Iberoamerican Journal of Project Management
ISSN 2346-9161

ANÁLISE DE SEGURANÇA CIBERNÉTICA EM VEÍCULOS AUTÔNOMOS UTILIZANDO LÓGICA PARACONSISTENTE

CYBERSECURITY ANALISYS IN AUTONOMOUS VEHICLES USING PARACONSISTENT LOGIC

Michel B. F. Silva; Escola Politécnica – Universidade de São Paulo (USP)

Silvio E. Barbin; Escola Politécnica – Universidade de São Paulo (USP)

Luiz A. Lima; Universidade Paulista (UNIP)

Jair M. Abe; Universidade Paulista (UNIP)

Resumo

Este artigo tem como objetivo a análise da segurança cibernética de veículos autônomos (VA), os quais tem sido objeto de extensivos testes nos últimos anos. Para esse trabalho, serão necessários conceitos de Internet das Coisas (IoT), Segurança da Informação e Lógica Paraconsistente. Inicialmente, é definida uma classificação dos níveis de automação de veículos para sistemas autônomos. Os serviços básicos de segurança, Autenticação, Confiabilidade, Disponibilidade, Integridade e Não-Repudiação, são definidos e é utilizado um modelo em que existem objetos de interesse entre os serviços. Para este modelo, há quatro planos de análise e o plano de segurança cibernética é explorado. Em relação à Lógica Paraconsistente, é explicado como ela pode ser aplicada para análise de segurança de veículos autônomos. Adicionalmente, são analisados os resultados de alguns testes de fabricantes de VA e de guias de instituições automotivas americanas. Por fim, serão integrados os resultados de testes de direção de VA, guia para fabricantes com modelos de segurança de informação, verificando eventuais gaps.

Palavras-chave

Segurança da Informação; Veículos Autônomos, Segurança cibernética, Lógica Paraconsistente anotada evidencial Eτ, Lógica Paraconsistente Anotada.

Summary

This paper is focused the cybersecurity analysis of autonomous vehicles (AV), which have been extensively tested in recent years. For this work, this will be necessary concepts of Internet of Things (IoT), Information Security and Paraconsistent Logic. Initially, it is a defined the level of

Iberoamerican Journal of Project Management
ISSN 2346-9161

automation of vehicles based on the functions of the autonomous system. The basic security services, Authenticity, Reliability, Availability, Integrity and Non-repudiation, are defined and it is used a model which interests objects between them. For this model, there are four planes and the cyber security is explored. As for the Paraconsistent Logic, it is explained how it can be applied for the security analisys of autonomous vehicles. Additionally, it is analyzed the results of the tests from manufacturers of AV and some guidance from relevant American driving institutions. Then it will be understood how information security works on IoT devices and how are the tests of self-driving vehicles. Finally, the results are integrated from information security, VA´s driving test, guidance for manufacturers.

Keywords

Information Security, Autonomous Vehicles, Cybersecurity, IoT, Paraconsistent annotated evidential logic Eτ, Paraconsistent annotated logic.

1. Introdução.

A Internet das Coisas, em inglês *Internet of Things* (IoT), tem sido um assunto de extensivas pesquisas e investimentos como o projeto CASAGRAS, um estudo financiado pela União Europeia focado em padronizar questões relacionadas à tecnologia de identificação por Rádio Frequência, em inglês *Radio-Frequency Identifier* (RFID). Segundo o relatório final produzido por esse projeto (1), a Internet das Coisas pode ser definida como uma rede de infraestrutura dinâmica e global com capacidade de autoconfiguração baseada em padrões e protocolos de comunicação interoperáveis onde dispositivos ou equipamentos tanto físicos quanto virtuais possuem identidades, atributos físicos, características virtuais, usam interfaces inteligentes e estão integrados perfeitamente na rede de informação. Dessa forma, ocorre a integração dos milhões de serviços Web disponíveis na Internet como Facebook, Google, Netflix, PayPal, Waze, TV on line com bilhões de dispositivos ou "coisas" como sensores, microcontroladores, computadores de uma única placa, displays, motores entre outros dispositivos inteligentes tornando possível uma era com computação e comunicação ubíqua (2).
Diversos setores já aplicam soluções que utilizam dispositivos e arquiteturas de Internet das Coisas (3) como, por exemplo, as primeiras redes de sensores sem fio, agricultura, saúde, educação, *wearables,* indústrias, cidades inteligentes, automação residência e logística, em especial, veículos autônomos.

Cidades inteligentes podem ser compreendidas como uma estratégia de desenvolvimento urbano desenvolvida e gerenciadas pelas governantes da cidade visando planejar e alinhar a longo prazo o gerenciamento de diversos ativos de infraestrutura e serviços municipais e com um único objetivo de melhorar a qualidade de vida dos cidadãos (4). Um dos elementos de cidades inteligentes é o transporte inteligente. Um fato que demonstra a necessidade de ações para aumento da segurança é a a quantidade de vítimas fatais em acidentes de trânsito. Segundo dados

Iberoamerican Journal of Project Management
ISSN 2346-9161

do Bureau de Estatísticas de Transportes dos EUA de 2015, quase 32 mil pessoas são mortas e mais de dois milhões se ferem anualmente devido a colisões de automóveis, somente nos EUA. O impacto econômico e social é de US$ 800 bilhões por ano.

Um objeto de extensivas pesquisas e recentes testes principalmente nos EUA são os veículos autônomos (VA), *autonomous vehicles (AV)* ou *self-driving cars*. Entre os principais benefícios desses veículos, pode-se considerar: a redução dos acidentes de trânsito provocados por fatores humanos, com a consequente diminuição de mortes no trânsito, redução da emissão de poluentes e de consumo de combustível, a pessoa que antes iria dirigir pode realizar outras tarefas durante o transporte, como checar e mandar e-mails, assistir seus programas de TV, cochilar, realizar ligações, haverá um aumento da capacidade de tráfego das vias com a redução das distâncias entre os veículos, dados que o tempo de reação será bem menor.

1.1 Veículos autônomos (VAs).

A tecnologia dos Veículos Autônomos vem realizando importantes evoluções para a sociedade na forma sistemas automatizados, para veículos de pesquisa ou comerciais (5). A Sociedade dos Engenheiros Automotivos (SAE) elaborou uma classificação que estabelece o nível de automação no qual o veículo está com base nos papéis assumidos pelo sistemas automatizados, como mostrado na Tabela 1.

Tabela 1 – Níveis de Automação para veículos autônomos definidos pelo SAE

Nível	Nome do Nível	Papel do Sistema Automatizado
0	Sem automação	Autonomia zero. O motorista realiza todas as tarefas da direção.
1	Assistência do Motorista	Veículo é controlado pelo motorista, mas somente algumas funções de assistência à direção podem ser incluídas no projeto do carro.
2	Automação Parcial	Existe uma combinação de funções automatizadas como aceleração e direção, mas o motorista deve estar atento ao trajeto e monitor o ambiente durante todo o tempo.
3	Automação Condicional	O motorista é necessário, mas não é requerido o monitoramento do ambiente. O motorista deve estar pronto para assumir o volante quando for preciso.
4	Alta Automação	O automóvel é capaz de executar todas as funções para direção sob alguma condições. O motorista pode ter a opção de assumir o volante.
5	Completa Automação	O automóvel é capaz de executar todas as funções para direção em todas as condições. O motorista pode ter a opção de assumir o volante

Fonte – adaptado de SAE Níveis de Automação (6)

Iberoamerican Journal of Project Management
ISSN 2346-9161

A NHTSA é a agência do governo americano responsável pela administração nacional de segurança rodoviária. A maioria dos benefícios dos veículos autônomos apontados anteriormente requer nível de automação 4 ou 5. Os carros sem condutor requerem uma extensiva coleta e análise de dados devido à sua ligação a serviços de tráfego e navegação baseados na nuvem, à verificação de obstáculos e necessidade de alteração de faixa, entre outros pontos de ligação. As funções de percepção do veículo, são realizadas por sensores que monitoram o ambiente. Um computador do automóvel combina os dados dos sensores com mapas de alta-definição que localizam o veículo.

Um argumento que corrobora com o estudo dos veículos autônomos é de que 90% das batidas de veículos, segundo a Administradora Nacional de Segurança nas Estradas (7), são causadas por falhas humanas como dirigir em alta velocidade, não perceber o movimento dos outros carros, consumo de álcool, fadiga, entre outros.

Com a adoção de veículos autônomos, será possível eliminar muitos dos erros rotineiros que os motoristas cometem. O desempenho também será melhorado porque há nos veículos autônomos uma melhor percepção, sem pontos cegos, uma tomada de decisão mais precisa e uma melhor execução com um controle mais rápido e preciso do câmbio, freios e aceleração.

Entretanto, os veículos autônomos podem não eliminar todas as batidas. Por exemplo, em variações de tempo abruptas e em ambientes de direção complicada, os veículos autônomos podem desempenhar até pior que os motoristas humanos em algumas circunstâncias. Ademais, existe até um risco de ciberataque no veículo.

No caso do Chevrolet Cruise AV, um veículo autônomo que está em testes nos EUA, existem dezesseis câmeras, vinte e um radares e cinco LiDARs, acrônimo de *Light Detection and Ranging*, um sensor que utiliza feixes de laser que ajudam a mapear o ambiente, quando voltam para o sensor. A Figura 1 ilustra essa composição de elementos perceptivos e sua localização.

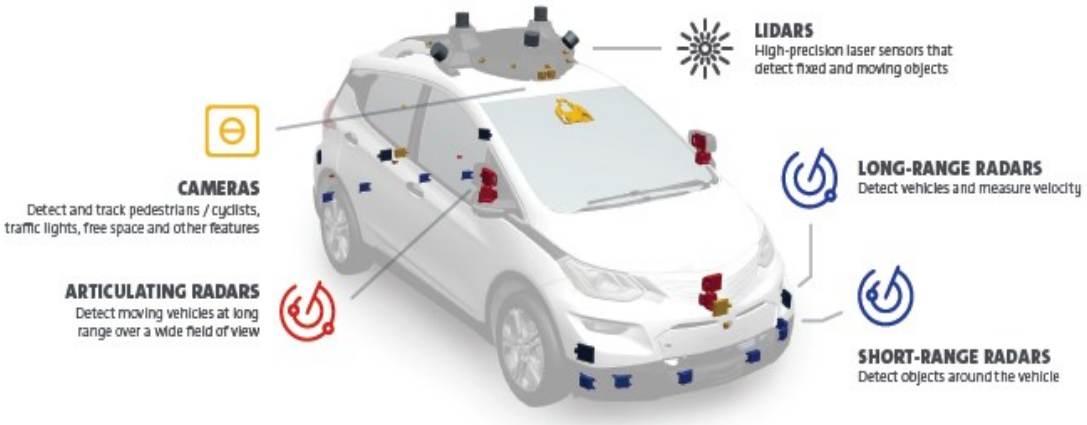

Figura 1 – sensores, câmeras e radares no chevrolet cruise av
Fonte – (8)

Iberoamerican Journal of Project Management
ISSN 2346-9161

Assim, é imperativo que as empresas façam sua devida diligência para assegurar o monitoramento e a análise adequados a esse novo fluxo de dados. Entretanto, a complexidade do controle distribuído de centenas de milhares de carros não pode ser ignorada ou diminuída. Em caso de catástrofes naturais, os veículos devem coordenar suas atividades para uma evacuação das áreas mais críticas.

Quando existe um conjunto de veículos autônomos trafegando dados em uma mesma região, é formada uma rede de veículos inteligentes, ou *vehicle-to-grid*, quando diversos veículos são equipados com sensores que geram significativas quantidades de dados por segundo. Os veículos autônomos devem cooperar eficientemente para manter um fluxo de tráfego nas estradas e rodovias. Simultaneamente, a estrada é instrumentada com tags RFID, microcontroladores embarcados, câmeras de monitoramento formando uma Nuvem Veicular, ou *Vehicular Cloud*.

1.2 Segurança da informação em veículos autônomos (VA).

Uma das áreas mais críticas em dispositivos IoT de diversas áreas de aplicação é a segurança e tem sido um assunto de diversas pesquisas (9), posto que o ataque de um invasor pode ser de diversos tipos, ter diferentes níveis de ameaça para o dispositivo e comportamento do usuário. Para garantir que os veículos autônomos alcancem sua promessa de maior segurança e conveniência ao motorista, é essencial que a indústria de veículos autônomos proteja a sua conectividade com a internet. Dessa forma, as empresas devem implementar uma abordagem de ponta a ponta para identificar vulnerabilidades de softwares antes de serem exploradas.

A Segurança de Informação é uma coleção de atividades que protegem o Sistema de informações e os dados armazenados nele (10). Existem diferentes aspectos que caracterizam a segurança em sistemas de informação, denominados de serviços de segurança. Os serviços básicos de segurança são Autenticidade, Confidencialidade, Disponibilidade, Integridade e Irretratabilidade.

A Autenticidade representa a garantia de que a origem de uma mensagem seja corretamente identifica pelo receptor. Uma boa prática de segurança a verificação de autenticidade após todo o processo de identificação.

A Confidencialidade de Dados garante que qualquer informação armazenada num sistema seja revelada, acessada e /ou manipulada somente por usuário devidamente autorizados. Relacionado diretamente com a confidencialidade de dados, existe a privacidade que é a garantia que os indivíduos controlem ou influenciem quais informações sobre eles podem ser coletadas e armazenadas e por quem e para quem tais informações podem ser reveladas.

A Disponibilidade busca garantir que os usuários legítimos não sejam indevidamente impedidos de acessarem os recursos e informações de sistema.

Por sua vez, a Integridade possibilita a verificação da consistência da informação contida nos dados, impedindo que seja alterada indevidamente de maneira imperceptível. Dessa forma, se os dados forem alterados sem autorização, a alteração será sempre detectada.

Iberoamerican Journal of Project Management
ISSN 2346-9161

Por fim, com a Irretratabilidade, a origem e o destino das informações não podem negar a sua transmissão, recepção ou posse, e está relacionada às assinaturas digitais.

Em relação aos veículos autônomos, a NHTSA desenvolveu um guia voluntário *Automated Driving Systems 2.0 – A Vision for Safety* (6) com doze elementos de segurança. São eles: Segurança do sistema, domínio de projeto operacional, detecção e resposta a objetos e eventos, *fallback* (condição de mínimo risco), métodos de validação, interface homem-máquina, segurança cibernética do veículo, resistência ao choque, comportamento pós-choque, armazenagem dos dados, educação e treinamento do consumidor e leis federais, estaduais e municipais.

1.3 Lógica paraconsistente em sistemas inteligentes.

Sistemas inteligentes estão cada vez mais estão sendo utilizados por especialistas na construção de sistemas que podem ser utilizados em automatizações com princípios baseados em lógicas ditas como clássica e não clássicas. A Lógica Paraconsistente permeia a classificação das lógicas não clássica. O termo "paraconsistente" significa literalmente "próximo à consistência". No entanto, em 1976, o filósofo cientista Francisco Miró Quesada, chamou a lógica de "Paraconsistente". De acordo com a Lógica Paraconsistente, uma sentença e sua negação podem ser ambas verdadeiras. Em meados da década de 1950, o polonês S. Jaskowski e o matemático lógico paranaense Newton C. A. da Costa, nascido em 1929, propuseram a contradição na estrutura lógica e ficaram conhecidos como os fundadores da Lógica Paraconsistente (11).

No cotidiano, diversas capturas de informações ditas contraditórias abrem um espaço de incertezas que culminam em constantes contradições e caracteriza aberturas em futuras contestações. Em áreas como análises de exames clínicos, onde pelo menos dois ou mais especialistas estão à frente de decisões, sempre haverá apontamento de diferentes opiniões.

A Lógica Paraconsistente Lógica Evidencial Eτ (12) é uma classe de Lógica Paraconsistente que trabalha com proposições do tipo p (μ, λ), onde p é uma proposição e (μ, λ) indicam os graus de evidência favorável e evidência contrária respectivamente. O par (μ, λ) é chamado de constante de anotação, com os valores de μ e λ sendo limitados entre 0 e 1. Uma forma de representar a lógica paraconsistente que permite perceber o alcance real assim extrair resultados para subsidiar a tomada de decisão, se depara com a compreensão do diagrama e seus graus de certeza e incerteza, agrupados em estados extremos identificados nos resultados. Entre um e quatro são estados extremos e não-extremos mostrados nos resultados (entre cinco e doze), com valores de controle ajustáveis representando valores-limites: C1 = C3 = ½ e C2 = C4 = -½;

- C1: Vcve = valor máximo do controle de certeza;
- C2: Vcfa = valor mínimo de controle de certeza;
- C3: Vcic = valor máximo do controle de incerteza;
- C4: Vcpa = valor mínimo do controle de incerteza

Iberoamerican Journal of Project Management
ISSN 2346-9161

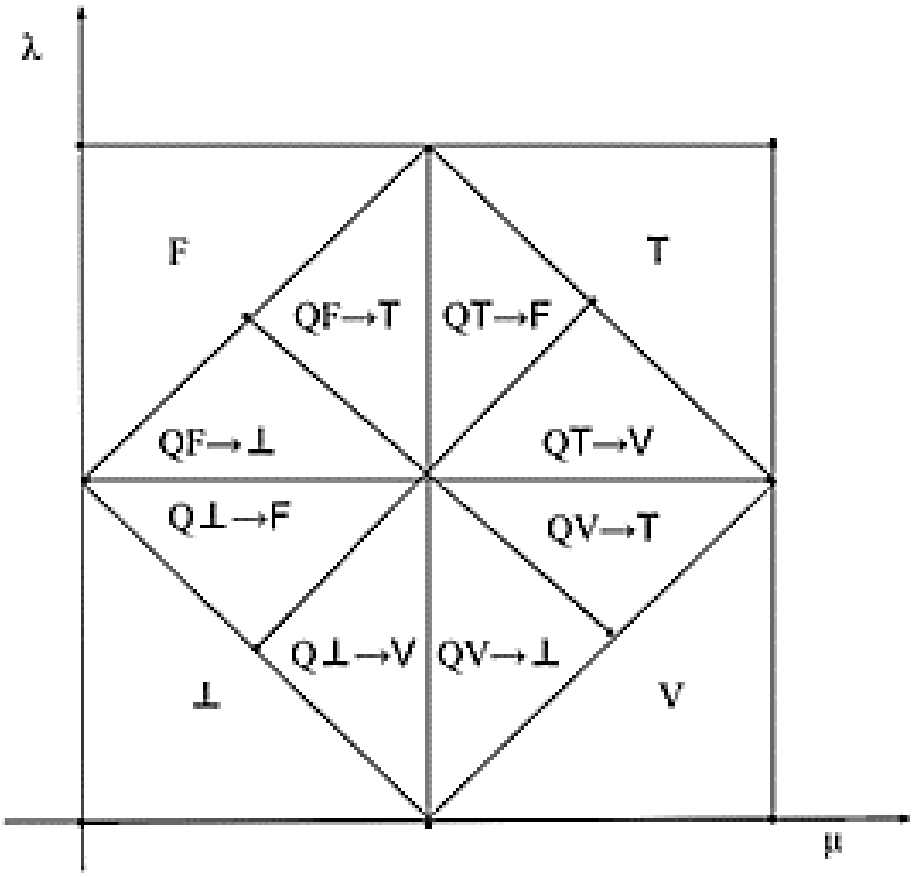

Figura 2 - diagrama com graus de certeza e incerteza, com valores ajustáveis de controle de limite indicados nos eixos.

Fonte - (11).

Na representação do diagrama, foram utilizados os seguintes entendimentos com símbolos e seus 12 resultados possíveis, sendo 1 a 4 estados extremos e 5 a 12 estados não extremos:

Tabela 2 – representação de estados extremos da lógica paraconsistente

Item	Símbolo	Descrição
01	V	Verdadeiro
02	F	Falso
03	T	Inconsistente
04	⊥	Paracompleteza

Fonte – Autor

Iberoamerican Journal of Project Management
ISSN 2346-9161

Pode-se representar a lógica paraconsistente de forma a atender às novas proposições e assim conseguir obter novos resultados para auxiliar na tomada de decisão, temos a representação do diagrama e seus graus de certeza e de incerteza, agrupados em vinte estados:

Tabela 3 – representação de estados não extremos da lógica paraconsistente

Item	Símbolo	Descrição
05	QV → T	Quase verdadeiro tendendo para o inconsistente
06	QV → ⊥	Quase verdadeiro tendendo para Paracompleteza
07	QF → T	Quase falso tendendo para o inconsistente
08	QF → ⊥	Quase falso tendendo para Paracompleteza
09	QT → V	Quase inconsistente tendendo a verdadeiro
10	QT → F	Quase inconsistente tendendo a falso
11	Q⊥ → V	Quase Paracompleteza tendendo para verdadeiro
12	Q⊥ → F	Quase Paracompleteza tendendo para falso

Fonte - Autor

A definição do ParaconsistentDecisionMethod (MPD), proposta nos estudos (11-13), reflete o método utilizado para tomada de decisão através da Lógica Paraconsistente. No caso de um sistema com inteligência artificial, as redes neurais (13), também conhecidas como *Machine Learning*, que partem do estudo do reconhecimento de padrões, o aparecimento de contradições no raciocínio lógico é inevitável quando tentamos refletir o comportamento humano. Em resposta à contradição, temos a LogicParaconsistent. Uma alternativa é utilizar lógica fuzzy como em (14-15).

A lógica paraconsistente anotada é uma classe de Lógica Paraconsistente que trabalha com proposições do tipo p [μ, λ], onde p é uma proposição e [μ, λ] indicam os graus de evidência favorável e evidência contrária, respectivamente. O par [μ, λ] é chamado de constante de anotação, com os valores de μ e λ sendo limitados (1 entre 0 e 1). Ao fomentar o uso da Lógica Paraconsistente Anotada em apoio à tomada de decisão em carros inteligentes, abre-se novos caminhos em estudo de algoritmos que possibilite mitigar inúmeras falhas que causam acidentes e põe em riscos vidas humanas.

O processo unificado de Lógica Paraconsistente Anotada Evidencial Eτ, exposto na tabela 4, tem como objetivo facilitar o entendimento da Lógica Paraconsistente Anotada Evidencial Eτ ao implementar em sistema computacional (16), assim como foi no sistema AITOD (Apoio Inteligente na Tomada de Decisão), como um auxílio na tomada de decisão (16), como segue:

Tabela 4 – PULPA-Processo Unificado de Lógica Paraconsistente Anotada Evidencial Eτ.

Item	Processo	Subprocesso
1	Definição	Definir Proposição; Definir fatores; Definir seção; Definir base de dados;

Iberoamerican Journal of Project Management
ISSN 2346-9161

2	Transformação	Gerar Normalização; Coletar Evidências (favorável e desfavorável);
3	Cálculos	Calcular Maximização; Calcular Minimização; Calcular evidência (Min resultante, Max resultante); Calcular Grau (Gce: Certeza, Gco: Contradição); Calcular variável Análise Global
4	Parâmetros	Parametrizar valores limites;
5	Processamento	Processamento do algoritmo Para-analisador;
6	Suporte a decisão	Auxílio na tomada de decisões;

Fonte - Autor

A seguir, será detalhada cada etapa atividade do Processo Unificado de Lógica Paraconsistente Anotada Evidencial Eτ (PULPA).

1. Definição: listar as informações necessárias para auxiliar à tomada de decisões. Definir Proposição: Definir proposição apropriada para propor assistência na decisão.
Seção Define: Identifique as seções de cada fator que permitem dar condições aos fatores (sucesso ou fracasso) que ajudarão na tomada de decisão.
Definir banco de dados: Coleta de dados: colete dados e organize-os de acordo com as seções que atendem aos fatores.

2. Transformação: Deve-se traduzir dados que sirvam como entradas para o processamento da Lógica Paraconsistente Anotada Evidencial Eτ.
Normaliza Dados: Normaliza dados organizados (por seções) para representar as entradas na lógica paraconsistente. Técnicas utilizadas tais como, Linear no intervalo [0 e 1], valor máximo dos elementos, padrão Z-Score.
Defina Evidência Favorável Ef (μ): dados coletados refletindo opiniões de especialistas (por seções). Esses dados, depois de normalizados, representam as entradas Ef (μ) para o processamento da Lógica Paraconsistente Anotada Evidencial Eτ.
Definir Evidências Desfavoráveis Ed (λ): dados coletados que refletem opiniões de especialistas (por seções). Estes dados, depois de normalizados, representam as entradas Ed (λ) para o processamento da Lógica Paraconsistente Anotada Evidencial Eτ.

3. Cálculo: Calcular Maximização MaxEf (μ): Em cada dado (por seções) coletados como evidência favorável Ef (μ), use o maior valor entre eles (por seções) para representar a maximização da evidência favorável Ef (μ).
Calcular MinEd Minimização (λ): Em cada dado (por seções) coletados como evidência desfavorável Ed (λ), use o menor valor entre eles (por seções) para representar a minimização da evidência desfavorável Ed (λ).
Calcular Evidência ResultingMinEf (μ): O resultante deve ser usado, quando os dados são agrupados por especialistas e precisam cruzar entre suas entidades (Camera X Radar). Em cada

Iberoamerican Journal of Project Management
ISSN 2346-9161

dado (por seções) coletado como evidência favorável Ef (μ), use o menor valor (por seções) entre camera e radar para representar o resultado de minimizar evidência favorável Ef (μ) exemplo 1: o menor valor entre evidências favoráveis Ef (μ) camera e evidência favorável Ef (μ) radares.
Calcular Resultante EvidenceMaxEd (λ): O resultante deve ser usado quando os dados são agrupados por especialistas e precisam cruzar entre suas entidades (camera X radar). Em cada dado (por seções) coletadas como evidência desfavorável Ed (λ), use o maior valor (por seções) entre camera e radar para representar o resultado da maximização da evidência desfavorável Ed (λ). Exemplo 1: maior valor entre evidência desfavorável Ed (λ) camera e evidência desfavorável Ed (λ) radares.
Calcular o grau de certeza (Gce): Com base nas evidências (por seções) coletadas, deve ser possível calcular o grau de certeza, pois consegue-se fazer a diferença entre a evidência favorável Ef (μ) e a evidência desfavorável Ed (λ) o grau de certeza (Gce). Exemplo 1: GCe = Ef (μ) - Ed (λ).
Calcular o Grau de Contradição (Gco): Com base nas evidências (por seções) coletadas, deve ser possível calcular o grau de contradição, pois consegue-se fazer a soma entre a evidência favorável Ef (μ) e a evidência desfavorável Ed (λ), usando o resultado da soma na extração de uma unidade (1) e assim obter o Grau de Contradição (Gco). Exemplo 1: GCe = (Ef [μ] + Ed [λ]) -1.
Calcular Global Certainty Analysis (BGce): Com base nos graus (por seções) de certeza calculados, deveser possível calcular a Análise Global como a média aritmética dos graus de certeza e, assim, resultar na Análise Global do Grau de Certeza (BGce). Exemplo 1: BGCe = ΣGce / Gce Quantidade.
Análise Global de Grau de Contradição (BGco): Com base nos graus (por seções) da contradição calculada, deve ser possível calcular a Análise Global como a média aritmética dos graus de contradição e assim resultar na Análise Global do Grau de Contradição (BGco). Exemplo 1: BGCo = ΣGco / Quantidade de Gco.

4. Parametrização: são os limites que limitam as regiões para análise (valores altos o suficiente para serem considerados) independentemente dos princípios lógicos.
Limite de parametrização TLV (True limit value): São condições parametrizadas pelo engenheiro do conhecimento com o objetivo de obter respostas aceitáveis como verdadeiras, nas condições em que o valor do grau for menor, maior ou igual ao valor do parâmetro.
Limite de parametrização FLV (False limit value): Estes parâmetros são parametrizados pelo engenheiro de conhecimento para obter respostas aceitáveis como falsas, nas condições em que o valor do grau for menor, maior ou igual ao valor do parâmetro.
Limite de parametrização PLV (Valor limite Paracompleto): Estes parâmetros são parametrizados pelo engenheiro de conhecimento com o objetivo de obter respostas aceitáveis como paracompleto total, nas condições em que o valor do grau for menor, maior ou igual ao valor do parâmetro.
Limite parametrizado ILV (Valor limite inconsistente): São condições parametrizadas pelo engenheiro do conhecimento com o objetivo de obter respostas aceitáveis como inconsistentes, nas condições em que o valor do grau for menor, maior ou igual ao valor do parâmetro.

Iberoamerican Journal of Project Management
ISSN 2346-9161

5. Processamento: Neste processo, o objetivo deve ser executar o algoritmo do Analisador de Parâmetros para obter os parâmetros de acordo com a entrada dos dados.

6. Tomada de Decisão: Neste processo, o objetivo deve ser analisar o grau de contradição, que pode ter valor para cima e para baixo. Na existência de um alto grau de contradição (Gco), indica que não há certeza para auxiliar a tomada de decisão e, portanto, pode ser preciso buscar novas evidências. A existência de um baixo grau de contradição (Gco), juntamente com um alto grau de certeza (Gce), indica a possibilidade de uma análise conclusiva sobre a proposição.

2. Métodos e materiais.

O item a ser detalhado nessa seção e nas seções posteriores é a Segurança cibernética do veículo que visa a proteção do sistema de controle do automóvel e da informação dos passageiros de acesso não autorizado.

Existem diversos modelos de segurança para sistema de IoT na literatura. Um dos modelos de Segurança para IoT, apresentado em (17), verifica as camadas e as funções de segurança necessárias em cada camada. A primeira utiliza uma estrutura tridimensional em formato piramidal, no qual processos, pessoas, tecnologia e organização são vértices e trata-se de uma abordagem cognitiva e sistêmica. As interações entre os nós são dinâmicas e complexas, gerando tensões em um sistema 3D, que compõe um requisito de segurança

Nesta visão, ilustrada na Figura 3, existem quatro nós, representando processos, pessoas, sistema tecnológico e objetos inteligentes. A inclusão de objetos inteligentes resulta em um aumento da complexidade do sistema, dado que a interação desses objetos e das pessoas são de difícil previsão por causa do crescente número de objetos por pessoa e da presença ubíqua dos objetos. Adicionalmente, existem quatro planos, representados pelos planos de Acesso, Segurança para Riscos Inesperados, Segurança para Riscos Inesperados ou contingência, Planos de Segurança e plano de cibersegurança.

Iberoamerican Journal of Project Management
ISSN 2346-9161

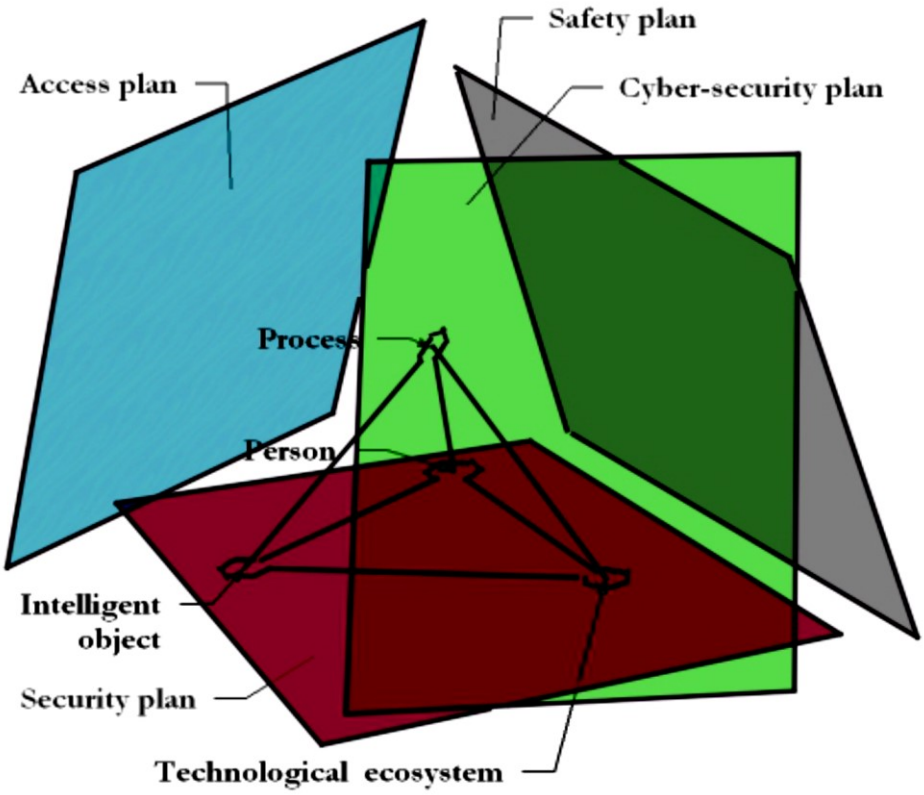

Figura 3 – Abordagem de segurança para IoT.

Fonte – (17)

As conexões entre os nós são complexas e dinâmicas em razão das alterações do ambiente. Essas conexões podem ser referidas como tensões por causa do conflito ou cooperação entre os nós para se obter um ambiente seguro.

Essas tensões entre os nós são chamadas de: identificação, confidencialidade, privacidade, responsabilidade, confiabilidade, segurança e imunidade própria. A identidade está relacionada à possibilidade de escolha do sensor ou adaptador que a pessoa deseja. A confiabilidade está relacionada ao correto funcionamento de um atuador frente a um comando da pessoa. Para evitar danos ao sistema, somente algumas pessoas autorizadas terão responsabilidade do sistema atribuídas. A privacidade deve ser garantida em todo o processo. Deve-se manter a segurança das pessoas e do equipamento enquanto ele estiver acionado. Por fim, o objeto inteligente deve possui imunidade contra-ataques físicos e lógicos de intrusos.

Em relação aos planos, o plano de segurança cibernética será descrito e este inclui o objeto inteligente, o processo, e as tecnologias conhecidas para o sistema. O objetivo é conseguir garantir as propriedades de segurança de um ambiente IoT contra riscos de segurança, Por exemplo, teste de

Iberoamerican Journal of Project Management
ISSN 2346-9161

operações e tecnologias necessárias para implementar os procedimentos de segurança durante a interação com objetos são uma tarefa muito crítica. A confiabilidade de um equipamento de comunicação significa que deve ser garantida as técnicas de gerenciamento da confiança entre os objetos deve ser implementada e estados de responsabilidade devem ser atribuídos e a autoimunidade do objeto inteligente. A Figura 4 ilustra o plano da segurança cibernética, mostrando os nós e as tensões entre esses nós.

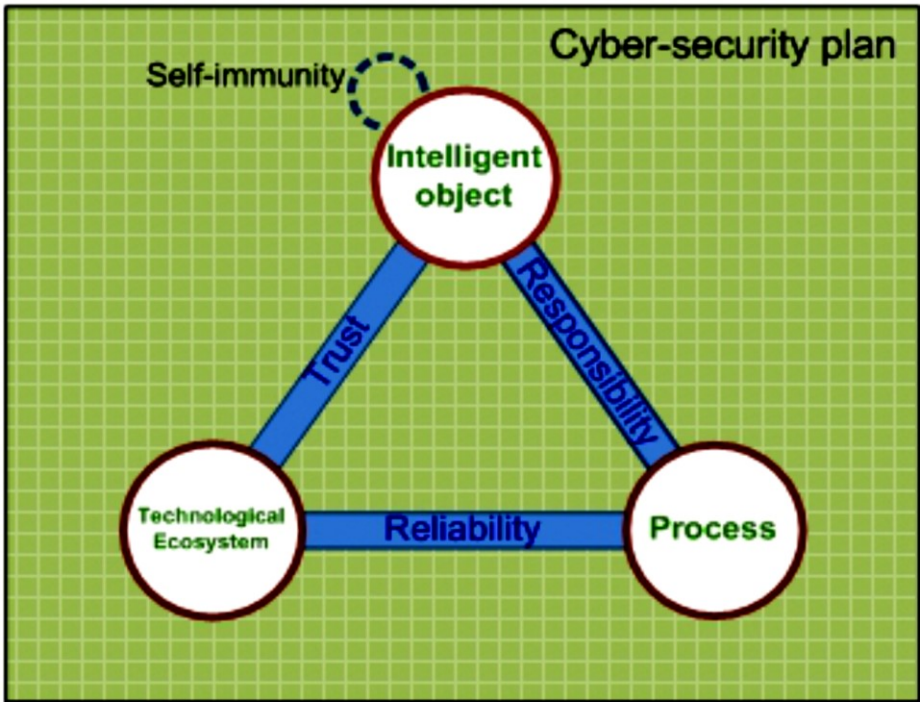

Figura 4 – Abordagem de Segurança para IoT – Plano Segurança cibernética

Fonte – (17)

As comunicações com os VAs devem ser seguras para prevenir ataques maliciosos que no caso de veículos autômatos podem ser fatais uma vez que não há um controle ou chance de intervenção de um motorista, que pode estar aproveitando o entretenimento do carro. Quando o software de carro autônomo está ligado à nuvem, os dados correm o risco de violações de segurança e podem se tornar propensos a hackers.

Segundo a NHTSA (6), a segurança cibernética protege a operação do sistema autônomo e de outros sistemas críticos de veículos contra interferência maliciosa e suporta a alta confiança do cliente na operação e na utilização do veículo.

Os especialistas em segurança cibernética desse órgão estão integrados ao restante da equipe de desenvolvimento de veículos autônomos para criar segurança cibernética em no processo de

Iberoamerican Journal of Project Management
ISSN 2346-9161

engenharia de segurança de sistemas dos fabricantes americanos. Essa equipe analisa e aborda a segurança cibernética em todos os sistemas de controle veicular, bem como em qualquer serviço autônomo de veículo conectado (como OnStar), aplicativos móveis e aplicativos veiculares criados para a experiência de dirigir sozinho. A equipe de desenvolvimento usa práticas integradas de engenharia de segurança de sistemas e uma estratégia de "segurança por projeto" para atender aos requisitos de segurança para todo o ecossistema de veículos autônomos.

Assim como em outras áreas do veículo, o uso completo de ferramentas de análise e avaliação, como varreduras de software e modelos de ameaças, aciona recursos de design que respondem aos riscos da segurança cibernética. Esses recursos, baseados em uma abordagem de "defesa em profundidade", incluem uma variedade de controles de mitigação, como registro de dispositivos, autenticação de mensagens, programação e diagnósticos seguros e intrusão, detecção e prevenção. Durante a implementação e validação, usamos ferramentas adicionais, como testes de penetração, para verificar se a implementação atende aos nossos objetivos de eliminar e minimizar os riscos. Além disso, nosso processo ativo de gerenciamento de frota permitirá que os técnicos de manutenção monitorem regularmente anormalidades relacionadas à segurança. Se necessário durante a implantação, nós ter recursos robustos de resposta a incidentes para monitorar e tratar potenciais novos riscos cibernéticos.

Tanto hardware como software de VA serão extensivamente testados, assim como são realizados testes com sistemas de aviação. Entretanto, certamente serão necessárias atualizações de sistemas de forma análoga à necessária no celular, no computador pessoal. Tal fato cria um desafio de confiabilidade do sistema, como as atualizações de software pode precisar de compatibilidade com modelos de carro e sistemas de sensores anteriores.

Adicionalmente, com o incremento do número de modelos oferecidos, software e suas atualização devem ter um desempenho crescente em diversas plataformas, tornando confiabilidade e garantia assegurada para todos objetivos ainda mais desafiadores.

3. Resultados e discussões

Para assegurar que o sistema seja seguro, é fundamental a criação de um ambiente computacional que envolva computadores, sensores, RFID tags, protocolos e equipamentos de rede e aplicações.

A atualização de software evidencia uma preocupação limítrofe com VA: a segurança do sistema. Carros que estão a conectar uns aos outros, ou à Internet são crescentemente expostos a um ataque cibernético. O veículo está conectado a uma variedade de produtos, e o ponto de entrada do veículo é a Internet, portas USB ou telefone celulares.

Até mesmo veículos autônomos desconectados à Internet podem estar sob risco. Atualizações de softwares comumente vão requisitar conexão à Internet, que cria a possibilidade de ataque por vírus de computador que corrompem o sistema, por exemplo, um vírus pode entrar no sistema ao se mascarar por uma legítima atualização. Evitar isso requer conexões extremamente seguras para atualizar servidores e um número de mecanismos de *handshake* para garantir que a fonte de atualizações - e as atualizações em si - sejam legítimas e não corrompidas.

Iberoamerican Journal of Project Management
ISSN 2346-9161

Atores mal-intencionados e descontrolados podem ser capazes de comandar um único veículo (ou uma frota de veículos) para cometer crimes, ou mesmo atos de terrorismo.

A segurança de software não é a única preocupação. Vândalos ou criminosos podem usar bloqueadores de GPS ou enviar outros sinais de interferência para atrapalhar os sensores VA ou transmitir leituras falsas do sensor aos sensores de um veículo; por exemplo, o envio de uma falsa Lidar retorna a um veículo que está usando o mapeamento tridimensional para navegar pelo ambiente. Embora isso possa ser mais difícil de ser alcançado, ele também pode ser mais difícil de ser detectado, pois as leituras falsificadas do sensor podem parecer legítimas.

Os proprietários de veículos também apresentam possíveis ameaças à segurança. Muitos entusiastas da tecnologia buscam acesso a seus próprios sistemas para obter controle sobre elementos que são bloqueados pelo fabricante. Os termos "quebra de cadeia" e "enraizamento" se referem ao ato de violar a segurança embutida para telefones celulares, a qual é muitas vezes realizada através de adulteração física, para fornecer o proprietário com maior acesso e flexibilidade; por exemplo, mover o telefone de uma operadora para outra.

Os VAs certamente serão uma tentação tão grande quanto a "quebra de prisão", já que os usuários procuram melhorar o desempenho ou executar seu próprio software, quase certamente, enquanto arriscam a segurança. Isso exigirá que os fabricantes garantam que os usuários não possam invadir os sistemas de hardware e software do veículo. Também pode exigir que os estados realizem inspeções anuais da integridade do sistema do veículo.

Os problemas de segurança ainda não são bem compreendidos, à medida que os veículos se tornassem mais informatizados e mais conectados, eles fornecessem outro aspecto da infraestrutura crítica e um alvo em potencial para um ataque cibernético.

A responsabilidade está fortemente relacionada aos direitos de acesso ou aos privilégios de autorização. Por exemplo, se um objeto IoT está configurado por uma entidade, ele deve ser capaz de lidar com conexões de outros objetos e distinguir diferentes direitos de acesso. Então, isto garante autorizações de acordo com os direitos de acesso aos equipamentos.

Em relação à autoimunidade, os nós pode ser usados em áreas distantes e/ou hostis. Eles se tornaram desprotegidos a ataques físicos e às restrições do site, como falta de confiabilidade de links de comunicação sem fio disponíveis, limitações de recursos, proteção física insuficiente dos nós, ausência de um robusto sistema de gestão de confiança. Os riscos potenciais podem estar relacionados à privacidade (inventariação ou varredura rastreamento / rastreamento para trás / para frente) ou para segurança ataque, falsificação de tag ou clonagem, ataque de retransmissão, negação de serviço, engenharia reversa de tags. Os sistemas de VA devem ser projetados para resistir a possíveis invasões de hackers, citando um exemplo em que hackers conseguiram acessar os sistemas eletrônicos de um carro por meio de um sistema aparentemente inócuo para monitorar a pressão dos pneus. As medidas de segurança precisam se aplicar a todos os caminhos de comunicação no carro, seja Wi-Fi, comunicações celulares ou DSRC. Assim, os mecanismos de defesa devem ser abordados. Um exemplo é o uso de sistemas de detecção de intrusão (IDS) / Sistemas de Prevenção de Intrusão (IPS). A operação padrão em um IDS é a comparação entre o comportamento atual do sistema com o seu comportamento na ausência de intrusões.

Iberoamerican Journal of Project Management
ISSN 2346-9161

Como qualquer tecnologia, os VAs terão falhas e violações. O recurso mais importante será a capacidade do sistema de detectar falhas e violações e agir com segurança - mudando para um sistema de segurança simples e rigidamente controlado ou se recusando a se envolver. A Tabela 4 ilustra o nível atual de desenvolvimento dos serviços básicos de segurança nos veículos autônomos, com bases nas pesquisas, testes, riscos apontados e necessidade de melhorias.

Tabela 4 – Nível de desenvolvimento e serviços de segurança

Serviços de Segurança	Nível de Desenvolvimento
Autenticidade	
Confidencialidade	
Disponibilidade	
Integridade	
Irretratabilidade	

Fonte: Autoria Própia.

4. Conclusões

Existem diversas questões referentes à segurança da informação que ainda não foram endereçadas como a interação quando existirem uma frota de veículo autônomos de diferentes fabricantes com diversas versões de hardware e software, a forma de a proteção dos dados do usuário.

A utilização de diferentes objetos com padrões de comunicação diversos gera uma maior complexidade nas questões de segurança, pois a compatibilização da comunicação ou demandará processamentos adicionais ou, ainda pior, poderá deixar informações desprotegidas.

Adicionalmente, deve se verificar se os requisitos de segurança estão sendo cumpridos para os produtos a serem lançados. Deve-se tomar cuidado no desenvolvimento da aplicação para não permitir potenciais ameaças, já que a programação para uma rede IoT terá requisitos diferentes das redes de computadores utilizadas anteriormente.

Iberoamerican Journal of Project Management
ISSN 2346-9161

O sistema de um veículo autônomo é bastante complexo e exige que tanto hardware como software de VA sejam extensivamente testados, da mesma forma como são realizados testes com sistemas de aviação. Entretanto, mesmo que forem realizados milhares de testes, as situações reais podem diferir de todos os testes realizados e o sistema automatizado irá precisar de um bom sistema de apoio à decisão. Existem métodos que pode auxiliar na tomada de decisão como a Lógica Paraconsistente Anotada (LPA) e com isso, tem-se a possibilidade de mitigar inúmeras falhas que causam acidentes e põe em risco vidas humanas.

Um ponto que ainda não endereçado é como será realizada a colaboração para compartilhamento dos dados de sensores dos veículos. Estão previstas novas aplicação utilizam informações de muitos sensores de maneira colaborativa.

Iberoamerican Journal of Project Management
ISSN 2346-9161

5. Referencias bibliográficas.

(1) CASAGRAS EU FP7 Project. 2009. "CASAGRAS Final Report: RFID and the Inclusive Model for the Internet of Things", 2009, pp. 10-12.

(2) ITU. 2005. "ITU Internet Reports 2005: The Internet of Things – Executive Summary", International Telecommunation Union (ITU), Genebra, Suiça, 2005.

(3) RAJ, Pethuru, RAMAN, Anupama. 2017. Internet of things (IoT) : technologies, applications, challenges, and solutions. CRC Press, 2017, Boca Raton, EUA.

(4) DUSTDAR, Schahram, NASTIC, Stefan, SCEKIC, Ognjen. 2017. Smart Cities: The Internet of Things, People and Systems. Springer, Suíça.

(5) BRUMMELEN, Jessica Van. O'BRIEN, Marie. GRUYER, Dominique. NAJJARAN, Homayoun. 2018. "Autonomous vehicle perception: The technology of today and tomorrow". Transport Research Part C 89 (2018) 384-406.

(6) NHTSA. 2017. Automated driving system 2.0: A vision for safety, EUA, Setembro/2017. Disponível em www.nhtsa.gov. Acessado em 20/08/2018.

(7) NHTSA, Preliminary Statement of Policy Concerning Automated Vehicles, National Highway Traffic Safety Administration, 2013. Disponível em www.nhtsa.gov. Acessado em 20/04/2018.

(8) GENERAL MOTORS. 2018 Self-Driving Safety Report. EUA. 2018.

(9) RAZZAQ, Mirza Abdur.QURESHI, Muhammad Ali. GIL, Sajid Habib. ULLAH, Saleem. 2017. "Security Issues in the Internet of Things (IoT): A Comprehensive Study". *IJACSA-International Journal of Advanced Computer Science and Applications*. Vol. 8. No. 6, 2017.

(10) KIM, D. ; SOLOMON, M. G. 2014. Fundamentos de Segurança de sistemas de informação, ISBN 978-85-216-2507-0, 1 ed, Rio de Janeiro: Editora LTC, 2014.

(11) ABE, Jair M.; AKAMA, S.; NAKAMATSU, K., 2015. Paraconsistent Intelligent-Based Systems - New Trends in the Applications of Paraconsistency. 1. ed. Switzerland: Springer International Publishing, v. 1, 2015. ISBN DOI: 10.1007/978-3-319-17912-4.

(12) ABE, Jair M. 2010. Paraconsistent logics and applications. In: 4th International Workshop on Soft Computing Applications., IEEE, 2010, p. pp. 11–18.

(13) ABE, Jair M. 2004. Paraconsistent Artificial Neural Networks: An Introduction. In: NEGOITA, M.; HOWLETT, R.; JAIN, L. Knowledge-Based Intelligent Information and Engineering, 23206-3 DOI: 10.1007/978-3-540-30133-2_124. Disponivel em:<http://dx.doi.org/10.1007/978-3-540-30133-2_124>.

(14) JOANNI, Acanda, IRANIA, Izquierdo, JAVIER, ARZA, YOBANY, Piñero Pedro, ALEJANDRO, Lugo José, "*Modelo de Evaluación de programas basado en indicadores y*

Iberoamerican Journal of Project Management
ISSN 2346-9161

Lógica Borrosa", Iberoamerican Journal of Project Managemet (IJoPM), ISSN 2346-9161. Vol. 6, Nº 2, A.I. pp. 43-63. 2015.

(15) GARCÍA, José Alejandro Lugo, LÓPEZ, Surayne Torres, PÉREZ, Pedro Piñero, VICTORE, Roberto Delgado, "*Control de la ejecución de proyectos basado en indicadores y lóguca borrosa". "*, Iberoamerican Journal of Project Managemet (IJoPM), ISSN 2346-9161. Vol. 4, Nº 1, A.I. pp. 15-35. 2013.

(16) LIMA, Alessandro. W. B.; LIMA, Luiz.; ABE, Jair M.; GONÇALVES, Rodrigo F.; ALVES, Davis.; NAKAMATSU, kazumi. 2018. "Paraconsistent Annotated Logic Artificial Intelligence Study in Support of Manager Decision-Making", *2018 2nd International Conference on Business and Information Management (ICBIM 2018)-Session 1: Information Technology and Information Management,* Barcelona, Spain, 2018, ISBN:978-1-4503-6545-1, ISSN:2010-023X, DOI:10.18178/IJTEF, ISSN:2301-3567, DOI:10.18178/JOEBM.

(17) RIAHI, A.; NATALIZIO, E.; CHALLAL, Y.; MITTON, N.; IERA, A. 2014. "A systemic and cognitive approach for IoT security", *2014 International Conference on Computing, Networling and Communications*, Honolulu, EUA, 2014, pp. 183-186.

6. Correspondência

Michel Bernardo Fernandes da Silva
Laboratório de Comunicações e Sinais (LCS), Escola Politécnica – USP, Av. Prof. Luciano Gualberto, tr. 3, 158, Cidade Universitária, São Paulo, SP, Brasil,
mbfsilva@lcs.poli.usp.br; michel.silva@docente.unip.br .

Silvio Ernesto Barbin
In memoriam (2018)

Jair M. Abe
Programa de Pós-Graduação em Engenharia de Produção-Métodos Quantitativos, Univerisdade Paulista – UNIP, Rua Dr. Bacelar, 1212 - Vila Clementino - São Paulo – SP, CEP 04026-002, Brasil, jairabe@uol.com.br

Luiz A. de Lima
Programa de Pós-Graduação em Engenharia de Produção-Métodos Quantitativos, Univerisdade Paulista – UNIP, Rua Dr. Bacelar, 1212 - Vila Clementino - São Paulo – SP, CEP 04026-002, Brasil, luizlima@unip.br