



UNIVERSIDADE DE TAUBATÉ

Autarquia Municipal de Regime Especial
pelo Dec. Fed. nº 78.924/76
Recredenciada Reconhecida pelo CEE/SP
CNPJ 45.176.153/0001-22

Departamento de Engenharia Elétrica
Rua Daniel Danelli s/nº Jardim Morumbi
Taubaté-Sp 12060-440
Tel.: (12) 3625-4190
e-mail: eng.eletrica@unitau.br

**JOÃO VITOR MORAES FERREIRA
LUCAS DOS SANTOS FONSECA**

Utilização de RFID para controle de áreas industriais

Taubaté - SP
2021

**JOÃO VITOR MORAES FERREIRA
LUCAS DOS SANTOS FONSECA**

Utilização de RFID para controle de áreas industriais

Trabalho de Graduação apresentado ao Departamento de Engenharia Elétrica da Universidade de Taubaté, como parte dos requisitos para obtenção do diploma de Graduação em Engenharia Elétrica e Eletrônica.

Orientador (a): Prof. Rubens Castilho Junior

Grupo Especial de Tratamento da Informação - GETI
Sistema Integrado de Bibliotecas – SIBi
Universidade de Taubaté - Unitau

F676u Fonseca, Lucas dos Santos
Utilização de RFID para controle de áreas industriais / Lucas dos Santos
Fonseca; João Vitor Moraes Ferreira. -- 2021.
46 f. : il.

Monografia (graduação) – Universidade de Taubaté, Departamento de
Engenharia Mecânica e Elétrica, 2021.

Orientação: Prof. Rubens Castilho Junior, Departamento de Engenharia
Elétrica.

1. Controle de acesso. 2. Segurança. 3. RFID. I. Ferreira, João Vitor
Moraes. II. Universidade de Taubaté. Departamento de Engenharia
Mecânica e Elétrica. Graduação em Engenharia Elétrica e Eletrônica.
III. Título.

CDD – 621.384



UNIVERSIDADE DE TAUBATÉ

Autarquia Municipal de Regime Especial
pelo Dec. Fed. nº 78.924/76
Recredenciada Reconhecida pelo CEE/SP
CNPJ 45.176.153/0001-22

Departamento de Engenharia Elétrica
Rua Daniel Danelli s/nº Jardim Morumbi
Taubaté-Sp 12060-440
Tel.: (12) 3625-4190
e-mail: eng.eletrica@unitau.br

Utilização de RFID para controle de áreas industriais

**JOÃO VITOR MORAES FERREIRA
LUCAS DOS SANTOS FONSECA**

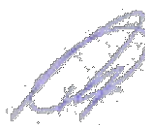
ESTE TRABALHO DE GRADUAÇÃO FOI JULGADO ADEQUADO COMO PARTE
DO REQUISITO PARA A OBTENÇÃO DO DIPLOMA DE “GRADUADO EM
ENGENHARIA ELÉTRICA E ELETRÔNICA”

**JOÃO VITOR MORAES FERREIRA
LUCAS DOS SANTOS FONSECA**

Utilização de RFID para controle de áreas industriais

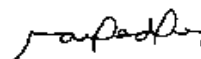
BANCA EXAMINADORA:

Prof. Esp. RUBENS CASTILHO JUNIOR
Orientador/UNITAU-DEE



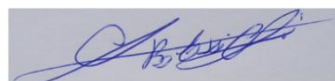
Assinatura: _____

Prof. Dr. MAURO PEDRO PERES
UNITAU-DEE



Assinatura: _____

Prof. Me. SANDRO BOTOSSI DOS SANTOS
UNITAU-DEE



Assinatura: _____

AGRADECIMENTOS

A Deus, primeiramente, por ter me dado forças para superar todas as dificuldades e por possibilitar mais essa conquista.

Agradeço aos meus familiares e, principalmente, aos meus pais, *Glauco e Patrícia*, que sempre me incentivaram, torceram e apoiaram em todos os momentos. Quero agradecer a meu pai em especial, por ter me proporcionado cursar uma faculdade e por todo apoio durante esse período. Agradeço também minha irmã *Mayara* e, também, minha namorada *Sueny*, que sempre estiveram do meu lado, me apoiando e ajudando no que era preciso.

Agradeço à Universidade de Taubaté e a todos meus professores, pelas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação profissional ao longo desses anos. Gostaria, também, de os parabenizar pelo dom de ser professor.

Por fim, agradeço a todos os meus amigos de turma, que tive a oportunidade de conhecer e de conviver durante todos esses anos.

João Vitor Moraes Ferreira

AGRADECIMENTOS

Agradeço primeiramente a Deus pela minha vida, por ter me dado forças para superar todas as dificuldades e por possibilitar mais essa conquista.

Agradeço aos meus pais, *Sumair* e *Rosely*, que sempre me incentivaram, torceram e apoiaram em todos os momentos, quero agradecer meu pai em especial, por ter me proporcionado cursar uma faculdade. Agradeço também minhas irmãs *Silvia* e *Fernanda*, minha namorada *Francini*, e aos meus cunhados *Vinicius* e *Elder*, que sempre estiveram do meu lado, me apoiando e ajudando no que era preciso.

Agradeço à Universidade de Taubaté e a todos meus professores, por todo ensinamento e conhecimento passados. Os parabênizo, também, pelo dom de ser professor. Agradeço em especial ao nosso orientador que se tornou um grande amigo, *Prof. Esp. Rubens Castilho Junior* por toda paciência e esforço em nos ajudar, e por tudo que fez por mim.

Por fim, agradeço a todos meus amigos que tive a oportunidade de conhecer, que sempre estiveram do meu lado, por toda ajuda e compreensão e por fazer parte dessa conquista.

Lucas dos Santos Fonseca

“O sucesso nasce do querer, da determinação e persistência em se chegar a um objetivo. Mesmo não atingindo o alvo, quem busca e vence obstáculos, no mínimo fara coisas admiráveis.”

José de Alencar

RESUMO

Este projeto propõe o desenvolvimento de um sistema de controle de acesso para uma empresa, trazendo mais segurança, bem como o monitoramento dos colaboradores, gerando relatórios mensais com carga horária de trabalho e permitindo a seu supervisor monitorar a jornada de trabalho. Para manter o sistema funcionando da maneira correta foram utilizados equipamentos e sistemas de última geração, os melhores existentes em mercado. Foram utilizadas controladoras, receptores, leitores, sistemas de bloqueio, cartão RFID, leitor biométrico e senha. Com isso conseguimos realizar a delimitação de áreas de livre acesso, bem como a hora que cada colaborador pode e deve acessar o local determinado, com isso visamos diminuir o tempo de perda de serviço e aumentar a produtividade dos colaboradores, tornando o processo produtivo mais competitivo em relação ao custo-benefício dos serviços prestados. Buscamos também melhorar a segurança operacional, controlando com mais eficiência as pessoas que circulam na área, diminuindo a possibilidade de acontecer algum acidente dentro da empresa.

PALAVRAS-CHAVE: Controle de Acesso. Segurança. RFID.

ABSTRACT

This project proposes the development of an access control system for a company, bringing more security, as well as monitoring employees, generating monthly reports with workload and allowing your supervisor to monitor the workday. To keep the system working correctly, the latest equipment and systems were used, the best on the market. Controllers, receivers, readers, blocking systems, RFID card, biometric reader and password were used. With this, we were able to delimit free access areas, as well as the time that each employee can and must access the specified location, with this we aim to reduce the time of lost service and increase employee productivity, making the production process more competitive in relation to the cost-benefit of the services provided. We also seek to improve operational safety, controlling people who circulate in the area more efficiently, reducing the possibility of an accident occurring within the company.

KEYWORDS: Access Control. Security. RFID.

LISTA DE FIGURAS

Figura 1 – Transponder RFID	17
Figura 2 – Arquitetura Clássica do Sistema RFID	17
Figura 3 - chaveiro RFID.	17
Figura 4 – Ilustração do Controle de Acesso.....	20
Figura 5 – Arquitetura Básica do Sistema de Controle de Acesso.....	22
Figura 6 – Protocolo Wiegand.....	23
Figura 7 – Catraca.....	25
Figura 8 – Ilustração de uma porta	26
Figura 9 – Leitora com teclado.....	27
Figura 10 – Leitora RFID	28
Figura 11 – cartão RFID.....	28
Figura 12 – Leitor Biométrico	29
Figura 13 – Cabo UTP.....	31
Figura 14 – Software	32
Figura 15 – Guarita IP	33
Figura 16 – Placa do Guarita IP.....	34
Figura 17 – Vista Externa do Guarita IP	34
Figura 18 – Acesso via Internet	35
Figura 19 – Crimpagem do Cabo	36
Figura 20 – Ilustração CTW-4A.....	36
Figura 21 – Ilustração da Leitora LN-001	37
Figura 22 – Conexão da Leitora com o Receptor.....	38
Figura 23 – Leitora LN5-P	39
Figura 24 – Projeto Controle de Acesso.....	40

LISTA DE TABELAS

Tabela 1 – Classificação RFID	18
Tabela 2 – Classificação RFID	19
Tabela 3 – Tabela de Preços	43

LISTA DE ABREVIATURAS E SIGLAS

RFID	Radio Frequency Identification
CAN	Controller Area Network
TAG	Etiqueta
PIN	Personal Identification Number
TCP	Protocolo de Controle de Transmissão
IP	Protocolo de Internet
UTP	Unshielded Twisted Pair
PVC	Policloreto de Vinil
MHz	Megahertz
kHz	Kilohertz
Mbps	Megabytes por segundo
Gbps	Gigabytes por segundo
TAG	Chaveiro
VDC	Tensão em Corrente Contínua
AC	Corrente Alternada
DC	Corrente Contínua
USB	Universal Serial Bus
PC	Computador
LED	Light Emitting Diode
V	Tensão
HTML	Hyper Text Markup Language

SUMÁRIO

1	INTRODUÇÃO.....	15
2	DESENVOLVIMENTO	16
2.1	RFID	16
2.1.1	Classificação RFID	18
2.2	CONTROLE DE ACESSO	19
2.2.1	Recursos dos sistemas de controle de acesso.....	20
2.2.2	Arquitetura dos sistemas eletrônicos de controle de acesso	22
2.3	O PROTOCOLO WIEGAND	23
2.4	REDE CAN	23
2.5	CONTROLADORA	24
2.6	BLOQUEIOS.....	24
2.6.1	Catracas eletrônicas	25
2.6.2	Portas, portões e portais.....	25
2.7	RECEPTORES	26
2.7.1	Teclados	26
2.7.2	Cartões	27
2.7.3	Biometria	29
2.8	CABOS UTP	30
2.9	SOFTWARE.....	31
3	METODOLOGIA	33
3.1	CONTROLADORA GUARITA IP.....	33
3.1.1	Especificações e características.....	33
3.1.2	Conexão via USB	35
3.1.3	Conexão via serial rs232	35
3.1.4	Conexão via TCP/IP	35
3.2	RECEPTOR WIEGAND CTW-4 ^a	36
3.2.1	Especificações.....	36
3.3	LEITORAS	37
3.3.1	Leitora LN-001	37
3.3.2	Leitora LN5-P.....	39
3.4	SOFTWARES	40
3.5	PROJETO	40
3.5.1	Descrição.....	40
4	RESULTADOS E CONCLUSÕES	42
	REFERÊNCIAS.....	44

1 INTRODUÇÃO

Hoje em dia se tornou cada vez mais comum pessoas que prezam e buscam por mais segurança e melhor controle de suas vidas, seja em aspectos profissionais ou até mesmo pessoais. Muito se fala sobre segurança no ambiente de trabalho hoje em dia, sabendo-se quem são e onde estão as pessoas que circulam por uma empresa. Para que seja posta em prática essa segurança, faz-se necessário, às vezes, estabelecer algum tipo de bloqueio físico de certas áreas e locais, permitindo que apenas pessoas autorizadas tenham acesso. Mesmo tendo portas e fechaduras já instaladas, elas não garantem o mesmo nível de segurança que um sistema de controle de acesso pode fornecer.

Portanto, será abordado neste projeto o controle de entrada e saída de áreas produtivas, áreas de atuação direta de colaboradores terceiros e ou visitantes.

Nos últimos anos tivemos um avanço muito significativo nas tecnologias, permitindo que o controle de pessoas evoluísse para sistemas mais robustos e com ainda mais informação para os administradores de empresas e até mesmo de áreas produtivas.

Neste projeto iremos passar por todos os componentes necessários para uma implantação do sistema de controle de acesso, que é a responsável pelo controle de entrada e saída de pessoas em locais delimitados. Todos os componentes abordados neste projeto são interligados e concentram a informação em um software que realiza o gerenciamento do controle a partir de como foi programado, permitindo ou não ao usuário acesso ao local. Além disso, o sistema armazena toda informação em um banco de dados para uma futura consulta, se necessário, possibilitando maior controle sobre todos os colaboradores.

2 DESENVOLVIMENTO

2.1 RFID

Identificação por Radiofrequência (RFID) é uma forma de comunicação sem contato que utiliza ondas de rádio para identificar e rastrear objetos. Um sistema RFID é composto por leitores e etiquetas que se comunicam via rádio (WANT, 2006).

Nos últimos anos, a identificação por radiofrequência (RFID) tem se tornado cada vez mais utilizada. Ela permite a identificação de etiquetas em até certa distância, e suas etiquetas são mais práticas e suportam uma quantidade maior de identificadores únicos do que os códigos de barra (WANT, 2006).

Etiquetas RFID são pequenas e requerem pouca energia para funcionar, não necessitando de baterias e podendo ser ativadas por indução eletromagnética. Isso faz com que elas sejam baratas e torna fácil sua aplicação em qualquer objeto que se queira identificar ou rastrear.

Podemos dividir as RFID em duas classes. A primeira delas é a classe ativa, cujas etiquetas requerem uma fonte de energia para funcionar, necessitando estarem conectadas a uma alimentação externa ou alimentadas por uma bateria interna. Um exemplo de aplicação de um sistema de RFID ativo são os transponders de aeronaves, que identificam a aeronave e sua origem, conforme a figura 1 temos um transponder RFID.

A segunda classe é a RFID passiva, cuja etiqueta não requeira baterias ou manutenção.

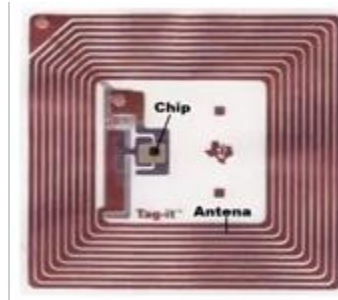
As etiquetas passivas são constituídas de três partes: uma antena, um chip anexado à antena e algum invólucro, que pode ser desde um pequeno frasco de vidro até adesivos ou carteirinhas. O leitor de etiquetas é responsável por alimentar a etiqueta e se comunicar com a etiqueta, enquanto a antena captura a energia e a transfere ao seu identificador único da etiqueta, em um processo controlado pelo chip (WANT, 2006).

O sistema de tecnologia RFID é utilizado há muito tempo em nosso meio, aproximadamente desde a Segunda Guerra Mundial, onde foi utilizado nos sistemas de radares por vários países, permitindo assim que os responsáveis de bases militares tivessem a ciência da proximidade de aviões e podendo se preparar para ataques. O sistema foi inventado pelo físico escocês Robert Alexander Watson-Watt.

O sistema RFID já é uma tecnologia utilizada em larga escala no mundo e já conquistou o seu espaço no mercado, podendo ser ampliada ainda mais no que se refere a identificação de produtos, controle de estoque de empresas e até mesmo no controle de

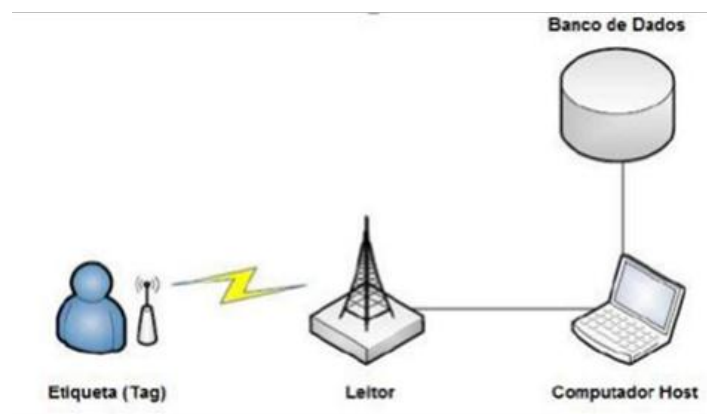
peças que podem acessar uma determinada área ou não. Na figura 2 temos uma arquitetura clássica do sistema RFID e na figura 3 temos um chaveiro RFID.

Figura 1 – Transponder RFID



Fonte: <https://portal.vidadesilicio.com.br/modulo-rfid-rc522-mifare/>

Figura 2 – Arquitetura Clássica do Sistema RFID



Fonte: http://www.abepro.org.br/biblioteca/TN_STO_206_219_27426.pdf

Figura 3 - chaveiro RFID.



Fonte:

https://www.monografias.ufop.br/bitstream/35400000/2222/3/MONOGRAFIA_SistemaControleAcesso.pdf

2.1.1 Classificação RFID

As Tabelas 1 e 2 a seguir trazem a classificação dos sistemas RFID por frequência, suas aplicações e particularidades.

Tabela 1 – Classificação RFID

Tipo	LF	HF
Faixa de Frequência	125 ou 134,2 kHz	13,56 MHz
Alcance para leitura	< 0,5m	≥ 1m
Particularidades	Precisa de antenas grandes, o que resulta em altos custos de produção. Sofre pequena degradação do sinal na presença de líquido e metais.	Melhor aproveitamento em alcance que as LF. É a melhor escolha para sistemas que não exijam um longo alcance e não seja necessária a leitura de um grande número de etiquetas ao mesmo tempo.
Fontes de Energia	Acoplamento magnético (campo próximo)	Acoplamento magnético (campo próximo)
Aplicações Típicas	Controle de Acesso Identificação de animais Imobilização de veículos	Controle de Acesso Controle de pagamento Identificação de objetos Controle de bagagens
Leitura Múltipla	Lenta	Média
Leitura em ambientes metálicos ou com líquidos	Melhor	Média
Tamanho da etiqueta	Grande	Médio

Fonte: <http://www.sabereletronica.com.br/secoes/leitura/685>

Tabela 2 – Classificação RFID

Tipo	UHF	Microondas
Faixa de Frequência	860 ou 930 MHz	2,45 ou 5,8 GHz
Alcance para leitura	Entre 4 e 5 m	≥ 1m
Particularidades	Muito mais baratas que as LH e HF. Tem os chips mais avançados e permitem a leitura de múltiplas etiquetas ao mesmo tempo.	Características parecidas com a UHF, com diferença de ser muito mais rápida na transmissão de dados. É muito afetada na presença de líquidos e metais.
Fontes de Energia	Acoplamento eletromagnético (campo distante)	Acoplamento eletromagnético (campo distante)
Aplicações Típicas	Identificação de caixas de equipamentos	Coleta de dados em tempo real. A frequência 5,8GHz vem sendo abandonada pelos sistemas RFID
Leitura Múltipla	Rápida	Rápida
Leitura em ambientes metálicos ou com líquidos	Ruim	Pior
Tamanho da etiqueta	Pequeno	Pequeno

Fonte: <http://www.sabereletronica.com.br/secoes/leitura/685>

2.2 CONTROLE DE ACESSO

O controle de acesso é uma parte importante de todo o sistema RFID, ele é o componente que faz o controle via proximidade do cartão ou biometria para a liberação de fluxo de pessoas em um determinado local, permitindo a entrada ou não. Com isso não existe a necessidade de ter uma pessoa física fazendo a liberação de pessoas, o próprio sistema já entende que a pessoa está liberada para acessar aquele ambiente, tudo isso é possível, pois cada indivíduo possui a sua TAG, que pode ser controlada através de um sistema único de programação. O processo de liberação a um determinado local ocorre através de um cadastro realizado no banco de dados e gravação das informações do indivíduo por crachá de aproximação ou Biometria, com qualquer indivíduo podendo acessar locais previamente autorizados.

Um sistema de controle de acesso eletrônico pode permitir uma auditoria de maneira descomplicada. Um sistema eletrônico pode manter um registro de hora e data de cada acesso ou tentativa de acesso à uma área de acesso restrito, podendo identificar sobre a pessoa que realizou a tentativa de acesso (DEUTSCH, 2018).

Os leitores são montados do lado de fora das portas e são a única parte do sistema de controle de acesso que a maioria das pessoas veem. Em um sistema de controle de acesso moderno, os leitores são responsáveis por alguma maneira de autenticação. Se o sistema usar um leitor de código, você insere um número de identificação pessoal (PIN) em um teclado

para se identificar no sistema. Com um leitor de credenciais, você apresentaria um cartão ou chaveiro. Um leitor biométrico deve ler uma parte de você (DEUTSCH, 2018).

As credenciais de controle de acesso geralmente vêm na forma de cartões ou etiquetas que podem ser penduradas no chaveiro. As credenciais mais comuns são cartões de identificação por radiofrequência (RFID), que podem ser lidos à distância. Em alguns casos, eles não precisam ser removidos do bolso para serem usados (DEUTSCH, 2018).

Um sistema de acesso eletrônico também pode permitir a restrição de acesso com base em diferentes políticas de acesso, tais como restrição de hora e dia em que o acesso pode ser realizado por uma determinada pessoa, quantidade máxima de vezes que uma determinada pessoa pode acessar em um intervalo de tempo, e outros critérios, como o saldo do usuário disponível no sistema. Abaixo, na figura 4, temos uma ilustração do controle de acesso.

Figura 4 – Ilustração do Controle de Acesso



Fonte: <https://gestaodesegurancaprivada.com.br/sistema-controle-de-acesso-definicoes-como-funciona/>

2.2.1 Recursos dos sistemas de controle de acesso

Os sistemas eletrônicos de controle de acesso são implementados através de uma integração entre software e hardware. Todos os parâmetros do sistema são configurados nos softwares e o hardware fica responsável para fazer a comunicação do meio de identificação utilizado com o software e, também, para fazer o chaveamento do dispositivo de bloqueio por ele controlado.

Os softwares de gerenciamento de controle de acesso devem possuir basicamente os seguintes recursos:

- Permitir o controle de acesso de pessoas que utilizam o sistema frequentemente, funcionários de uma empresa, por exemplo, e visitantes e tratar essas informações de forma independente;
- Permitir configuração zonas, as quais são o conjunto de áreas delimitadas por bloqueios físicos que restringem e controlam o acesso. Pode-se atribuir direito de acesso a todas as áreas de uma zona ou somente a uma ou algumas delas;
- Permitir configuração de tabelas de horários, dias da semana e feriados criados para que os acessos sejam restritos ou permitidos somente em alguma faixa horária e/ou dias da semana e feriados, associado à zona permite um controle mais rigoroso do acesso;
- Permitir que a associação das tabelas de áreas e horários seja associada para cada pessoa ou grupo de pessoas que terão que obedecer às mesmas políticas de segurança. A associação das tabelas forma um conceito denominado direitos de acesso. As definições dos direitos de acesso são feitas em conjunto entre as gerências dos diversos departamentos e da gestão de segurança patrimonial, em muitas empresas a gestão de segurança é feita pelo departamento de recursos humanos. Reúne-se a gerência de todas as áreas, pois o controle de acesso, muitas vezes, não é aplicado somente pela segurança patrimonial, mas sim também pela segurança do trabalho.
- Armazenar todos os eventos do sistema, tanto os de acessos autorizados quanto os de acessos negados, para possibilitar consultas futuras;
- É possível no cadastro das pessoas inserirem informações de departamento, empresa e categoria;
- Permite emissão de relatórios e importação deles em diversos formatos, como arquivos texto, planilhas e pdf, por exemplo, para facilitar a análise dos mesmos.
- Monitoramento em tempo real dos eventos de acesso que estejam ocorrendo, esses eventos podem alertar o operador do sistema de que uma pessoa não autorizada está tentando acessar a uma área na qual não tem permissão e, também, informa ao operador se algum dispositivo de bloqueio permanece aberto por mais tempo que o necessário.

Da mesma forma que os softwares de gerenciamento precisam ter alguns recursos, o hardware deve atender alguns requisitos básicos para possibilitar um bom projeto. Desses aspectos básicos se destacam:

- Possuir interface de comunicação serial ou ethernet – as interfaces seriais estão deixando de ser utilizadas por possuir muitas particularidades na sua implementação, como limitações de distância, as interfaces ethernet que utilizam protocolo TCP/IP estão substituindo as seriais pela facilidade de configuração e por muitas vezes permitir o aproveitamento de infraestrutura da rede existente, o que facilita e reduz custos de instalação do sistema;
- Permitir memória interna para armazenamento das listas de cartões e tabelas do sistema para eventual falha de comunicação com o servidor;
- Possuir entrada para conexão de sensores que notificarão o sistema de que houve passagem pelo dispositivo de bloqueio ou mesmo que o dispositivo de bloqueio está aberto por mais tempo do que necessário;

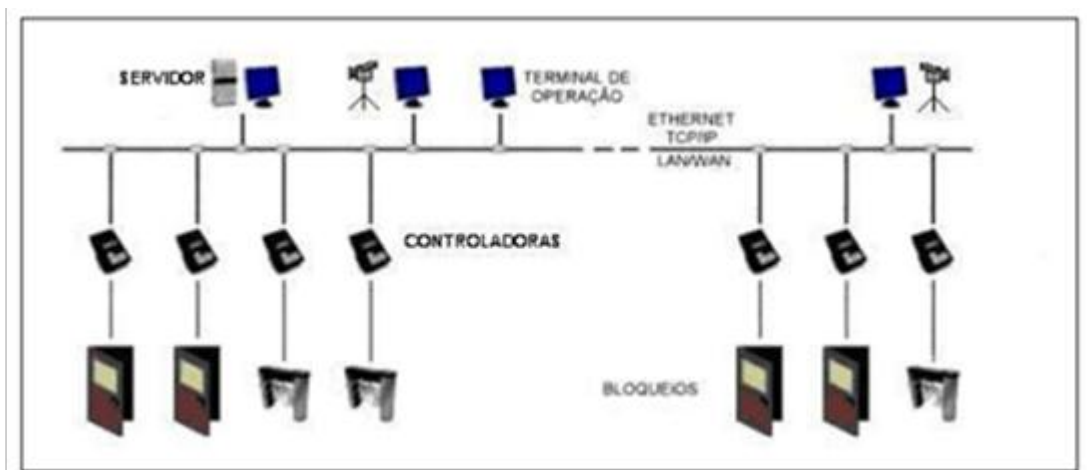
- Entrada para conexão de sinais que indicam emergência como dispositivos de quebra de vidro para liberação do dispositivo de bloqueio;
- Possuir saídas de contato seco, ou seja, relés para que possam ser adaptadas a diferentes dispositivos de bloqueio;
- Possuir entrada para identificadores preferencialmente no protocolo Wiegand, o qual funciona com praticamente todos os leitores RFID e biométricos.

Integrando os recursos de software e hardware é possível projetar sistemas de controle de acesso conforme, que podem ser instalados em diferentes áreas segregadas entre si por algum dispositivo de bloqueio, que podem ser portas, cancelas, catracas ou portões.

2.2.2 Arquitetura dos sistemas eletrônicos de controle de acesso

Existem muitos fabricantes de software e hardware para sistemas de controle de acesso, a partir dos quais a grande maioria possibilita que os sistemas instalados atendam aos critérios citados anteriormente. Dessa forma, independentemente do fabricante escolhido, há uma arquitetura básica necessária para implementação do sistema, a qual pode ser representada pela figura 5.

Figura 5 – Arquitetura Básica do Sistema de Controle de Acesso.



Fonte: <http://lyceumonline.usf.edu.br/salavirtual/documentos/2141.pdf>

Note, na figura, que o sistema é composto por servidor, rede ethernet, terminais de operação, controladoras, bloqueios e identificadores. Todos esses elementos são integrados entre si de forma que a identificação chegue ao servidor e este “responda” se o acesso será ou não permitido.

2.3 O PROTOCOLO WIEGAND

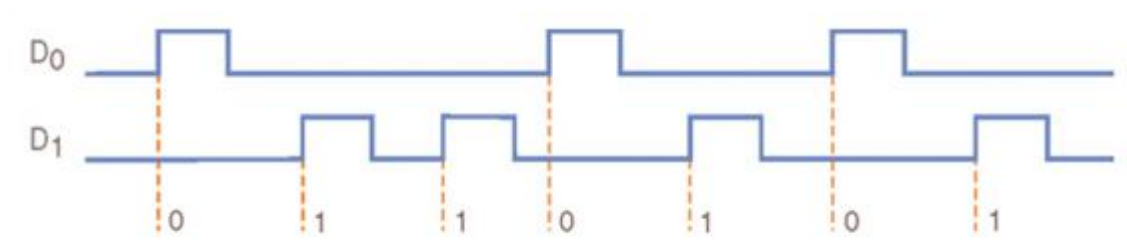
O Wiegand é um protocolo desenvolvido pela empresa HID, muito utilizado no mercado de controle de acesso. As especificidades desse protocolo são baseadas em dois fios, um denominado DATA0 e outro denominado DATA1, que se alternam para o envio de informações.

Quando o equipamento de leitura está em um estado “inativo” ambos os fios, tanto o DATA0 quanto o DATA1, ficam em estado 0. Caso seja enviado um bit 0, o DATA0 modifica o estado de 0 para 1, e o estado do DATA1 permanece em 0. Caso seja enviado o bit 1, o DATA1 modifica seu estado, ficando em 1, e o estado do DATA0 permanece em 0. Essa alteração de estado ocorre sempre respeitando uma determinada temporização que, segundo o protocolo padrão, deveria ser de 50µs. Após esse tempo, o DATA1 ou DATA0 volta para 0 e o próximo bit é enviado somente após 100ms.

O tamanho da informação contida no cartão possui particularidades. O protocolo apresenta a informação de 26 bits, sendo o primeiro e o último bit de paridade, os 8 bits seguintes ao primeiro o facility-code (código de acesso) e os 16 bits restantes o user-code, onde a informação é armazenada.

Os bits de paridade são calculados da seguinte maneira: o primeiro bit refere-se aos 12 próximos bits do código e o último bit se refere aos outros 12 bits. Isso faz com que exista um controle de integridade de informação para que não haja problemas na comunicação. A figura 6 traz uma ilustração de como seria a identificação de um bit 0 ou bit 1, porém nesta ilustração estes ocorrem quando estas linhas estão em nível alto.

Figura 6 – Protocolo Wiegand



Fonte: <http://www.sabereletronica.com.br/secoes/leitura/685>

2.4 REDE CAN

A rede CAN é o sincronismo entre os módulos conectados a uma rede que é feito em relação ao início de cada mensagem lançada ao barramento, trabalhando sempre com um

conceito que podemos chamar de multi-mestre, pois todos os módulos ligados a ele podem se tornar um mestre em determinado momento e escravo em outro. Outro ponto positivo da rede CAN é o envio de mensagens em um regime que chamamos de multicast, que é caracterizado pelo envio de qualquer tipo de mensagem para todos os módulos interligados na rede.

2.5 CONTROLADORA

Este módulo é o responsável pelo gerenciamento do controle de acesso propriamente dito. Recebem do servidor os dados necessários tais como listas de cartões, áreas habilitadas, feriados e outros. Gerencia as solicitações de acesso dos leitores, verifica as restrições e autoriza ou nega o acesso conforme o caso. Todos os eventos detectados nos módulos são informados ao servidor e são armazenados no banco de dados. Possui interfaces para a conexão de leitores de cartões ou identificadores biométricos, saídas de relé para comandar a liberação dos bloqueios e entradas de sinal para confirmação de passagem pelo bloqueio.

O controlador de acesso serve justamente para liberar a entrada daqueles que possuem permissão e segurar aqueles que não possuem autorização até que ela seja concedida.

O cidadão pode ser reconhecido por meio de biometria, senhas, reconhecimento facial, cartões de proximidade, código de barras, QR Code, entre outras ferramentas.

Por meio de aplicativos e softwares específicos, é possível administrar permissões a distância, como nas portarias remotas. Determinado cidadão pode receber permissão de acesso com hora marcada ou apenas a alguns ambientes.

Os mecanismos de identificação se integram facilmente com catracas, torniquetes, cancelas, clausuras e outras barreiras.

2.6 BLOQUEIOS

São as barreiras físicas utilizadas para segregar as áreas controladas das de uso comum, ou seja, é o meio de conexão do indivíduo (pessoa ou veículo) às áreas de acesso restrito. Vários dispositivos de bloqueio podem ser controlados por sistemas eletrônicos de controle de acesso, pois praticamente todos são chaveados por contato eletromecânico, seja por um simples pulso de contato seco ou por chaveamento de um dos fios que alimentam o dispositivo. São exemplos de dispositivos de bloqueios: portas, portões, cancelas, catracas dentre outros.

2.6.1 Catracas eletrônicas

As catracas são dispositivos eletromecânicos utilizados para controle de passagem de pessoas. São normalmente instaladas em recepções, por não haver necessidade de dividir o ambiente com paredes e portas para restringir a passagem. A vantagem é que, por seu controle ser giratório, é permitido que passe uma pessoa por vez evitando que uma pessoa não autorizada aproveite a passagem da pessoa anterior. Normalmente requerem uma atividade anterior como o cadastramento dos visitantes e cadastramento dos funcionários. Abaixo, na figura 7, temos a demonstração de uma catraca com funcionalidade de senhas e crachá.

Figura 7 – Catraca

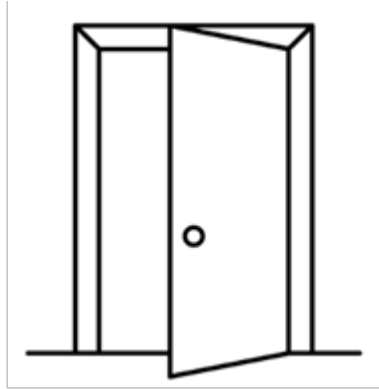


Fonte: <https://lojadoponto.com.br/catraca-de-acesso-lumen-sf-henry-bio-prox-e-cofre-coletor.html>

2.6.2 Portas, portões e portais

São muito utilizadas para separar ambientes que necessitem de mais segurança. Para que uma porta funcione em um sistema de controle de acesso é instalada uma fechadura eletromagnética para substituir a fechadura existente ou para funcionar em conjunto com a mesma como redundância de segurança. O tipo de porta é projetado de acordo com a área na qual serão instalados, os diversos sistemas podem utilizar portas duplas formando uma eclusa na qual uma só pode ser aberta com a outra fechada, as portas também podem ser giratórias para que passe somente uma pessoa por vez e ainda portais com detectores de metais.

Figura 8 – Ilustração de uma porta



Fonte: <http://www.ultracoloringpages.com/pt/p/porta-aberta-desenho-para-colorir/675ef794cbd1f0cadbee6913abfeca6b>

2.7 RECEPTORES

Os identificadores são definidos como a tecnologia utilizada para identificação da pessoa ao sistema. Podem ser utilizados teclados para digitação de senhas, leitores de cartões (RFID ou código de barras), leitores biométricos (identificação de impressões digitais, geometria da mão, reconhecimento facial dentre outros).

2.7.1 Teclados

Os sistemas com teclados permitem o acesso da pessoa a partir da correta digitação da senha desta forma o dispositivo de bloqueio é liberado. A desvantagem deste sistema é a grande facilidade para copiar a senha e com o tempo o desgaste do teclado facilitará a descoberta das senhas pelas teclas que ficam visivelmente mais desgastadas. Isso não impede que um indivíduo forneça sua senha para outro, desta forma não há garantia de quem ingressou, porém são registrados data e horário dos acessos.

Os sistemas com teclados são indicados somente para áreas com pouco fluxo de pessoas e em áreas restritas. A figura 9 abaixo ilustra um teclado utilizado em sistemas de controle de acesso. O usuário digita uma senha para ter acesso o nível de controle é baixo, pois senha pode ser divulgada. Pouquíssimo usado em segurança, devido à sua fragilidade.

Figura 9 – Leitora com teclado



Fonte: https://nice.com.br/novo2017/wp-content/uploads/2018/06/FACE_SHEET_LN-001-25-08-17.pdf

2.7.2 Cartões

Os cartões são sistemas bastante empregados pelo baixo custo e pela variedade de possibilidades que oferecem os softwares que lhes dão suporte. Podem ser de memória de contato ou de proximidade, para leitura de código de barras ou tarjas magnéticas, sendo que os dois últimos estão deixando de ser utilizados pela quantidade de problemas e pela facilidade de cópia dos cartões.

Os cartões de proximidade possuem um protocolo de codificação chamado Wiegand, que permite codificação dos cartões em 26 ou 32 bits, tornando praticamente impossível a incidência de cartões repetidos. A cópia de cartões é impossível.

Os cartões de proximidade utilizam tecnologia de identificação por rádio frequência (RFID). Esses cartões podem ser ativos ou passivos.

Os cartões de proximidade passivos possuem um circuito constituído de bobina entre o substrato plástico que dá a forma do cartão, essa bobina é excitada quando aproximada do leitor o qual emite um campo eletromagnético, no mesmo leitor há um receptor que capta o sinal emitido pelo cartão e o envia para placa controladora.

Os cartões de proximidade ativos possuem uma bateria interna para alimentação de seu circuito, que emite um sinal sem necessidade de estar muito próximo ao leitor. Um exemplo de aplicação dos cartões ativos é o serviço de “Sem Parar”, oferecido nos pedágios por suas concessionárias.

Os cartões de proximidade são extremamente seguros, sendo quase impossível copiá-los. Considerando sua durabilidade seu custo pode ser considerado médio.

Esse meio de identificação possui um bom nível de segurança. As leitoras de proximidade são especificadas de acordo com a distância máxima admissível para que elas reconheçam o cartão. Uma observação importante em relação aos sistemas que utilizam cartões de proximidade, que pode ser considerada uma desvantagem, é que os cartões de um fabricante não funcionam com leitores de outro e vice-versa. Outra desvantagem é o fato de que podem ser utilizados por pessoas não autorizadas, seja por extravio, perda, roubo ou furto. A figura 10 tem a ilustração de uma leitora RFID e na figura 11, um cartão RFID.

Figura 10 – Leitora RFID



Fonte: <https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSIFT4oHs9q1HRYKnpjz-OHgA25Q2SvC9q9qcw&usqp=CAU>

Figura 11 – cartão RFID.



Fonte: <https://www.i9automacaocomercial.com.br/cartao-de-proximidade-rfid-branco/>

2.7.3 Biometria

É estudo estatístico das características físicas ou comportamentais dos seres vivos. Recentemente esse termo também foi associado às pessoas como forma de identificá-las unicamente. Hoje é usada na identificação criminal, controle de ponto, controle de acesso etc. Como dito anteriormente, o reconhecimento do indivíduo será dado por características físicas dele. Foram criadas leitoras biométricas para aplicações em indústrias, empresas e condomínios, para restringir o acesso de pessoas não autorizadas ao estabelecimento, e até controlar horários de funcionários com forma de marcar o ponto.

O controle biométrico é extremamente confiável, pois sua estrutura básica consiste no registro de certas características físicas ou comportamentais de cada pessoa, que são comparadas a um arquivo armazenado em seu banco de dados. Esses sistemas se tornaram possíveis com a evolução das técnicas de processamento digital de sinais, utilizando essas técnicas as características são amostradas, digitalizadas e armazenadas em um banco de dados associada a um código (BRASILIANO, 2003, p. 47).

O custo dos equipamentos que permitem registro e leitura de características biométricas é muito alto se comparado aos anteriores, por isso são utilizados somente em áreas consideradas de alta segurança ou de alto risco (BRASILIANO, 2003, p. 48).

Na figura 12 temos uma demonstração de um leitor biométrico.

Figura 12 – Leitor Biométrico



Fonte:

https://lh3.googleusercontent.com/proxy/mEIR3FhtmksFdh8Nbi3IOv0b5j52FRV1x3sXodYdgVv4HLZEz1Y363YP6FUxAzo011UQHESZ0E9rQ7qpKD-YXSpPuOgH7Ba-ug2oHg-kKSbmkEzkOMMU_-g4j3981k

2.8 CABOS UTP

O cabo UTP tem como origem o cabo coaxial, muito utilizado nos anos 90 em redes locais Ethernet para reduzir interferências, mas de pouca flexibilidade e com taxa de transferência máxima de somente 10 Mbps.

Para superar essas limitações, empresas se reuniram e desenvolveram os cabos Unshielded Twisted Pair (UTP), também conhecidos como cabos de par trançado sem blindagem. Eles são de uma fiação mais leve, flexível e barata, que não necessita de aterramento, e com impedância constante de 100 OMHs – desenvolvida para suportar velocidades, a princípio, de até 100 Mbps, ou 250 MHz, na considerada Fast Ethernet.

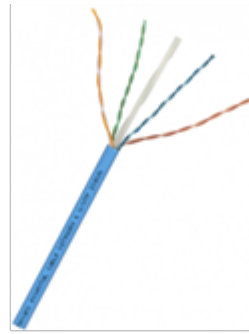
O cabo UTP tem, geralmente, quatro pares de fios condutores trançados com saídas de dados positivas e negativas, cada qual com sua finalidade específica, protegidos por um invólucro de PVC. Ao serem trançados uns aos outros em espirais virtuais aos pares, esse tipo de cabeamento cria uma espécie de campo magnético que aumenta a proteção contra interferências na rede e reduz as chances de ocorrência de ruídos externos durante a transmissão de informações.

Para diferenciar os tipos de cabos UTP, eles foram divididos em categorias de acordo com suas características físicas e lógicas, e numerados conforme o surgimento de novas gerações.

- Categoria 1: cabos telefônicos tradicionais, utilizados nos anos 90, com capacidade de transportar somente voz.
- Categoria 2: utilizados antes das redes Ethernet, com capacidade de transmissão de até 4 Mbps.
- Categoria 3: primeira categoria desenvolvida para redes de computadores de até 10 Mbps, com capacidade transmissora de 16 MHz, e em que teve início a padronização dos pares trançados.
- Categoria 4: com 4 pares trançados, essa categoria de cabeamento possibilitou a utilização de redes com transmissão de dados com até 20 MHz e velocidade de 16 Mbps.
- Categoria 5: o maior salto de modernidades dos cabos UTP. Essa nova categoria permitiu transmissões com até 100 MHz e transferências de 100 Mbps.
- Categoria 5e e 6: onde surge a Gigabit Ethernet, pois esse cabeamento suporta envio de dados de até 1 Gbps.
- Categoria 6a: a mais moderna entre as existentes, com capacidade para até 10 Gbps e ondas de 500 MHz, porém, atualizada para reduzir as interferências entre os pares de cabos.

Na figura 13 temos uma demonstração de um cabo UTP.

Figura 13 – Cabo UTP



Fonte: https://www.connectlan.com.br/?navega=paginas_interna&id_pag=28&interna=315

2.9 SOFTWARE

É um sistema no qual é capaz de controlar de forma dinâmica e em tempo real o fluxo de entrada e saída de pessoas registrando por meio de eventos as pessoas autorizadas ou não a entrar em um lugar

O sistema informa as informações mais úteis para uma identificação rápida e segura.

O fluxo de acesso fica registrado e disponível em forma de relatórios para possíveis futuras consultas. Além disso, há opção de filtrar os relatórios para facilitar a busca de um determinado perfil.

O sistema também é capaz de identificar controladoras, módulos e leitoras biométricas que estão online no sistema, facilitando a identificação de algum problema no hardware.

O software é totalmente integrado com sistemas de TAG, biometria, QR Code, cartões de proximidade, chaveiros, senhas, botoeira, além de poder controlar portas, portões, cancelas, catracas, torniquetes, urnas coletoras, dispensadores de cartões etc.

Figura 14 – Software



Fonte: <https://firstcontrol.com.br/servicos/control-guarita/>

3 METODOLOGIA

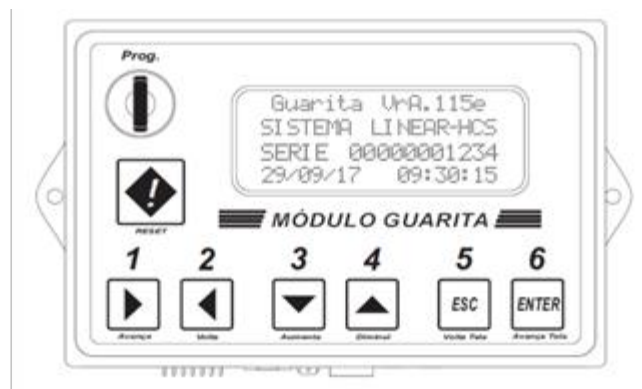
A metodologia utilizada consiste em desenvolver um projeto que irá auxiliar o controle de acesso às áreas restritas de uma empresa. O objetivo do projeto será de ter um sistema robusto e seguro.

No projeto foram utilizados alguns componentes existentes no mercado, sendo eles a controladora, leitora e o receptor, todos da marca Nice Brasil e foram utilizados sistemas de bloqueios e software de controle. Com isso foi realizado o desenvolvimento de todo um sistema físico de controle de acesso e, também, de inteligência, que auxilia um administrador de todo o sistema a controlar e acompanhar todo o processo de pessoas dentro da empresa.

3.1 CONTROLADORA GUARITA IP

A controladora escolhida foi a guarita IP, que é um dos principais componentes de todo o processo, sendo utilizada para gerenciar e controlar o acesso de pessoas dentro da empresa, interligando-se aos receptores e dispositivos de controle. Os dispositivos de controle podem ser do tipo Tag ativo, Tag Passivo, cartões RFID, Senhas e Biometrias. O Guarita IP pode, em conjunto com os receptores dos dispositivos, funcionar em modo de comando de abertura direta do portão ou fechadura

Figura 15 – Guarita IP



Fonte: https://nice.com.br/novo2017/wp-content/uploads/2018/06/M%C3%93DULO-GUARITA-IP_NICE.pdf

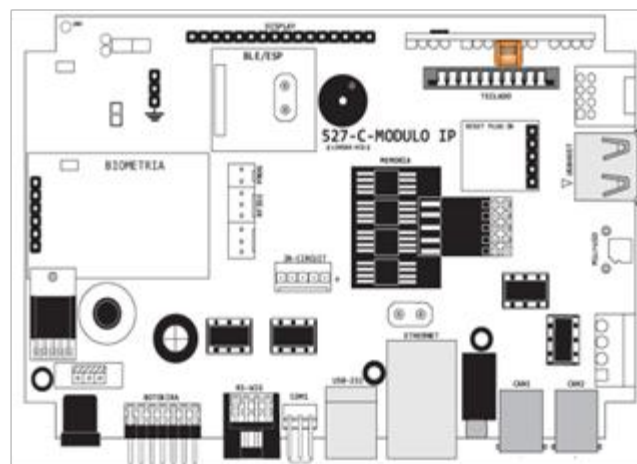
3.1.1 Especificações e características

- Necessita de uma fonte de alimentação externa, de 12VDC e com uma corrente de 1ª com filtro contra transientes de rede elétrica de entrada (corrente alternada - AC) e de saída (corrente contínua - DC);

- Operar interligada com os receptores Linear-HCS, possibilitando a restrição ou liberação de acesso de um determinado dispositivo a locais específicos;
- Uma entrada USB Host para conexão com Pen Drive para atualização de firmware, backup completo de dados do equipamento, leitor USB para cadastramento de dispositivos e teclado de computador para facilitar a inserção dos dados dos usuários durante a programação.
- Uma porta de comunicação RS232 para interface com computador.
- Uma porta USB Device para interface com PC.
- Uma porta de comunicação TCP/IP para interface com computador;
- Uma entrada para leitores Wiegand “26 ou 34bits” ou RS485 externos para facilitar o cadastramento de biometrias, cartões e chaveiros de proximidade.
- Duas portas CAN independentes para comunicação com receptores ou placas controladoras Linear-HCS.

Abaixo, na figura 15, temos, com detalhes, a placa do Guarita IP e na figura 16 temos a vista externa da mesma.

Figura 16 – Placa do Guarita IP



Fonte: https://nice.com.br/novo2017/wp-content/uploads/2018/06/M%C3%93DULO-GUARITA-IP_NICE.pdf

Figura 17 – Vista Externa do Guarita IP



Fonte: https://nice.com.br/novo2017/wp-content/uploads/2018/06/M%C3%93DULO-GUARITA-IP_NICE.pdf

O Guarita IP pode se comunicar com o PC por meio de softwares específicos, que serve tanto para manutenção quanto configuração, que é disponibilizado pela Nice, para a conexão pode se utilizar USB Device, Serial RS232 ou TCP/IP.

3.1.2 Conexão via USB

Para a conexão via USB, é necessário ter previamente instalado no computador o software da Nice.

3.1.3 Conexão via serial rs232

Para a conexão via serial RS232 é necessário ter instalado no computador o software da Nice. De acordo com a norma existente, é recomendada a utilização de cabos seriais com até 15 metros. Para distâncias acima de 15 metros recomenda-se a utilização da comunicação via TCP/IP.

3.1.4 Conexão via TCP/IP

Para a configuração via internet se utiliza uma HTML interna, e para obter o acesso, digite em um navegador de internet o endereço de IP do Guarita IP.

Figura 18 – Acesso via Internet

Configurações de Fábrica	
IP	192.168.0.10
Acesso	http://192.168.0.10/
Usuário	admin
Senha	linear

Fonte: https://nice.com.br/novo2017/wp-content/uploads/2018/06/M%C3%93DULO-GUARITA-IP_NICE.pdf

A ligação física entre o Guarita IP e o computador é feita conforme o padrão TIA-568A, crimpado pino a pino (crimpagem idêntica nas duas extremidades do cabo), conforme a ilustração da figura 19 Para a rede TCP/IP os cabos indicados são os CABOS UTP CAT5 e CAT6.

Figura 19 – Crimpagem do Cabo



Fonte: https://nice.com.br/novo2017/wp-content/uploads/2018/06/M%C3%93DULO-GUARITA-IP_NICE.pdf

3.2 RECEPTOR WIEGAND CTW-4ª

Figura 20 – Ilustração CTW-4A



Fonte: <https://nice.com.br/novo2017/wp-content/uploads/2018/06/GUIA-R%C3%81PIDO-CTW-4A-RECCTW4-D-HW-459-SW-%E2%89%A5-1.001x.pdf>

O receptor escolhido para o projeto foi o CTW4 da Linear, da marca Nice Brasil. Os receptores são responsáveis pelo recebimento e envio de informações entre controladora e leitora. Eles que garantem a identificação de acesso e a localização do mesmo com mais segurança. Permitindo, ou não, a liberação da catraca ou portas de acesso. Este equipamento é um dos principais itens que dispõem de recursos especiais no auxílio da segurança de áreas e dos usuários do sistema. Podemos interligar até 8 receptores, simultaneamente, em um módulo Guarita IP. Cada receptor instalado pode comandar até quatro portas, catracas, dispondo sempre de um sistema de ligação CAN, que permite restringir o acesso de determinada pessoa a um ou mais receptores da rede, de acordo com a programação.

3.2.1 Especificações

- Independentemente do número de receptores ou sequência de ligação do varal, sobrarão 2 pontos no início e final da interligação, onde devem ser inseridos resistores de fim de linha de 100R nas extremidades.
- Em casos de dificuldades na comunicação CAN mesmo utilizando o cabo indicado, aterre cada ponto da rede ligando a malha ao painel de aterramento.
- Funciona interligado ao Módulo Linear HCS 2010 e Guarita IP;

- Aceita até quatro leitores Linear RFID;
- Utilizar fonte de alimentação 12VDC x 2ª

3.3 LEITORAS

As leitoras utilizadas para o projeto foram a LN-001 para acesso com senha e cartão RFID e LN5-P para acesso com biometria, ambas são da Nice Brasil. A leitora é responsável pela leitura de informações contidas em cartões, senhas e biometrias, sendo a melhor escolha para garantir um perfeito funcionamento e segurança das áreas que são controladas. Ela envia as informações para o receptor que, por sua vez, comunica com a controladora e libera ou não o acesso ao local.

3.3.1 Leitora LN-001

Leitora de acesso via cartão e PIN.

Figura 21 – Ilustração da Leitora LN-001



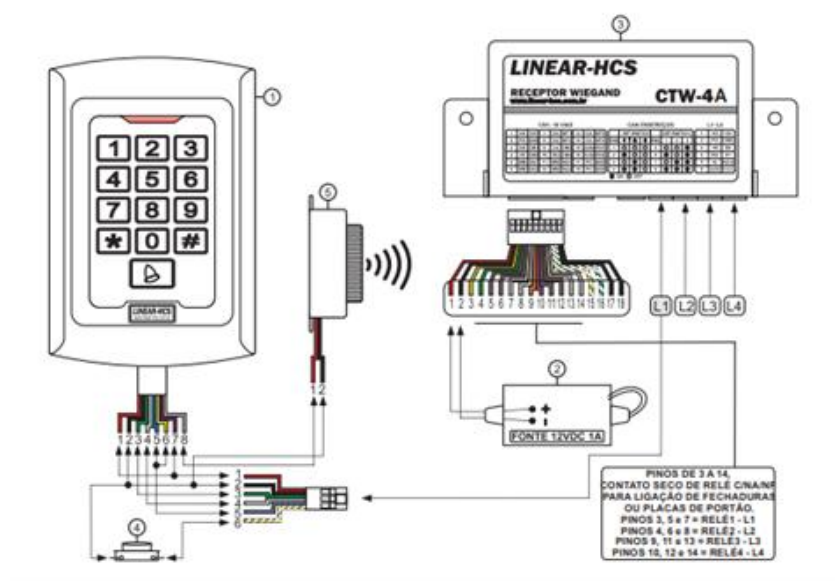
Fonte: https://nice.com.br/novo2017/wp-content/uploads/2018/06/GUIA-R%C3%81PIDO-LN-001-_26-02-16.pdf

3.3.1.1 Características

- Comunicação por protocolo Wiegand;
- Funciona interligado ao Receptores CTW-4ª e ao Guarita IP
- Sinalizações de status por led e buzzer;
- Resistente a respingos d'água (não deve ser instalado ao tempo);
- Consumo de alimentação 12VDC x 100mAh (deve ser alimentado pela saída 12V do receptor ou em caso de fonte exclusiva, deve ter os terras unificados);
- Evite passar o cabeamento dos equipamentos Linear-HCS pela mesma tubulação de cercas elétricas. Evite também a proximidade entre os equipamentos e cerca ou cabos dela.

3.3.1.2 Conexão com o receptor CTW-4A

Figura 22 – Conexão da Leitora com o Receptor



Fonte: https://nice.com.br/novo2017/wp-content/uploads/2018/06/GUIA-R%C3%81PIDO-LN-001-_26-02-16.pdf

- 1 - LEITOR LN-001 COM TECLADO;
- 2 - FONTE DE ALIMENTAÇÃO 12VCC 1A;
- 3 - RECEPTOR LINEAR-HCS CTW-4A;
- 4 - BOTÃO AUXILIAR PARA ABERTURA DE PORTÃO (OPCIONAL);
- 5 - CAMPAINHA 12V OPCIONAL.

Ao apresentar um cartão ou chaveiro de proximidade ao Leitor LN-001 ocorre uma sinalização auxiliar por meio do led frontal, acompanhado de um alerta sonoro que permite reconhecer a compatibilidade do dispositivo com o sistema, funcionamento do cartão e validação do acionamento.

3.3.1.3 Acionamento com cartão ou chaveiro não compatível

O leitor emite o alerta de um bip acompanhado de uma piscada de luz verde sincronizada e logo em seguida outro alerta de cinco bips rápidos acompanhado de cinco piscadas de luz verde sincronizadas.

3.3.1.4 Acionamento com cartão ou chaveiro compatível não cadastrado

O leitor emite o alerta de um bip acompanhado de uma piscada de luz verde sincronizada.

3.3.1.5 Acionamento válido (com um cartão ou chaveiro cadastrado)

O leitor emite o alerta de três bips sequenciais, sendo o primeiro mais longo e dois mais breves, acompanhado de três piscadas de luz verde sincronizadas a este mesmo tempo.

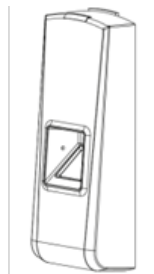
3.3.1.6 Acionamento com cartão ou chaveiro compatível cadastrado em endereço CAN não correspondente ao do leitor acionado

O leitor emite o alerta de dois bips acompanhado de duas piscadas de luz verde sincronizada.

3.3.2 Leitora LN5-P

Leitora de acesso via biometria.

Figura 23 – Leitora LN5-P



Fonte: <https://nice.com.br/novo2017/wp-content/uploads/2018/06/30009400-MANUAL-INST-CONTR-DIGITAL-LN5-P-Rev-01.pdf>

3.3.2.1 Características e indicações

- Não instalar este equipamento exposto ao tempo.
- Recomendamos que se utilize proteção total contra sol e chuva em toda e qualquer instalação deste equipamento.
- O contato com água danificará os sensores biométricos, podendo apresentar funcionamento impreciso, erro na leitura ou mesmo tentativa de reconhecimento de digital sem que haja alguém utilizando o equipamento.
- A luz solar também danificará o sensor, pois o mesmo não é munido de proteção eletrônica ou mecânica contra o forte calor e incidência de luz solar direta.
- 3.000 (1 digital) ou 1.500 (2 digitais) usuários;
- TCP/IP, RS 485, USB, e Wiegand 66 (opção 26 bits);
- 50.000 registros de eventos off line;

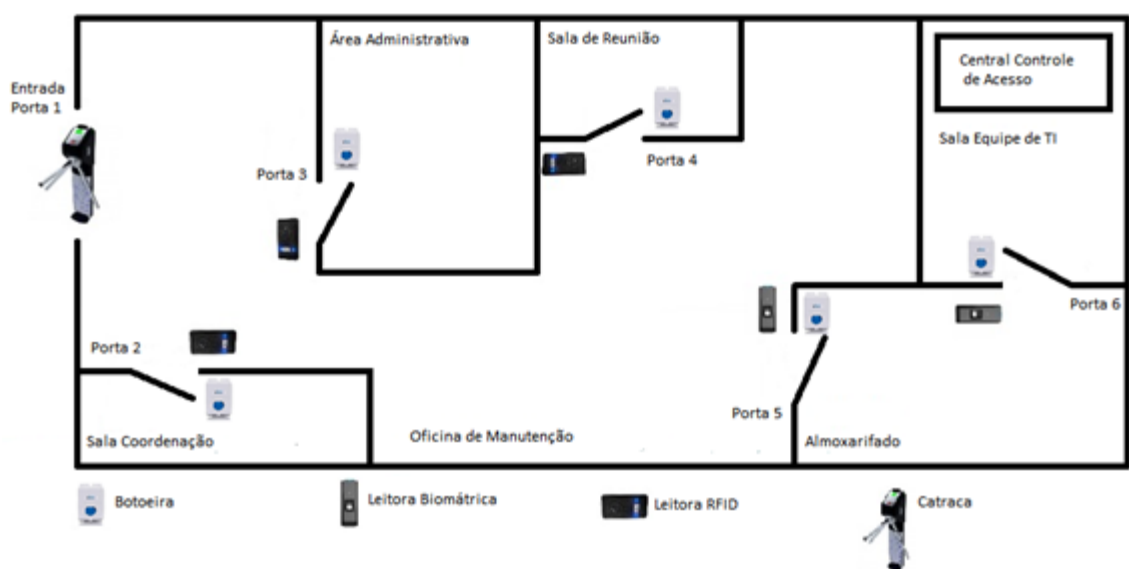
- Alimentação 12 VDC 1A (fonte não inclusa).

3.4 SOFTWARES

Todo o sistema se comunica por meio de softwares exclusivos, podendo ser utilizados para manutenção e configuração inicial do programa. Para tal conexão pode-se utilizar um dos meios de comunicação disponíveis, sendo eles USB Device, Serial RS232 ou TCP/IP. De acordo com a norma existente, recomenda-se a utilização de cabos seriais com até 15 metros. Para distâncias acima de 15 metros recomenda-se a utilização da comunicação via TCP/IP.

3.5 PROJETO

Figura 24 – Projeto Controle de Acesso



Fonte: Próprios Autores

3.5.1 Descrição

Para o projeto foram utilizados 1(uma) central controladora (Guarita IP), 2(dois) receptores (CTW 4A), 3(três) leitoras de cartão RFID e senha, e 2(duas) leitoras biométricas, todos da marca Nice do Brasil. Utilizamos também 5 botoeiras para realizar a abertura interna das portas. Ao todo, 5 salas estão sendo controladas quanto a entrada de pessoas, possibilitando apenas o acesso de pessoas autorizadas, devido a criticidade de cada área.

A instalação foi executada de maneira com que o responsável tivesse todo o controle e relatório possível de sua empresa, deixando um ambiente mais seguro e com melhor aproveitamento das atividades internas, sejam elas operacionais ou administrativas.

No acesso de todos a empresa, pela porta 1(um), foi instalada uma catraca conforme descrito no item 2.6.1, que servirá para ter um maior controle da hora de entrada e saída de todos os funcionários. Nas portas 2(dois), 3(três) e 4(quatro) foram utilizados leitores RFID com teclado, LN-001, conforme descrito no item 3.3.1, que serão utilizados pelos funcionários para realizar a abertura das portas conforme necessidade do seu dia a dia de serviço, as portas são liberadas por cartão de aproximação e/ou senhas pré-cadastradas que são disponibilizados para cada colaborador, tendo sempre uma pessoa que ficará responsável pelo cadastro do funcionário no sistema, o cadastro de cada colaborador é controlado e registrado, garantindo assim uma maior eficácia.

Nas portas 5(cinco) e 6(seis) foram utilizados leitores biométricos, devido a criticidade da área pois as leitoras biométricas LN5-P são mais seguras em comparação com as leitoras de cartão e senhas, seu acesso é mais seguro pois impossibilita que pessoas acessem locais sem a sua própria digital, a descrição da leitora Biométrica está no item 3.3.2. Geralmente, esse tipo de leitora é instalado em locais com maior necessidade de segurança, neste caso foram instaladas no almoxarifado, devido ao grande valor de peças e componentes em seu interior, e na sala de TI, onde se encontra toda informação, sistemas integrados da empresa e todo o sistema de controle de acesso.

Também utilizamos botoeiras nas portas 2(dois), 3(três), 4(quatro), 5(cinco) e 6(seis), componentes esses que são responsáveis pela abertura das portas na parte interna das áreas controladas, pois o sistema entende que, uma vez tendo o acesso liberado a pessoa pode sair sem apresentar uma identificação de cartão/senha ou biométrica.

As comunicações entre todos os componentes instalados na área para o controle de acesso de pessoas foram feitas através ligações elétricas e eletrônicas, utilizando o cabo de comunicação CAT5, levando toda informação até a central controladora que está localizada dentro da sala de TI. Esse será o local de processamento de toda informação recebida das leitoras que, após uma análise sistêmica da programação inserida na central, que irá permitir o acesso ou bloquear o mesmo para determinado usuário.

4 RESULTADOS E CONCLUSÕES

Com o projeto foi possível observar a necessidade de implementação de um sistema de controle de acesso dentro de uma empresa e, até mesmo, em outras áreas de produção, melhorando a desempenho dos funcionários e garantindo mais segurança em todo o processo. Utilizamos diversos componentes para chegar ao resultado final e esperado com a implementação do projeto, componentes de alto desempenho que entregam os melhores resultados do mercado.

Mesmo com todo o sistema implementado e em pleno funcionamento, é sempre preciso que as pessoas, sejam os responsáveis ou funcionários, adquiram conhecimento e recebam treinamento sobre o que está sendo feito de melhoria em sua empresa/área, pois somente com o entendimento correto das pessoas o sistema irá funcionar corretamente, sem que ninguém tente alterar ou manipular as programações e seus respectivos bloqueios.

Contudo, após toda elaboração do projeto, conseguimos concluir que o desenvolvimento e uma futura implementação irá contribuir para uma melhor organização, controle, segurança e melhorar os dados atrelados aos funcionários, tendo relatório de todos os acessos e fluxo de entrada e saída, possibilitando um melhor gerenciamento de informações que, por várias vezes, são consideradas como críticas dentro de uma organização.

Com a implementação do projeto conseguimos capturar um retorno financeiro com o melhor desempenho e utilização do tempo dos funcionários e com a diminuição de furtos de componentes importantes para o processo, pois, com o controle de acesso por área, apenas responsáveis e importantes para o processo podem acessar a sua respectiva área. Contudo, tivemos um custo de implementação inicial de todo o sistema em um valor aproximado de R\$ 20.600,00, que está detalhado na tabela abaixo, com os custos.

Tabela 3 – Tabela de Preços

Descrição	Quantidade	Valor Unitário	Valor total
Modulo Guarita IP	1	R\$ 1.110,00	R\$ 1.110,00
Receptor CTW-4A	2	R\$ 400,00	R\$ 800,00
Leitora LN-001	3	R\$ 780,00	R\$ 2.340,00
Leitor Biométrico	2	R\$ 1.400,00	R\$ 2.800,00
Catraca	1	R\$ 4.200,00	R\$ 4.200,00
Cabo UTP Cat5 (caixa)	4	R\$ 800,00	R\$ 3.200,00
Botoeira	5	R\$ 30,00	R\$ 150,00
Cartão/Chaveiro RFID	200	R\$ 5,00	R\$ 1.000,00
Estimativa de mão obra	1	R\$ 5.000,00	R\$ 5.000,00
		Total	R\$ 20.600,00

Fonte: Próprios Autores

Já o processo de instalação na empresa citada levará em média 1 mês, utilizando mão de obra especializada de empresa contratada, que ficará responsável por toda parte de integração entre os sistemas, e o investimento é considerado baixo, tendo em vista o controle e a segurança que o sistema pode fornecer para a empresa.

REFERÊNCIAS

ALEXAG. **Can bus Barramento controller area network “conceituação”**. São Paulo, [s.d.]. Disponível em: http://www.alexag.com.br/CAN_Bus_Parte_2.html. Acesso em: 21 out. 2021.

ANATEL. **Guarita IP**. [s.l.], [s.d.]. https://nice.com.br/novo2017/wp-content/uploads/2018/06/M%C3%93DULO-GUARITA-IP_NICE.pdf. Acesso em: 14 out. 2021

BLOG Garen. **Leitor biométrico**: saiba tudo sobre o conceito e a tecnologia necessária. [s.l.], 2019. Disponível em: <https://www.garen.com.br/blog/leitor-biometrico/>. Acesso em: 05 nov. 2021.

CIRIACO, D. **Como funciona a RFID?** TecMundo, 2009. Disponível em: <https://www.tecmundo.com.br/tendencias/2601-como-funciona-a-rfid-.htm>. Acesso em: 24 out. 2021.

CITRIX. **O que é controle de acesso?** [s.l.], [s.d.]. Disponível em: <https://www.citrix.com/pt-br/solutions/secure-access/what-is-access-control.html>. Acesso em: 16 set. 2021.

CONTROL iD. **Controle de acesso por senha**. [s.l.], [s.d.]. Disponível em: <https://www.controlid.com.br/controle-de-acesso/senha/>. Acesso em: 08 nov. 2021.

CONTROL iD. **Qual a função de um controlador de acesso?** Disponível em: <https://www.controlid.com.br/blog/controle-de-acesso/controlador-de-acesso/>. Acesso em: 28 out. 2021.

FIRSTCONTROL. **Control Guarita**. [s.l.], [s.d.]. Disponível em: <https://firstcontrol.com.br/servicos/control-guarita/>. Acesso em: 21 out. 2021.

GALHARDO, A. T. **Sistemas eletrônicos de controle de acesso**. Monografia (TCC em Engenharia Elétrica – Universidade São Francisco, Campinas, 2011. Disponível em: <http://lyceumonline.usf.edu.br/salavirtual/documentos/2141.pdf>. Acesso em: 06 nov. 2021.

INTELBRAS Blog. **Controle de acesso: qual sua importância e como funciona?** [s.l.], 2016. Disponível em: <https://blog.intelbras.com.br/controle-de-acesso/>. Acesso em: 16 out. 2021.

ISP Blog. **Cabo UTP: você sabe como funciona?** [s.l.], 2016. Disponível em: <https://www.ispblog.com.br/2016/07/01/cabo-utp-voce-sabe-como-funciona/>. Acesso em: 27 out. 2021.

LEGAT, M. **Sistema de controle de acesso em IOT**. Tse (TCC em Ciências da Computação) – Universidade Federal de Santa Catarina, Florianópolis, 2018. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/187880/TCC_CCO_UFSC___Matteus_Legat-4.pdf?sequence=1&isAllowed=y. Acesso em: 24 out. 2021.

LINEAR-HCS. **Guia rápido CTW**. São Caetano do Sul, 2016. Disponível em: <https://nice.com.br/novo2017/wp-content/uploads/2018/06/GUIA-R%C3%81PIDO-CTW-4A-RECCTW4-D-HW-459-SW-%E2%89%A5-1.001x.pdf>. Acesso em: 05 nov. 2021.

LINEAR-HCS. **Guia rápido LN-001**. São Caetano do Sul, 2016. Disponível em: <https://nice.com.br/novo2017/wp-content/uploads/2018/06/GUIA-R%C3%81PIDO-CTW-4A-RECCTW4-D-HW-459-SW-%E2%89%A5-1.001x.pdf> . Acesso em: 14 set. 2021.

LINEAR-HCS. **MANUAL-INST-CONTR-DIGITAL**. São Caetano do Sul, 2015. Disponível em: <https://nice.com.br/novo2017/wp-content/uploads/2018/06/30009400-MANUAL-INST-CONTR-DIGITAL-LN5-P-Rev-01.pdf>. Acesso em: 14 set. 2021.

NET Alarmes. **Leitor Controle de Acesso Linear Hcs Ln-104c em 125 kHz Rfid**. São Paulo, [s.d.]. Disponível em: <https://www.netalarmes.com.br/interfonia-e-portaria/controle-de-acesso/leitores-e-receptores/controle-rdif-linear>. Acesso em: 28 out. 2021.

NICEGROUPBRASIL. **LN-104C**. [s.l.], [s.d.]. Disponível em: <https://nice.com.br/novo2017/wp-content/uploads/2018/06/30010252-MANUAL-INST-LN-104C-V2-Rev-00.pdf>. Acesso em: 21 out. 2021.

NOGUEIRA, M. L. B.; MELCHIORS, C. **Um pequeno estudo sobre par trançado**. [s.l.], 1996. Disponível em: <http://penta.ufrgs.br/rc952/Cristina/utpatual.html>. Acesso em: 04 nov. 2021.

OXX. **Empresa de catracas com tag RFD**. São Paulo, [s.d.]. Disponível em: <https://www.oxx.sampa.br/artigos/empresa-de-catracas-com-tag-rfid>. Acesso em: 27 out. 2021.

RFID. **Capítulo 2**. [s.l.], 2013. Disponível em: https://www.gta.ufrj.br/grad/13_1/rfid/cap2_1.html. Acesso em: 23 out. 2021.

RFID. **Conclusão**. [s.l.], 2013. Disponível em: https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2013_2/rfid/Concluso.html. Acesso em: 23 out. 2021.

RSL Tecnologia. **Controle de acesso RFID**. São Paulo, [s.d.]. <https://www.rsltecnologia.com.br/controle-acesso-rfid>. Acesso em: 22 out. 2021.

SEGWARE. **Como funciona um sistema de controle de acesso**. [s.l.], [s.d.]. Disponível em: <https://www.segware.com/post/como-funciona-um-sistema-de-controle-de-acesso>. Acesso em: 14 set. 2021.

SENIOR Blog. **Como funciona um sistema de controle de acesso para empresas?** [s.l.], 2018. Disponível em: <https://www.senior.com.br/blog/como-funciona-um-sistema-de-controle-de-acesso>. Acesso em: 16 out. 2021.

SEU Domínio. **Como funciona um sistema de controle de acesso?** [s.l.], 2017. Disponível em: <https://www.seucondominio.com.br/noticias/como-funciona-um-sistema-controle-acesso>. Acesso em: 04 nov. 2021.

SILVA, A. V. da. **Proposta de interfaceamento entre rede de controle LonWorks e RFID**. [s.l.], [s.d.]. Disponível em: https://semanaacademica.org.br/system/files/artigos/lonworks_e_rfid.pdf. Acesso em: 30 out. 2021.

SOUZA, R. **Cabos de par trançado**: categorias e tipos. TECHENTER. Disponível em: <https://techenter.com.br/cabos-de-par-trancado-categorias-e-tipos/>. Acesso em: 25 out. 2021.

TIDALIS. **Controle de acesso por cartão de proximidade**. São Paulo, [s.d.]. Disponível em: <https://www.tidalis.com.br/controle-acesso-cartao-proximidade>. Acesso em: 06 nov. 2021.

TIDALIS. **Sistema de controle de acesso RFID**. São Paulo, [s.d.]. Disponível em: <https://www.tidalis.com.br/sistema-controle-acesso-rfid>. Acesso em: 23 out. 2021.