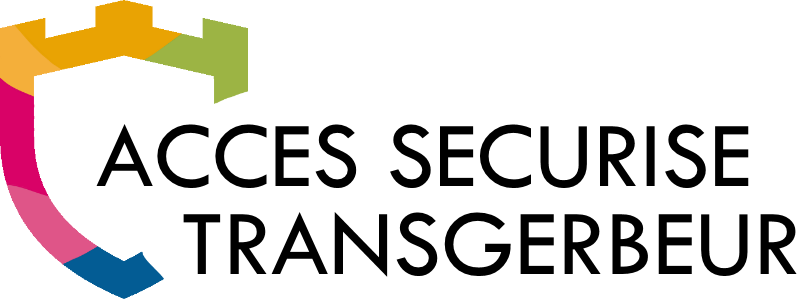
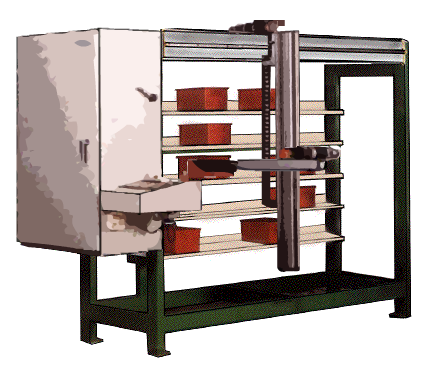
FORESTIER Edouard Session 2017

CHANCEREL Nicolas

LEHUCHER Sébastien

Projet BTS SN | Accès Sécurisé Transgerbeur







Professeur référent : Monsieur HOURDIN (BTS SN)

Monsieur GILBERT (BTS Maintenance)

SOMMAIRE

PRESENTATION DU PROJET 2

RESUME 3

ROLE PERSONNEL 4

SPECIFICATIONS FONCTIONNELLES 4

LECTURE D’UN BADGE 5

GESTION D’ACCES 5

VISUALISATION ETAT DE L’ACCES 5

CONSULTATION HISTORIQUE 6

CREATION BADGE D’ACCES 6

GESTION DES BADGES 6

SPECIFICATIONS NON FONCTIONNELLES 7

CONTRAINTE FINANCIERES 7

CONTRAINTE DE DEVELOPPEMENT 7

CONTRAINTE FIABILITE, SECURITE 7

IHM  7

ETAT DU SYSTEME 7

GESTION DES BADGES 8

Technologies 11

MODBUS TCP 11

WPF 11

LANGAGES 11

Analyse 11

AFFICHAGE ETAT SYSTEME 11

GESRION DES BADGES 11

HISTOTIQUE 11

PRESENTATION DU PROJET

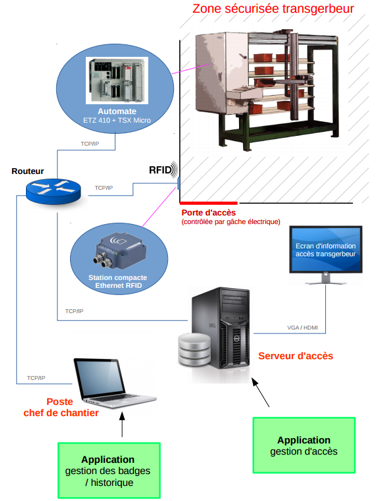
Résume :

Le transgerbeur est un système robotisé sur 3 axes, capable de stocker et déstocker des caisses référencées sur ordre d’un opérateur. Nous souhaitons, à travers ce projet, sécuriser l’accès au transgerbeur grâce à une gestion d’accès par badge.

Les opérateurs pourront y accéder selon leur niveau de qualification et selon son état (Marche | Arrêt | en cycle). Une Serrure électrique sera commandée par l’automate pour contrôler l’accès.

L’enregistrement de toutes les tentatives d’accès réussies ou échouées permettra à une personne responsable d’avoir un suivi.

Synoptique du système avec gestion d’accès



Partie  
 à réaliser

############

Rôle Personnel :

Opérateur :

* Peut rentrer que si l’automate est Arrêter

Technicien Supérieur :

* Peut rentrer si l’automate est :
  + Arrêter
  + En Marche sans cycle
  + En Marche Avec cycle

Chef de chantier :

* Peut ajouter un nouvel utilisateur
* Peut modifier un utilisateur (ex : changer son rôle)
* Peut supprimer un utilisateur (ATTENTION : son compte est conservé), son état passe en « supprimé »
* Peut suspendre un utilisateur (ex : congé maladie), sont état passe en « suspendu »
* Peut changer l’état d’un utilisateur en « actif »

SPECIFICATIONS FONCTIONNELLES

Lecture d’un Badge RFID :

La lecture du badge RFID se fait par une tête de lecture RFID (Schneider XGCS850C201) reliée au réseau Ethernet. Le serveur Communique avec elle en ModBus TCP.

Le lecteur RFID est en attente d’un badge. Lorsqu’elle détecte la présence d’un badge RFID, il récupère le TAG RFID puis répond au serveur d’accès avec en données, le TAG RFID.

Gestion d’accès :

Après la lecture du Badge, le serveur d’accès va chercher à identifier l’opérateur, grâce au TAG RFID, en effectuant une requête dans la base de données.

Lorsque celui-ci est identifié, le serveur effectue une demande d’accès auprès de l’automate pour un rôle donné.

Selon le rôle donné et l’état du système, l’automate déverrouille ou non l’accès, puis retourne une réponse au serveur pour indiquer l’opération qu’il vient d’effectuer (« Déverrouillage Porte » | « Tentative d’accès refusé »), puis retourne son état au moment de la demande.

Visualisation de l’état de l’accès :

Un écran placé à proximité de la porte indiquera l’état de l’automate et de la serrure électrique.

Etat pour l’automate :

* Arrêt
* Marche, aucun cycle en cours
* Marche, Cycle en cours

Etat pour la serrure électrique :

* Accès Refusé
* Accès Autorisé

Consultation de l’historique des accès :

Le chef de chantier peut consulter une interface listant les demandes d’accès acceptées et refusées.

Les informations affichées sont :

* Le nom / prénom rôle de l’opérateur
* L’état du transgerbeur au moment du passage de badge
* La date et l’heure de la demande d’accès
* La réponse de l’automate (ouverture porte | déverrouillage non autorisé)

Interface de l’historique intégré à l’application de gestion des badges.

Création d’un badge d’accès :

La création d’un badge implique la création d’un utilisateur dans la base de données.

Un utilisateur aura :

* Des informations personnel (Nom, Prénom …)
* Un rôle (opérateur, chef de chantier, technicien)
* Un numéro de badge (TAG RFID)

\* Ces informations seront stockées dans la base de données.

Au passage du Badge, le TAG RFID sera récupéré, assigner à l’utilisateur, et le nom et prénom seront stockés dans la mémoire du badge RFID.

Une confirmation d’enregistrement sera affichée une fois l’opération terminé.

Un Badge peut être réutilisé mais ne doit pas être attribué à deux utilisateur en même temps. Il faudra donc vérifier si le TAG est déjà utilisé lors de la création de l’utilisateur, si oui, il faudra supprimer l’utilisateur précèdent.

Gestion des badges :

Le chef de chantier aura une application de gestion des badges où il pourra modifier les utilisateurs, et a une page de configuration pour modifier les informations des connexions à la station RFID et le serveur d’accès.

SPECIFICATIONS NON FONCTIONNELLES

Contraintes financières :

Budget alloué de **1200€** pour l’achat d’une station RFID ainsi que des badges RFID, à la charge de la section BTS maintenance de l’établissement.

Contraintes de développement :

Les logicielles seront développe en C# à l’aide du logiciel Microsoft Visual studio 2015.

Les données seront stockées sur un serveur de base de données MySQL, et héberge sur l’ordinateur serveur d’accès.

Les modules logiciels communiqueront en ModBus TCP avec la station compact RFID et l’automate TSX Micro.

Contraintes qualité :

L’application de gestion des badges pourra être installé sur tout poste connecté au réseau local de l’automate (WIFI | Filaire).

Une page de configuration des accès à la station RFID et au serveur de base de données sera accessible sur l’application de Gestion des badges.

Une démonstration devra être réalisée en fin de projet :

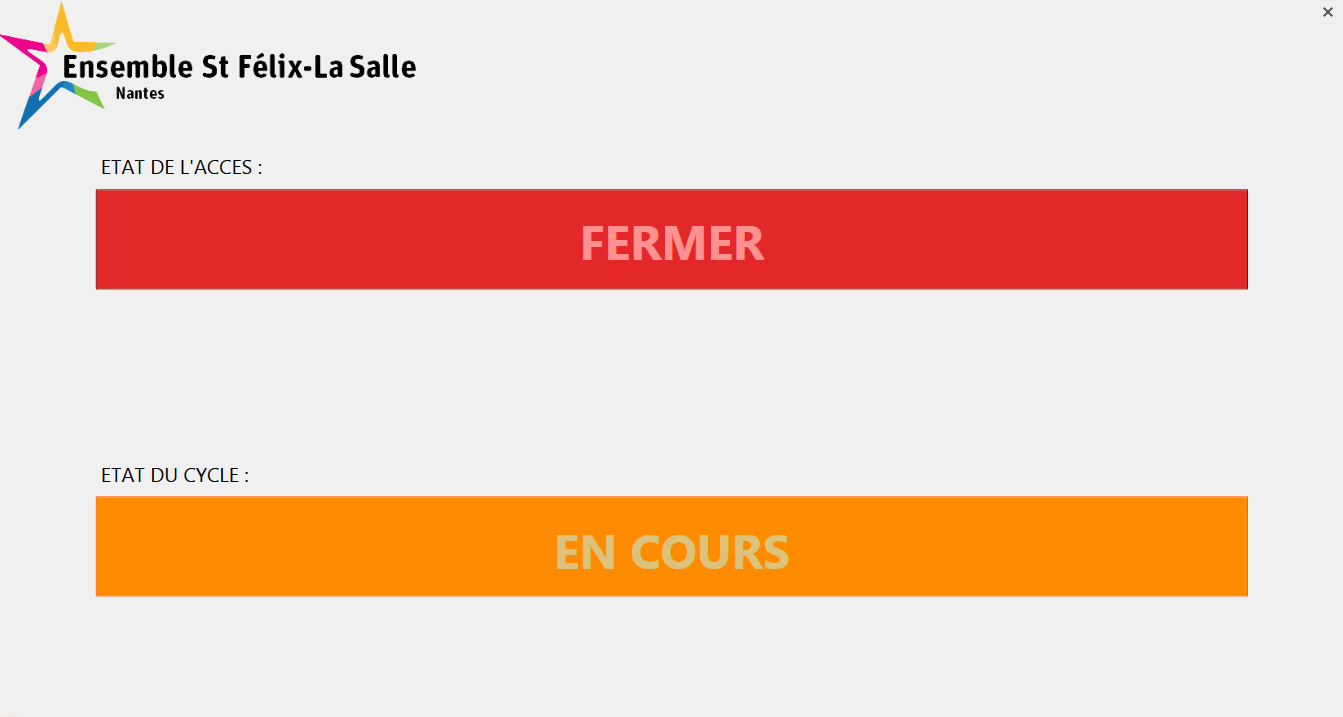
* Un chef de chantier peut créer, modifier, réattribuer des badges.
* Un passage de badge valide déverrouille l’accès, que l’indication est affiché à l’écran d’information opérateur, et qu’en conséquence l’historique indique cet accès.

Contraintes fiabilité, sécurité :

La gâche électrique libèrera l’accès que seulement si l’ensemble des informations demandés pour autorisé un accès seront réunis (TAG RFID, rôle, état cycle en cours)

IHM

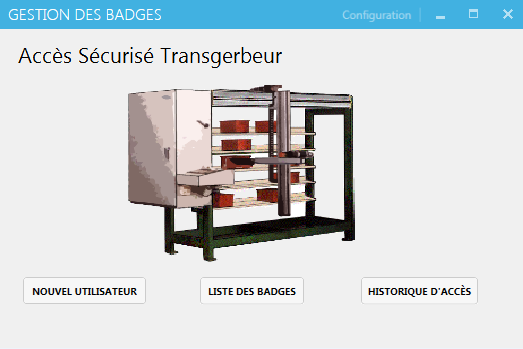
Affichage état du système



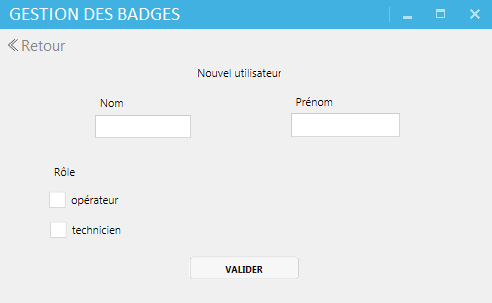
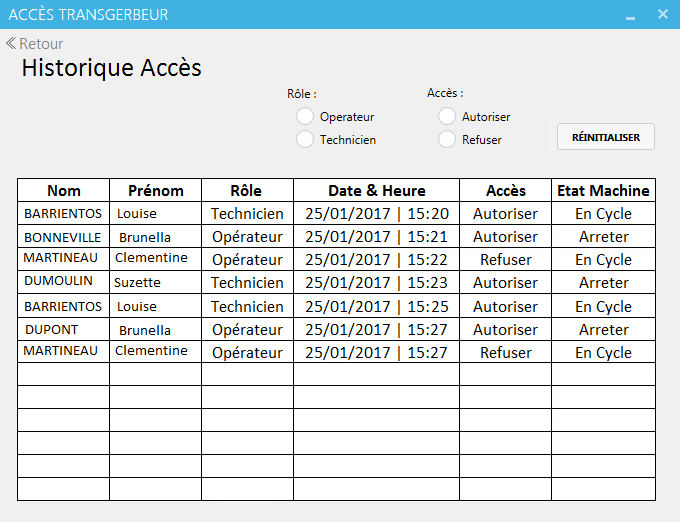
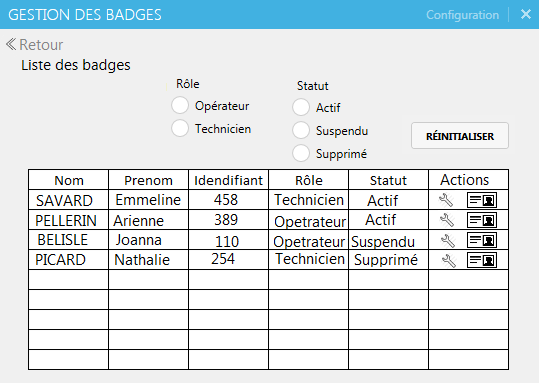
ETAT DE L’ACCES :  
 OUVERT :  
  
 FERMER :  


ETAT DU CYCLE MACHINE :  
 EN CYCLE :  
  
 PAS DE CYCLE :  
 FERMER :  


Gestion des badges

Page d’accueil du Logiciel :

Configuration du logiciel :  


Création nouvel utilisateurs  
  
  
Historique des accès :   
  
Liste des Badges   


Modifier un Utilisateur

|  |  |
| --- | --- |
| C:\Users\nicolas.chancerel\AppData\Local\Microsoft\Windows\Temporary Internet FilesContent.Word\IHM_Liste_Modif.png | Ce bouton servira à   enregistré les informations de   l’utilisateur dans le badges RFID  le chef de chantier devra   présenter un badge a la station   une fois ce bouton cliqué |

TECHNOLOGIES

ModBus TCP :

**MODBUS** est un protocole de communication non-propriétaire, utilisé pour des réseaux d'automates programmables, relevant du niveau 7 (applicatif) du Modèle OSI. En mode TCP il fonctionne sur le mode Client / Serveur. Les clients sont tous actifs, le serveur est complètement passif. Chaque client lit et écrit dans le serveur.

WPF :

**Windows Presentation Foundation** (WPF) (nom de code Avalon) est la spécification graphique de Microsoft .NET 3.0. Il intègre le langage descriptif XAML qui permet de l'utiliser d'une manière proche d'une page HTML pour les développeurs.

Langages utilisés :

Langage de programmation orienté objet : **C#**,

Langage de balisage : **XAML**,

Langage de gestion de données : **SQL**,

RESSOURCE MISE A DISPOSITION

Ressource matériel :

1 PC Windows 7 1 pour le serveur d’accès

1 PC portable Windows 7 pour le poste chef de chantier

1 station compact RFID OsiSense XG

Plusieurs Badges RFID

Un automate sur maquette, programmé pour le projet

Ressource logiciel :

Microsoft Visual Studio 2015 Community Edition

Bibliothèque .Net ModBusTCP

Wampserver sous Windows pour l’hébergement de l’application  
 Web et de la base de données de la solution

EVOLUTION POSSIBLE DU PROJET

Module de sécurité :

L’application de gestion des badges est le centre de ce système de sécurité, mais elle n’est elle-même pas suffisamment sécurisé (Session bureautique chef de chantier). Un module de sécurité du type authentification pourra être ajouter à l’application de gestion des badges pour contrôler les accès de l’application.

ANALYSES

Affichage état du système :

Diagramme de cas d’utilisation :

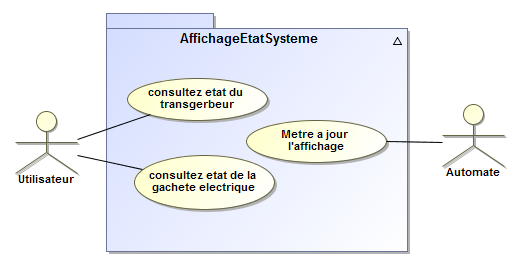
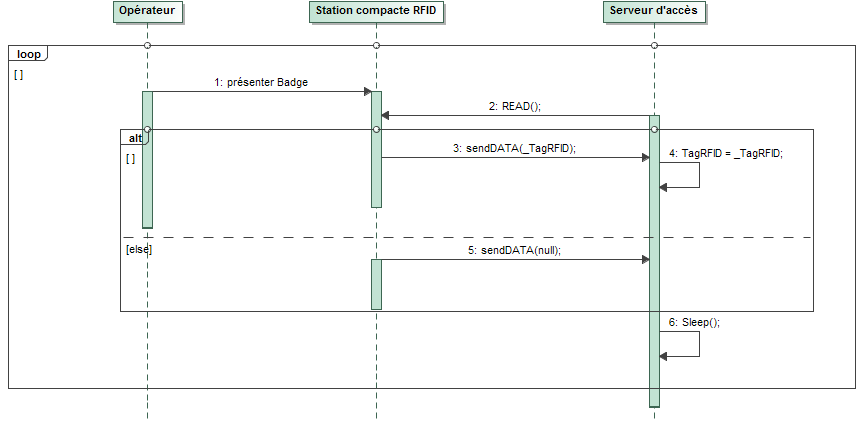
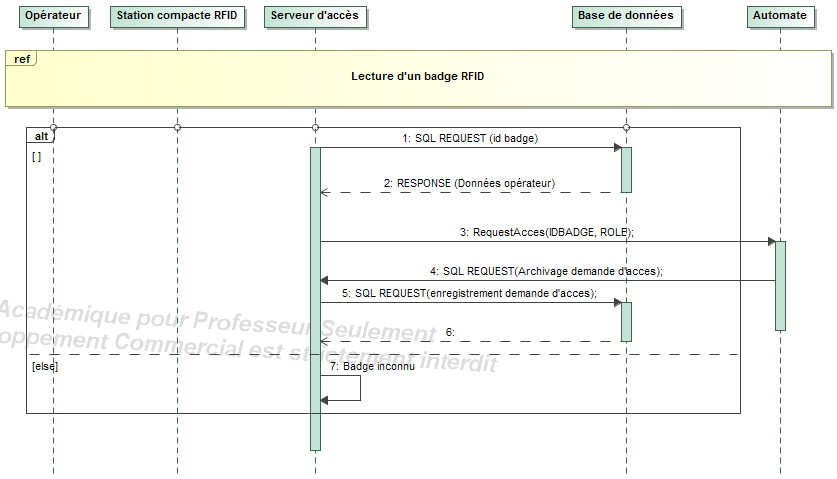


Diagramme de séquence :

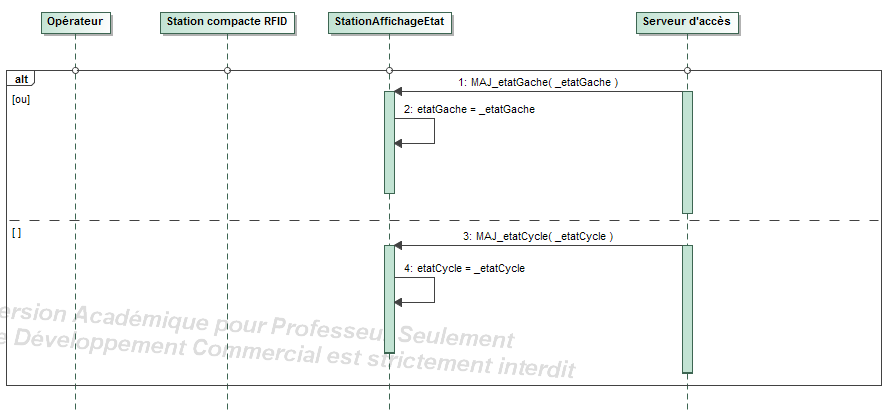
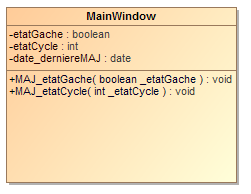
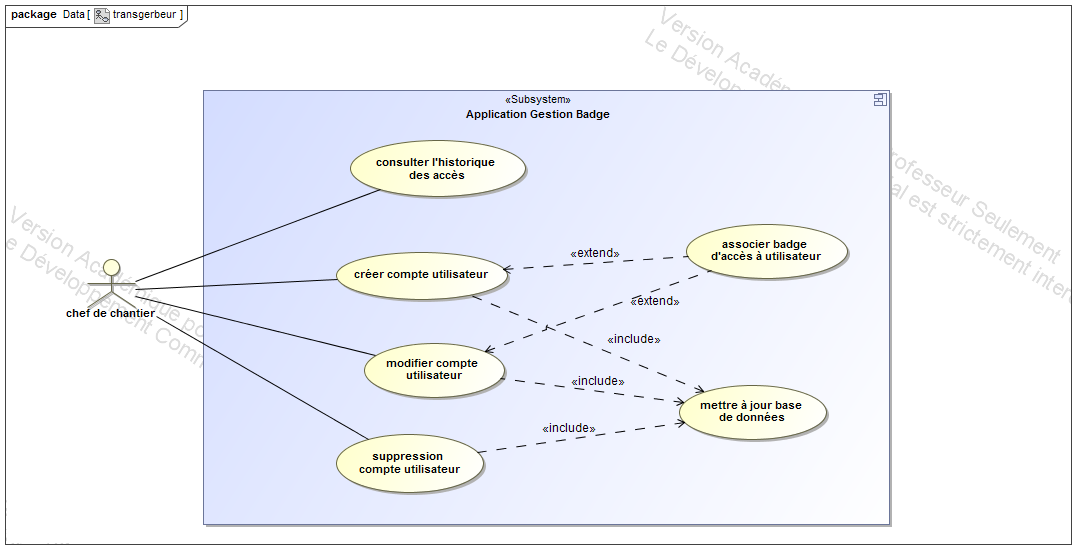


Diagramme de classe :



Application Gestion des badges :

Diagramme de cas d’utilisation :



Gestion des badges :

Diagramme de séquence :

Diagramme de classe :

Historique :

Diagramme de séquence :

Diagramme de classe :