CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS CEFET-MG

Curso de Engenharia de Automação Industrial

ESTUDO E DESENVOLVIMENTO DE UM SISTEMA DE CONTROLE DE ACESSO À AREAS RESTRITAS

MICHEL RESENDE CAMPOS

Araxá-MG

2016

Michel Resende Campos

ESTUDO E DESENVOLVIMENTO DE UM SISTEMA DE CONTROLE DE ACESSO À AREAS RESTRITAS

Trabalho de conclusão de curso apresentado ao curso de Engenharia de Automação Industrial do CEFET-MG Araxá, como requisito para a obtenção do título de Engenheiro de Automação Industrial.

Orientador: Dr. Henrique José Avelar
Coorientador: M.e Luis Paulo Fagundes.

Araxá-MG
2016

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA DE MINAS GERAIS CEFET-MG

Curso de Engenharia de Automação Industrial

Trabalho de conclusão de curso intitulado: “Estudo e desenvolvimento de um sistema de controle de acesso às áreas restritas”, de autoria do graduando. **Michel Resende Campos,** aprovada pelo seguinte banca examinadora:

Prof. Dr. Henrique José Avelar - Orientador
Instituição: Centro Federal de Educação Tecnológica de Minas Gerais
Assinatura: _____

Prof. M.e Luis Paulo Fagundes - Coorientador
Instituição: Centro Federal de Educação Tecnológica de Minas Gerais
Assinatura: _____

Prof. Dr. Mário Guimarães Júnior
Instituição: Centro Federal de Educação Tecnológica de Minas Gerais
Assinatura: _____

Prof. Dr. Admarço Vieira da Costa
Instituição: Centro Federal de Educação Tecnológica de Minas Gerais
Assinatura: _____

Data da aprovação: ___/ ___/___

Araxá, ___ de julho de 2016.

AGRADECIMENTO

Agradeço primeiramente a Deus pela proteção e por nunca ter me deixado desistir deste sonho.

Agradeço aos meus pais e irmãos pelo incentivo, à minha esposa Samanta que sempre segurou a barra nos momentos em que tive que me dedicar mais aos estudos do que à família e aos meus filhos Melissa e Samuel que me fazem querer todo dia ser uma pessoa melhor.

Agradeço também aos meus colegas de curso que batalharam todos esses anos ao meu lado e ao meu orientador e coorientador pelo apoio.

RESUMO

Algumas áreas dentro das empresas requerem controle de acesso e/ou do tempo de permanência de pessoas e/ou veículo. Isto devido ao risco eminente que esta atividade pode trazer a quem o executa e também como medida de controle para os gestores das áreas. Para supervisionar e controlar o acesso e a permanência das pessoas e dos equipamentos móveis nestas áreas é necessário o desenvolvimento de um sistema que faça tal controle. O presente trabalho apresenta um sistema de controle de acesso que determina qual empilhadeira e usuário terão acesso a uma determinada área, monitora o acesso e o tempo de permanência desta pessoa e/ou equipamento móvel e faz o recolhimento destas informações em um banco de dados onde tais informações são tratadas e disponibilizadas em forma de relatórios, o que permite que gestores das áreas possam fazer verificações e consultas para tomadas de decisões.

.

Palavras-chave: Controle de acesso, área restrita, segurança patrimonial, monitoramento de equipamentos.

Abstract

Some areas within companies require access control and/or the length of stay of people and/or vehicle. This is due to the imminent risk that this activity can bring who performs as well as a control measure for managers of areas. To supervise and control the access and permanence of people and mobile equipment in these areas is necessary to develop a system that makes such control. This paper presents a system of access control that determines which fork-lift and user will have access to a certain area, monitors access and this person stays and/or mobile device and makes the gathering of this information in a database where such information is processed and made available in the form of reports, which allows area managers can make checks and consultations for decision-making..

Palavras-chave: Access control, restricted area, property security, equipment monitoring.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

INTRODUÇÃO

O controle de acesso a áreas restritas está presente nos mais variados setores da indústria, comércio e até mesmo em residências. A restrição de acesso pode se dar por diversos fatores, tais como segurança e proteção de patrimônio e pessoas contra invasores, proteção de pessoas não autorizadas a áreas restritas, onde se pode ter exposição a fatores de risco como gases, radioatividade, choque elétrico e também na restrição de veículos a determinada área. O controle de acesso também é encontrado em lugares que requerem controle de entrada como bancos, refeitórios, hospitais, etc.

O acesso a áreas restritas por pessoas, como entregadores, prestadores de serviço, visitantes dentre outros, deve ser gerenciado pelo sistema de controle de acesso, permitindo assim que estas pessoas tenham acesso à área restrita, mas que seja também registrada a frequência e a duração da permanência destas pessoas em tais áreas.

Os sistemas de controle de acesso são também utilizados para prover registros de eventos que podem ser utilizados de forma investigativa e no controle estatístico de movimentação de pessoas ou veículos (GALHARDO, 2011).

No projeto de um sistema de controle de acesso, é possível destacar quatro interfaces: os equipamentos de bloqueio, tipo de tecnologia de identificação, sistemas para gestão e infraestrutura de comunicação adequada (THOMÉ *et al.*, 2012)

Os equipamentos de bloqueios são usualmente catracas, torniquetes, portas, portões, cancelas, etc. Já a tecnologia de identificação pode-se citar identificação por rádio frequência, também conhecida como *RFID* do inglês *Radio-frequency Identification, Smart Cards ou Mifare,* leitura biométrica, dentre outras, tais tecnologias serão abordadas no capítulo 1.

O sistema para gestão deve possibilitar o gerenciamento do acesso permitindo a recuperação de informações de acesso, tais como eventos de entrada e saída, tempo de permanência no local, frequência de entrada e saída de pessoas, veículos ou materiais, emissão de permissões temporárias, dentre muitas outras informações que possam ser requisitadas pelo setor de gestão.

Por fim a infraestrutura de comunicação deve se adequar às necessidades do projeto, possibilitando que a informação trafegue de forma adequada prevenindo acessos indevidos, roubos de senhas e autorizações.

Os investimentos relativos à segurança têm aumentado consideravelmente em todo mundo, principalmente dentro das organizações. Além do patrimônio que deve ser assegurado, há também as informações sigilosas e os processos industriais que envolvem anos de pesquisas, por exemplo. A proteção do patrimônio e de dados particulares é fundamental a todas as organizações. Controlar acesso de pessoas e/ou veículos é uma necessidade de proteção dos bens e de informações sigilosas da empresa. Um local protegido por um sistema eficiente e assistido por um serviço de monitoramento competente não fica vulnerável.

Tendo em vista a segurança patrimonial e o monitoramento de acesso a áreas restritas, o presente trabalho tem por objetivo o desenvolvimento de um sistema de controle de acesso que determina quais equipamentos móveis terão acesso a uma determinada área, monitora o acesso e o tempo de permanência do equipamento móvel e faz o recolhimento destas informações em um banco de dados onde tais informações são tratadas e disponibilizadas em forma de relatórios, o que permite que gestores das áreas possam fazer verificações e consultas para tomadas de decisões.

ESTADO DA ARTE

O Brasil tem experimentado nos últimos anos um aumento na violência urbana. Moreira (2007) mostra que existe uma ausência de metodologia e legislação sobre o assunto, e apresenta um estudo sobre as aplicações de medidas de segurança patrimonial nas edificações.

O uso de tecnologias de automação visando garantir o controle de acesso já foi apresentado em alguns trabalhos, como em (JANES, 2009), onde é relatado um estudo sobre os sistemas de segurança utilizados em instalações elétricas automatizadas. É mostrado o sistema de controle de acesso físico utilizando circuitos fechados de televisão e controle por biometria, bem como as vantagens e desvantagens do uso dos mesmos. Além disso, é mostrado que dentre as

tecnologias de reconhecimento biométrico, a que apresenta melhores resultados é a leitura da íris, contudo possui custo elevado e não atende os requisitos do presente trabalho.

Já em Narciso (2008) é mostrado o uso da tecnologia por radiofrequência também chamada de RFID para controle de bens patrimoniais pela web. São apresentados o funcionamento, aplicações e vantagens desta tecnologia, bem como um estudo de caso. O trabalho detalha bem a implementação da tecnologia, mas não aborda bem o uso na segurança patrimonial.

O controle de fluxo de pessoas utilizando também RFID é apresentado em Teixeira (2011), bem como os detalhes para implementação do mesmo. Os resultados são demonstrados por meio de um experimento gerenciando o registro de entrada e saída de alunos em uma escola.

São evidenciadas ainda algumas desvantagens da aplicação com RFID tais como alto investimento, manutenção, necessidade de portar a tag a todo o momento, privacidade e segurança.

Os parâmetros utilizados na implantação de um sistema de controle de acesso físico em empresas são apresentados em Thomé et al. (2012). São mostrados os requisitos como equipamentos de bloqueio, tipo de tecnologia de identificação, sistema para gestão e infraestrutura de comunicação. É destacado também que para a implantação de um sistema de controle de acesso eficiente é necessário a capacitação do gestor do sistema, bem como treinamento para os usuários, de forma que haja uma perfeita sinergia entre o homem e a tecnologia.

Dentre as principais preocupações do presente projeto se destaca o sistema de controle de acesso que deve ser projetado para veículos. Em (GALHARDO, 2011) é apresentado um sistema de controle de acesso de veículos. É mostrado que a identificação pode ser realizada por leitura da placa, controle remoto, tag ativo ou passivo, dentre outros. São apresentadas também as vantagens de um sistema de controle de acesso automatizado para a segurança patrimonial. Nascimento et al. (2015) apresentam também o uso de tecnologia RFID para o controle de veículos em um condomínio. Estas soluções também não atendiam aos requisitos do presente projeto devido a necessidade de robustez no sistema.

Outro ponto importante nos sistemas de controle de acesso diz respeito ao armazenamento e recuperação das credenciais. Em (BRENNER e BIZARRIA, 2011)

é apresentado um software para a recuperação e armazenamento das credenciais, o sistema é implementado em linguagem C#, que é uma linguagem de fácil manipulação, e utiliza leitores biométricos de baixo custo. A opção de identificação biométrica foi levada em conta, contudo a fim de se reduzir custo, a identificação por meio de usuário e senha se demonstrou uma opção mais interessante para o presente trabalho.

E, finalmente, um fator determinante nos sistemas de controle de acesso é a capacidade de processar informações. O controle informatizado de uma biblioteca é apresentado em (JUNIOR e LEITE, 2009), onde é utilizado uma catraca e são gerados dados estatísticos sobre os usuários, tais como número de acessos, frequência de acesso por usuário, períodos, dentre outras. Tais informações podem ser utilizadas para auxiliar o gestor da biblioteca. O trabalho exemplifica bem o uso da informação de acesso para gerar informações ao gestor da área, ponto este que é considerado de extrema importância para o presente trabalho, tendo em vista que uma das exigências do sistema de controle de acesso a ser implementado é que o mesmo possa fornecer informações a respeito dos usuários que adentraram a área de segurança.

Como pode-se observar, a literatura atual apresenta diversos trabalhos na área de segurança patrimonial e controle de acesso, contudo devido às particularidades de cada projeto, nenhum trabalho contempla os requisitos do projeto atual.

Assim o presente trabalho tem como objetivo geral o estudo e desenvolvimento de um sistema de controle de acesso de veículos às áreas restritas. E como objetivos específicos pretende-se restringir o acesso de pessoas não autorizadas, registrar as entradas e saídas, e o tempo de permanência nessas áreas a fim de gerar relatórios aos gestores da área.

1. REVISÃO BIBLIOGRÁFICA

1.1. Equipamentos de Bloqueio

Os equipamentos de bloqueio são estruturas usualmente feitas de metais como o aço, e são utilizadas para evitar a passagem de pessoas não autorizadas em áreas restritas.

O controle dos equipamentos de bloqueio envolve a identificação da pessoa que tenta acessar a área por meio de *tokens*, cartões, leituras biométrica dentre vários outros, e posteriormente a detecção da passagem da pessoa.

Um dos principais equipamentos de bloqueio para uso em controle de acesso é a catraca eletrônica. Este equipamento é composto por uma parte mecânica feita de aço e utiliza solenoides (eletroímãs), servomotores ou motores de passo, para bloquear ou não o movimento de giro do dispositivo. Já a permissão de acesso é verificada por meio de leitura de cartões pessoais, senhas ou ainda leituras biométricas do corpo (MOREIRA, 2007).

A figura 1 mostra uma catraca eletrônica muito utilizada em academias para gerenciar o acesso de usuários.

Figura 1 - Catraca eletrônica com leitura biométrica e teclado numérico.

Fonte: Página da Topdata.
Disponível em: https://www.topdata.com.br/catraca-eletronica/

Outro sistema de bloqueio muito utilizado são as catracas torniquetes. Os torniquetes constituem uma barreira física para controle de acesso de pessoas a áreas restritas ou de acesso condicionado. São compactos e robustos, e constituem uma maneira eficiente de restringir o acesso a áreas restritas de pessoas não autorizadas. Assim como as catracas estes apresentam o sistema de identificação por senha, leitura biométrica ou cartão magnético (JANES, 2009).

A figura 2 mostra uma imagem de uma catraca torniquete.

Figura 2 - Catraca Torniquete.

Fonte: (JANES, 2009)

As cancelas são também equipamentos de bloqueio de acesso, contudo não restringem completamente o acesso, sendo possível a invasão por meio destas. Podem ser cancelas retas, ou articuladas (figura 3) e abranger áreas grandes como até 6 metros.

Figura 3 - Cancelas reta e articulada.

Fonte: Página da Rossi Portões.
Disponível em: http://www.rossiportoes.com.br/produto?id=30

Portões deslizantes (figura 4) são também utilizados como equipamentos de bloqueio, tais portões deslizam sobre trilhos e apresentam cremalheira junto ao portão que trabalha juntamente com um motor a fim de prover movimento linear ao portão (GALHARDO, 2011).

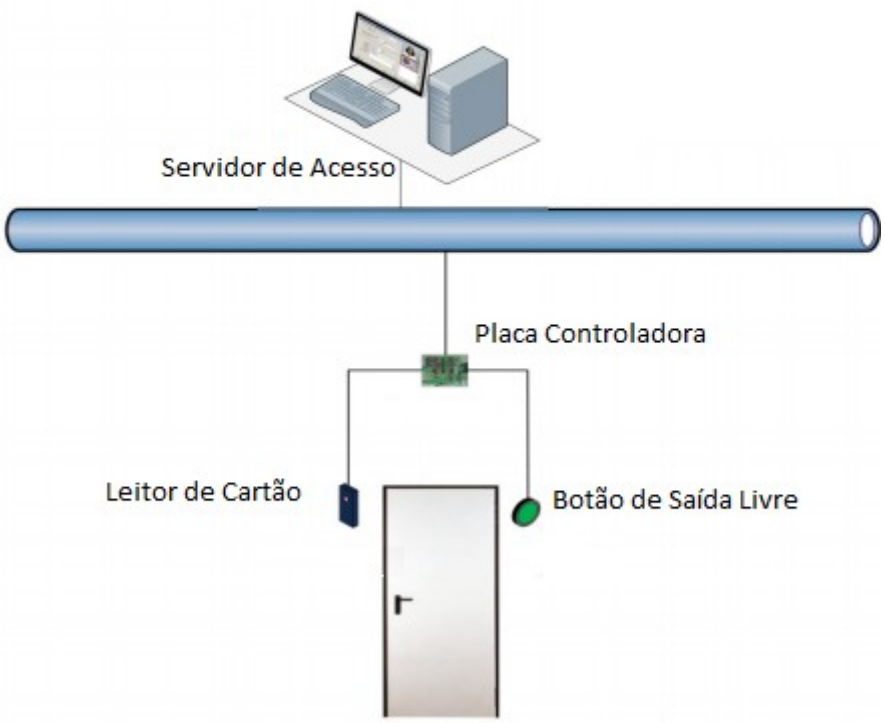
Figura 4 - Portões Deslizantes

Fonte: Elaboração própria.

As portas constituem também em um sistema de bloqueio de acesso e são muito utilizadas para isolar ambientes que necessitam de um controle de acesso. Para que as portas funcionem em um sistema de controle de acesso as fechaduras convencionais são substituídas por fechaduras eletromagnéticas, que possuem seu controle conectado ao sistema de controle de acesso (GALHARDO, 2011).

A figura 5 apresenta um sistema de controle de acesso utilizando portas.

Figura 5 - Sistema de controle de acesso utilizando portas.



Fonte: Adaptado de (GALHARDO, 2011).

Os sistemas de bloqueios são responsáveis por impedir o acesso físico a ambientes controlados ou que contenham objetos de valor, mas devem prever formas de permitir o acesso em situações de risco, como no caso de incêndios, ou falta de energia. Nestes casos o sistema deve garantir que pessoas que estão dentro do ambiente controlado possam sair sem exigir identificação, como pode ser observada na figura 5, a porta possui um botão de saída livre, o qual permite que pessoas dentro dos ambientes possam sair livremente.

No caso de falta de energia, devem ser contempladas também formas mecânicas de liberar o acesso por pessoas que estão dentro das salas controladas, mas não externamente (MOREIRA, 2007).

Os sistemas de bloqueio são subordinados ao sistema central de controle de acesso e necessitam da autorização do mesmo para permitirem a entrada na área controlada. A identificação de pessoas autorizadas pode ser feita por diversas formas, o próximo tópico irá tratar algumas formas de identificação muito utilizadas em projetos de controle de acesso.

1.2 Tipos de tecnologias de identificação

1.2.1 Cartões no controle de acesso

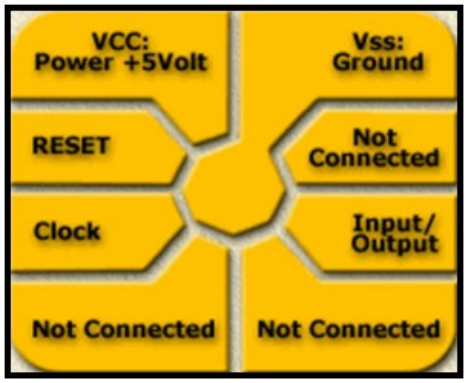
Os cartões inteligentes conhecidos também como smart cards são os novos substitutos dos antigos cartões magnéticos. Estes cartões permitem a identificação do usuário com leitura e gravação de informações no cartão.

A maioria dos cartões inteligentes possui uma memória EEPROM para armazenamento de dados, e algumas ainda possuem um processador, sendo estas últimas um pouco mais raras devido ao custo do cartão (JANES, 2009).

O tipo de acesso com os cartões inteligentes podem ser de dois tipos, os por contato físico e sem contato físico.

Nos cartões inteligentes por contato físico, os mesmos são inseridos em leitores onde há contatos elétricos responsáveis por fazer a conexão com o cartão permitindo assim a leitura e escrita de dados. Tais cartões possuem uma vida útil de média de 10 mil ciclos, e seus terminais são padronizados de acordo com a norma ISO/IEC 7816, a figura 6 mostra o padrão de conexão elétrica.

Figura 6 – Conexões elétricas de cartão inteligente de acordo com ISSO/IEC 7816



Fonte: (JANES, 2009).

Já os cartões inteligentes sem contato físico utilizam a tecnologia RFID (Radio Frequency Identification), que significa identificação por radiofrequência, e que utiliza ondas eletromagnéticas para acessar o conteúdo do cartão. Este tipo de cartão por não necessitar de contato garante uma maior vida útil ao mesmo (GALHARDO, 2011). As distâncias de reconhecimento entre o cartão e o leitor variam de alguns centímetros a um metro e meio, em média. A figura 7 mostra um cartão inteligente e seu respectivo leitor.

Figura 7 – Cartão inteligente sem contato e leitor.

Fonte: Adaptado de http://www.acr120u.com/.

Dentre as tecnologias de cartões inteligentes sem contato físico se destaca a tecnologia MIFARE®, desenvolvida pela NXP Semiconductors e que hoje se destaca como uma das mais difundidas no mundo.

Utiliza uma frequência de 13,56 MHz com alta capacidade de leitura e escrita é muito encontrada como cartões de transporte público e também aplicada no controle de acesso de funcionários (SOUZA, 2011).

Os cartões apesar de serem baratos ainda oferecem alguns riscos de acesso, como perda e extravio do mesmo, o que faz com que seu uso seja inviabilizado em aplicações onde se exige um nível de segurança maior, neste contexto têm-se as aplicações de leitura biométrica, que é assunto do próximo tópico.

1.2.2 Leitores Biométricos no controle de acesso

Os leitores biométricos fazem uso de características físicas individuais para identificação. São encontrados em diversas aplicações tais como identificação criminal, controle de acesso, controle de ponto, acesso a terminais eletrônicos como caixa de bancos, dentre outros (TEIXEIRA, 2011).

As técnicas de leitura biométrica só se tornaram possíveis com o avanço das técnicas de processamento de sinais digitais, e têm como base o registro de características físicas e comportamentais dos indivíduos que são armazenadas em um banco de dados e então comparadas (BRASILIANO e BLANCO, 2003).

Dentre os sistemas biométricos podem-se destacar o de uso da geometria da mão, impressões digitais, leitura de retina ou íris, identificação facial, reconhecimento de voz e reconhecimento de caligrafia.

Na leitura da geometria da mão as características podem variar com o tempo e por isso esta técnica é utilizada para autenticação e não para identificação. Neste tipo de leitura um scanner captura a imagem da geometria da mão da pessoa, tais como tamanho dos dedos e largura da mão e compara com as imagens armazenadas em um banco de dados, quando o padrão é compatível com alguma mão pré-cadastrada o acesso é permitido (JANES, 2009). A figura 8 mostra um scanner de leitura biométrica da mão.

Figura 8 – Scanner de leitura biométrica da mão.

Fonte: (JANES, 2009).

A biometria por meio da impressão digital é a mais comum devido ao menor custo e consiste em analisar elementos principais e únicos chamados minutiae, que podem ser linhas capilares presentes nos dedos ou poros (BONATO e NETO, 2012).

A figura 9 mostra alguns desses elementos.

Figura 9 – Pontos identificadores das digitais (minutiae).

Fonte: (JANES, 2009; BONATO e NETO, 2012).

Estes pontos apresentam diferenças mesmo para gêmeos idênticos, o que acaba sendo uma vantagem em relação aos testes de DNA e de reconhecimento facial. Contudo é suscetível a fraudes, pois os sistemas não conseguem verificar se

o dedo que está sendo identificado é um protótipo sintético ou se é realmente da pessoa.

O reconhecimento da retina ou íris também é utilizado para controle de acesso de pessoas. Cada íris possui uma estrutura única, e um padrão complexo o que garante uma alta eficiência na identificação. Já no caso da retina, alguns especialistas afirmam que suas características podem mudar com o aparecimento de algumas doenças (JANES, 2009). No caso da retina é feito um mapeamento dos vasos sanguíneos presentes no globo ocular. Já na íris é feito um também um mapeamento, mas dos anéis coloridos em torno da pupila. Estes métodos são muito eficientes, mas também são muito caros, e apresentam a desvantagem de necessitarem de ser higienizados constantemente para evitar a contaminação de algumas doenças como a conjuntivite e, além disso, apresentam um desconforto para o usuário no momento da leitura (GALHARDO, 2011). A figura 10 apresenta leitores de íris e retina.

Figura 10 – Leitores de íris e retina.

Fonte: (GALHARDO, 2011).

O reconhecimento fácil está também inserido no contexto da biometria. Utilizando técnicas de identificação de imagem, um computador por meio de uma câmera identifica um rosto humano em uma determinada região e compara com uma base de dados previamente cadastrada (VICTOR *et al.*, 2002).

Para reconhecer um rosto, os programas se focam em pontos principais como olhos, nariz, queixo, maçãs do rosto, orelhas, lábios, sobrancelhas e a relação entre eles, como a distância e assim iniciar o processo de comparação (JANES, 2009).

Estes sistemas são capazes de identificar indivíduos que tenham sua aparência modificada levemente, mas não mudanças bruscas, o que faz com que estes sistemas sejam pouco utilizados. A figura 11 mostra um software fazendo a detecção de uma face.

Figura 11 – Software de reconhecimento facial.

Fonte: (JANES, 2009).

Na identificação pela voz, esta é captada, e transformada de uma onda analógica para dados digitais, onde ruídos são removidos e o som é dividido em fonemas, para só então ser comparado. O processo se dá em três etapas, captura, extração e comparação. Na etapa de captura o usuário fala em um microfone uma frase que pode ou não ser pré-estabelecida e o processo é repetido algumas vezes para se ter um perfil da fala. O equipamento biométrico realiza a extração de um sinal único da voz e então é criado um padrão para aquele indivíduo. Então no processo de comparação o usuário pronuncia uma frase e esta é comparada com o padrão pré-estabelecido (LUZ e FRESSATTI, 2015).

Outra tecnologia de reconhecimento biométrico mas que é pouco utilizado é o reconhecimento da assinatura. O indíviduo escreve no aparelho biométrico com uma caneta especial, e o aparelho identifica o padrão da assinatura, pressão, angulação da caneta e velocidade. Contudo estes aparelhos apresentam um alto custo relativo, o que faz com que seu uso ainda seja limitado (GALHARDO, 2011). A figura 12 mostra um sistema de reconhecimento de assinatura.

Figura 12 – Sistema de reconhecimento de assinatura.

Fonte: FingerTech.

Apesar de muitas vantagens, os sistemas de reconhecimento biométrico ainda apresentam como desvantagem o alto custo dos equipamentos, e tal fator é limitante no presente trabalho, de forma que outras formas de identificação e reconhecimento foram consideradas. O próximo tópico é tratado o tipo de identificação por rádio frequência.

1.2.3 RFID no controle de acesso

A tecnologia RFID do inglês *Radio Frequency Identification* é uma tecnologia baseada em radio frequência que é capaz de captar, analisar e gerenciar sinais provenientes de sensores e dispositivos eletrônicos (TEIXEIRA, 2011).

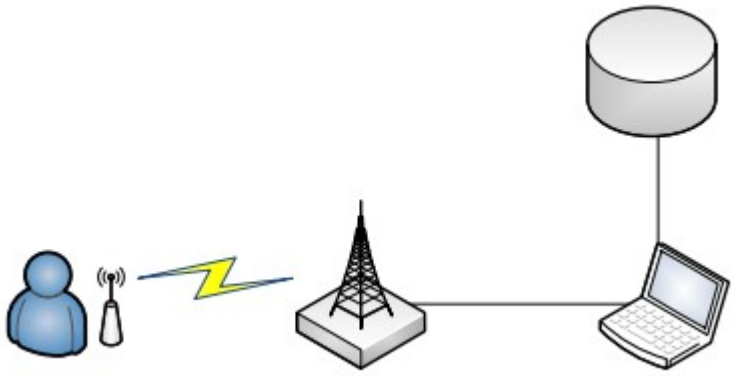
Usualmente esta tecnologia utiliza quatro componentes principais, sendo eles, o *transponder*, *transceiver*, antenas e *middleware.*

O *transponder* é também chamado de *tag* ou etiqueta. Este componente é acoplado junto ao item que deve ser identificado e possui informações sobre o item, tais como tipo, nome, autorizações dentre outras. Pode ser ativa, quando envia sinais, ou passiva quando apenas responde a sinais de estímulo (NARCISO, 2008).

Os *transceiver* ou leitor são responsáveis por ler e decodificar as informações contidas nas etiquetas e fazem isso por meio de uma antena, que envia um sinal que ativa a troca de informação entre o leitor e a etiqueta.

Após receber as informações da etiqueta o leitor envia os dados para o middleware, que é um software responsável por manipular o fluxo de dados entre os componentes do sistema. A figura 13 mostra uma arquitetura clássica de um sistema RFID.

Figura 13 – Arquitetura de um sistema RFID.



Fonte: (GINES e TSAI, 2007).

A distância de funcionamento do sistema RFID está sujeito ao ambiente. Locais que possuem grande presença de água e metais podem alterar as ondas eletromagnéticas fazendo assim com que a distância de comunicação seja encurtada. Nestes casos são utilizadas etiquetas ativas, que por possuírem antena e bateria interna conseguem se comunicar por uma distância maior.

Dentre as diversas aplicações utilizando RFID se destacam o seu uso em cartões de transporte, no uso de monitoramento de condenados, que utilizam pulseiras com RFID e que sinalizam caso tentem ser removidas.

A questão de segurança do RFID ainda é problemática, pois a simplicidade das etiquetas impede que protocolos complexos sejam implantados. Este problema tem dificultado o uso de RFID para identificação de pessoas (GINES e TSAI, 2007).

A tabela 1 mostra uma comparação entre as frequências de utilização do RFID e suas aplicações.

Tabela 1 – Características gerais de sistemas RFID.

Frequência	Baixa Frequência 125- 134,2 KHz	Alta Frequência 13,56 MHz	Frequência Ultra Alta 860 – 960 MHz	Microondas 2,45 GHz e 5,8 GHz
Alcance de leitura	0,5 m	1,0-1,5 m	3,0 m	5,0-10,0 m
Capacidade de leitura (metais e líquidos)	Excelente	Boa	Média	Baixa
Dimensão da etiqueta	Muito Grande	Grande	Média	Pequena
Fonte de Energia	Passiva, indução eletromagnética.	Passiva, indução eletromagnética.	Ativa com bateria integrada.	Ativa com bateria integrada.
Aplicações	Monitoramento de animais e controle de acesso.	Smart Cards, monitoramento de produtos e controle de acesso.	Monitoramento de containers, sistemas de transporte.	Cadeia de suprimento e sistemas de transporte.

Fonte: (GINES e TSAI, 2007).

1.3 Sistemas para Gestão da Informação

Os sistemas de gestão da informação são constituídos por um conjunto de hardware e software que trabalham junto de forma organizada a fim de manter a integridade do sistema.

Enquanto o software é responsável pela lógica do sistema, o hardware é a parte física que é responsável pela comunicação com o sistema de controle de acesso.

1.3.1 Requisitos de Software e Hardware

Neste tópico são descritos alguns dos requisitos mais comuns dos sistemas de controle de acesso.

Os softwares de controle de acesso devem permitir o controle de pessoas e veículos de uma empresa, bem como de visitantes e tratá-los de forma individual, permitindo o registro de horário de entrada, saída, tempo de permanência na área controlada, dentre outros.

Em relação ao controle das áreas, deve ser possível gerenciar de forma individual, concedendo acesso a uma área específica a um funcionário específico, ou por níveis de acesso, garantindo assim que apenas pessoas que necessitem adentrar uma área específica tenham acesso à mesma. As definições de nível de acesso são usualmente feitas em conjunto da gerência dos diversos setores, com o pessoal de gestão patrimonial e recursos humanos (GALHARDO, 2011).

A criação de tabelas de horários, dias da semana e feriados também é um requisito, de forma que a restrição de acesso se dê também em função destes itens, garantindo um controle mais rigoroso.

Um gerenciamento de eventos como acessos autorizados e não autorizados deve ser feito, e o sistema deve possibilitar a emissão de relatórios, tanto na forma de arquivos texto, planilhas e pdf, para facilitar a análise dos mesmos.

O software também deve permitir o monitoramento em tempo real, a fim de alertar possíveis tentativas de acesso a áreas restritas, como também se dispositivos de bloqueio ficaram abertos por mais tempo do que o necessário.

Já se tratando do hardware, pode-se dizer que este é basicamente um computador comum, com interfaces de comunicação baseada em ethernet, entradas usb para conexão de sensores, e memória suficiente para armazenar os dados cadastrais.

As interfaces ethernet que trabalham com o protocolo TCP/IP tem substituído as antigas interfaces seriais por poderem aproveitar as estruturas de redes

existentes, serem de baixo custo e garantir altas velocidades de tráfego. A conexão com sensores é importante para se detectar o momento em que houve acesso, bem como se o sensor permanece aberto por mais tempo do que o necessário. Já a memória para armazenamento deve ser suficiente para armazenar os dados cadastrais para o caso de uma eventual perda de comunicação com os servidores.

1.3.2 Web Services

No atual contexto tecnológico, para as empresas se manterem competitivas faz-se necessário a integração entre as diversas áreas de negócios da empresa.

Assim uma tecnologia que visa garantir a integração entre diversos setores da empresa é a chamada Web Service.

Um Web Service é um sistema que permite a interoperabilidade entre diferentes aplicações e protocolos sobre uma mesma rede (MORO *et al.*, 2011).

Os Web Services incorporam conceitos fundamentais de sistemas orientados a objetos e de sistemas orientados a componente. Princípios como orientação a objeto, encapsulamento, troca de mensagens e ligações dinâmicas estão presentes. São sistemas fracamente acoplados e independentes de plataforma e de linguagens de programação.

Com o uso de Web Service é possível que aplicações diferentes, desenvolvidos em plataformas diferentes sejam compatíveis entre si e enviem e recebam informações em formatos variados, que são traduzidos entre um padrão e outro de acordo com o emitente e destinatário. Um exemplo de linguagem universal é a XML, acrônimo para *eXtensible Markup Language.* Que nada mais é do que uma linguagem padronizada para a troca de informação entre plataformas (FREITAS, 2006).

No caso de sistemas de controle de acesso, o uso de um Web Service faz-se necessário para transmitir informações de registros e relatórios de acessos para sistemas gerenciais, como pode ser o caso de um sistema ERP (Enterprise Resource Planning – Sistema de Planejamentos de recursos da Empresa).

1.3.3 Sistema de Banco de Dados

Um banco de dados é uma coleção de dados agrupados de forma consistente, que visam gerar informações administrativas para uma determinada empresa (ROCHA e DIAS, 2015).

De uma forma geral, a função dos bancos de dados é o armazenamento, gerenciamento e recuperação dos mesmos. Para isso são criadas tabelas compostas por diversos registros que visam organizar os dados com características comuns, permitindo a recuperação dos mesmos por meio de comandos específicos.

Os bancos de dados são gerenciados por um sistema SGBD (Sistema de Gerenciamento de Banco de Dados), que são uma coleção de softwares encarregados de gerenciar e manter a integridade do banco de dados.

A forma de acesso aos bancos de dados é independente de linguagem, isto é, qualquer linguagem, seja ela, java, c/c++, python dentre outras, são capazes de buscar dados em um banco de dados.

A figura 14 apresenta uma estrutura de banco de dados, explicitando a posição do SGBD e dos usuários.

Figura 14 – Estrutura de um SGBD.

Fonte: (ROCHA e DIAS, 2015).

Existem basicamente três tipos de banco de dados, os relacionais, os temporais e os bancos de dados orientados a objeto.

Os bancos de dados relacionais são os mais comuns e apresentam grandes vantagens por permitirem que diversas relações entre objetos sejam criadas. Já os bancos temporais, concentram-se em registros temporais e são muito aplicados em sistemas de automação, onde a dinâmica e o histórico das variáveis apresentam maior interesse.

Nos bancos de dados do modelo orientado a objeto os dados são armazenados na forma de objetos e só podem ser manipulados por métodos presentes nas classes às quais esse objeto pertence. Ainda é muito pouco difundido no mercado.

As diversas tecnologias apresentadas no presente capítulo nortearam o desenvolvimento do trabalho, contudo nem todas foram utilizadas por não contemplarem os requisitos do sistema. No próximo capítulo será detalhada a metodologia utilizada para a produção do trabalho, bem como tecnologias utilizadas que não foram detalhadas até então.

2. Metodologia

Os itens a seguir apresentam a metodologia empregada para a obtenção de um sistema de controle de acesso a Áreas controladas. Serão descritos os requisitos do sistema, bem como as medidas tomadas e tecnologias adotadas para atender todos os requisitos.

2.1 Sistema de controle de acesso a Áreas Controladas

O sistema proposto tem como objetivo controlar o acesso de pessoas e veículos em determinadas áreas de uma mineradora da região, por meio de senhas particulares e intransferíveis, limitando assim o acesso apenas a pessoal previamente autorizado, gerar relatórios de tempo de permanência, nome dos usuários que acessaram, se o acesso foi por pedestre ou veículo. Além disso, o sistema deve disponibilizar todas essas informações em tempo real via web.

Algumas atividades desempenhadas dentro da mineradora requerem controle de acesso e de permanência dentro de uma área. A necessidade deste controle de acesso e do tempo de permanência dentro de uma área específica varia de acordo com a necessidade de cada empresa, seja ela para não sofrer penalidades trabalhistas ou mesmo para supervisionar e controlar o acesso das pessoas nestas áreas.

Com o objetivo de manter o projeto em baixo custo, a solução proposta partiu de um sistema de rastreamento de veículos já consolidado, e modificações foram feitas de forma a atender os requisitos do projeto, efetuando de forma sistêmica o controle de acesso à área.

A figura 15 ilustra a área a ser controlada, bem como alguns componentes do sistema de controle.

Figura 15 – Área restrita.

Fonte: Autoria própria.

Os próximos tópicos irão descrever o sistema e seus componentes.

2.2 Componentes do Sistema de Controle de Acesso à área controlada

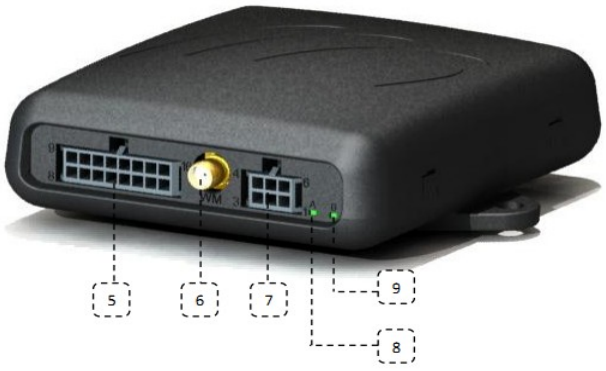
O sistema de controle de acesso tem como cérebro principal dois rastreadores, o MTC550 e o MXT 151, ambos da MAXTRACK®.

O MTC-550 é um rastreador que pode ser aplicado em diversas atividades, tais como operações de logísticas, gerenciamento de risco, inteligência embarcado, sistemas de transporte coletivo e avaliação do comportamento do condutor.

Este módulo possui também uma função denominada “ações embarcadas” que permite uma customização do módulo, de forma a atender as necessidades do usuário.

A figura 16 mostra uma visão geral do MTC550.

Figura 16 – Rastreador MTC550 da Maxtrack.



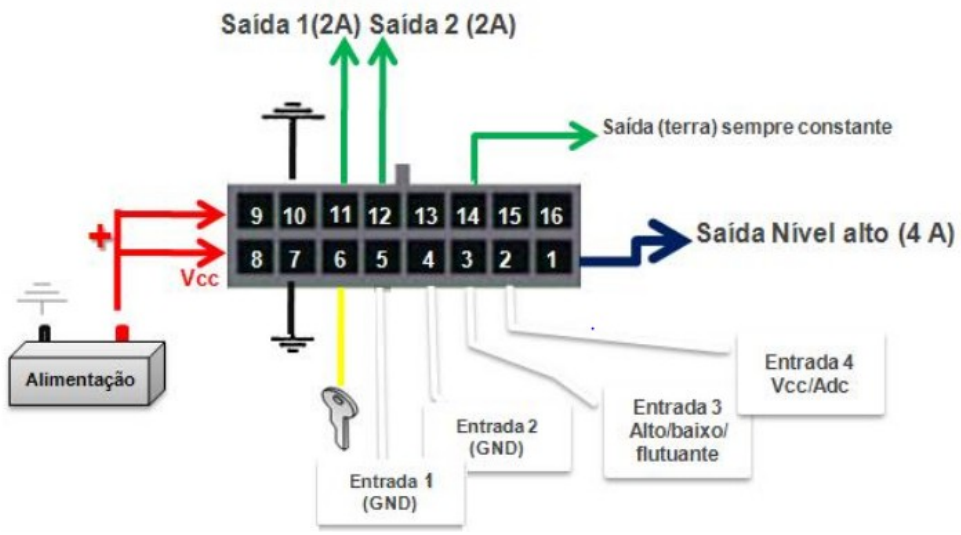
1: Alto-falante	5: Microfit 16 vias
2: Microfone	6: Antena GPRS
3: RS 485	7: RS 232
4: Antena GPS	8: Led GSM/GPRS
	9: Led GPS

Fonte: (MAXTRACK, 2015a).

Como pode-se observar, o MTC550 apresenta diversas funções, dentre as principais pode-se citar a antena GPRS que permite o envio de dados em tempo real, o GPS que permite a localização do módulo e o barramento de entradas e saídas *microfit* de 16 vias.

O *microfit* de 16 vias é mostrado na figura 17.

Figura 17 – Barramento de entradas e saídas microfit 16 vias.



Fonte: (MAXTRACK, 2015a).

As entradas desse módulo suportam até 12 volts, e as saídas são capazes de prover até 2 amperes.

Outro componente de grande importância no sistema de controle de acesso é o MXT151 da MAXTRACK®.

O MXT 151+ é um modulo de rastreamento de veículos que utiliza a rede GPRS para troca de informações com um servidor Web. Por meio desse módulo é possível detectar informações como posição global, sensores e atuadores do veículo, dentre outros.

Dentre as principais aplicações do MXT 151+ pode-se citar (MAXTRACK, 2015b):

Monitoramento de veículos;

Operações de logística;

Gestão de frota de veículos.

A figura 18 mostra o módulo MXT 151+.

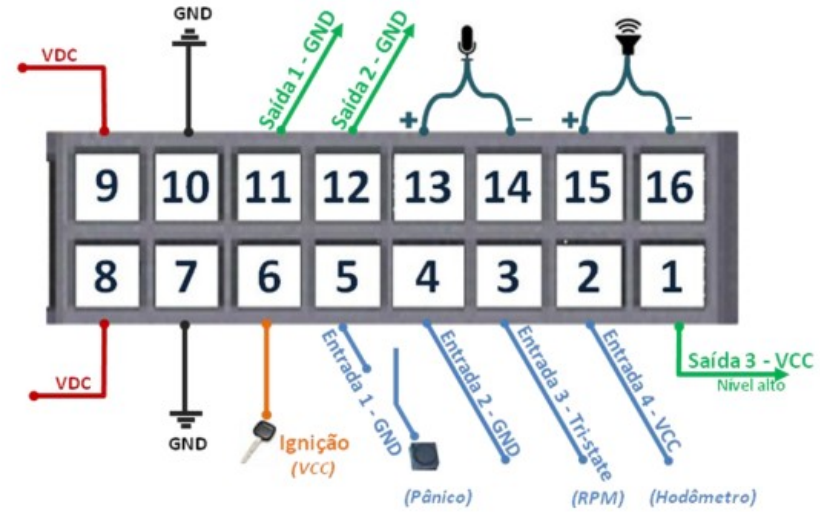
Figura 18 – Módulo MXT 151+.

Fonte: (MAXTRACK, 2015b).

Assim como o módulo MTC550, o MXT 151+ possui um barramento de entradas e saídas, que permite a integração com sensores e atuadores, permitindo ao usuário uma maior customização do projeto.

A figura 19 mostra o barramento do MXT 151+.

Figura 19 – Barramento do módulo MXT 151+.



Fonte: (MAXTRACK, 2015b).

Como podem ser observados pela figura 17 e 19, os conectores dos módulos MTC550 e MXT151+ são semelhantes, contudo o MXT 151+ apresenta a possibilidade de comunicação com um controle remoto denominado WT110.

O controle WT110 é um dispositivo de autenticação que interage com o MXT 151+ por meio do protocolo de comunicação Zigbee.

O protocolo Zigbee é um protocolo de comunicação aberto (FAGUNDES et al., 2015), que permite comunicações robustas e opera na frequência ISM (Industrial, Scientific and Medical), 868 MHz (1 Canal), 915 MHz (10 canais) e 2,4 GHz (16 Canais) .O WT110 trabalha com 16 canais a 2,4 GHz.

Neste projeto foram utilizados WT110 dentro das empilhadeiras para enviar o comando de abertura dos portões. O esquema de ligação será detalhado no próximo tópico.

A figura 20 mostra um WT110.

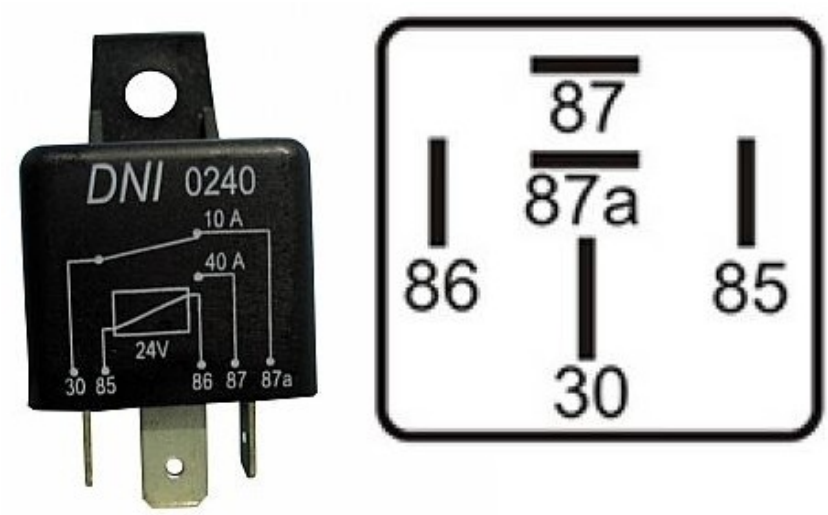
Figura 20 – Controle remoto WT110.

Fonte: (MAXTRACK, 2015b).

Os dois módulos controladores fazem apenas a parte de comando lógico, para a operação de comandos de força foram escolhidos os relés automotivos da série DNI0240, pois são de baixo custo e a mineradora dispunha de vários em seu estoque.

O DNI0240 é um relé automotivo de 5 terminais, com 1 contato normalmente aberto e um contato normalmente fechado. Suporta até 24 volts e 40 ampéres, mas pode ser acionada com 12 volts. A figura 21 mostra uma imagem do relé DNI0240.

Figura 21 – Relé automotivo DNI0240.



Fonte: (DNI, 2015).

Outro componente utilizado no sistema de controle de acesso foi o terminal de dados TD-50. Este terminal consiste em um dispositivo com tecnologia embarcada e permite a interação do usuário com o sistema de controle no qual estará integrado, possibilitando diversas modalidades de mensagens e funções.

O TD-50 foi utilizado no painel local próximo ao portão para que o usuário pudesse abrir o portão por um backup, inserindo seu usuário e senha.

O terminal apresenta as seguintes características:

- Tamanho: 200mm x 180m x 33mm;
- Consumo normal: 30 mA @ 12Volts e Consumo máximo: 180 mA @ 12 volts;
- Texto livre do TD-50 para a central, 120 caracteres;
- Texto livre da central para o TD 50, 240 caracteres;
- Bibliotecas, limite máximo de 160 mensagens;
- Memória Flash 128K (EPROM);
- Memória RAM 8K;
- Teclado alfanumérico emborrachado, com 64 teclas;
- Teclas especiais para acesso direto às funções de controle (F0 a F9);
- Display de LCD gráfico com 240×64 pixels e backlight;
- Cabo espiralado para alimentação e comunicação de dados.

A figura 22 mostra o TD-50.

Figura 22 – Terminal de dados TD-50.

Fonte: (MAXTRACK, 2015a).

A posição da empilhadeira foi confirmada por meio de sensores de posição. Primeiramente foi utilizado um sensor de barreira IRA 315, o qual consiste em um sensor de barreira por infravermelho.

Este sensor foi posteriormente substituído por um sensor de massa metálica devido a problemas como necessidade de alinhamento, passagem de pedestres ou obstáculos que ativavam o mesmo.

A figura 23 apresenta o IRA 315.

Figura 23 – Sensor de barreira IRA 315.

Fonte: (JFL, 2015).

A figura 24 mostra o sensor IRA 315 instalado em campo.

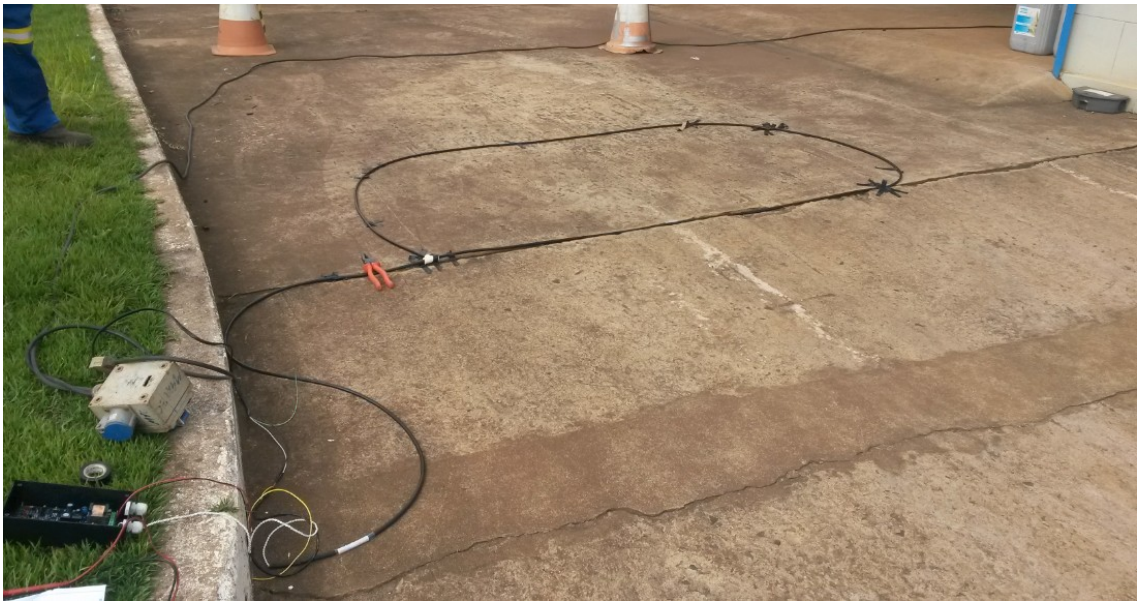
Figura 24 – Sensor de barreira IRA 315 instalado em campo.

Fonte: Autoria própria.

Os sensores IRA 315 foram substituídos pelos sensores de massa metálica M-GAGE Q7M, estes sensores utilizam de um laço indutivo que pode ser colocado no chão em sulcos de apenas 15 mm. Quando o veículo se aproxima do laço um contato normalmente aberto é fechado sinalizando a presença do veículo. Foram utilizados sensores tanto para entrar quanto para sair da zona controlada.

A figura 25 mostra o sensor M-GAGE Q7M instalado acima do solo, durante a fase de testes na mineradora.

Figura 25 – Sensor de massa metálica M-GAGE Q7M.



Fonte: Autoria própria.

Foi utilizada também uma torre de sinalização para indicar em que condição o sistema se encontra, se armado ou desarmado, e se o veículo se encontra na posição correta. Para sinalização foi utilizado um sinalizador visual D212 da Decibel®.

A figura 26 mostra o sinalizador utilizado.

Figura 26 – Sinalizador visual D212 da Decibel.

Fonte: (DECIBEL, 2015).

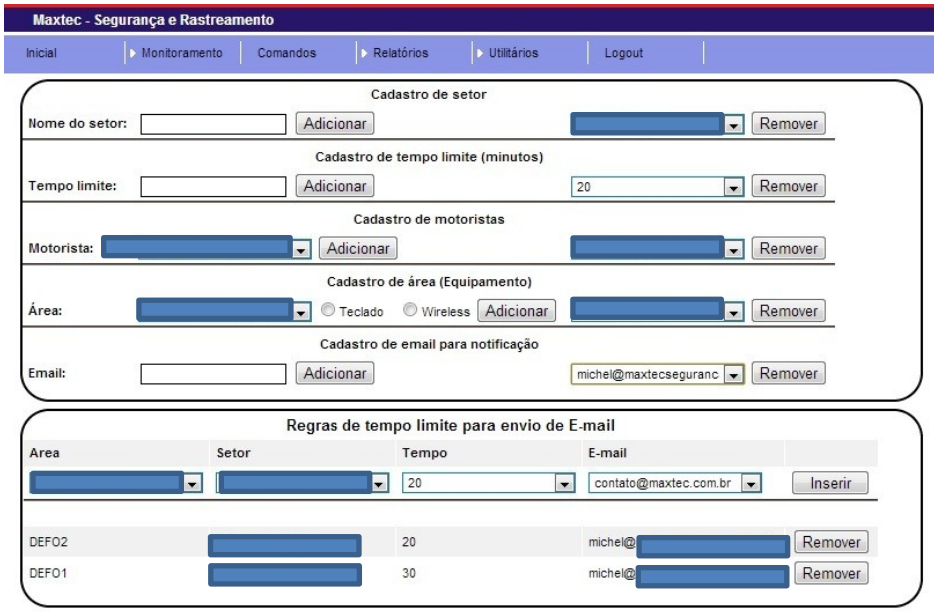
E por último, um dos componentes essenciais do sistema de controle de acesso é o portal de rastreamento da Maxtec®.

O portal de rastreamento da Maxtec é um web service que permite a disponibilização de informações a respeito dos veículos cadastrados no sistema. O portal é online 24 horas e recebe informações via GPRS dos módulos MTC550 e MXT151.

Todos os eventos como *login* de usuário, abertura de portão, fechamento, dentre outros, registrados pelos módulos MTC550 e MXT151, tanto do sistema de controle de acesso quanto da Empilhadeira são registrados no portal de rastreamento para futura geração de relatórios.

A figura 27 mostra uma imagem do portal de rastreamento Maxtec.

Figura 27 – Portal de Rastreamento Maxtec.



Fonte: Autoria própria.

2.3 Funcionamento do Sistema de Controle de Acesso à área controlada

A figura 28 mostra o sistema de controle de acesso montado em painel próximo ao portão.

Figura 28 – Painel Montado em campo.

Fonte: Autoria própria.

Já a figura 29 mostra o painel internamente com os componentes utilizados, dando destaque para o MTC550 e o MXT151, bem como as fontes de alimentação.

Figura 29 – Painel Interno.

Fonte: Autoria própria.

O sistema de controle de acesso é dividido em acesso local e acesso remoto. O acesso local é feito por intermédio de um terminal de dados TD-50 instalado na entrada da área controlada. A figura 30 mostra o terminal TD-50 instalado em campo.

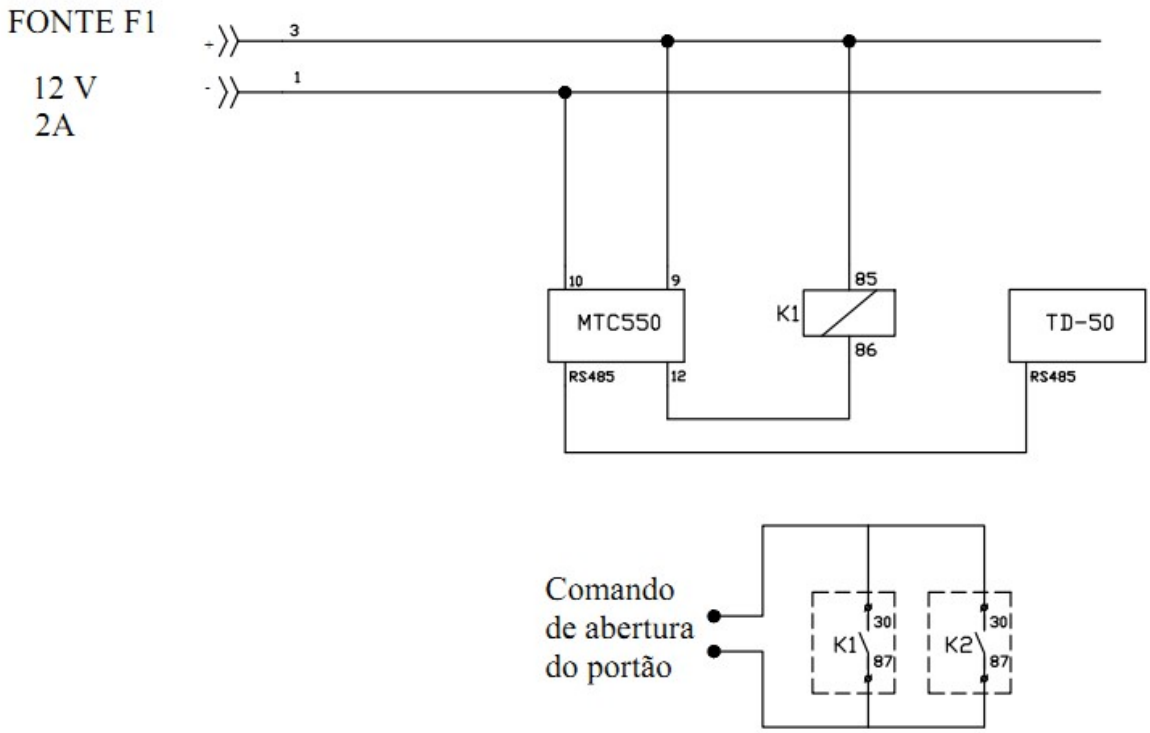
Figura 30 – Terminal de dados TD-50.

Fonte: Autoria própria.

Por meio desse terminal o usuário pode entrar com o seu usuário e senha e executar a abertura do portão.

O terminal de dados TD-50 é interligado com o módulo MTC550 por meio de cabo RS485. A figura 31 mostra o esquema de ligação do circuito 1, responsável pela abertura do portão em local, o mesmo diagrama pode ser visto em tamanho maior no apêndice A. Neste mesmo diagrama é possível observar também a ligação do TD-50 com o MTC550.

Figura 31 – Esquema de ligação do Circuito 1.



Fonte: Autoria própria.

O circuito de ligação das fontes F1, F2 e F3, podem ser vistos no apêndice A.

O MTC550 é alimentado pelos bornes 9 e 10 do *microfit* de 16 vias, de acordo com a figura 31. Observa-se também o relé automotivo DNI0240 representado na figura como K1.

Quando o usuário faz o *login* com nome de usuário e senha por meio do TD-50, o MTC550 reconhece e permite o comando de abertura e também registra essas ações no Web Service por meio de comunicação GPRS. Ao executar o comando de abertura, o borne 12 é colocado em nível baixo e o relé K1 é energizado, fechando os contatos K1(30,87), estes contatos por sua vez são ligados na placa de comando de abertura do motor e fazem o portão abrir.

O contato K2(30,87) permite ao circuito 2, que é o circuito de acionamento remoto do sistema de controle de acesso, abrir o portão.

Um sensor infravermelho IRA315 que possui a função de segurança, é instalado junto ao portão, de forma que, quando é detectada a passagem de pessoa ou veículo, um comando de abertura é enviado diretamente para a placa de controle do motor a fim de evitar esmagamento.

O sensor IRA 315 junto ao portão é mostrado na figura 32.

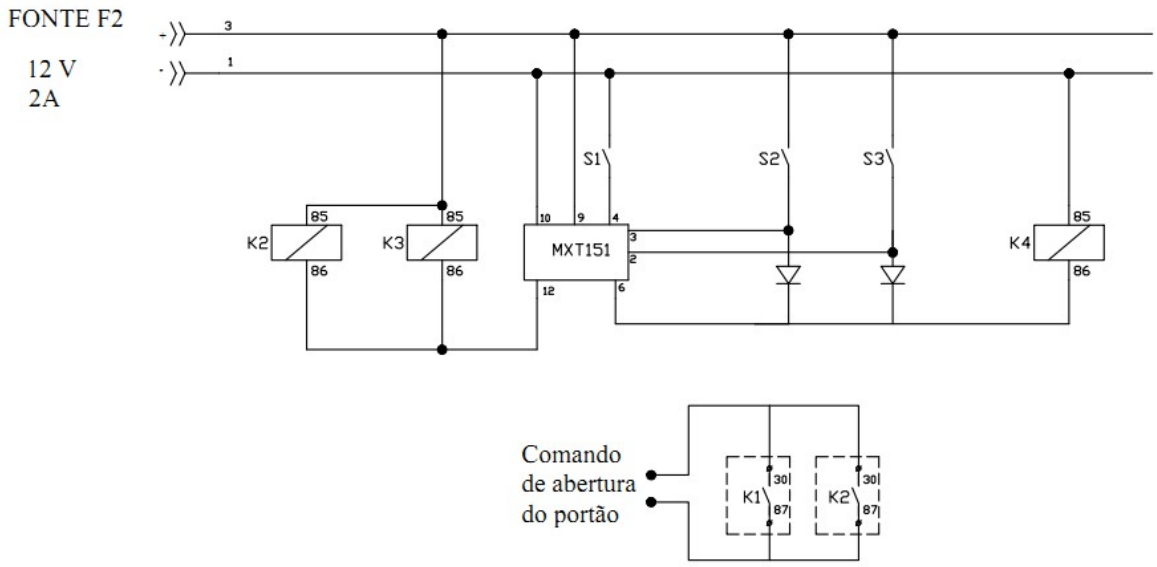
Figura 32 – Sensor de Segurança IRA 315.

Fonte: Autoria própria.

O segundo modo de operação que é o modo de operação remoto, é executado a partir da empilhadeira por meio de um controle remoto denominado WT110 e funciona em conjunto com o MXT151 e estão associados ao circuito 2.

O circuito 2 é mostrado na figura 33, e também pode ser visto no apêndice A.

Figura 33 – Esquema de ligação do Circuito 2.



Fonte: Autoria própria.

Na figura 33 é possível observar o circuito 2 ou circuito de acionamento remoto do sistema de controle de acesso.

O sensor S1 é um sensor de fim de curso do portão que indica se o mesmo está aberto. Os sensores S2 e S3 são sensores de laço indutivo do tipo M-GAGE Q7M e estão localizados respectivamente na entrada e na saída da área.

Ao ser acionado o circuito S2 energiza o borne 3 com 12 volts e também aciona a bobina do relé K4, o qual é responsável por indicar que o posicionamento da empilhadeira está correto. Os diodos são utilizados para que o acionamento da entrada ou da saída não indique ambas as situações.

É importante notar que o posicionamento da empilhadeira tornou-se uma condição necessária, porque muitas vezes uma empilhadeira enviava o comando de abrir para uma determinada área e esse mesmo comando abria uma área adjacente, assim optou-se por utilizar um sensor de posicionamento.

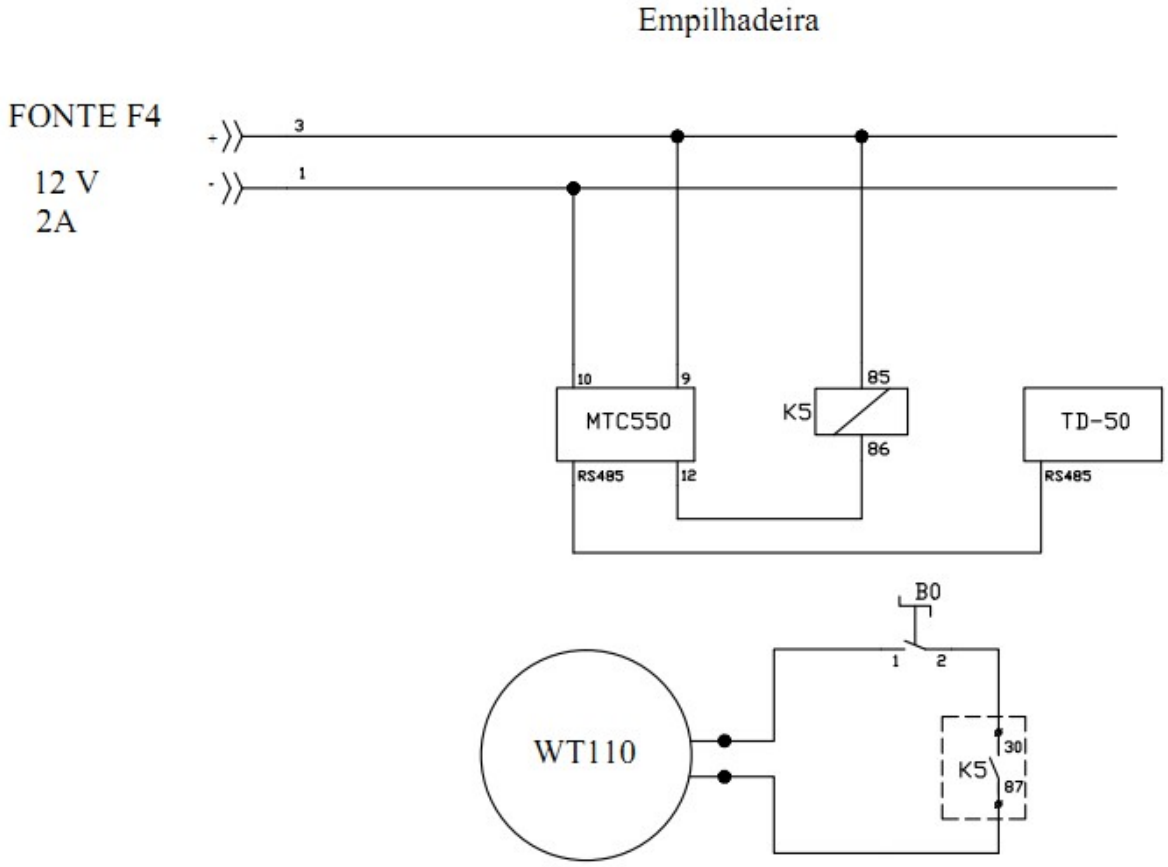
O relé K2 serve para acionar o comando de abertura do portão, é energizado quando recebe um comando vindo do controle WT110 da empilhadeira e é verificado se o usuário da empilhadeira tem permissão para adentrar a área em questão. Cada empilhadeira possui um identificador único.

Já o relé K3 é usado para indicar que o sistema está apto a receber o comando de abertura.

As empilhadeiras já possuíam um sistema de usuário que fazia uso de um módulo de rastreamento MTC550, de forma que este sistema foi utilizado em conjunto com o módulo WT110 para permitir o acesso à área de controle.

O módulo WT110 foi adaptado a uma botoeira para garantir maior durabilidade no ambiente industrial, e foi ligado em série com um contato do sistema MTC550 da empilhadeira, como mostra o esquema da figura 34, o mesmo esquema pode ser visto em tamanho maior no apêndice A.

Figura 34 – Esquema de ligação do Circuito 3.



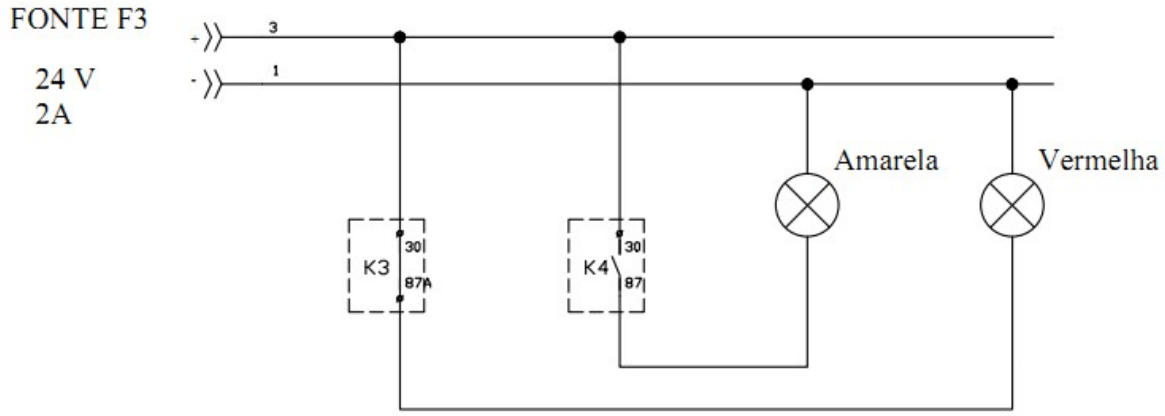
Fonte: Autoria própria.

Quando o usuário realiza o *login* na empilhadeira, tal ação é registrada no portal de rastreamento da Maxtec por meio de GPRS e o relé K5 é acionado, permitindo assim que, ao acionar a botoeira B0, o WT110 envie um comando para a central de controle de entrada da área em questão.

A central da área, no caso o módulo MXT151, recebe o sinal do WT110 por zigbee e verifica no Web Service qual usuário está logado na empilhadeira em questão, caso o usuário tenha acesso aquela área, o sistema envia o comando de abertura do portão e todos estes eventos são registrados no Web Service para futura geração de relatórios.

O circuito que comanda a sinalização do sistema é o circuito 4, que pode ser visto na figura 35, ou no apêndice A em tamanho maior.

Figura 35 – Esquema de ligação do Circuito 4.



Fonte: Autoria própria.

O relé K3 possui um contato normalmente fechado, que é ligado na lâmpada de sinalização vermelha, assim quando o sistema está armado e pronto para receber um comando de abertura, a lâmpada vermelha estará acesa. Já o relé K4 possui um contato normalmente aberto que só é ativado quando a empilhadeira se encontra na posição correta, assim a lâmpada amarela é acesa indicando que a empilhadeira está posicionada.

O sistema só envia o sinal, efetivamente, quando as duas lâmpadas estão acesas.

É importante ressaltar também que o sistema de controle de acesso só permite que um novo comando de abertura do portão seja efetuado após transcorridos 15 segundos de um comando de abertura.

Neste capítulo foram descritos o sistema, seus componentes e a funcionalidade de cada componente. O próximo capítulo aborda os resultados alcançados com a implantação do sistema de controle de acesso à área.

3. Resultados

A implantação do sistema de controle de acesso à área partiu de uma solução previamente implantada, que foi o sistema de rastreamento nas empilhadeiras. Tal sistema foi inicialmente proposto para que se pudessem controlar os usuários autorizados a utilizar as empilhadeiras bem como o tempo de trabalho nestes equipamentos, garantindo assim mais informações para a gerência.

Ao se verificar a necessidade de controle de acesso à áreas restritas, foi proposto a implementação de um sistema a partir do sistema de rastreamento das empilhadeiras. A solução se mostrou de baixo custo e graças à familiaridade com o projeto anterior, de rápida implantação.

Foi garantido o controle de acesso às áreas restritas por veículos e por usuários, isto é, para cada usuário que adentra a área restrita é registrado o dia, hora e tempo de permanência na área.

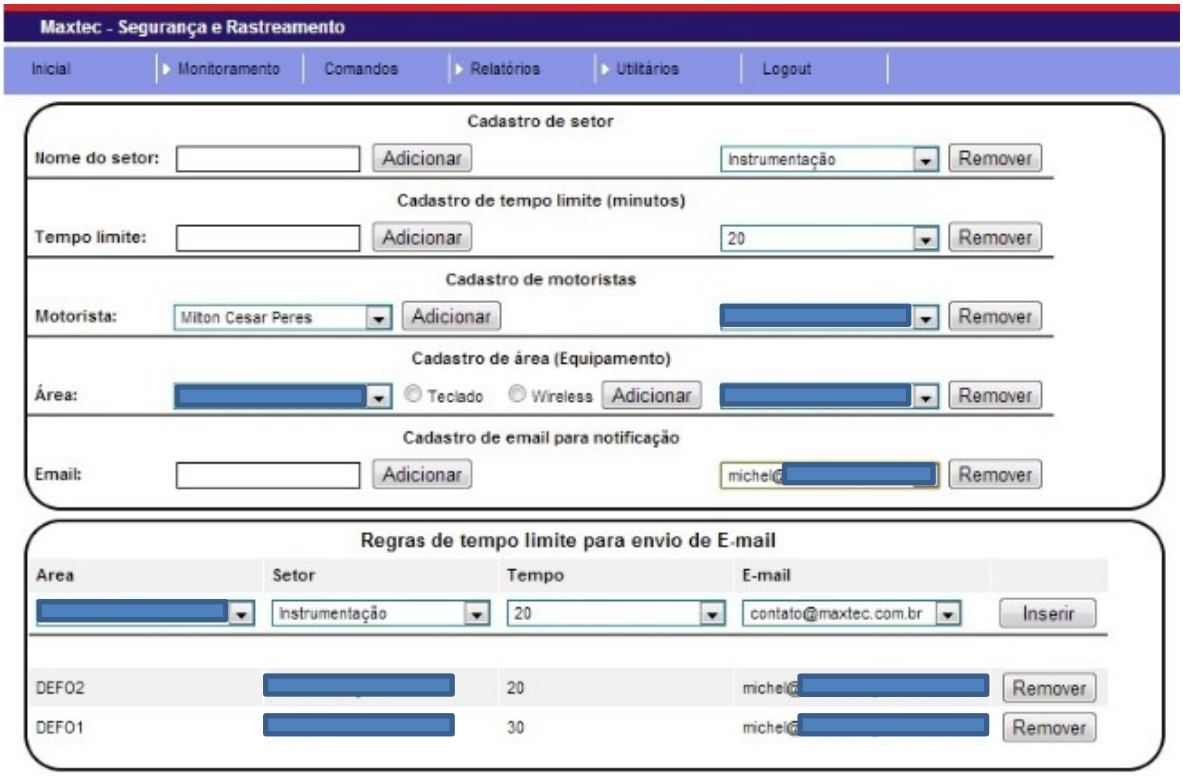
O sistema permanece online 24 horas, permitindo o acesso via web, de forma que qualquer dispositivo com um navegador é capaz de acessar o portal e obter informações gerencias do controle de acesso.

Um sistema de relatório foi implementado no portal de forma que as informações podem ser buscadas utilizando filtros como data, horário, usuário e veículo.

O gerenciamento de acesso às áreas restritas, com novas autorizações e cancelamentos de acessos, pode ser feito por meio do portal, sem a necessidade de intervenção física no local, garantiu maior agilidade no processo.

A figura 36 mostra o portal de rastreamento, onde é possível ver algumas das funções implementadas, como cadastro de setor, cadastro de tempo limite, cadastro de motoristas e cadastro de área, além da guia de emissão de relatórios.

Figura 36 – Portal de Rastreamento Maxtec.



Fonte: Autoria própria.

O próximo capítulo apresenta a conclusão a respeito do presente trabalho.

4. Conclusão

O presente trabalho abordou o tema de controle de acesso a áreas restritas. Foi mostrado que soluções simples e de baixo custo podem surgir de sistemas já implementados que não tiveram totalmente suas funções esgotadas. Com um pouco de engenharia foi possível a confecção de um sistema de controle de acesso que atendeu os requisitos de projeto solicitados pelo cliente

Em relação à manutenibilidade do projeto, o mesmo foi feito visando garantir a melhor possível em relação à economia de tempo, pessoal e dinheiro. Os componentes foram escolhidos aproveitando o estoque do cliente, de forma a minimizar possíveis contratempos em relação a falhas.

Atualmente o sistema de controle de acesso proposto nesse trabalho está implementado em 11 áreas da mineradora da região e funciona satisfatoriamente.

Como trabalhos futuros sugere-se o estudo da minimização de componentes, de forma a diminuir ainda mais o custo de implementação, bem como a disponibilização das informações gerenciais diretamente em sistemas ERP.

5. Referências

BONATO, C. D. S.; NETO, R. M. F. **Um Breve Estudo Sobre Biometria**. Catalão-GO: Universidade Federal de Goiás**:** 4 p. 2012.

BRASILIANO, A. C. R.; BLANCO, L. **Planejamento Tático e Técnico Em Segurança Empresarial.** . Ed. 1 Sicurezza. São Paulo: 2003.

BRENNER, G. P. S. E.; BIZARRIA, W. **Sistema de controle de acesso com biomeria digital**. Resende - RJ: VIII Simpósio de Excelência em Gestão e Tecnologia**:** 14 p. 2011.

DECIBEL. Sinalizador visual D212. 2015. Disponível em: < http://www.decibel.com.br >. Acesso em: 10/05/2016.

DNI. Relé Automotivo DNI0240. 2015. Disponível em: < http://www.dni.com.br >. Acesso em: 16/04/2016.

FAGUNDES, F. D. et al. Comunicação Zigbee Aplicada em um Sistema de Controle. **Holos,** v. 1, p. 263-271, 2015.

FREITAS, L. C. D. **Web Services**. Americana-SP: Faculdade de Tecnologia de Americana**:** 4 p. 2006.

GALHARDO, A. T. **Sistemas Eletrônicos de Controle de Acesso**. Campinas-SP**:** 54 p. 2011.

GINES, F. H.; TSAI, T. T. **Projeto e Implementação de um Sistema de Identificação por RFID para uma Aplicação de Automação Residêncial**. São Paulo-SP: Universidade de São Paulo**:** 94 p. 2007.

JANES, R. **Estudo Sobre sistemas de segurança em instalações elétricas automatizadas**. 2009. 121 (Dissertação de Mestrado). Universidade de São Paulo, São Paulo - SP.

JFL. Sensor Infravermelho IRA 315. 2015. Disponível em: < http://www.jfl.com.br/ >. Acesso em: 10/04/2016.

JUNIOR, A. G.; LEITE, L. L. **Sistema de controle de acessoinformatizado**. MAFRA - SC: Universidade do Contestado**:** 64 p. 2009.

LUZ, J. G.; FRESSATTI, W. **RECONHECIMENTODE VOZ UTILIZANDO ARDUINO**. Paranavai-PR: Universidade Paranaense**:** 5 p. 2015.

MAXTRACK. **Manual de Instruções MTC-55**. Belo Horizonte: Maxtrack Inovações em Rastreamento**:** 54 p. 2015a.

_____. **Manual MXT151+**. Belo Horizonte-MG: Maxtrack Inovações em Rastreamento**:** 55 p. 2015b.

MOREIRA, K. B. R. **Diretrizes Para Projeto de Segurança Patrimonial em Edificações**. São Paulo - SP: USP**:** 205 p. 2007.

MORO, T. D.; DORNELES, C. F.; REBONATTO, M. T. **Web services WS versus Web Services Rest**. Passo Fundo-RS: Universidade de Passo Fundo**:** 16 p. 2011.

NARCISO, M. G. **Aplicação da Tecnologia de Identificação por Rádio Frequencia (RFID) para Controle de Bens Patrimoniais pela Web**: Global Science and Technology. 01**:** 50-59 p. 2008.

ROCHA, J. F.; DIAS, J. W. **Importância do banco de dados nas aplicações**. Curitiba-PR: Universidade Paranaense**:** 5 p. 2015.

SOUZA, W. B. D. **Cartão Mifare Classic ataques e medidas de contorno**. 2011. 205 (Dissertação de Mestrado). Universidade de São Paulo, São Paulo.

SYSTEMS, A. C. Contactless Smart Card Reader. 2016. Disponível em: < http://www.acr120u.com/ >. Acesso em: 10/04/2016.

TECH, F. Coletor de Assinatura StepOver. 2016. Disponível em: < http://www.nitgen.com.br/ >. Acesso em: 10/04/2016.

TEIXEIRA, T. **Conrole de Fluxo de Pessoas Usando RFID**. São José - SC: Instituto Federal de Santa Catarina**:** 73 p. 2011.

THOMÉ, M. L. et al. **CONTROLE DE ACESSO FÍSICO NAS EMPRESAS**. Guaratinguetá**:** 9 p. 2012.

VICTOR, B.; BOWYER, K.; SARKAR, S. **An evaluation of face and ear biometrics**. Pattern Recognition, 2002. Proceedings. 16th International Conference on. 1**:** 429-432 vol.1 p. 2002.

6. Apêndice A – Diagramas de Ligação