

PILOTO BNDES IOT
CIDADES INTELIGENTES
CONTRATO Nº 2.198.115

ANÁLISE DE VIABILIDADE TÉCNICO ECONÔMICO
FINANCEIRA:
PROJETO-PILOTO EM SEGURANÇA PÚBLICA

Apoiadora:



Executora:



Avaliadora:

Deloitte.

Parcerias:



28/11/2024 **Controle de Informação de Documentos**

Identificação do documento	WP1372
Nome do documento	Relatório de Análise de Viabilidade Técnica e Econômico-Financeira
Nome do Projeto	Pilotos IoT Cidades Inteligentes: ✓ Piloto 1 - Segurança Pública ✓ Piloto 2 – Mobilidade Urbana
Cliente	LSI-TEC / BNDES
Elaboração do documento	Manoel Celso Gomes
Versão do documento	2

Histórico de edições

Versão	Data	Adição/Alteração	Desenvolvido/Revisado por
1	28/11/2024	Relatório de Avaliação de POC	Andrey Capecchi Camargo
2	21/03/2025	Revisão Geral	Laisa Costa De Biase

Sumário

1. Introdução	5
2. Apresentação da LSI-TEC	5
3. Contexto	5
4. Objetivo	6
5. Descrição da Solução Testada	7
5.1 Arquitetura da Solução	8
5.1.1 Dispositivos de detecção	8
5.1.2 Concentradores/Gateways LoRaWAN	9
5.1.3 Servidor de Rede LORA	9
5.1.4 Servidor de aplicação	9
5.2 Diagrama de blocos do dispositivo de identificação e notificação de emergências	9
5.3 Funcionalidades	11
5.3.1 Detecção e leitura de placas de automóveis (OCR)	11
5.3.2 Detecção de acidentes	11
5.3.3 Notificação de eventos	13
6. Abordagem tecnológica para a implantação das funcionalidades	17
7. Restrição da Solução	18
8. Protótipo	19
9. Descrição da solução testada	22
9.1 Descrição dos testes em campo realizados e Restrições dos testes	22
9.4 Cronograma do projeto	25
10. Metodologia Deloitte: Gerenciamento do Ciclo de Vida dos KPI's e Resultados	26
10.1 Premissas, Restrições e Dependências	26
10.2 Determinação dos Controles e Objetivos	27
10.2 Seleção, Avaliação e Atribuição	28
10.3 Definição de Valores-Alvo	28
10.4 Resultados preliminares dos testes	29
10.5 Relatório de Performance e Controle	29
10.6 Resultados esperados	30
10.7 Apresentação da análise econômica e financeira e viabilidade técnica	30
10.8 Revisão e Ajuste do Controle do Modelo	30
Estruturação de modelo de negócio sustentável para difusão da das soluções	30
Cenário de vendas de dispositivos para uma amostra de venda de 100 dispositivos anuais	31
CAPEX (Despesas operacionais anuais)	31
OPEX (Despesas operacionais anuais)	31
Projeção de faturamento anual	31

Cenário: Assinatura de Serviços	32
Resumo financeiro	32
10.9 Conclusão	32
10.10 Sugestões e Recomendações	32
10.11 Modelo de Mercado e Escalabilidade	33

1. Introdução

Este relatório apresenta a análise de viabilidade técnico econômico-financeira da implementação da solução de IoT referente ao Piloto 1 - com foco na Segurança Pública, desenvolvido pela LSI-TEC.

2. Apresentação da LSI-TEC

A LSI-TEC é uma associação civil de direito privado, sem fins lucrativos, e uma Instituição Científica Tecnológica (ICT) fundada por professores e funcionários do Laboratório de Sistemas Integráveis da Escola Politécnica da Universidade de São Paulo (LSI-USP) e tem como missão beneficiar a sociedade com o desenvolvimento de soluções inovadoras, aplicando o conhecimento gerado na Universidade. A LSI-TEC possui ampla experiência de pesquisa e desenvolvimento com grandes impactos na sociedade, tendo intensa participação em projetos multidisciplinares de desenvolvimento de tecnologias e aplicações voltadas à Educação e ao estado da arte em Meios Eletrônicos Interativos, com ênfase em suas aplicações na área de Internet das Coisas, sistemas interativos, realidade virtual, simuladores, jogos educacionais, formação de professores e portais educativos. Juntamente com a LSI-TEC estão as parcerias desse piloto na área de mobilidade SMT-SP / CET, Greenwave e no piloto de Segurança Pública SSP-SP/Bombeiros, Stellantis, SMART MODULAR, American Tower, Deloitte e BNDES.

3. Contexto

De acordo com a Organização Mundial da Saúde (OMS), as ocorrências de trânsito serão a sétima principal causa de morte no mundo até 2030, sendo que atualmente cerca de 1,35 milhão de pessoas morrem por ano. O Brasil, infelizmente, é um dos países que lidera as estatísticas em acidentes de trânsito, com 32 mil vítimas fatais durante o período de um ano e mais de 400 mil sobreviventes com sequelas graves. Por outro lado, a criminalidade no país também é preocupante, estando os motoristas

sujeitos a assaltos, arrastões, sequestro relâmpago, roubos e furtos. Segundo o Anuário Brasileiro de Segurança Pública 2019, anualmente são roubados ou furtados aproximadamente 500.000 veículos, mais de 1% da frota de veículos (45 Milhões), totalizando 33% de todos os crimes contra o patrimônio no Brasil.

Nesse contexto, os danos causados por essas e outras situações de risco são agravados pela demora no atendimento às vítimas, que pode levar a fatalidades, agravar lesões e dificultar o trabalho da polícia. Uma das causas dessa demora ocorre por causa dos serviços de emergência atuais no Brasil que são baseados em solicitações por telefone, em que as pessoas explicam a ocorrência e informam a localização do evento. Como as pessoas podem estar desorientadas e sob forte estresse em emergências, a passagem de informações é sujeita a imprecisões e ambiguidades, aumentando o tempo de espera para o envio do socorro.

Atualmente, apesar de existirem sistemas de segurança para o condutor e passageiros, tais como airbags, cintos de segurança, e travas automáticas nas portas, não há um sistema integrado nos veículos capaz de detectar e automaticamente reportar situações de risco aos motoristas e passageiros e às autoridades de segurança pública e a centrais de socorro privadas.

A segurança veicular envolve tecnologias, ferramentas e medidas para gerar mais proteção para os motoristas, passageiros e pedestres. O conceito é de extrema importância, dada a quantidade expressiva de mortes e os altos índices de violência associados às situações de condução dos veículos.

4. Objetivo

A principal motivação deste projeto é proporcionar os primeiros socorros em emergências de trânsito, pelo desenvolvimento de um sistema de processamento automatizado de notificações aos serviços de emergência das cidades embarcado em automóveis.

5. Descrição da Solução Testada

O Piloto Vigilância Urbana avaliou tecnologias para utilização de carros de passeio como uma rede de sensoriamento móvel para a identificação e para a notificação de situações de risco à vida e de ações criminosas, mais especificamente: (1) acidentes, e (2) veículos envolvidos em ocorrências policiais pela leitura de placas automotivas.

Foi utilizado um dispositivo IoT capaz de identificar ocorrências pelo processamento de dados de sensores veiculares. A partir da caracterização da ocorrência, o dispositivo pode enviar notificações automáticas para as autoridades para o atendimento a emergências, permitindo um socorro muito mais rápido.

Faz parte do projeto a integração de:

1. Sentinela ou Equipamento de Sensoriamento Móvel: dispositivo IoT que identifica tanto a ocorrência de acidentes como faz a leitura de placas dos automóveis próximos, gerando notificação geolocalizada para uma central da PMESP.
2. Módulo de Recebimento de Notificações de Sensores IoT. O recebimento das notificações é realizado por uma API extensível, permitindo o recebimento de novos tipos de notificações. As notificações são encaminhadas a uma central que tem a lógica de negócio para despachar abordagens policiais.

Notas: *Soluções semelhantes existem na Europa (eCall) e na Rússia (ERA-GLONASS), que visam a detecção automática e a notificação de acidentes. Nestes sistemas, há ganho nos tempos de resposta a emergências em até 30%. Eles funcionam com a notificação para um Posto de Atendimento de Segurança Pública no caso de acidente rodoviário grave ser detectado pelos sensores do veículo. Sistemas de solicitação de socorro baseados no eCall foram trazidos ao Brasil por algumas montadoras, que estabelecem central de socorro responsável pela ligação para o serviço de emergência.*

No Brasil, a Polícia Militar do Estado de São Paulo desenvolve sistemas para diminuir o tempo de atendimento a emergências e ampliar sua rede de monitoramento. Um exemplo é o uso de um aplicativo de celular, o SOS Mulher, para gerar solicitações deslocalizadas de socorro de maneira

rápida e precisa. Em um esforço conjunto do Ministério da Justiça com a PM do Estado de São Paulo, projetos piloto de unificação de bases de dados e de um sistema de atendimento a acidentes têm sido desenhados. A Polícia Militar do Estado de São Paulo e a LSI-TEC têm colaborado, com o apoio do BNDES, para o desenvolvimento de um sistema de monitoramento utilizando Internet das Coisas.

5.1 Arquitetura da Solução

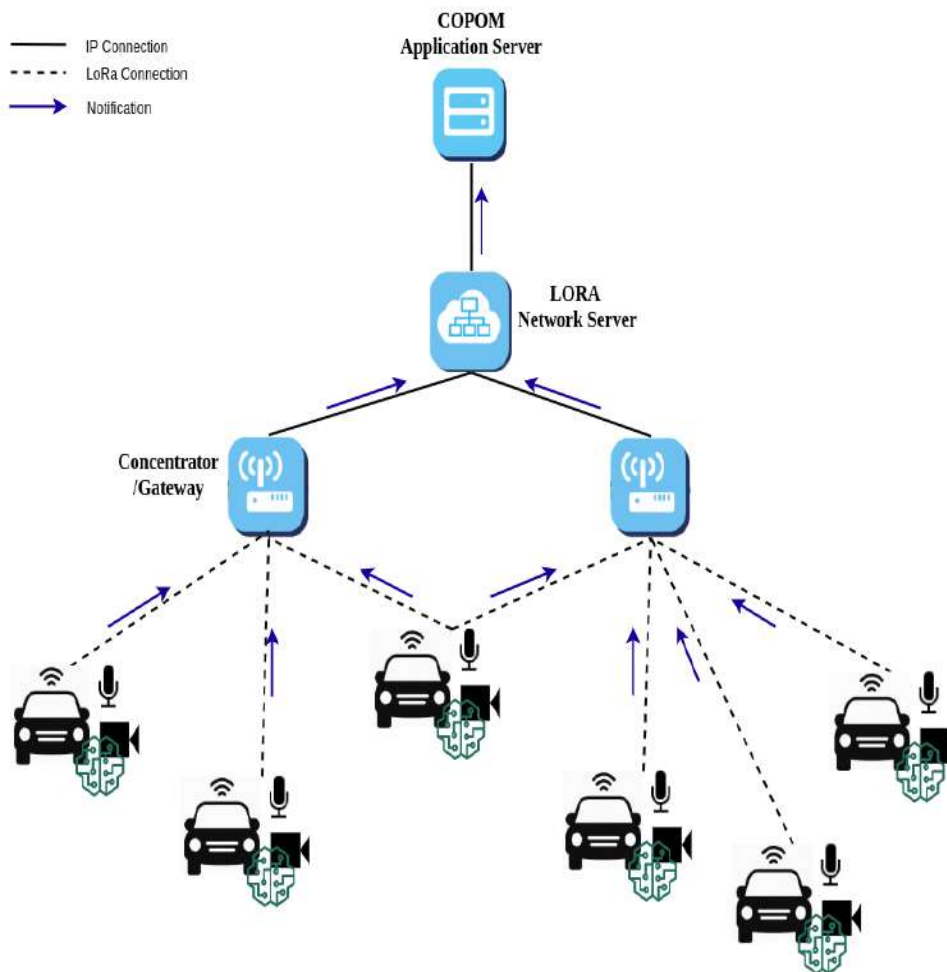


Figura 4.1: Arquitetura de Implantação do Piloto de IoT Segurança Pública

5.1.1 Dispositivos de detecção

Dispositivos finais de detecção de eventos de interesse, instalados em veículos.

5.1.2 Concentradores/Gateways LoRaWAN

Recebem as mensagens de notificações geradas pelos dispositivos e enviadas através da rede LoRaWAN. Envia as notificações através de IP para o Servidor de Rede.

5.1.3 Servidor de Rede LORA

Recebe as mensagens dos Gateways LORA e as reenvia via IP para o servidor de aplicação. No caso do piloto, o servidor de aplicação está instalado no COPOM.

5.1.4 Servidor de aplicação

Servidor final de aplicação que recebe as notificações dos eventos detectados.

5.2 Diagrama de blocos do dispositivo de identificação e notificação de emergências

Na figura abaixo está indicado o diagrama de blocos do dispositivo de identificação e notificação de emergências.

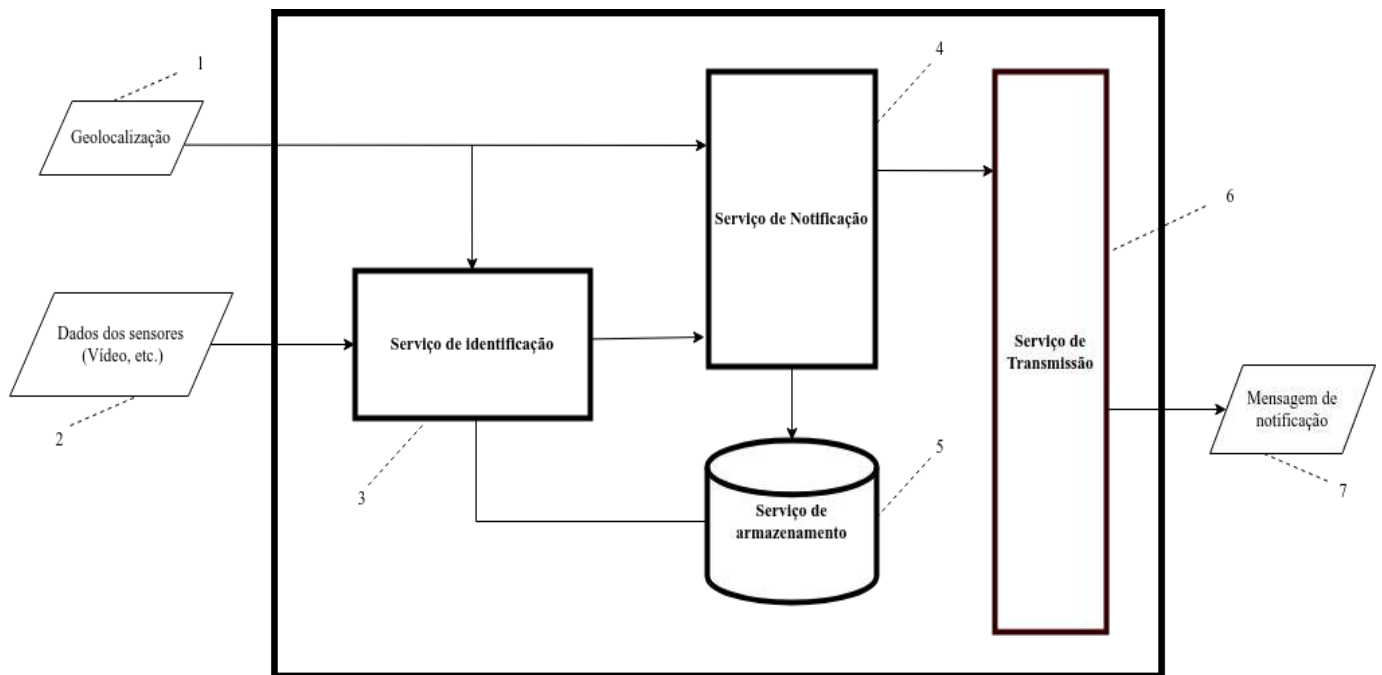


Figura 4.2: Diagrama de blocos do dispositivo

Geolocalização: Dados de geolocalização e horário do dispositivo obtidos por um sensor GNSS (Global Navigation Satellite System – Sistema de Navegação Global via Satélite) que são utilizados pelo serviço de identificação (3) e pelo serviço de notificação (4).

Dados dos sensores: dados de sensores internos sobre a operação do veículo (aceleração, capotamento, acionamento de airbags, acionamento de cinto de segurança, máxima tensão do cinto de segurança, temperatura, submersão) e vídeo dos arredores do veículo.

Serviço de identificação: detecta os eventos de interesse, processando os dados dos sensores e informações de geolocalização. Os eventos são detectados utilizando algoritmos de detecção e visão computacional.

Serviço de notificação: recebe informações de identificação de evento (3) e informação de geolocalização (1). A informação é processada para decidir se uma mensagem de notificação (7) deve ser gerada. Este serviço define o destino das mensagens e cria o objeto de notificação. Finalmente, transmite o objeto de notificação para o serviço de transmissão (6) a fim de criar e transmitir as mensagens de notificação (7).

Serviço de armazenamento: armazena internamente as evidências dos eventos de interesse detectados. Tais evidências são imagens, mensagens e logs do sistema.

Serviço de transmissão: transmite mensagens de notificação (7) através dos canais de comunicação disponíveis. O objeto de notificação é codificado (CBOR), criptografado e assinado antes da transmissão. O módulo de transmissão pode usar mais de um canal de comunicação para a transmissão das mensagens. No piloto foi utilizada transmissão por LoRaWAN.

Mensagem de notificação: mensagens geradas e transmitidas pelo serviço de transmissão. Contém a notificação do evento de interesse detectado, além de outras informações relevantes.

5.3 Funcionalidades

5.3.1 Detecção e leitura de placas de automóveis (OCR)

O dispositivo IoT detecta placas de automóveis e faz a leitura dos caracteres localmente, montando uma notificação contendo data/hora, localização e a placa do veículo, que é enviada por LoRaWAN.

A leitura das placas dos veículos é realizada utilizando técnica de visão computacional com ferramentas de software aberto e livre: o framework darknet, a biblioteca OpenCV, e redes neurais YoLo, com treinamento específico.

Quando o reconhecimento de caracteres é realizado com uma precisão superior a um limiar, o evento é enviado para o Serviço de Notificação. Os quadros de evidência são armazenados localmente e podem ser solicitados posteriormente.

5.3.2 Detecção de acidentes

Acidentes são uma recorrente ameaça a motoristas, passageiros e pedestres, responsáveis por milhares de mortes no Brasil todos os anos. Uma das medidas para minimizar o impacto de acidentes consiste na prestação de socorro o mais brevemente possível, visando reduzir fatalidades e a extensão de lesões resultantes. Nesse cenário, considera-se sensores embarcados no veículo para a detecção de acidentes graves, e em caso de detecção a realização de solicitação automática de socorro.

O dispositivo IoT monitora sensores veiculares e no caso de reconhecer um padrão associado a um acidente veicular grave, envia automaticamente notificações para o serviço público de atendimento a emergências. Esta mensagem contém data/hora, localização e a placa do veículo, que é enviada por LoRaWAN. Foi desenvolvido um algoritmo para processar as informações dos sensores de interesse. Uma vez detectado o acidente, o sistema gera uma notificação contendo a leitura de alguns sensores veiculares para prover informações sobre o acidente para a equipe de socorro para melhorar a efetividade do socorro. Estas informações foram especificadas em conjunto com o time de resgate do Corpo de Bombeiros de São Paulo.

Acionamento de serviços de segurança pública

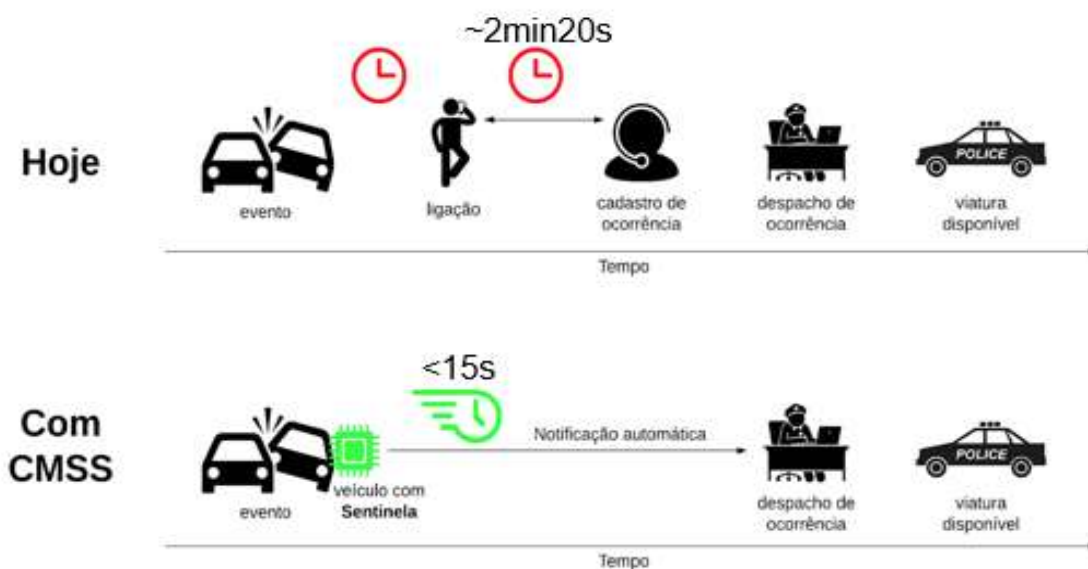


Figura 4.3: Comparação de acionamento de chamado

Código do Sensor	Descrição
AIRBAG	Informa se houve abertura de airbag.
SEATBELT_BUCKLE	Informa se o cinto de segurança está afivelado.
SEATBELT_TENSIONER	Medida da maior tensão realizada pelo pré-tensionador do cinto de segurança.
ACCELERATION	Medida da maior variação de aceleração sofrida pelo veículo no último minuto.
ROLLOVER	Medida do número de giros realizados pelo carro sobre o seu próprio eixo (em caso de capotamento).
TEMPERATURE	Medida de temperatura na cabine.
SUBMERSION	Medida de umidade na cabine.

Tabela 4.1. Sensores considerados no sistema

5.3.3 Notificação de eventos

Foi especificada uma API para notificação de eventos gerados automaticamente pelo Sentinela para os serviços públicos de emergência da cidade de São Paulo. Funciona da seguinte maneira:

- As notificações são codificadas e protegidas para envio através da rede LoRaWAN.
- As notificações são recebidas por um gateway LoRaWAN, que as encaminha para um servidor de aplicações do provedor de rede.
- As mensagens de notificação são então enviadas via HTTPS e através de uma VPN do servidor do provedor para o servidor do COPOM, onde são tratadas.
- A API proposta inclui três aspectos: o modelo de dados da Notificação, os formatos de serialização suportados e a especificação do Servidor de Notificações.

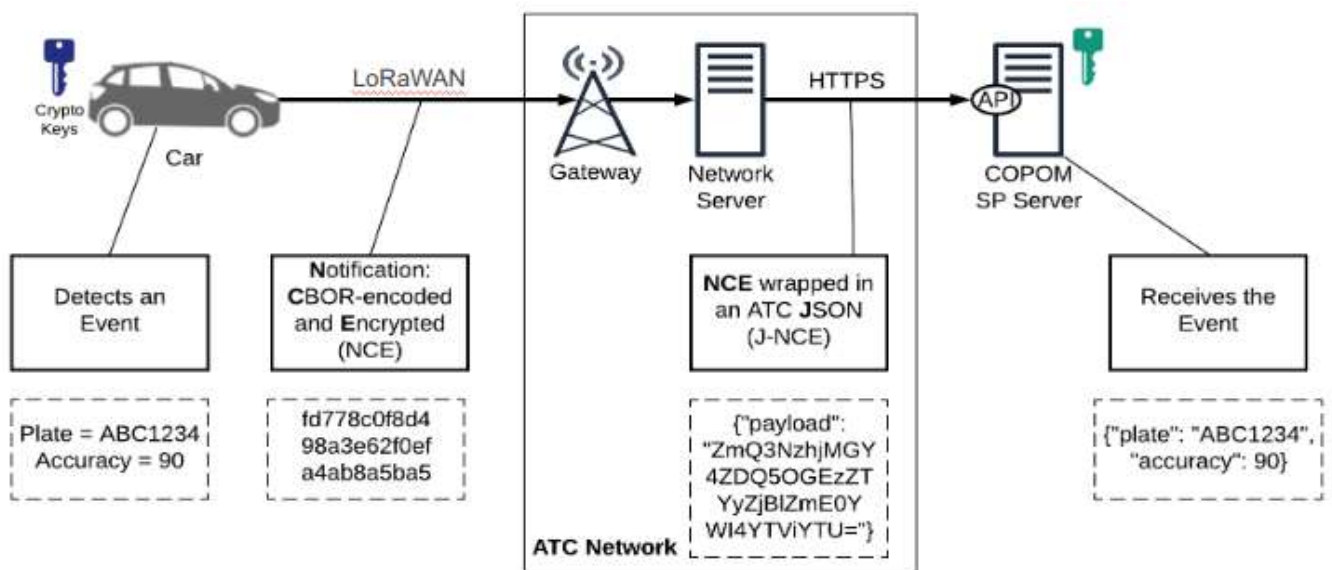


Figura 4.4: Fluxo dos eventos

Formato de serialização

O formato de serialização adotado no projeto é o *Concise Binary Object Representation (CBOR)*.

Modelo de dados de notificação

- As notificações possuem um modelo de dados extensível, que pode receber mais tipos de eventos a serem notificados, que podem ser definidos futuramente.
- As informações contidas na notificação indicam o evento identificado, data e horário, posição por código GPS, a direção que o veículo está seguindo, a identificação do veículo emissor e um campo de testes.
- O veículo emissor é identificado a partir de um conjunto de caracteres, no caso do piloto, está sendo utilizada a especificação Decentralized Identifiers (DIDs) v1¹.0.
- O evento é identificado pelo seu tipo, pelos sensores que fizeram as leituras que levaram à geração do evento e pelo nível de confiança que o sistema tem de que o evento ocorreu.
- O tipo de evento é extensível, sendo inicialmente definidos os tipos: placa de veículos e acidentes.

Nome completo	Índice	Tipo de dados	Obrigatório?	Descrição
senderId	0	String	Sim	Identificação única do emissor da notificação. Número do chassi, para automóveis.
isTest	1	Boleano	Não	Indica se a mensagem é um teste.
timestamp	2	Inteiro	Sim	Informa horário e data, utiliza formatação UNIX Timestamp.
position	3	String	Sim	Posição do veículo, fornecida por GPS interno.
direction	4	Inteiro	Sim	Direção do veículo, em graus sexagesimais.
events	5	Array	Sim	Lista de eventos detectados. Consulte a Tabela 5.

Tabela 4.2: Estrutura de notificação

¹ <https://www.w3.org/TR/did-core/?ref=blog.identity.foundation>

Nome completo	Índice	Tipo de dados	Obrigatoriedade	Descrição
eventType	0	Inteiro	Sim	Consulte a Tabela 1 e a Tabela 5.
triggeredSensors	1	Objeto	Não	Matriz associativa de chaves inteiras e valores decimais (consulte a Tabela 6).
accuracy	2	Inteiro	Sim	Precisão do evento identificado (1-100).

Tabela 4.3: Especificação de campo de evento para notificação: Events.

Segurança e privacidade

Considerando a empregabilidade do sistema para o direcionamento de ativos do sistema de emergência da cidade (ambulâncias, viaturas policiais etc.), passa a ser importante que as notificações tenham imputabilidade. Adicionalmente, há uma questão de privacidade envolvida, já que as mensagens contêm a posição e a identificação do carro emissor e dos carros ao redor. Por isso, é importante adicionar requisitos de sigilo às notificações.

Visando a proteção dos dados, foi adotada a RFC8152 (<https://tools.ietf.org/html/rfc8152>), com as seguintes parametrizações:

- Para criptografia, o padrão AES-CCM-16-64-128.
- Para assinaturas digitais, o COSE ES256.
- Para o estabelecimento da chave, o ECDH-SS (ECDH com chaves Estáticas-Estáticas) com a função de derivação de chave baseada em HKDF (HMAC (código de autenticação de mensagens baseado em Hash)).
- A curva elíptica NIST P-256 deve ser usada nas chaves públicas usadas para ECDH e ECDSA.

Esta abordagem usa padrões abertos e interoperáveis, sendo facilmente extensível para o recebimento de eventos de outras fontes.

Descrição do serviço semântico

O serviço para recebimento de notificações segue o modelo de serviços web RESTFUL via HTTPS na Internet. Esta abordagem usa padrões abertos e interoperáveis, sendo facilmente extensível para o recebimento de eventos de outras fontes.

```
{
  "@id": "https://<POLICE_SERVER>/cmss-notification-server/",
  "description": "Recebe notificação para ocorrências de placas
    E eventos",

  "operations": [
    {
      "entry": "/notification",
      "description": "Recebe uma notificação de emergência",
      "method": "POST",
      "expects": "NotificationMessage",
      "returns": "ReceiptAcknowledgment"
    }
  ]
}
```

Tabela 5.1: Especificação do serviço de recebimento de notificações de emergência.

6. Abordagem tecnológica para a implantação das funcionalidades

A plataforma de hardware utilizada e integrada baseia-se no Programa Caninos Loucos, o qual desenvolve Computadores de Placa Única (SBC - Single Board Computers) abertos para Internet das Coisas (IoT). SBCs são computadores completos integrados numa única placa de circuito impresso, que normalmente possuem dimensões muito reduzidas, próximas ao tamanho de um cartão de crédito, e custo acessível da ordem de algumas dezenas de dólares. Apesar das dimensões e custos reduzidos, funcionalmente os SBCs são computadores muito poderosos incorporando várias interfaces de entrada e saída de propósito geral (GPIOs General Purpose I/O), conexão com a Internet sem fio e cabeada, portas USB, portas para sensores e atuadores. Com a evolução da tecnologia, SBCs se tornaram plataformas essenciais para o desenvolvimento IoT e de grande valor para a diminuição do tempo de desenvolvimento de novos produtos.

A abordagem utilizada baseia-se na leitura de sensores automotivos e de informações de contexto e na realização de processamento destes sinais com aplicação de técnicas de lógica tradicionais associadas a redes neurais artificiais para a detecção do evento de risco.

O desenvolvimento foi realizado utilizando a estratégia de computação de borda (edge computing), na qual o processamento é realizado no próprio dispositivo, sem depender de rede de comunicação ou processamento remoto (na nuvem). A computação na borda traz como vantagem a maior garantia de privacidade, já que os dados coletados no veículo não são trafegados em redes de comunicação e nem processados em servidores remotamente. Isto é especialmente relevante para os casos que buscamos identificar neste projeto, que envolvem capturas de áudio e vídeo, por câmeras e microfones, no interior e no entorno do veículo.

Além disso, esta abordagem tende a produzir resultados com maior confiabilidade e menor latência, já que não depende da rede de comunicação. Também possui maior escalabilidade por não depender de processamento centralizado que concentraria o processamento em tempo real de dados que potencialmente chegaria a milhões de automóveis. Por fim, há redução de custos de telecomunicações, visto que não há necessidade de transmissão de grandes quantidades de dados, como acontece na transmissão de áudio e vídeo.

7. Restrição da Solução

A eficácia da detecção e leitura de placas automotivas depende primariamente da qualidade das imagens de entrada, uma melhor qualidade de imagem, com menos ruído, melhor contraste etc., gera um ganho na confiança das leituras efetuadas e subsequentemente uma maior proporção das leituras são consideradas válidas para o limiar de confiança utilizado, exemplos de fatores com efeito relevante são:

- **Condição de iluminação:** Situações com iluminação ambiente menos intensa como ambientes noturnos ou fechados podem gerar imagens com menos contraste e ruído mais perceptível, ainda mantemos um nível mínimo de detecção mesmo em situações noturnas devido a iluminação da placa traseira imposta pelo artigo 250 do código de trânsito brasileiro e pela iluminação pública, para ambientes fechados/internos ficamos dependentes da iluminação local;
- **Condições ambientais:** Condições como chuva ou névoa mais intensas podem gerar obstrução da visibilidade necessária para leitura das placas, céu nublado apresenta uma iluminação reduzida;
- **Obstáculos:** objetos que cubram a placa podem impedir a sua leitura ou gerar um descarte por baixa confiança, podendo ser desde uma sujeira no para-brisa até uma ocultação intencional da placa, uma situação análoga ocorre se a placa está danificada.

O sistema efetua a leitura apenas do melhor candidato a placa veicular em cada imagem de entrada, os outros candidatos a placa tendem a ter uma confiança de leitura menor, maior chance de serem descartados quando analisados, assim, foi dada preferência a utilizar o processamento em uma imagem seguinte que fora de uma situação de congestionamento tende a ter outros veículos para leitura, principalmente ao considerarmos vias com visibilidade para o contrafluxo.

A notificação das detecções é dependente da disponibilidade (requisito não funcional) das redes instaladas de LoRaWAN (ATC Network da seção 2.4.3), de internet e da VPN disponibilizada para acesso seguro do COPOM, também dependemos da cobertura instalada para LoRaWAN, que atualmente cobre toda a Região Metropolitana de São Paulo (RMSP) mas ainda está sendo implantada para outras áreas. Um ponto possivelmente relevante para escalabilidade da solução é o fato de que um gateway de recebimento LoRaWAN pode deixar de fornecer acknowledgement (ACK) para as mensagens caso receba um tráfego elevado, onde o reenvio das mensagens geraria um aumento da sobrecarga no

gateway, assim, gerando uma necessidade de aumento na densidade de gateways na rede instalada em paralelo a adoção ampla da nossa solução para manter a qualidade de transmissão de eventos.

O sistema proposto é implementado com uma eletrônica externa ao veículo, descrita na subseção seguinte, transformar o sistema proposto em uma ECU e realizar a integração com uma plataforma automotiva é um passo que pode ser realizado futuramente junto às montadoras.

O desenvolvimento da funcionalidade de detecção de acidentes está sendo realizado utilizando valores simulados para os sensores, caso contrário precisaríamos simular acidentes veiculares em ambiente controlado.

8. Protótipo

O protótipo atual do dispositivo de detecção e notificação, denominado Sentinela, é apresentado nesta seção. A placa Labrador, Pulga Stack, cabo plano e antena estão contidos em uma caixa impressa em 3D com aberturas de ventilação e conexão. A câmera USB é montada no topo da caixa. A caixa é instalada sobre o painel do veículo, e o cabo de alimentação é conectado à tomada de energia do veículo. Exemplos dessa configuração são mostrados na figura abaixo.

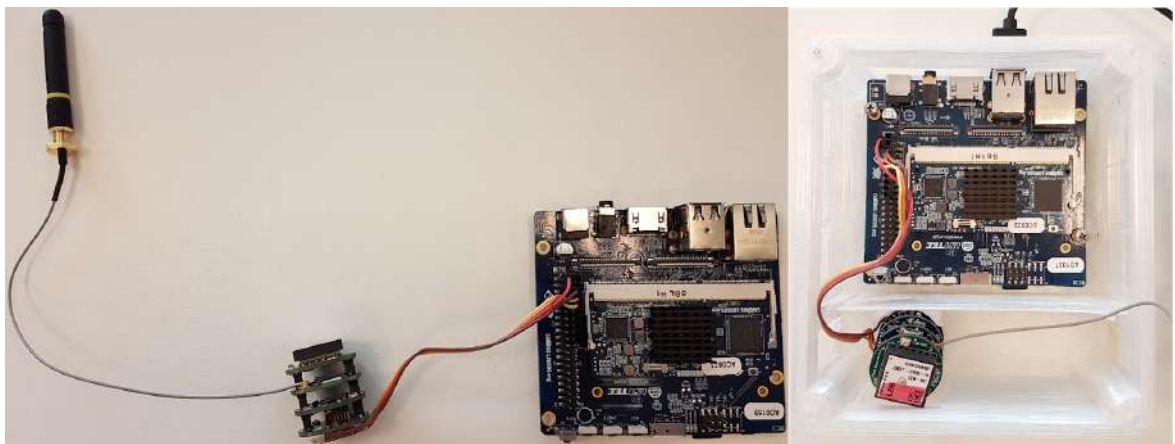


Figura 8.1: Protótipo – eletrônica



Figura 8.2: Protótipo - Dispositivo

A tabela abaixo apresenta os componentes utilizados para a implementação dos protótipos da prova de conceito e a estimativa de custos para uma implementação em larga escala.

Item	Custo do protótipo (USD CIF) ²	Estimativa de custo em grande escala (1M/ano) (USD CIF)
Câmera (Action Cam ref. ELP-USB8MP02G-SFV)	68.0 * 1.27 ³	47.6 * 1.27
Invólucro Sentinela ⁴	2.58	2
Antena dipolo 2,4 GHz, 3 dBi ⁵	2	1.4
Caninos Loucos Labrador 64bits (Coreboard 64 e Baseboard M)	150	105
Caninos Loucos Pulga Core	63.8	44.66
Caninos Loucos Pulga GPS	33	15
Caninos Loucos Pulga LoRa	55	15
Cabo de alimentação veicular ⁶	3.4	1
Total	396.14	244.512

Tabela 8.1: Componentes para implementação do Protótipo

² 1 USD = R\$5,00

³ Tributação NCM 8525.80.22 de 27%

⁴ Custo de impressão 3D: R\$0,10/g, Tampa: 107g; caixa: 122g

⁵ R\$10,00

⁶ 12V Carregador Cabo Veicular Inversor Power Cable

A tabela abaixo apresenta o custo final do produto considerando o custo dos componentes, fabricação e instalação dos dispositivos. Considerando os componentes, produção e instalação e oportunidade de mercado o valor de venda foi estimado entre R\$3.800,00 e R\$5.000,00 por unidade de produto em produção anual menor que 1M/ano.

Item	Estimativa de custo do dispositivo	Estimativa de custo em grande escala
Custo dos componentes	R\$ 1980,00	R\$ 1222,00
Custo de fabricação por unidade	R\$ 990,00	R\$ 693,00
Custo de instalação	R\$ 250,00	R\$ 175,00
Total	R\$ 3220,00	R\$ 2090,00

Tabela 8.2: Custo de implementação.

A tabela abaixo apresenta a especificação técnica dos componentes necessários para a implementação da Sentinela.

CPU	64-bit quad-Core ARM Cortex A53 1,3GHz
RAM	2 GB LPDDR3 SDRAM
Sistema Operacional	Debian 11 Linux Kernel
Áudio	microfone
Conectividade	LoRaWAN™ com antena externa
Armazenamento	2 GB
Sensores	Câmera, microfone, temperatura, sensores veiculares
Posicionamento	GPS
Energia	5~12V @ 3W
Especificações da câmera	8MP, >1fps, Varifocal 5-50 mm or Fisheye 170° lens

Tabela 8.3: Especificação técnica dos componentes para implementação do protótipo.

9. Descrição da solução testada

9.1 Descrição dos testes em campo realizados e Restrições dos testes

Os testes em campo para a validação do sistema foram realizados em parceria com o departamento de Polícia Militar do Estado de SP. Os Protótipos foram instalados em viaturas policiais para coletar informações de placas de veículos, que são enviadas via LoRaWAN para o Centro de Operações da Polícia Militar (COPOM). Estrategicamente, os dados podem ser usados pelo departamento para verificar se os veículos detectados estão envolvidos em ocorrências policiais. Os testes de campo (teste piloto) foram conduzidos como parte deste acordo. No total, 20 Sentinelas foram instalados em carros de polícia. Os dispositivos foram fixados nos painéis das viaturas, conforme mostrado na figura 8.2, capturando imagens do ambiente enquanto os veículos estavam ligados.

9.2 Indicadores coletados

Coletamos os seguintes indicadores dos dispositivos instalados no teste em campo:

- Delay de transmissão, diferença entre o timestamp da detecção do evento na borda, vindo do GPS do dispositivo, e do timestamp do registro do evento no servidor, vindo da rede.
- Taxa de recebimento de mensagens, porcentagem das mensagens enviadas pelos dispositivos que chegam íntegras e são registradas no servidor final, mensurando as perdas de pacotes no fluxo de envio.
- Precisão de leitura de placas, porcentagem das leituras que não foram descartadas pelo limiar de confiança que tiveram uma leitura correta da placa completa/nenhum erro de OCR.

Em um computador foi passado as imagens de um dataset pelo sistema para calcular a sensibilidade do sistema, a porcentagem das placas detectadas pelo sistema em relação a quantidade de placas presentes nas imagens de entrada.

9.3 Resultado dos testes

Taxa de recepção	Delay médio	Desvio padrão
60,92 %	6,5 s	6,5 s

Tabela 9.1: Delay de transmissão rede LoRaWAN

Taxa de recepção	Delay médio	Desvio padrão
100 %	1,65 s	0,4 s

Tabela 9.2: Delay de transmissão rede 4G

O valor apresentado é a média dos delays encontrados nas sentinelas instaladas, passando uma ideia da situação média que seria encontrada na cidade de São Paulo tanto para a rede LoRaWAN como para a rede 4G.

Detecções consideradas	Detecções corretas	Precisão
3311	3105	93,78 %

Tabela 9.3: Precisão da leitura de placas em testes em campo

Na tabela acima vemos que o sistema atingiu um bom nível de precisão, a maior parte dos erros ocorre quando temos um caractere que devido a contraste reduzido e/o ruído fica confusa com um parecido mesmo ao olho humano, por exemplo B com 8 ou O com Q.

O método de produção das placas brasileiras por estampagem gera uma linha vertical (em relevo) na parte inferior esquerda do caractere 5 que o deixa parecido com um 6 para a rede neural mesmo sem pintura, sendo a confusão mais relevante para o sistema proposto.

Para o teste de sensibilidade utilizamos as imagens do dataset de teste das redes neurais que tinham placas automotivas legíveis, mesmo que com dificuldade, para um humano, encontrando o valor de 27,43% de placas não lidas. Esse valor é considerável, e se dá pelo alto threshold de confiança utilizado pelo sistema para considerar uma leitura válida.

Na imagem abaixo os pontos destacados em amarelo correspondem aos locais dos eventos detectados, compreendendo a área que foi percorrida utilizando 20 veículos entre eles viaturas da polícia e da equipe de pesquisa, onde foi realizado o monitoramento dos veículos durante os testes.

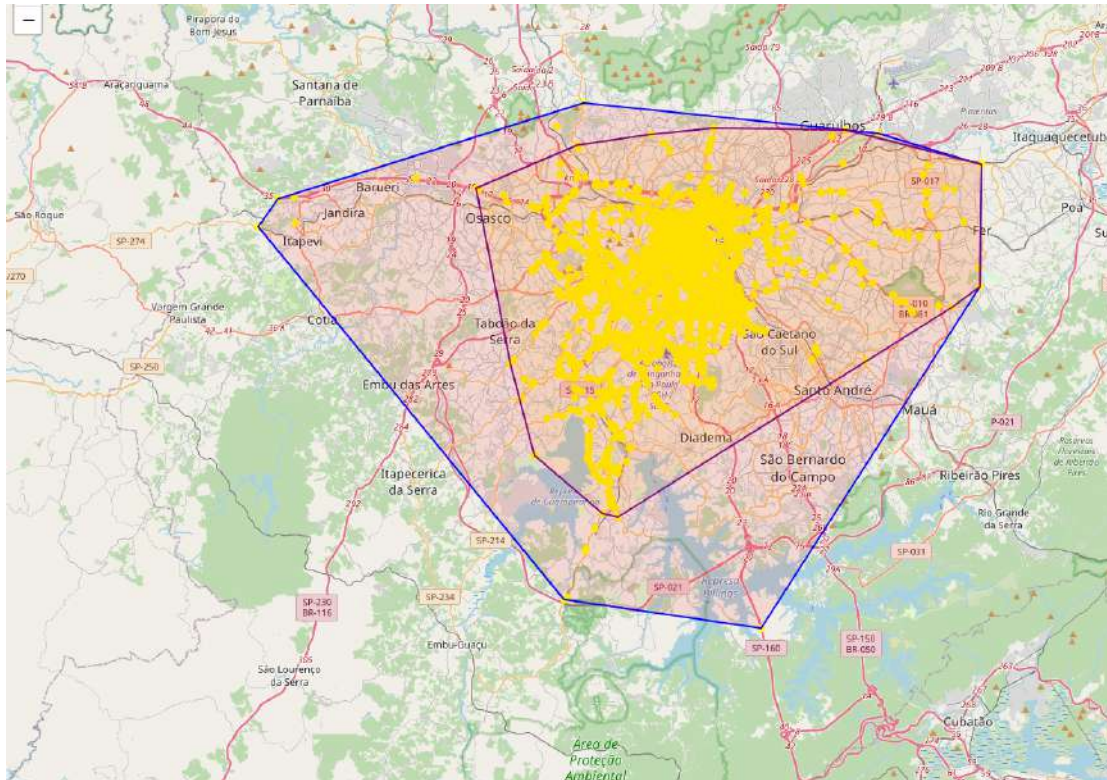
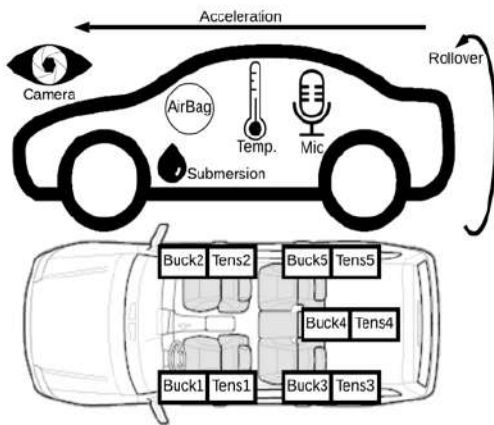


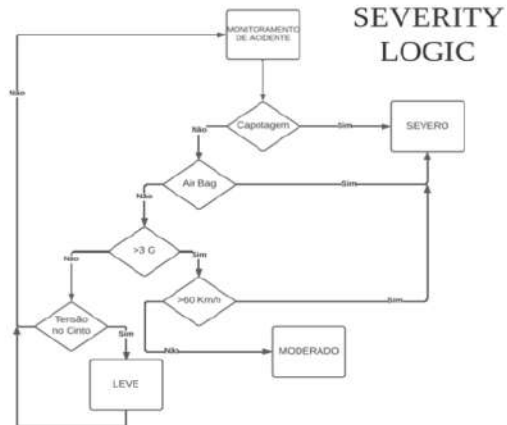
Figura 9.1: Área de testes realizado em campo

O teste-piloto não contemplou testes físicos em veículos para detecção de acidentes, no entanto utilizou software de simulação para atestar a funcionalidades e grau de severidade conforme fluxo mostrado na Figura 9.2 e as mensagens foram enviadas por API conforme Figura 4.4: Fluxo dos eventos. os resultados dos testes de simulação não foram compartilhando para esse relatório.

Detecção de acidentes



Monitoramento dos sensores veiculares.
Detecção de acidentes.



Fluxograma para classificação da gravidade do acidente.

Figura 9.2: Fluxograma para classificação de acidentes.

9.4 Cronograma do projeto

	2020	2021	2022	2023	2024
Desenvolvimento/planejamento	X	X	X		
Testes em laboratório			X		
Testes em campo				X	
Análise					X

10. Metodologia Deloitte: Gerenciamento do Ciclo de Vida dos KPI's e Resultados

A Deloitte tem o papel de Avaliador e utilizará de técnicas e metodologias para avaliação técnico-econômica-financeira. Foi utilizada a metodologia “KPI Lifecycle and Results Management Process” com o objetivo de ter clareza dos indicadores, modo de avaliação, acompanhamento e possíveis ações a serem tomadas com a avaliação dos resultados apresentados pelos indicadores dentro do contexto da POC de IoT para Cidades inteligentes.



*Key Process Indicator (KPI)

10.1 Premissas, Restrições e Dependências

Premissas:

- Testes dos dispositivos em laboratório.
- Testes dos dispositivos em campo.
- Ter disponível ao menos 50% dos sensores previstos para POC para testes em campo com fornecimento de dados de fontes confiáveis para avaliação da solução econômica e financeira.
- Fornecimento de informações referente aos custos envolvidos na produção dos dispositivos de IoT.

Restrições:

- Os testes de funcionalidades de acidentes e emergência foram restritos à simulação em laboratório.

Dependências:

- Massa de dados dos testes realizados em campo.
- Oportunidades e desafios para solução testada em campo (Testes a serem realizados com o uso dos dispositivos).

10.2 Determinação dos Controles e Objetivos

Nesta etapa, serão definidos os indicadores principais para a avaliação dos resultados alcançados com a POC.

Os controles são baseados em indicadores quantitativos e qualitativos para avaliação técnica e econômico-financeira da POC dentro do escopo considerando as seguintes fontes:

- Fontes de dados da solução de IoT (Monitoramento e Consumo de dados):
 - Monitoramento dos dispositivos em campo - acesso à fonte de dados.
 - Levantamento dos custos da solução.
- Fontes de dados da Polícia Militar de São Paulo
 - Levantamento de dados do sistema Muralha Paulista de identificação de veículos aquisitados com os dispositivos fixos (Dados de Produção).
 - Fontes de dados do Corpo de Bombeiros de São Paulo

Como objetivo definimos:

- Avaliação dos benefícios financeiros e de custos relacionados à utilização de tecnologia IoT empregada na POC para realização de avaliação econômico-financeira em relação às questões operacionais e recomendações de melhorias.

10.2 Seleção, Avaliação e Atribuição

Nesta POC foram definidos os principais KPI's para análise e obtenção de resultados considerando o monitoramento de coleta de dados de dispositivos e respectivo consumo e custos relacionados.

10.3 Definição de Valores-Alvo

A solução de IoT do piloto de Segurança Pública e Vigilância urbana possui imenso potencial financeiro, porém para efeito de avaliação dessa iniciativa está sendo considerado apenas os benefícios qualitativos devido às limitações iniciais de informações quanto a composição dos custos de operações das atividades de registros do Copom e economia na logística de atendimento das vítimas envolvidas em acidentes. Os indicadores serão classificados nas perspectivas de Processos e Serviços.

Perspectivas	Objetivos	Motivadores	KPIs
Processos e Serviços	Agilizar o tempo de registro de ocorrências de emergência.	Agilidade no envio de resgate devido precisão do registro do local da ocorrência	Redução de danos às vítimas
	Possibilitar maior capilaridade na detecção de placas de veículos (que possam estar envolvidos em alguma contravenção) na extensão das vias de São Paulo	Controle e monitoramento de veículos	Ampliação do monitoramento de veículos nas vias

10.4 Resultados preliminares dos testes

Perspectivas	Objetivos	KPIs	Resultado KPIs com uso da solução de IoT
Processos e Serviços	Agilizar o tempo de registro das ocorrências de emergência.	Redução de danos às vítimas	Redução de 80% ⁷ do prazo de registro da chamada de emergência devido cadastro automatizado com ou uso de API (através de simulação do acionamento dos sensores)
	Possibilitar maior capilaridade na detecção de placas de veículos (que possam estar envolvidos em alguma contravenção) na extensão das vias de São Paulo	Ampliação do monitoramento de veículos nas vias	Aumento de capilaridade ⁸ OCR de placas veiculares: De 0,001% para 100% Racional: foi considerada a área de testes da região metropolitana da cidade de São Paulo atualmente coberta por 877 radares OCR fixos, que representa 0,001% das vias da cidade que totalizam cerca de 20.000km

10.5 Relatório de Performance e Controle

O objetivo dessa seção é avaliar a evolução do Piloto. O Piloto teve processo de engenharia de construção do dispositivo IoT realizado de forma satisfatória conforme testes de laboratório e em campo demonstrados anteriormente nesse documento.

⁷ Não foi realizado testes com veículo e envolvendo vítima

⁸ O aumento da capilaridade não está diretamente relacionado a quantidade de placas lidas em comparação ao OCR fixo, vide item 7 restrições da solução.

10.6 Resultados esperados

Análise do desempenho técnico-econômico da solução testada do Piloto 1.

10.7 Apresentação da análise econômica e financeira e viabilidade técnica

Considerações :

- Análise quantitativa do processo de revenda da solução a nível de piloto considerando a frente de Vigilância Pública.
- Foi considerado o investimento inicial de R\$500.000,00 referente a aquisição de 100 unidades de sensores para instalação em 100 veículos.

Análise de viabilidade econômica:

Ítems	Valores estimados
Investimento Inicial da Implementação da Solução de IoT	R\$ 500.000,00
Taxa de desconto	12%
NPV	R\$ 137.814,84
TIR	0,24
Taxa de Lucratividade	1,28
PayBack	2,92 anos

10.8 Revisão e Ajuste do Controle do Modelo

Estruturação de modelo de negócio sustentável para difusão da das soluções

Tendo em vista que a solução de IoT atende tanto tecnicamente como de forma econômico-financeira pode considerar as alternativas de fornecimento da solução que pode ser desenvolvida em grande escala por dezenas de empresas no Brasil comercialização diretamente com as prefeituras das cidades para instalação em veículos públicos, bem como para atender as demandas da

Polícia Militar e Civil através de venda ou locação dos dispositivos através de serviço de assinatura mensal.

Cenário de vendas de dispositivos para uma amostra de venda de 100 dispositivos anuais

Venda direta de dispositivos	
Item	Estimativa de Custo (R\$)
Instalação da solução de IoT	20.000,00
Vendas da Solução de IoT	500.000,00
Treinamento e Capacitação	5.400,00
Total do CAPEX	525.400,00

CAPEX (Despesas operacionais anuais)

Venda direta de dispositivos	
Item	Custo Anual (R\$)
Serviço de conectividade e armazenamento de dados	12.000,00
Total do OPEX	12.000,00

OPEX (Despesas operacionais anuais)

Venda direta de dispositivos				
Fonte de Faturamento	Quantidade	Custo Unitário	Preço unitário de Venda	Faturamento Total
Venda dos dispositivos	100	3.220	5.254	525.400

Projeção de faturamento anual

Total CAPEX: R\$ 525.400,00

Total OPEX: R\$ 12.000,00

Total faturamento anual: R\$ 537.400,00

Cenário: Assinatura de Serviços

No exemplo abaixo foi considerada a assinatura anual de 100 sensores.

Locação de dispositivos	
Item	Estimativa de Custo (R\$)
Locação dos sensores	160.000,00
Serviço de plataforma de dados e Manutenção	100.000,00
Total do OPEX	260.000,00

Resumo financeiro

Total de faturamento anual: R\$ 260.000,00

10.9 Conclusão

O presente documento demonstra com avaliação favorável considerando que a tecnologia atende os requisitos técnicos atendendo às demandas de segurança da informação e se coloca como uma alternativa economicamente viável para investimento e com potencial de escalabilidade nas cidades, podendo ser replicada tanto pelo poder público como pela iniciativa privada como montadores de veículos.

10.10 Sugestões e Recomendações

Tendo em vista o custo-benefício da solução adotou-se hardware e comunicação de baixo custo em atendimento ao Piloto. Para novas aplicações é possível aumentar a capacidade de captura de imagem se for empregado um hardware com maior definição e aumentar a eficiência da cobertura de rede LoRaWAN, ou utilização de redes 4G ou 5G.

10.11 Modelo de Mercado e Escalabilidade

Existe potencial de escalabilidade empregando automatização do processo de cadastro de chamadas de emergências no Centro de Operações da Polícia Militar (Copom), bem como implementação em veículos diretamente pelas montadoras ou através de oferta para adaptação em automóveis da frota brasileira.

Com relação à automatização do cadastro de chamadas de emergência existe uma demanda do Copom do Estado de São Paulo onde é recebido cerca de 50 mil ligações por dia por meio do 190, ferramenta utilizada para casos de emergência e pedidos de ajuda o que representa mais de 80% das chamadas de emergência dos Ciops (Centro Integrado de Operações e Segurança Pública) dos outros estados da federação.

Considerando:

- Segundo dados de Produtividade⁹ do Copom em 2023, acidentes de trânsito com vítimas representaram 5,14% dos atendimentos.
- Sendo em média 2570 ligações por dia.
- Considerando mão-de-obra de 40 atendentes em média, que estão divididos em turnos. O atendimento funciona 24 horas e atende todo o território paulista. Ao receber a ligação, o atendente detecta o tipo de problema e, de acordo com as necessidades da vítima, pode encaminhá-la para um setor especializado da central.
- O emprego da solução de IoT poderia reduzir mão-de-obra nos atendimentos relacionados a acidentes de trânsito devido agilidade no processo de cadastro da ocorrência tem o potencial de reduzir mais de 85% o tempo do registro da ocorrência conforme testes referenciados na Figura 4.3.
- O número de acidentes: Em 2023, foram registrados 85.549 acidentes de trânsito nas rodovias federais, resultando em 2.906 mortes
- Frota total: Em outubro de 2024, o Brasil tinha aproximadamente 65 milhões de veículos em circulação, em média, cerca de 13 veículos a cada 10.000 se envolvem em acidentes de trânsito no Brasil.

⁹ <https://www.saopaulo.sp.gov.br/spnoticias/ultimas-noticias/entenda-como-funciona-o-190-da-policia-militar-de-sp/>

- Considerando essa taxa, os carros que estiverem utilizando a Solução IoT para Segurança Pública poderão se beneficiar de atendimento mais eficiente devido automatização do processo do cadastro da ocorrência e precisão do local do sinistro para melhor deslocamento da viatura de prestação de socorro e diminuição do tempo de atendimento hospitalar.

No entanto o piloto se encontra em TRL 4 e não será possível nesse momento fazer uma análise quantitativa para ganho em escala com processo de registro de cadastro no Copom e validação de economia com diminuição do tempo de atendimento hospitalar¹⁰, restringindo apenas em uma análise qualitativa contudo a solução poderá contar com um **mercado potencial de cerca 65 milhões de veículo em todo Brasil, seja através de instalação em automóveis particulares ou incluindo a solução como item de série na fabricação dos veículos diretamente das montadoras para carros novos, que são em média 3 milhões ao ano.** Atualmente a cidade de São Paulo possui uma frota de aproximadamente 8 milhões de veículos¹¹. O sistema proposto tem potencial de escalar para atender também à frota de veículos da Polícia Militar e Civil do país, que conta com aproximadamente 120 mil veículos.

A Rede LoRaWAN está presente em todas as regiões do Brasil, cobrindo áreas que representam 62% do PIB nacional¹². A grande São Paulo possui cobertura da rede e essa região, conforme informação que consta no site da CET¹³, é coberta por 877 radares fixos o que representa aproximadamente 0,001% de extensão das vias da cidade de São Paulo, que totalizam aproximadamente 20.000km¹⁴. A solução de IoT possibilitará atuar na capilaridade aumentando a cobertura de monitoramento ao longo das vias, com potencial de cobertura total à medida em que for adotado o monitoramento móvel na cidade.

¹⁰ Dados estatístico de acidentes: <https://www.ipea.gov.br/atlasviolencia/arquivos/artigos/7018-td2565.pdf>, <https://www.ssp.sp.gov.br/estatistica/corpo-de-bombeiros>,

¹¹ Frota de Veículos da cidade de São Paulo: <https://www.redesocialdecidades.org.br/br/SP/sao-paulo/frota-de-veiculos-na-cidade>

¹² **Rede Lora Wan:** <https://iot-labs.io/rede-neutra-iot-lorawan-da-american-tower/#cobertura>

¹³ **Radares fixos:** <https://app.powerbi.com/view?r=eyJrIjoiNmZmZjRlYmYtYjZjZS00YWE1LTlkYTUyMGU4NTZmYmYxMzE2liwidCI6ImYzOThkZjJjLWZkMGMtNDgyOS1hMDAzLWw3NzBhMWM0YTA2MmYjJ9>

¹⁴ Qual é a quilometragem de vias do Município de São Paulo? <https://www.cetsp.com.br/perguntas-frequentes.aspx>, <https://expresso.estadao.com.br/sao-paulo/2023/05/12/saiba-quais-sao-as-10-vias-mais-longas-da-capital/>

Considerando as informações preliminares do piloto na frente de monitoramento é possível auferir um benefício qualitativo pela capilaridade de cobertura das vias e abre possibilidade para aprofundamento do estudo em benefícios financeiros que podem ser oriundos de melhoria da logística e diligências policiais.

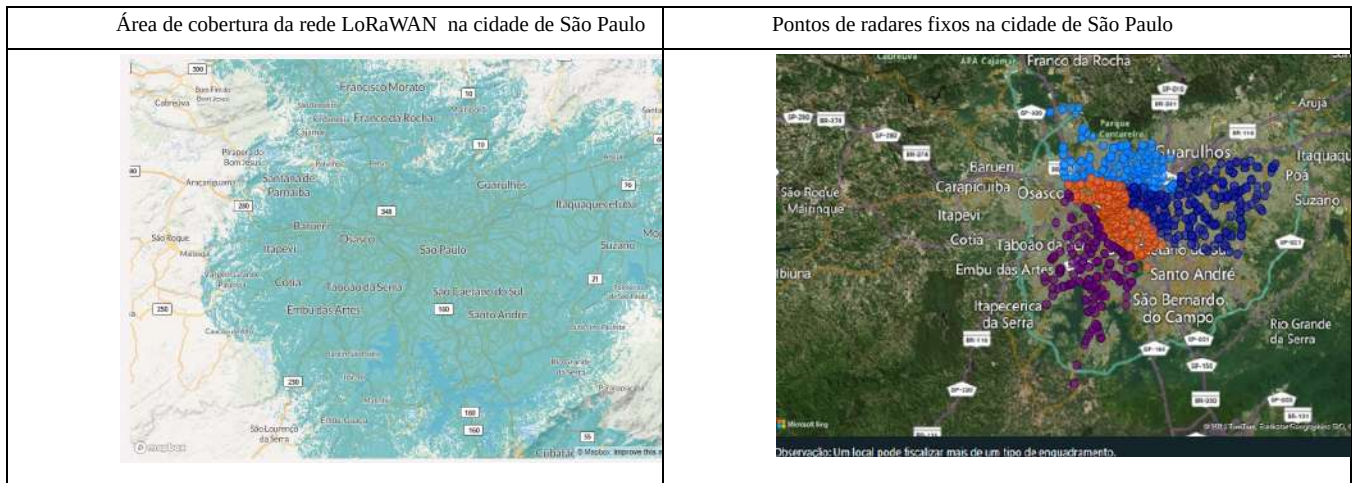


Figura 11.1: Cobertura da rede LoRaWAN e Radares fixos

About Deloitte

As used in this communication, 'Deloitte' means Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries and territories, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 220,000 professionals are committed to making an impact that matters.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2024. For information, contact Deloitte Touche Tohmatsu Limited.