



Universidade do Porto

Faculdade de Engenharia

FEUP

Conceito de Sistema

AM3 - Smart Safe Box

Versão 1.0

Equipa N

Conceito de Sistema executado no âmbito da unidade curricular
"Engenharia de Sistemas", do primeiro ano do
Mestrado em Engenharia Electrotécnica e de Computadores

Controlo de Versões

Histórico de versões e atualizações realizadas ao presente "Conceito de Sistema".

Versão 1.0 - 10 de março de 2023

- Versão inicial do documento.

Índice

1	Abreviaturas e Símbolos	4
2	Introdução	5
3	Objetivos	6
4	Requisitos do Sistema	7
4.1	Requisitos Funcionais	8
4.2	Requisitos Não-Funcionais	8
5	Conceito de Sistema	10
6	Arquitetura Funcional	12
7	Estudo de Mercado	13
7.1	Concorrência	13
8	Conclusão	14

1 Abreviaturas e Símbolos

CAGR *Compound Annual Growth Rate*

OOP *Object-oriented programming*

2 Introdução

O presente documento tem como objetivo a definição do sistema a projetar, deixando claro as suas funcionalidades e principais características, assim como a sua arquitetura e organização.

Consequentemente, serão identificados todos os subsistemas, os requisitos, funcionais e não funcionais, definidos pelo cliente e pela equipa, o conceito do sistema e a sua arquitetura funcional.

3 Objetivos

O uso de cofres tem-se tornado cada vez mais indispensável para proteger bens valiosos, quer sejam documentos importantes, dinheiro, jóias, entre outros. Na verdade, os cofres conferem aos seus utilizadores um espaço seguro e fiável, contribuindo para a sua tranquilidade, visto que não se precisam de preocupar com danos ou roubos dos seus bens.

Existem vários tipos de cofres com diferentes tipos de fechaduras que fornecem diferentes níveis de segurança. Os tipos de fechaduras mais comuns são fechaduras mecânicas, eletrónicas e inteligentes.

Este projeto foca-se no desenvolvimento de um cofre com uma fechadura inteligente com duas interfaces, uma aplicação móvel e um *keypad*, que permitem o acesso aos conteúdos do cofre. Comparativamente com os restantes tipos de fechaduras, um cofre com uma fechadura inteligente permite um acesso rápido e simples sem necessitar obrigatoriamente da introdução de códigos no cofre ou chaves físicas. Para além disso, permitem o controlo remoto do cofre, assim como uma monitorização dos seus acessos.

A dificuldade do projeto reside na interconexão dos diferentes componentes do sistema, assegurando ao mesmo tempo a segurança dos dados dos utilizadores. Mais informações sobre os requisitos e o conceito do sistema podem ser obtidas nas secções seguintes.

4 Requisitos do Sistema

Para a realização do projeto, será necessário respeitar alguns requisitos essenciais definidos pelo cliente aquando da divulgação do projeto, e outros discutidos nas reuniões entre a equipa e cliente.

Na seguinte tabela encontram-se listados os requisitos estabelecidos pelo cliente.

CR1	O utilizador pode abrir a fechadura através de duas interfaces, <i>keypad</i> ou por uma aplicação móvel
CR2	O utilizador pode definir um novo código através de ambas as interfaces
CR3	Quando o código é inserido de forma incorreta no <i>keypad</i> é enviada uma notificação para a aplicação
CR4	O sistema tem de estar preparado para uso indoor
CR5	O sistema deve ter uma conexão com a rede Wi-Fi
CR6	Em caso de perda do código, a aplicação deve estar preparada para que o utilizador consiga recuperar o seu código
CR7	A aplicação deve notificar o utilizador quando o cofre é desbloqueado
CR8	A aplicação deve possibilitar a existência de um administrador de sistema
CR9	A aplicação deve permitir ao administrador alocar cofres a utilizadores e definir permissões de acesso

Tabela 1: Requisitos do cliente

De forma a cumprir com todos os critérios estabelecidos, a equipa definiu alguns requisitos, funcionais e não-funcionais, para descrever o funcionamento ideal do sistema. Na seguinte tabela encontram-se os códigos utilizados para a identificação de cada categoria de requisito e a respectiva descrição.

Código	Descrição
F	Funcional
NF	Não-Funcional
RB	Rede e <i>Backend</i>
HW	<i>Hardware</i>
APP	Aplicação

Tabela 2: Tabela de Códigos e Cores de Identificação

4.1 Requisitos Funcionais

Os requisitos funcionais representam o que o sistema deve ser capaz de fazer, descrevendo as suas funcionalidades e características.

Código	Descrição	Requisitos do Cliente	Prioridade
FRB1	A rede deve ter capacidades sem fios, de forma a garantir a simplificação das ligações.	CR5	Must
FRB2	A rede deve ser encriptada, para oferecer segurança ao cliente.		Must
FRB3	A rede deve ter capacidade de ligação à internet, de forma que o cliente possa interagir com a base de dados e o <i>backend</i> .	CR5	Must
FRB4	A rede deve ter a capacidade de retransmissão de dados entre as interfaces de utilizador, para garantir a resolução de erros que possam ocorrer.		Should
FRB5	O <i>backend</i> deve ter a capacidade de armazenar as informações relevantes numa base de dados remota.		Must
FHW1	O <i>Hardware</i> deve estar conectado a uma rede conhecida.	CR5	Must
FHW2	Deve ser possível alterar a palavra-passe no <i>Hardware</i> . Adicionalmente essa alteração deve ser refletida na base de dados.	CR6	Must
FHW3	O <i>Hardware</i> deve manter-se operacional pelo menos duas horas após falha de energia.		Must
FHW4	O <i>Hardware</i> deve bloquear a inserção de novos códigos por <i>keypad</i> após 3 tentativas falhadas.		Must
FAPP1	A aplicação deve permitir aos utilizadores criar uma conta com o seu e-mail.	CR6, CR8, CR9	Must
FAPP2	A aplicação deve exibir o estado do cofre.	CR7	Must
FAPP3	A aplicação deve exibir os acessos do cofre.	CR7	Must
FAPP4	A aplicação deve exibir o número de pessoas com acesso ao cofre.	CR9	Must

Tabela 3: Requisitos Funcionais

4.2 Requisitos Não-Funcionais

Os requisitos não.funcionais representam a forma como o sistema deve agir para atender às necessidades dos seus utilizadores. Desta forma, descrevem o desempenho, fiabilidade, segurança e outras características do sistema.

Código	Descrição	Requisitos do Cliente	Prioridade
NFRB1	A rede e o <i>backend</i> devem ser escaláveis.		Must
NFRB2	A rede deve garantir a compatibilidade entre os outros dois módulos.	CR1, CR2, CR3	Must
NFRB3	A rede e o <i>backend</i> devem ser fiáveis.	CR1, CR2	Must
NFRB4	A rede deve ser capaz de suportar ligações em simultâneo.		Must
NFHW1	O <i>Hardware</i> deve ser projetado para uso interior.	CR4	Must
NFHW2	O <i>Hardware</i> deve ter um teclado numérico com tecla adicional (“cardinal” ou “asterisco”) e quatro caracteres adicionais.	CR1, CR2	Must
NFHW3	O <i>Hardware</i> deve conseguir efetuar com sucesso uma atualização na base de dados em menos de um segundo.	CR2, CR6	Must
NFHW4	O <i>Hardware</i> deve estar pronto para integrar fechaduras de 12 Vdc e até 2 A.		Must
NFHW5	O <i>Hardware</i> deve estar preparado para incorporar 6 fechaduras.		Must
NFHW6	O <i>Hardware</i> deve armazenar informação atualizada de utilizadores a cada trinta minutos.	CR2,CR6	Must
NFHW7	O <i>Hardware</i> deve ter um mostrador onde seja possível visualizar um pequeno menu e o número de caracteres inseridos.	CR1,CR2	Must
NFHW8	O <i>Hardware</i> deve suportar tensões de entrada de 230 VAC ou 110 VAC.	CR4	Must
NFHW9	O <i>Hardware</i> deve verificar ordens de abertura a cada 500 ms.	CR1, CR7	Must
NFAPP1	A aplicação deve solicitar autenticação ao utilizador para aceder e modificar as permissões.	CR1,CR2	Must
NFAPP2	A aplicação deve ter as palavras-passe encriptadas.		Must
NFAPP3	A aplicação deve ocultar informação sensível com opção de visualização.		Must
NFAPP4	A aplicação deve ser capaz de suportar grande volume de utilizadores em simultâneo.		Must
NFAPP5	A aplicação deve conseguir suportar um número crescente de utilizadores sem comprometer a segurança e desempenho.		Must
NFAPP6	A aplicação deve ser compatível com <i>Android</i> .		Must
NFAPP7	Mediante a alteração do código de acesso, a aplicação deve atualizar a informação em menos de cinco minutos.	CR2	Must
NFAPP8	Após o pedido de recuperação de palavra-passe, o e-mail deve ser enviado num intervalo de uma hora.	CR2,CR6	Must
NFAPP9	Após o desbloqueio do cofre na aplicação, este deve atuar num intervalo de 10 minutos.	CR1	Must
NFAPP10	A aplicação deve ser resiliente a erros e falhas sem perder informações do utilizador nem causar corrupção de dados.		Must
NFAPP11	A aplicação deve ser implementada de forma a garantir a sua manutenibilidade.		Should

Tabela 4: Requisitos Não-Funcionais

5 Conceito de Sistema

O conceito de sistema consiste numa descrição de alto nível do sistema, tendo como principal objetivo o esclarecimento dos seus objetivos e funcionalidades.

Um diagrama de *System Breakdown Structure* facilita a identificação e o papel de cada componente para alcançar os objetivos do sistema. O diagrama apresentado em baixo apresenta as relações e interações entre os diferentes componentes, estando dividido em duas categorias: produto e processos. Numa versão inicial, foram apenas incluídos os dois primeiros níveis do sistema.

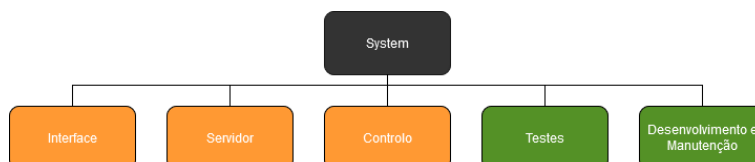


Figura 1: Diagrama do *System Breakdown Structure*

Na categoria de processos (a verde) foram definidas as componentes de *Teste* e *Desenvolvimento e Manutenção*. De facto, de modo a testar o funcionamento do sistema desenvolvido foram definidos diferentes tipos de testes:

- **Testes de Software:** consistem na verificação e validação da aplicação desenvolvida, permitindo a identificação de defeitos, erros ou *bugs* no *software* implementado. Estes testes incluem:
 - **Unit Testing:** teste individual e isolado das diferentes componentes do *software*, garantindo o seu correto funcionamento sem comprometer as restantes funcionalidades;
 - **Teste de Segurança:** teste da capacidade de proteção/segurança do sistema de forma a identificar vulnerabilidades na sua implementação;
 - **Acceptance testing:** verificar se o sistema está de acordo com os requisitos e especificações do cliente.
- **Testes de Hardware:** consistem na verificação do funcionamento das componentes físicas do sistema, de forma a garantir que este é estável e confiável;
- **Testes de Integração:** consistem no teste da compatibilidade dos vários componentes do sistema, verificando que estes funcionam corretamente quando combinados.

De forma a garantir a manutenção do sistema, toda a equipa deverá assegurar que este se encontra num bom estado de funcionamento, tomando especial atenção às componentes de *Hardware*. Para tal, deverá ser feita uma manutenção preventiva, que inclui a realização de inspeções de rotina, tentando evitar ao máximo a ocorrência de problemas de performance no sistema.

Para uma manutenção efetiva do *software* implementado, a equipa deverá tomar decisões proativas, tais como a utilização de conceitos de *Object-oriented programming (OOP)*. Na verdade, a utilização de *OOP*, facilita a identificação e isolamento de problemas e permite realizar alterações ao funcionamento de objetos sem afetar o resto do código, tornando o código implementado modular e reutilizável, facilitando futuras modificações.

De forma a garantir um desenvolvimento eficaz e organizado do sistema, a equipa deverá seguir as normas de funcionamento e métodos de trabalho estabelecidos no Manual de Qualidade.

Na categoria de produto (a cor laranja), foram definidas as componentes *Interface*, *Servidor* e *Controlo*. As funcionalidades e o papel de cada uma destas componentes será descrito com detalhe na secção seguinte.

6 Arquitetura Funcional

O desenho da arquitetura funcional pretende representar o sistema decomposto nos diferentes sub-conjuntos de funções e interações entre as mesmas.

No contexto de projeto de sistemas, o diagrama auxilia os membros da equipa de desenvolvimento e cliente a compreender a estrutura do produto.

Assim, desenvolveu-se o diagrama da figura 2.

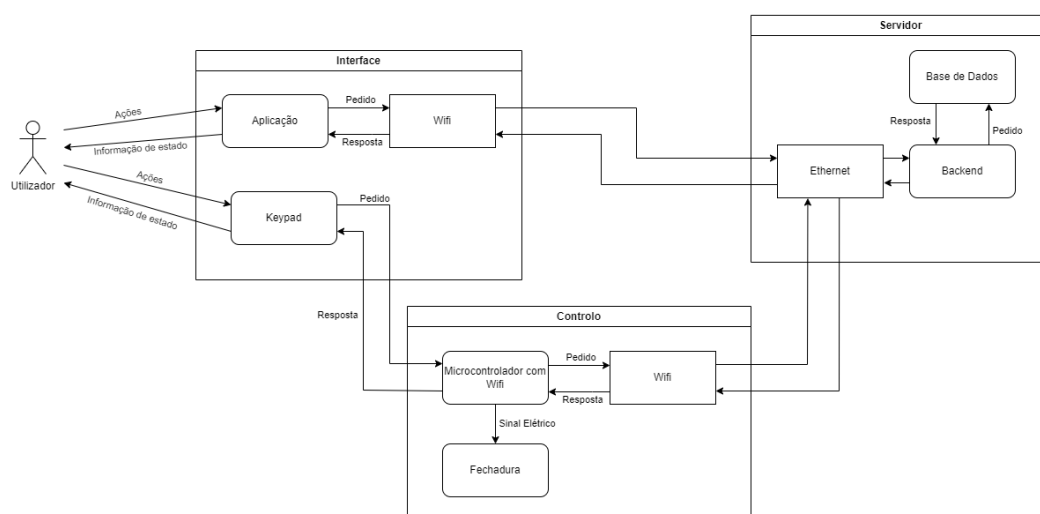


Figura 2: Diagrama da Arquitetura Funcional

No sistema destacam-se as seguintes funções principais: *User Interface*, Servidor e Controlo. A estes três domínios basilares do sistema, estão inerentes algumas funcionalidades a descrever de seguida:

- **Interface**, proporciona ao utilizador dois canais de interação com o sistema, através da Aplicação ou Keypad. A comunicação estabelecida pela Aplicação com o Servidor é feita maioritariamente para confirmar a autenticidade do utilizador no acesso ao cofre, requisitar a sua abertura e obter informação relevante ao utilizador (notificações de abertura, número de membros a partilhar o cofre, entre outros);
- **Servidor**, funciona como o coração da aplicação e gere toda a comunicação entre o dispositivo físico de segurança e aplicação. Neste serão armazenadas todas as informações dos utilizadores, tendo responsabilidade em lidar com todos os pedidos dos respetivos clientes (Microcontrolador e Aplicação);
- **Controlo**, garante o correto funcionamento do equipamento crítico/sensível (cofre). Este será composto pelo microcontrolador, bem como os componentes necessários para o controlo da fechadura e comunica diretamente com o servidor. Será ainda o microcontrolador deste módulo a processar todas as operações do Keypad e a solicitar os dados necessários ao servidor.

7 Estudo de Mercado

Estima-se que o mercado global de cofres inteligentes cresça a uma taxa anual de 6.5% (CAGR) até 2026. De facto, este crescimento do mercado deve-se principalmente ao aumento da demanda de soluções de armazenamento seguras e confiáveis e aos avanços significativos da tecnologia, incluindo a integração em *Smart Homes*.

Várias organizações, incluindo instituições financeiras, recorrem cada vez mais ao uso destes cofres visto que estes não só asseguram a proteção dos seus bens, como também permitem controlo remoto e monitorização de acessos em tempo real.

Contudo, espera-se que o mercado de cofres inteligentes enfrente algumas adversidades, maioritariamente causadas pelo uso crescente de pagamentos digitais. Na verdade, a expansão do *e-commerce* fez com que o uso de dinheiro físico diminuísse consideravelmente, sendo cada vez menos necessário o seu armazenamento em cofres. Para além disso, o custo elevado dos componentes, a possível necessidade de manutenções regulares e problemas relacionados com ciber segurança desafiam o crescimento do mercado dos cofres inteligentes.

7.1 Concorrência

De modo a criar um produto competitivo com as opções já existentes no mercado, têm de ser conhecidas as suas funcionalidades. Conhecendo o produto concorrente, é possível desenvolver um que se destaque ou apresente qualidade equivalente.

Após a pesquisa, destacam-se dois cofres inteligentes com características/funcionalidades pretendidas pelo cliente:

1. **Xiaomi - Mijia Smart Safe Deposit Box** (lançado em 2020)

- Pode aceder-se ao cofre através de impressão digital, palavra-passe temporária, remotamente na aplicação, palavra-chave de um utilizador e chave física;
- As palavras-chave no cofre físico têm 6 caracteres (podem ser digitados mais, sendo aberto caso a palavra-passe correta esteja contida na *string*);
- O cofre comunica com o exterior através de *Bluetooth* 5.0 (não consegue ligar diretamente ao router);
- O cofre permite a existência de 200 utilizadores (+administrador);
- Usa como fonte de alimentação 4 baterias AA (tempo de vida previsto de um ano);
- Preço mínimo encontrado é de aproximadamente 200 euros.

2. **Robern - IQ Digital Lock Box** (lançado em 2020)

- Pode aceder-se ao cofre remotamente na aplicação, palavra-chave de um utilizador e chave física;
- O código de acesso ao cofre físico pode ter entre 4 e 8 dígitos;
- O cofre comunica com o exterior através de Wi-fi;
- O cofre tem somente um utilizador (não existe nenhuma funcionalidade de partilha);
- Usa como fonte de alimentação 4 baterias AA (tempo de vida previsto de um ano);
- Preço mínimo encontrado é de aproximadamente 300 euros.

8 Conclusão

O projeto em questão apresenta uma característica modular e tem como componentes a comunicação em rede, a aplicação móvel e a fechadura, sendo possível adaptar os diferentes módulos conforme a necessidade, o que permite flexibilizar os custos envolvidos na implementação do sistema e garantir que a solução desenvolvida possa ser oferecida de maneira ampla no mercado.

Logo, a partir deste documento espera-se que os detalhes e módulos do sistema que compõem o projeto estejam claros na sua totalidade, e que a idealização realizada atenda às necessidades e visão do cliente para o produto, sendo a formalização conceptual apresentada a união dos conhecimentos técnico-científicos da equipa aliados aos *inputs* e *feedbacks* do cliente sobre os resultados esperados no fim do processo.

Referências

- [1] n.d. Wikipedia. Accessed March 9, 2023. <https://reports.valuates.com/reports/ALLI-Manu-2S93/smart-locks>.
- [2] “Safes and Vaults Market Size, Trends, Analysis | Industry Forecast 2026.” n.d. Technavio. Accessed March 9, 2023. <https://www.technavio.com/report/safes-and-vaults-market-industry-analysis>.
- [3] “Smart Lock Market is Projected To Reach USD 14,972.3 Million By 2030, Growing At A CAGR Of 20.1% - Valuates Reports USA - English - India.” 2022. PR Newswire. <https://www.prnewswire.com/news-releases/smart-lock-market-is-projected-to-reach-usd-14-972-3-million-by-2030--growing-at-a-cagr-of-20-1---valuates-reports-301551088.html>.
- [4] n.d. INTRODUCING IQ™ DIGITAL LOCK BOX TOTAL CONTROL PEACE OF MIND. Accessed March 9, 2023. http://kohlerrobern.blob.core.windows.net/media/345970/robern_iqdigitallockbox.pdf.
- [5] n.d. INTRODUCING IQ™ DIGITAL LOCK BOX TOTAL CONTROL PEACE OF MIND. Accessed March 9, 2023. http://kohlerrobern.blob.core.windows.net/media/345970/robern_iqdigitallockbox.pdf.
- [6] “ROBERN® IQ™ DIGITAL LOCK BOX NOW AVAILABLE IN A FREESTANDING DESIGN.” 2022. PR Newswire. <https://www.prnewswire.com/news-releases/robern-iq-digital-lock-box-now-available-in-a-freestanding-design-301584882.html>.
- [7] “xiaomi Smart Safe OX User Manual - Manuals+.” 2022. manuals.plus. https://manuals.plus/xiaomi/smart-safe-ox-manual#password_factory_mode.