

































<div><div></div><div></div></div> <div>CANVAS DO PROJETO IOT - VERSÃO 4.0</div>		NOME DO PROJETO: [Protótipo] SmartLock: Controle de Acesso Autônomo para Infraestrutura de Energia			
<div><div>JUSTIFICATIVAS (PASSADO)</div><p>O SmartLock assegura a proteção de religadores (Self-healing) de rede elétrica, fundamentais para a resiliência do smartgrid em smart cities. Este sistema IoT previne acessos não autorizados, mitigando riscos de falhas catastróficas e perda de vidas. Ao garantir manutenções seguras e autorizadas, o SmartLock eleva a confiabilidade operacional e fortalece a segurança pública, oferecendo um controle de acesso eficaz e eficiente.</p></div>	<div><div>PRODUTO IOT (NOME, TIPO E FINALIDADE)</div><p><b>Nome:</b> SmartGuardian <b>Tipo:</b> Sistema Integrado de Segurança IoT para Infraestrutura de Energia <b>Finalidade:</b> O SmartGuardian é projetado para garantir a segurança de gabinetes contendo equipamentos de self-healing em redes elétricas. Ele combina um sensor de alarme sofisticado com um atuador para controle automatizado de aberturas de porta e um sistema de identificação por RFID. A finalidade é prevenir acessos não autorizados, permitir manutenções programadas de forma segura e autenticar profissionais de manutenção, contribuindo para a resiliência do smartgrid e a segurança das smart cities.</p></div>		<div><div>STAKEHOLDERS EXTERNOS E FATORES EXTERNOS</div><p><b>Stakeholders Externos:</b> <b>Concessionária de Energia (Flávia Delicatto):</b> Como cliente do projeto, suas necessidades e expectativas definem os requisitos e o sucesso do protótipo. <b>Product Owner:</b> Responsável por definir as funcionalidades do SmartGuardian, priorizar o backlog do projeto e assegurar que os entregáveis atendam às necessidades do negócio. <b>Reguladores:</b> Órgãos regulatórios impactam diretamente o projeto com legislações e normas de segurança e privacidade de dados. <b>Sociedade:</b> A segurança das smart cities e a confiabilidade do smartgrid são de interesse público; a aceitação social do projeto pode afetar sua adoção. <b>Fornecedores de Tecnologia:</b> Empresas que fornecem componentes tecnológicos e plataformas de software são cruciais para o desenvolvimento do protótipo.</p></div>		<div><div>RESTRIÇÕES</div><p><b>Simulação de Hardware:</b> Como os sensores físicos não serão desenvolvidos, o projeto deve considerar a criação de simulações virtuais realistas desses componentes. <b>Escopo de Funcionalidades:</b> Restringir o protótipo às funcionalidades essenciais para validação do conceito, evitando complexidades desnecessárias que podem desviar o foco do projeto. <b>Integração com Fiware:</b> Limitar a integração apenas aos componentes essenciais da plataforma Fiware para manter o projeto alinhado e gerenciável. <b>Recursos de Desenvolvimento:</b> O desenvolvimento deve respeitar as limitações de tempo e orçamento disponíveis, focando em entregar um MVP (Produto Mínimo Viável). <b>Testes de Campo:</b> Sem hardware real, os testes em campo podem não refletir completamente o desempenho em cenários reais, o que deve ser considerado nas análises. <b>Dados de Entrada:</b> Os dados utilizados nas simulações devem refletir condições operacionais realistas para validade dos testes.</p></div>
	<div><div>COLETA DE DADOS</div><p><b>Sensor de Alarme:</b> Registra tentativas de acesso e estado da porta. <b>Leitor RFID:</b> Capta identificação digital dos técnicos. <b>Atuador:</b> Executa a abertura automática da porta após a verificação de credenciais. <b>Módulo de Comunicação:</b> Envia dados de acesso e alertas em tempo real.</p></div>	<div><div>IDENTIFICAÇÃO DE OBJETOS</div><p><b>Tag RFID:</b> Dispositivo portátil em posse do técnico que contém suas credenciais de identificação únicas. Quando o técnico se aproxima do gabinete, o leitor RFID do SmartGuardian escaneia a tag e verifica se as credenciais correspondem às autorizações de acesso pré-estabelecidas para aquela porta.</p></div>	<div><div>AÇÕES AUTÔNOMAS</div><p><b>Autenticação de Acesso:</b> À aproximação do técnico, o leitor RFID valida suas credenciais de forma autônoma. <b>Execução de Abertura:</b> Com credenciais confirmadas, o atuador inicia a abertura da porta de forma automatizada. <b>Alerta de Segurança:</b> O sensor de porta aciona um alerta imediato se uma abertura não autorizada for detectada. <b>Registro de Atividade:</b> Cada evento de acesso, autorizado ou não, é automaticamente documentado pelo sistema.</p></div>	<div><div>Fatores Externos:</div><p><b>Tendências Tecnológicas:</b> Inovações e mudanças no campo de IoT podem oferecer novas oportunidades ou desafios para o projeto. <b>Condições de Mercado:</b> A disponibilidade e o custo de componentes e serviços necessários são influenciados pelas condições do mercado global. <b>Cenário Econômico:</b> Flutuações econômicas podem afetar o financiamento e a priorização do projeto. <b>Condições Políticas:</b> Estabilidade ou instabilidade política pode influenciar regulamentos e a execução do projeto. <b>Questões Ambientais:</b> Considerações ambientais podem ditar a sustentabilidade e a aceitação do projeto, especialmente em termos de energia e recursos consumidos.</p></div>	<div><div>PREMISSAS</div><p><b>Especificações Técnicas Definidas:</b> Assume-se que as especificações técnicas do protótipo, estão claramente definidas e acordadas. <b>Recursos de Desenvolvimento:</b> Presume-se que os recursos de desenvolvimento, tanto humanos quanto tecnológicos, estão disponíveis e são adequados para a execução do projeto. <b>Apoio das Partes Interessadas:</b> Presume-se que há um alinhamento e apoio contínuo das partes interessadas para a progressão do projeto.</p></div>
<div><div>OBJETIVOS DO PROJETO</div><p>Implementar um sistema integrado de sensor e atuador para gabinetes de equipamentos de self-healing em redes elétricas, que alerta sobre aberturas não autorizadas e controla o acesso automatizado para manutenção programada. Utilizando identificação por RFID, o sistema garante que apenas profissionais autorizados possam realizar intervenções, fortalecendo a segurança operacional do smartgrid.</p></div>	<div><div>PROCESSAMENTO</div><p><b>Análise de Credenciais:</b> O SmartGuardian processa as informações da tag RFID em tempo real para validar as credenciais do técnico. <b>Decisão de Acesso:</b> Baseando-se na autenticação positiva, o sistema decide liberar ou negar o acesso (Os dados de autorização de acesso são pré-carregados periodicamente - Subscrição) <b>Monitoramento de Estado:</b> O sistema continuamente avalia o estado da porta para detectar e responder a acessos não autorizados. <b>Notificação e Resposta:</b> Em caso de uma tentativa de acesso não autorizado, o SmartGuardian inicia protocolos de segurança, como notificações para o centro de controle e ativação de medidas de segurança.</p></div>	<div><div>CONECTIVIDADE</div><p>Alternativas comuns ao ambiente operativo do setor de Energia: <b>NB-IoT:</b> Conexão eficiente para áreas extensas, ideal para dispositivos dispersos, com criptografia e autenticação celular para segurança. <b>LoRa:</b> Adequada para dados pequenos e distâncias longas, com segurança reforçada por criptografia em duas camadas. <b>4G/LTE:</b> Rápida e confiável para necessidades de comunicação em tempo real, com segurança via tunelamento e criptografia.</p></div>	<div><div>EQUIPE DO PROJETO</div><p>Elenice Costa Rodrigo Oliveira Bruno Macena</p></div>		

<div></div>		<div></div>			
<div><div></div><b>BENEFÍCIOS (FUTURO)</b><p>O SmartLock promete transformar a gestão de segurança em infraestruturas críticas. Seu benefício futuro inclui a detecção e prevenção proativa de acessos não autorizados, mantendo a integridade vital do smartgrid. Além disso, o acesso automatizado e seguro facilitará manutenções eficientes e confiáveis, minimizando interrupções no serviço. A longo prazo, a integração de RFID para autenticação de pessoal estabelecerá um novo padrão de segurança operacional, apoiando a evolução de smart cities mais seguras e resilientes.</p></div>		<div><div></div><b>SISTEMAS DE SOFTWARE</b><p><b>Fiware Orion Context Broker:</b> O componente central do Fiware que gerencia o estado dos dispositivos IoT em tempo real, facilitando a atualização e consulta de informações contextuais de maneira eficiente.</p><p><b>Fiware NGSI Interface:</b> Esta interface padroniza as operações de contexto entre dispositivos e o Orion Context Broker, promovendo integração e interoperabilidade.</p><p><b>Fiware IoT Agent:</b> Atua como intermediário entre os dispositivos IoT e o Orion Context Broker, traduzindo protocolos específicos do dispositivo para o padrão NGSI, permitindo uma comunicação uniforme e a integração de dispositivos de diferentes fabricantes.</p></div>	<div><div></div><b>INTERFACES DE USUÁRIO</b><p>O sistema SmartGuardian incluirá um indicador LED tricolor simples para comunicar o status de acesso ao gabinete do religador:</p><p><b>Verde:</b> Indica acesso autorizado, a porta foi aberta legitimamente.</p><p><b>Vermelho:</b> Alerta que houve uma abertura irregular, sem autorização.</p><p><b>Amarelo:</b> Avisa que um acesso não autorizado foi tentado, mas a porta permaneceu seguramente fechada.</p><p>Para o centro operativo, será fornecido um dashboard digital que exibe o status dos gabinetes do SmartGuardian em tempo real, oferecendo:</p><p><b>Indicadores de Estado:</b> Mostra o status atual dos gabinetes com códigos de cores correspondentes (verde, amarelo, vermelho) para acesso autorizado, tentativas de acesso e aberturas irregulares.</p><p><b>Alertas e Notificações:</b> Fornece notificações instantâneas e alertas para ações críticas, como tentativas de acesso não autorizado.</p><p><b>Registro e Histórico:</b> Mantém um log detalhado de todos os eventos de acesso para auditoria e análise subsequente.</p></div>	<div><div></div><b>ENTREGAS DO PROJETO</b><p><b>Protótipo Funcional:</b> Um modelo de trabalho do SmartGuardian, incluindo sensor de alarme, atuador, e leitor RFID.</p><p><b>Software de Integração:</b> Software para integrar o protótipo com a plataforma Powered by Fiware, incluindo a comunicação via interface NGSI.</p><p><b>Dashboard Operacional:</b> Uma interface de usuário para o centro de controle monitorar o status dos gabinetes.</p><p><b>Documentação Técnica:</b> Do sistema, e documentação de integração de software.</p><p><b>Relatório de Testes:</b> Documentação dos testes realizados e dos resultados obtidos com o protótipo.</p></div>	<div><div></div><b>RISCOS</b><p><b>Prazo Apertado:</b> O risco mais crítico é o tempo insuficiente para desenvolver, testar e iterar o protótipo, o que pode levar a falhas não descobertas ou funcionalidades não implementadas.</p><p><b>Comprometimento da Qualidade:</b> Sob a pressão do tempo, a qualidade do protótipo pode ser comprometida, com menos oportunidades para refinamento e otimização.</p><p><b>Dados Incompletos:</b> O curto prazo pode resultar em falta de dados completos e precisos para simulação, afetando a validade dos testes.</p><p><b>Recursos Subestimados:</b> A urgência do projeto pode levar a uma subestimação dos recursos necessários, resultando em sobrecarga da equipe e erros decorrentes de pressa.</p></div>
<div><div></div><b>NECESSIDADES (PARTES INTERESSADAS E NEGÓCIO)</b><p><b>Confiabilidade:</b> Garantir que o sistema seja robusto e funcione ininterruptamente, especialmente durante as manutenções programadas.</p><p><b>Usabilidade:</b> O sistema deve ser fácil de operar tanto pelos técnicos em campo quanto pelo pessoal do centro operativo.</p><p><b>Integração de Sistema:</b> Necessidade de integração fluida com a plataforma de gestão de operações da concessionária de energia e sistemas existentes.</p><p><b>Manutenção e Suporte:</b> O sistema deve ser fácil de manter e atualizar, com suporte técnico acessível.</p><p><b>Custo-Efetividade:</b> Desenvolver o SmartGuardian com atenção ao custo-benefício, considerando o investimento inicial e os custos operacionais.</p><p><b>Escala:</b> Possibilidade de expansão e adaptação do sistema à medida que a rede de energia e as demandas de segurança evoluem.</p></div>		<div><div></div><b>REQUISITOS INICIAIS</b><p><b>Autenticação RFID:</b> Desenvolver um método de autorização via RFID simples e seguro.</p><p><b>Atuador e Sensor:</b> Criar atuador e sensor de porta para testar o controle de acesso.</p><p><b>Indicadores status (LED):</b> Integrar indicadores status (LED tricolores) para sinalizar o status do acesso ao gabinete.</p><p><b>Comunicação de Alertas:</b> Estabelecer uma comunicação básica para enviar alertas de segurança.</p><p><b>Interface de Dashboard:</b> Projetar uma interface de usuário simplificada para o monitoramento operacional.</p><p><b>Compatibilidade Fiware:</b> Assegurar que o protótipo seja capaz de se comunicar com a plataforma Fiware.</p></div>			
<b>Adaptado de:</b> José Finocchio Junior ( <a href="http://pmcanvas.com.br/">http://pmcanvas.com.br/</a> )		<b>Material Fonte:</b> Da Silva, Danyllo Valente, et al. "Uma tecnologia para apoiar a engenharia de requisitos de sistemas de software iot." 23rd Iberoamerican Conference on Software Engineering. 2020			