Um Sistema Ciber-Físico para Operações de Segurança de Infra-Estruturas Críticas

Adriano A. Bossonaro, João L. C. de Moraes, Antonio F. do Prado, Wanderley L. de Souza e Regina B. de Araújo
Universidade Federal de São Carlos (UFSCar) - Rd. Washington Luís, km 235 – São Carlos – SP – Brasil

Resumo — **A Segurança de Infra-estruturas Críticas, como usinas hidrelétricas, usinas nucleares e estações de tratamento de água são cada vez mais importantes no atual cenário de instabilidade e violência crescente. Os Sistemas Ciber-Físicos podem apoiar a potencialização da doutrina militar de Garantia da Lei e da Ordem (GLO) para Operações de Segurança das Infra-estruturas Críticas. Neste artigo apresentamos um Sistema Ciber-Físico para a potencialização da doutrina militar atualmente utilizada nas Operações de Segurança de Infra-estruturas Críticas, adicionando métodos, técnicas e soluções de redes de sensores sem fio e de interfaces avançadas, para melhorar o nível de operacionalidade das equipes empregadas neste tipo de missão. Este trabalho contempla a unificação de outras pesquisas realizadas no Wireless Networking and Distributed Interactive Simulation Laboratory (WINDIS) da Universidade Federal de São Carlos (UFSCar), que tem como foco direcional o Projeto de Sistemas Integradores do Instituto Nacional de Ciência e Tecnologia em Sistemas Embarcados Críticos (INCT-SEC).**

Palavras-Chave — **Comando e Controle, Sistemas Ciber-Físicos, Segurança de Infra-estruturas Críticas.**

I. INTRODUÇÃO

Na atual conjuntura brasileira, os índices de violência atingiram níveis absolutamente intoleráveis, tornando o problema da Segurança Pública uma urgente prioridade nacional. Para a Garantia da Lei e da Ordem (GLO), as forças policiais e militares podem desenvolver uma variedade de operações, executadas individualmente ou em combinação.

Dentre estas operações, está a Operação de Segurança de Infra-estruturas Críticas, também conhecida no Exército Brasileiro como Posto de Segurança Estático (PSE). Uma infra-estrutura crítica, ou ponto sensível, pode ser definida como uma edificação ou estrutura física que, se for sabotada, danificada, paralisada ou destruída, comprometerá a sobrevivência da população local, regional ou nacional.

Infra-estruturas Críticas (IC), tais como as usinas hidrelétricas, usinas nucleares e estações de tratamento de água, são essenciais para a nossa sociedade e, portanto, devem estar disponíveis 24 horas por dia nos 365 dias do ano. Infelizmente, falhas acidentais e/ou ataques intencionais em uma IC podem resultar na interrupção de seus serviços. Essas falhas podem ser causadas por más condições atmosféricas, catástrofes naturais ou por ataques que podem variar de mero vandalismo a atividades terroristas [13].

O Exército Brasileiro, assim como as demais Forças, possui uma doutrina já definida para este tipo de operação. De uma maneira geral, subentende-se que todas as variantes destas doutrinas são baseadas em uma estrutura genérica que, a partir deste momento, será denominada “Doutrina de PSE”.

Este trabalho é parte do Projeto de Sistemas Integradores do Instituto Nacional de Ciência e Tecnologia em Sistemas Embarcados Críticos (INCT-SEC). A intenção deste artigo é integrar ideias e projetos de pesquisa realizados nos WINDIS para potencializar a Doutrina de PSE utilizando um Sistema Ciber-Físico que reúne métodos, técnicas e soluções de redes de sensores sem fio, interfaces avançadas e outras tecnologias da computação ubíqua para potencializar a operacionalidade das equipes empregadas em missões de segurança de infra-estruturas críticas, de forma que se possa estender suas possibilidades e aumentar a qualidade e a quantidade de informações disponíveis para o apoio a decisão.

Este artigo está organizado da seguinte forma: a Seção II apresenta alguns trabalhos relacionados, a Seção III descreve, sumariamente, a estrutura da Doutrina de PSE, a Seção IV apresenta conceitos sobre Sistemas Ciber-Físicos, a Seção V descreve as principais tecnologias concatenadas para a concepção do Sistema Ciber-Físico proposto, a Seção VI apresenta a arquitetura de suporte para integração das tecnologias utilizadas neste trabalho, a Seção VII apresenta a estrutura da Doutrina de PSE potencializada, a Seção VIII descreve um cenário de aplicação e, finalmente, a Seção IX apresenta uma conclusão.

II. TRABALHOS RELACIONADOS

Na Universidade da Virginia, John Stankovic pesquisa um sistema monitoramento militar chamado VigilNet, cujo foco principal é verificar informações sobre as capacidades do inimigo e as posições de alvos hostis. Essas missões frequentemente envolvem um alto grau de risco para os soldados empregados e, baseado nisso, verificou-se a necessidade de se implantar as redes de sensores sem fio nas missões de vigilância. Porém devido às restrições de energia dos nós sensores, os sistemas projetados para a vigilância militar exigem um projeto de energia consciente, que possam garantir a vida da rede durante toda a missão. O sistema VigilNet foi desenvolvido para ser uma rede auto-organizada. Seu projeto é baseado num regime de gerenciamento de energia capaz de obter tempo de vida mínimo de 3 a 6 meses para os nós sensores [23].

Na Universidade de Michigan, Jinzhu Chen pesquisa o aperfeiçoamento do uso de um Sistema Ciber-Físico na proteção de Infra-estruturas Críticas, propondo uma abordagem holística chamada Fidelity-Aware Utilization Control (FAUC) para Sistemas Ciber-Físicos de Vigilância Wireless, que combinam sistemas de sensores low-end com câmeras de vigilância ad-hoc em larga escala para ambientes não-planejados. Através da integração de fusão de dados com

controle de feedback, FAUC pode impor um limite de utilização da CPU para garantir a escalonabilidade do sistema em tempo real [5].

Na Universidade de Notre Dame, Michael Lemmon realiza pesquisas sob o enfoque de redes de sensores sem fio como o elo crítico de conexão entre a Internet com o mundo físico, dentro do contexto dos Sistemas Ciber-Físicos (SCF). Sua proximidade com o ambiente físico dinâmico exige que elas sejam autônomas e adaptativas. O autor propõe um novo modelo de programação de middleware chamado Agilla para facilitar aplicações autônomas e adaptativas em redes de sensores sem fio. A estrutura do Agilla é baseada em agentes móveis, que são processos de software capazes de se adaptar movendo-se entre os nós sensores ou até mesmo realizando sua própria clonagem nos mesmos para solucionar questões relativas à tolerância a falhas [12].

O Ministério da Defesa Brasileiro desenvolve, no nível estratégico, um Sistema Militar de Comando e Controle (SISMC^2) para coordenar as forças militares em operação, possibilitando o acompanhamento em tempo real das ações em curso. O SISMC^2 possui subsistemas que apóiam o processo de comando e controle e disponibilizam recursos que permitem o fluxo de dados confiável, dentro dos padrões militares, e o monitoramento das operações militares em sua esfera de atribuição [16]. A evolução e integração de outros recursos em tempo real para o aperfeiçoamento do sistema ainda depende de pesados investimentos, como por exemplo, a conclusão do Programa do Satélite Geoestacionário Brasileiro, ora em fase adiantada de especificação.

III. DOUTRINA ATUAL DE PSE PARA SEGURANÇA DE INFRA-ESTRUTURAS CRÍTICAS

O emprego das forças de policiais e militares nas operações de segurança de infra-estruturas críticas é orientado por procedimentos operacionais minuciosamente definidos e previamente ensaiados. As atividades protocolares podem ser organizadas em 05 (cinco) áreas distintas: controle de pessoal, inteligência, operações, logística e relações públicas.

Em uma operação de segurança de infra-estrutura crítica, as forças empregadas estão normalmente dispostas segundo 04 (quatro) grupos distintos: Grupo de Comando, Grupo de Sentinelas, Grupo de Patrulhas e Força de Reação [3].

O Grupo de Comando é formado pelo comandante da operação e seu Estado Maior. Esse grupo tem a função de tomar as decisões relativas ao controle e à segurança da infra-estrutura crítica com base na doutrina, nas regras de engajamento e nas informações que são reportadas pelas sentinelas, equipes de patrulhas e outras fontes confiáveis.

O Grupo de Sentinelas tem a função de ocupar postos de vigilância em pontos estratégicos para a defesa do perímetro da infra-estrutura crítica. Cada sentinela recebe um setor de observação e faz a vigilância durante todo o período em que estiver no posto sem, contudo, se afastarem sem autorização.

O Grupo de Patrulhas é responsável por realizar o patrulhamento do perímetro e das áreas internas da intra-estrutura. O patrulhamento normalmente é realizado em duplas e as ocorrências observadas neste procedimento são reportadas ao comando da operação.

A Força de Reação tem a finalidade de atuar prontamente em qualquer parte da infra-estrutura para repelir as tentativas de invasão ou apoiar de qualquer outra forma que o comando julgar conveniente [3].

O efetivo e a organização dos grupos são definidos pelo comando da operação, que considera fatores importantes como o terreno, equipamentos disponíveis, características da infra-estrutura crítica e outras informações que forem observadas no reconhecimento inicial da operação.

Para que se tenha uma ideia do teatro de operações baseado na doutrina padrão, segue um exemplo de organização básica para a segurança de intra-estruturas críticas. Na Fig. 1, pode ser observado o Grupo de Comando instalado em um local que facilite a transmissão e recebimento das ordens; a Força de Reação ocupando uma posição que facilite sua atuação para apoiar a defesa de qualquer parte do perímetro; os postos de vigilância ocupados por sentinelas, em pontos estratégicos para a defesa da infra-estrutura e as equipes de patrulha realizando o patrulhamento ostensivo no perímetro e nas áreas internas da edificação. Observa-se também o estabelecimento de uma entrada única, coma finalidade de aumentar o controle da entrada e saída de pessoas e viaturas na infra-estrutura crítica protegida.

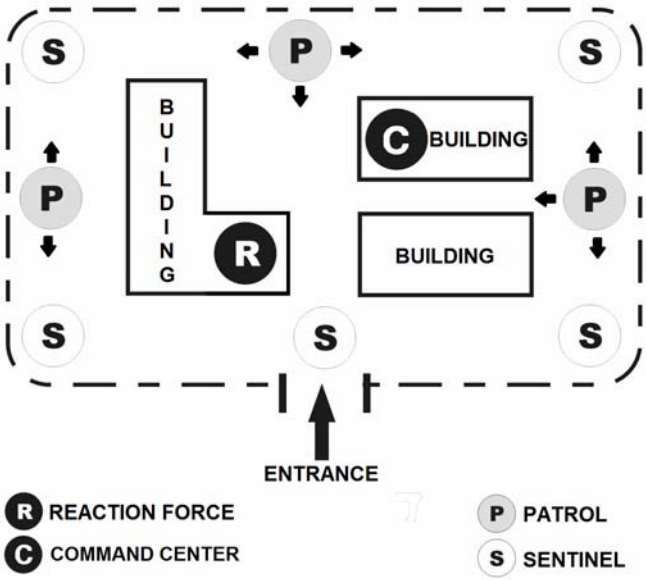

Fig. 1 – Organização Padrão para a Segurança de Infra-Estrutura [3]

Observando a Doutrina de PSE vigente, verificou-se a crescente e atual necessidade de pesquisas e soluções para aumentar a operacionalidade e a qualidade e quantidade de informações captadas e disponibilizadas para apoiar o processo decisório do comando da operação, frente aos diferentes problemas que ocorrerem durante a segurança de uma infra-estrutura crítica, principalmente em ambiente hostil. Um estímulo para o desenvolvimento desta pesquisa é que a atual Doutrina de PSE para operações para a segurança de infra-estruturas críticas se baseia fortemente na utilização de seus recursos humanos, colocando vidas em risco e causando grande fadiga física e mental nos integrantes das equipes empregadas para este fim, quando as atividades operacionais são realizadas por um grande período de tempo.

Outro fator a ser considerado é que a doutrina atual possui um enfoque baseado na segurança do perímetro real, menosprezando as ocorrências externas, que poderiam ser captadas e analisadas para facilitar a previsão de possíveis ações, permitindo um reajuste da disposição tática da tropa em tempo hábil para minimizar os riscos e custos.

Fundamentado pelas motivações acima citadas, foram analisadas algumas tecnologias cuja integração poderia ser utilizada para o desenvolvimento de um Sistema Ciber-Físico de suporte às Operações de Segurança de Infra-estruturas Criticas visando estender a operacionalidade neste tipo de missão, diminuindo as limitações atuais. As próximas Seções apresentam ideias sobre Sistemas Ciber-Físicos e posteriormente as tecnologias que foram combinadas para a potencialização da Doutrina de PSE, objetivo deste trabalho.

IV. SISTEMAS CIBER-FÍSICOS

Observando a sequência cronológica da Revolução Computacional, observamos que as décadas de 60 e 70 caracterizaram a Era dos Mainframes, que eram computadores com a finalidade de executar grandes aplicações de processamento de dados. Nas décadas de 80 e 90 caracterizou-se a Era dos Desktops onde os computadores pessoais estavam presentes em todas as residências para realizar atividades pessoais e profissionais. A década de 2000 foi caracterizada pelo surgimento da computação ubíqua, que se traduzia pelos numerosos dispositivos de computação em todo lugar e a todo tempo no ambiente humano, de forma transparente ao usuário.

A partir do ano de 2010, surge então a Era dos Sistemas Ciber-Físicos. Os avanços recentes nas áreas de comunicações e sistemas embarcados têm evidenciado este novo paradigma computacional [12].

Assim como a Internet transformou o modo como os humanos interagem e se comunicam uns com os outros, os Sistemas Ciber-Físicos estão transformando a maneira como os humanos interagem e controlam o mundo físico ao nosso redor. Os SCF são sistemas físicos e de engenharia, cujas operações são monitoradas, coordenadas, controladas e integradas por computação apoiada por um núcleo de comunicação, devendo atuar de forma confiável, segura, eficiente e em tempo real [17], conforme ilustra a Fig. 2.

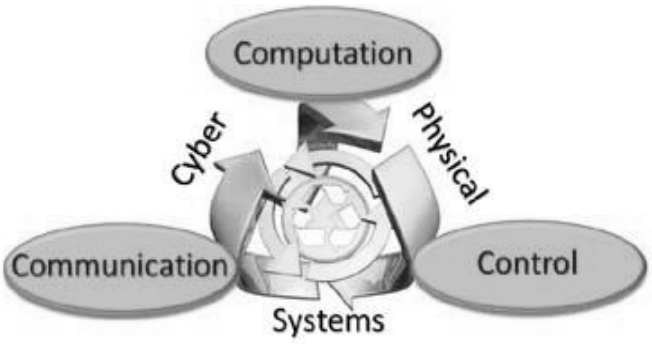

Fig. 2 – Composição holística um Sistema Ciber-Físico

O paradigma dos SCF é empurrado por várias tendências recentes: a proliferação de sensores de baixo custo, baixa potência, alta capacidade e tamanhos reduzidos; a revolução da comunicação wireless; a abundância da largura de banda na internet; a melhoria na capacidade de armazenamento de energia e uso de fontes alternativas de energia.

Exemplos de SCF incluem sistemas aeroespaciais, veículos de transporte inteligentes, sistemas de defesa, sistemas robóticos, controle de processos, controle de ambientes e segurança de infra-estruturas críticas [17].

A Proteção de Infra-estruturas Críticas (PIC) requer mecanismos de monitoramento que nos permitam detectar falhas e ataques no mais curto prazo. É possível que a infra-estrutura crítica possua uma extensão geográfica muito grande e necessite de mecanismos de monitoramento em uma escala bem maior. No contexto deste artigo, o Sistema Ciber-Físico em questão engloba diferentes tecnologias que combinadas, oferecem o suporte computacional necessário à potencialização de um sistema físico convencional de PIC. Estas tecnologias computacionais serão apresentadas na próxima seção.

V. TECNOLOGIAS COMBINADAS PARA SUPORTAR O SISTEMA CIBER-FÍSICO PROPOSTO

Segue a apresentação das principais tecnologias combinadas com a finalidade de fornecer suporte ao Sistema Ciber-Físico, objetivando a potencialização da atual Doutrina de PSE para operações de segurança de infra-estruturas críticas, proposta neste artigo.

A. Redes de Sensores sem Fio (RSSF)

No contexto da PIC, as RSSFs surgem naturalmente como uma solução em potencial. Particularmente, RSSFs pode ser facilmente implementadas em grande escala. Como sua estrutura é normalmente construída a partir de dispositivos de baixo custo, as RSSFs podem fornecer serviços de monitoramento com a relação custo-benefício favorecida, uma vez que estas não exigem nenhuma infra-estrutura computacional adicional. Além disso, a natureza distribuída de uma RSSF aumenta a capacidade de sobrevivência da rede em situações críticas, já que uma rede de sensores disposta em larga escala possui menor tendência a ser afetada em sua totalidade por falhas ou ataques intencionais. Em situações muito críticas, as RSSFs podem ainda fornecer informações suficientes sobre a IC que ajudem o operador de evitar outros danos e iniciar o processo de recuperação rapidamente [13].

As RSSFs consistem de um grande número de dispositivos sem fio, chamados de nós sensores, que são densamente distribuídos em uma região de interesse. Do ponto de vista da aplicação, as RSSF podem ser utilizadas em diversos cenários, incluindo monitoramento ambiental, rastreamento de eventos, coordenação de ações e também nos sistemas de segurança [4]. Sua utilização é bastante adequada em ambientes de difícil acesso, desde que a deposição dos sensores seja realizada de forma automatizada [3].

Os nós sensores são construídos com hardware de baixo custo que atualmente, devido aos avanços tecnológicos, são produzidos em escalas cada vez menores. Apesar deste progresso, as limitações computacionais convencionais de memória, processamento, comunicação e consumo de energia ainda estão presentes. O consumo de energia ainda pode ser

considerado a principal limitação. Para minimizar essa limitação, pesquisadores buscam desenvolver algoritmos que possam atender as aplicações observando a máxima economia de energia, resultando no aumento do tempo de vida da rede.

B. Veículo Aéreo Não Tripulado (VANT)

Veículos Aéreos Não Tripulados são equipamentos compostos de uma plataforma aérea com sensores embarcados, tais como: receptor GPS, câmera fotográfica, sistema de vídeo em tempo real, altímetro, velocímetro, sensor de temperatura, etc. Possuem também uma estação de controle em terra, composta de antenas de transmissão e recepção, terminais computacionais capacitados a visualizar e processar as informações recebidas. Essas plataformas podem ser visualizadas na Fig. 3, apresentada a seguir.

Fig. 3 – Plataformas Aérea e Terrestre do VANT

Seu emprego pode ser realizado por meio de condução manual, onde um operador tem o controle do equipamento, ou por meio de um voo planejado, onde o equipamento é programado para seguir uma rota determinada por waypoints.

O VANT possui sistemas de segurança automatizados que permitem seu retorno para base, caso ocorra qualquer problema. Isso evita que o equipamento se perca. No caso de uma queda, o VANT possui um pára-quedas que se abre automaticamente, preservando o recolhimento do aparelho e a segurança das populações afetadas [24].

No Instituto de Ciências Matemáticas e de Computação da USP, em São Carlos/SP, é desenvolvido, desde 1998, o Projeto ARARA (Aeronaves de Reconhecimento Assistidas por Rádio e Autônomas), cujo foco é dirigido para aplicações de monitoramento por meio da coleta de imagens de vídeo e de fotografias, que são posteriormente processadas para extração das informações de interesse [3].

C. Robôs Táticos para Ambientes Internos (RTAI)

Existem diversas definições sobre robôs. Segundo a Robotics Institute of Association (RIA), “um robô é um manipulador multifuncional e reprogramável projetado para movimentar materiais, ferramentas ou peças especiais, mediante movimentos programáveis e variáveis para a realização de uma variedade de tarefas”. A International Organization for Standardization (ISO) define o robô como "uma maquina manipuladora, com vários graus de liberdade, controlada automaticamente, reprogramável, multifuncional, que pode ter base fixa ou móvel para utilização em aplicações de automação industrial". Esta definição é utilizada pela Federação Internacional de Robótica, a European Robotics Research Network (EURON), e muitas outras comissões [20].

Um robô móvel é um dispositivo mecânico montado sobre uma base não fixa, que age sob o controle de um sistema computacional, equipado com sensores e atuadores que o permitem interagir com o ambiente. O modo como ele interage com o ambiente está intimamente ligado com a forma como seu sistema computacional foi desenvolvido para interpretar as variações neste ambiente. Esta interação pode ser caracterizada pela arquitetura utilizada para criação do sistema [2].

No contexto deste trabalho, os Robôs Táticos para Ambientes Internos, desenvolvidos no Laboratório de Robótica Móvel da USP [15] estão sendo integrados ao SCF proposto. Estes robôs realizam operações em ambientes fechados como prédios, instalações civis ou militares. Os RTAI podem ser usados de forma individual ou por meio da composição de esquadrões, capazes de atuar de modo colaborativo e coordenado em aplicações de segurança que envolvem tarefas de monitoramento, detecção de incidentes e resposta a incidentes. Os robôs são uma alternativa interessante nas missões mais críticas, onde as tarefas arriscadas podem ser realizadas por eles, sem colocar em perigo as vidas humanas, e cumprindo sua missão com um alto grau de confiabilidade frente as mais diversas situações.

D. Identificação por Radiofrequência (RFID)

A tecnologia de identificação por radiofrequência tem despertado interesse devido ao potencial apresentado para simplificar e tornar mais eficiente a identificação automática de objetos. Analisando os diversos sistemas que utilizam identificação por radiofrequência, pode se observar uma configuração básica, com adoção de três componentes principais, que são: etiquetas, leitores e um conjunto de software. Esta configuração pode sofrer variações decorrentes do tipo de etiqueta utilizada e os dados armazenados nas mesmas.

Considerando como chave a fonte de energia, podemos classificar as etiquetas eletrônicas em três tipos: (1) ativas, que têm fonte de energia própria e apresentam habilidade para iniciar suas comunicações; (2) semi-passivas, que também contém fonte de energia própria, mas apenas respondem as mensagens que chegam; (3) passivas, que se alimentam a partir do campo magnético criado pelo leitor e também apenas respondem as mensagens que chegam [27].

Apesar das promissoras aplicações da tecnologia de RFID, muitas dificuldades ainda impedem sua adoção em larga escala. As maiores dificuldades estão vinculadas à própria tecnologia em si, a padrões e a integração [3].

As dificuldades tecnológicas a serem superadas são

relacionadas à recepção de dados pela antena e a colisão causada pela transmissão simultânea de informação por diversas etiquetas. Os sistemas de RFID apresentam algumas falhas ou riscos relacionados à segurança dos dados, que são comuns às tecnologias de transmissão de dados sem fio. O uso de um conjunto de mecanismos de segurança que inclui protocolos e criptografia, é a solução adota nos sistemas de comunicação. Entretanto, a maioria das primitivas de segurança disponíveis, tem custo alto para ser implementada em um microchip de RFID [3].

O desenvolvimento de padrões internacionais para os sistemas de RFID garantiria a interoperabilidade entre etiquetas e leitores de diferentes fabricantes. Devido à intereporabilidade e a capacidade de troca entre os sistemas, a demanda por componentes e equipamentos de RFID poderia crescer, o que levaria a uma redução dos custos dos mesmos. Além do que, o uso de padrões internacionalmente aceitos, facilitaria a difusão desta tecnologia no mundo [15].

E. Interface Avançada de Comando e Controle (IACC)

A computação ubíqua tem, como uma de suas ideias centrais, a interação natural através das interfaces. Apesar da tela, teclado e mouse serem ferramentas úteis para suportar tarefas genéricas associadas ao computador, elas podem não ser ideais em muitas situações de uso, em que formas naturais de interação são desejadas.

As interfaces tangíveis buscam mudar o paradigma tradicional de entrada e saída de informações, criando novas possibilidades de interação que aproximam os mundos físico e digital. Na análise de interfaces tangíveis, é preciso ressaltar que existe um significado embutido na representação incorporada no dispositivo, o que o diferencia de dispositivos convencionais como um mouse, por exemplo. Este dispositivo não tem um significado próprio, ele não tem o propósito de representar algo. Ele é apenas uma ferramenta de entrada. As interfaces tangíveis, ao contrário, são ferramentas de interação que possuem um significado próprio, fortemente acoplado ao objetivo da atividade em questão [3].

As interfaces tangíveis representam novas possibilidades, algumas relativamente simples e baratas. O ponto não é a sofisticação da tecnologia, mas as formas inovadoras e bem adaptadas de interação.

O framework *open source* TUIO (*Tangible User Interface Objects*) define um protocolo e uma API para superfícies tangíveis. O protoloco permite descrever de forma abstrata interações feitas sobre uma superfície, incluindo toques e objetos tangíveis. É necessário, porém, que um tracker (geralmente uma aplicação baseada em visão computacional) receba os dados das interações e, por meio do protocolo TUIO, os envie para serem decodificados em aplicações clientes. Assim, a combinação do protocolo TUIO, tracker TUIO e implementação cliente baseada em TUIO permite a construção de uma superfície de controle que utilize os recursos de interfaces tangíveis e multitoques [9]. Uma superfície multitoques tangível foi construída em 2010 pelo WINDIS como parte do projeto do INCT-SEC do qual este trabalho também é parte integrante [3].

Combinando as ideias do protocolo padrão com as tecnologias baseadas em computação ubíqua e interfaces avançadas vistas nesta seção, verificou-se a necessidade de se definir uma arquitetura integradora, que será apresentada na próxima seção.

VI. ARQUITETURA DE SUPORTE DO SISTEMA CIBER-FÍSICO PROPOSTO

Sistemas Ciber-Físicos integram computação, comunicação capacidades de monitoramento e controle de entidades do mundo físico. Estes sistemas são geralmente compostos por um conjunto de agentes em rede, incluindo: sensores, atuadores, unidades de processamento de controle e dispositivos de comunicação, conforme ilustra a Fig.4.

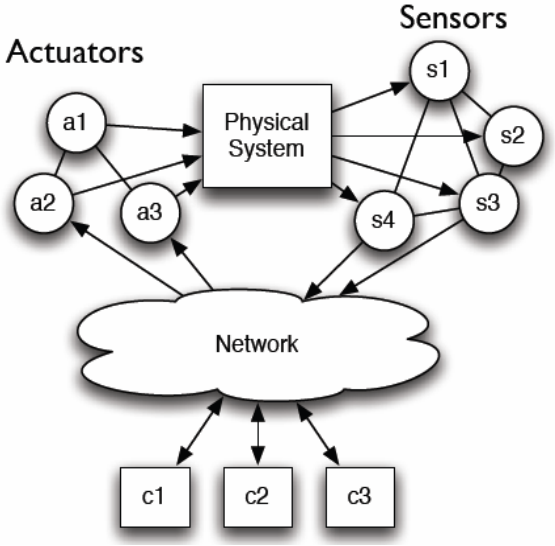

Fig. 4 – Estrutura Organizacional Genérica de um Sistema Ciber-Físico

No contexto dos SCF, alguns projetos em desenvolvimento no WINDIS envolvem a pesquisa de métodos, técnicas e soluções para o monitoramento de infra-estruturas críticas. A especificação e implementação de um middleware de serviços multi-camadas para RSSFs também é pesquisada como parte desse projeto maior [18]. O middleware especificado no WINDIS foi utilizado neste trabalho para suportar o desenvolvimento, manutenção, distribuição, e execução de aplicações de sensoriamento no cenário de operações militares de segurança de infra-estruturas críticas. A Fig. 5, apresentada a seguir, ilustra uma arquitetura que contextualiza a organização básica do trabalho proposto, integrando as diversas fontes de informações, caracterizadas pelos sensores fixos, VANTs e RTAIs ao sink, por meio deste middleware que foi abstraído em dois níveis: zero e um [3].

O nível 1 refere-se ao middleware de serviços que provê os serviços em nós mais robustos, como o sink. Este nível fornece suporte a um mecanismo de interpretação de contexto que realiza uma interpretação complexa que integra lógica fuzzy e ontologias para apoio à tomada de decisões do comando da operação. O middleware de nível 1 foi definido para prover serviços independentes de plataformas, sistema operacional ou da linguagem de programação das aplicações. O nível 0 do middleware provê mecanismos de subscrições e publicações de dados no interior da RSSF. Neste nível, uma interpretação simples (fusão/agregação de dados) é realizada

na camada de rede da pilha de protocolos de RSSFs. A variante baseada em conteúdo do publish/subscribe é utilizada para abstrair toda a complexidade de comunicação distribuída na RSSF fornecendo um modelo de comunicação flexível e assíncrono para as aplicações [1].

A aplicação compreende requisitos como o monitoramento em tempo real de todos os eventos da infra-estrutura crítica, gerenciamento de emergências e a disponibilização de recursos de apoio a decisão, dentro outros [3].

Para facilitar o gerenciamento, a aplicação disponibiliza 06 (seis) camadas de visualização: Camada de Topografia, Camada de Controle de Pessoal, Camada de Inteligência, Camada de Operações, Camada de Logística e Camada de Configuração.

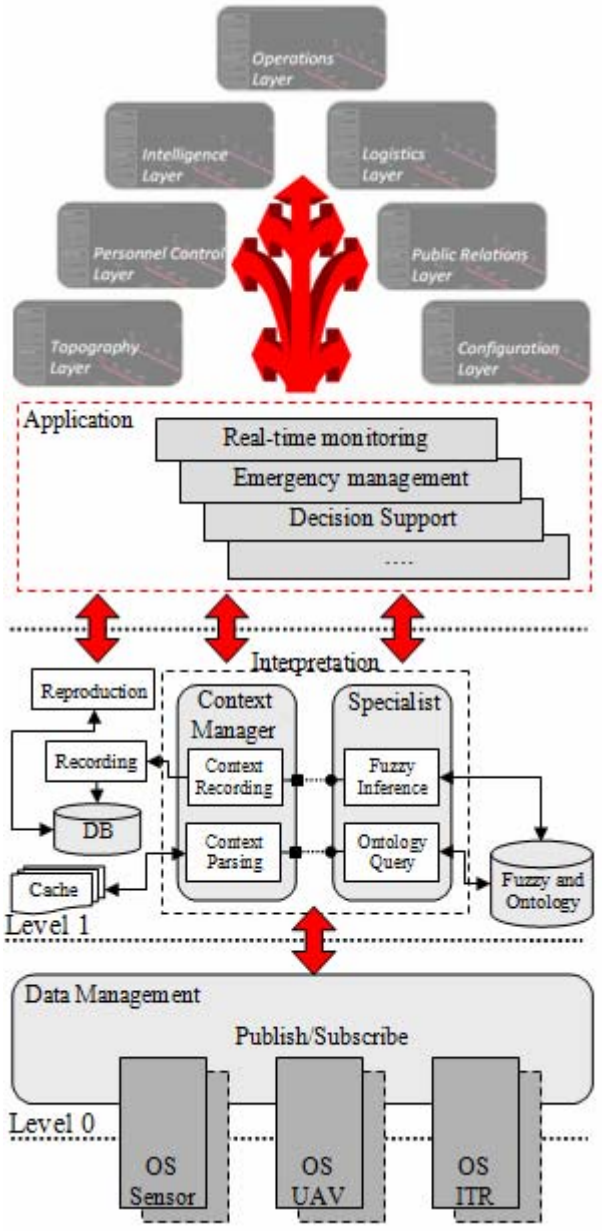

Fig. 5 – Arquitetura do Sistema Ciber-Físico proposto [3]

A *Camada de Topografia* exibe o mapeamento topográfico da região a ser preservada e a diagramação dos relacionamentos entre salas, espaços e outros aspectos físicos da estrutura, considerando inclusive, a escala das medidas das paredes, portas, janelas, o nome de cada ambiente e seu respectivo nível. Esta é a camada base sobre a qual todas as outras camadas serão sobrepostas.

A *Camada de Controle do Pessoal* exibe as informações quantitativas sobre o pessoal envolvido na operação. São representados os integrantes dos grupos de sentinelas, patrulha, força de reação, comando e também os funcionários presentes na área de segurança. Recursos de Realidade Aumentada permitem a verificação de informações adicionais sobre cada pessoa dentro da instalação.

A *Camada de Inteligência* mostra as informações relativas às ocorrências internas e externas ao perímetro de segurança. São representadas informações como tentativas de invasão, imagens do ambiente externo, produzidas pelo VANT, e demais informações de interesse que possam apoiar o processo decisório do comando da operação. Informações sobre o controle interno também são disponibilizadas. O afastamento de uma sentinela de seu posto de vigilância ou o não cumprimento do itinerário previsto por uma equipe de patrulha são monitorados continuamente e permitem a intervenção do comando em tempo real.

A *Camada de Operações* mostra a estrutura operacional montada para realizar a segurança da edificação. São mostradas as posições dos postos de vigilância, do centro de comando, da força de reação e do comandante e seus assessores quando eles estão fora do centro de comando. Informações sobre o posicionamento dos sensores no perímetro de segurança e itinerários dos robôs táticos e das equipes de patrulhamento também são mostradas nesta camada.

A *Camada de Logística* proporciona a visualização da localização das viaturas, helicópteros, armamento, munição, combustível, gêneros alimentícios, medicamentos e demais equipamentos de apoio à operação.

A *Camada de Configuração* exibe informações técnicas sobre os recursos computacionais agregados, considerando o posicionamento da rede de sensores, dos computadores de borda, sink, robôs táticos e VANT.

A seção VII, apresentada a seguir, descreve implementação do SCF para a potencialização da Doutrina de PSE.

VII. IMPLEMENTAÇÃO DE UM SISTEMA CIBER-FÍSICO PARA A SEGURANÇA DE IC

Baseado nas tecnologias apresentadas acima pesquisou-se um SCF capaz de potencializar a Doutrina de PSE para operações de segurança de infra-estruturas críticas, estendendo a capacidade de processar informações confiáveis e possibilitando em melhores condições o apoio a decisão e a economia dos recursos humanos empregados. São propostas a utilização de RSSF para monitorar todo o perímetro de segurança, principalmente nos pontos onde não havia postos de vigilância com sentinelas.

Antenas de RFID podem ser instaladas nos postos de vigilância para monitorar a permanência da sentinela em seu local correto. Este recurso também pode ser utilizado para monitorar as equipes de patrulhamento, que são identificadas ao passar pelos postos de vigilância, cumprindo o itinerário previsto, ou até mesmo para gerenciamento logístico de equipamentos, armamentos e munições sobressalentes. Etiquetas RFID passivas podem ser utilizadas nestes casos

por que elas possuem um raio de ação de aproximadamente 07 (sete) metros, ideal para este tipo de monitoramento [3].

Os VANTs podem ser utilizados para realizar o monitoramento das ocorrências externas ao perímetro, que podem ser captadas e analisadas para facilitar a previsão de possíveis ações, permitindo um reajuste da disposição tática da tropa em tempo hábil, minimizando os riscos e custos. Prioritariamente, a operação dos VANTs podem ser baseadas no vôo planejado, onde o comando determina a rota a ser seguida por meio de *waypoints*. Dada a sua capacidade de captar imagens no espectro infravermelho distante, focada em imagens termais, os VANTs também podem apoiar a segurança noturna, detectando, em sua rota externa ao perímetro, a presença de pessoas e objetos que permitam o sensoriamento térmico, ou seja, emitam calor. Neste sentido, os VANTs também podem ser empregados para auxiliar na identificação das características do invasor do perímetro, quando os sensores de presença foram acionados.

Todos os sensores podem ser conectados com um sink, caracterizado por uma superfície de comando e controle, baseada em interface tangível, que atua como um nó sorvedouro da rede, com a finalidade de permitir a visualização integrada e em tempo real das ocorrências, para apoiar o processo decisório do comando da operação. Essas ocorrências poderão ser dispostas segundo as visões de topografia, controle de pessoal, inteligência, operações, logística, relações públicas e configuração, que serão disponibilizadas em camadas e que podem ser sobrepostas ou escondidas conforme a necessidade da visualização. A estrutura potencializada pode ser vista em um esboço ilustrativo, mostrado na Fig. 6, que será apresentada a seguir.

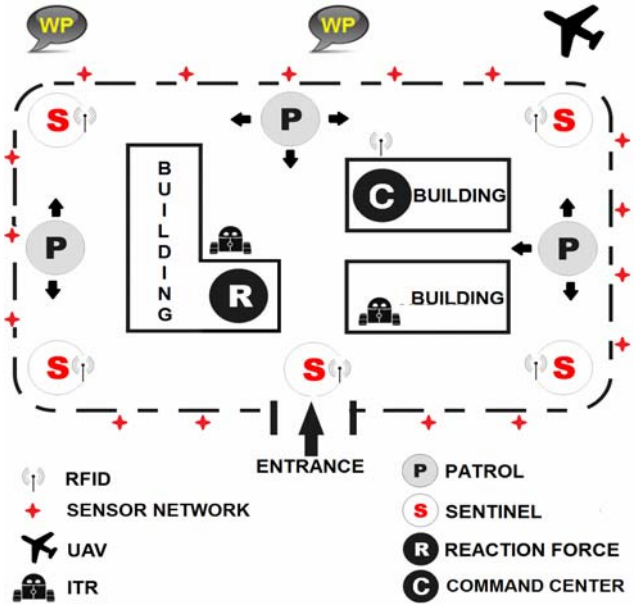

Fig. 6 – Estrutura Potencializada para a Segurança de Infra-Estrutura [3]

Para melhor visualização do SCF proposto, foi realizado um cenário de aplicação será sumariamente descrito na próxima seção.

VIII. CENÁRIO DE APLICAÇÃO

Trata-se de uma operação de segurança de uma Usina Hidrelétrica de médio porte, que oferece, além dos serviços convencionais de geração de energia, a eclusagem de embarcações entre os níveis alto e baixo da via fluvial. A tropa considerada nesta operação é uma força militar de valor batalhão, com 02 (duas) companhias de fuzileiros, caracterizando as peças de manobra, e demais elementos de apoio de fogo e apoio logístico.

Para que se tenha ideia do funcionamento do ambiente computacional empregado, evidenciou-se o cenário de uma aproximação não autorizada, caracterizada pela invasão do perímetro de segurança em um local monitorado pela RSSF. Ao detectar a presença do indivíduo, os sensores interagem entre si e enviam a informação para a interface avançada de comando e controle, que exibe o alerta na Camada de Inteligência, identificando a localização do sensor que detectou o problema, conforme ilustra a Fig. 7, apresentada a seguir.

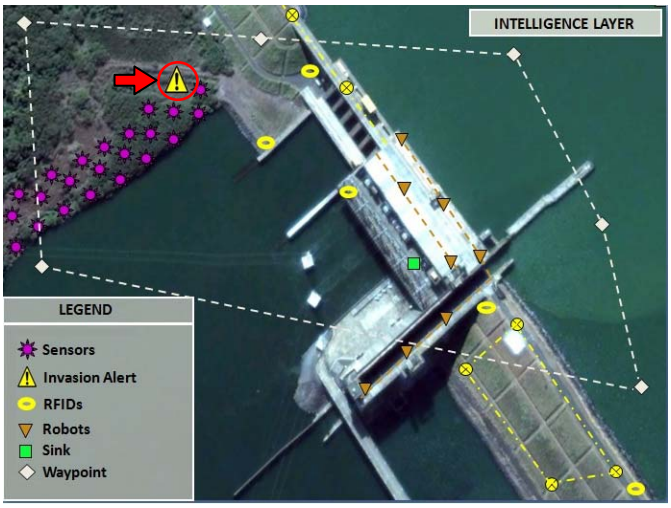

Fig. 7 – Detecção de uma Invasão (Camada de Inteligência) [3]

A representação do evento “invasão” na Camada de Inteligência disponibiliza informações confiáveis em tempo real, facilitando o processo decisório do Comandante e seu Estado Maior. Dessa forma, pode-se ajustar o dispositivo tático da tropa, determinar que sejam realizados reconhecimentos usando VANTs ou integrantes do Grupo de Patrulha e demais intervenções que permitam a correção da anormalidade evidenciada na IACC. A Fig. 8 ilustra o trabalho do grupo de comando apoiado pela interface avançada de comando e controle.

Fig. 8 – Interface Avançada de Comando e Controle (IACC) [3].

A seção seguinte apresenta uma conclusão sobre este artigo, onde serão evidenciadas também, algumas vantagens e desvantagens observadas na idealização de um Sistema Ciber-Físico para a potencialização da Doutrina de PSE na Segurança de Infra-estruturas Críticas ou Pontos Sensíveis.

IX. CONCLUSÃO

Este artigo apresentou um Sistema Ciber-Físico para a potencialização da Doutrina de PSE utilizada nas operações de segurança de infra-estruturas críticas, adicionando métodos, técnicas e soluções de redes de sensores sem fio, interfaces avançadas e outras tecnologias da computação ubíqua para melhorar a operacionalidade das equipes empregadas neste tipo de missão. Este trabalho contempla a unificação de outras pesquisas realizadas no WINDIS da UFSCar, que tem como foco direcional o Projeto de Sistemas Integradores do INCT-SEC.

As vantagens proporcionadas pela utilização de um Sistema Ciber-Físico na proteção de IC se caracterizam pela economia dos recursos humanos na segurança do perímetro, pelo aumento na quantidade e qualidade das informações disponíveis em tempo real para o apoio a decisão e pela maior facilidade e confiabilidade no armazenamento de informações sobre a operação. A utilização das tecnologias computacionais propostas proporcionam também, maior controle dos militares em operação, por meio da utilização de RFID, permitindo o rastreamento das equipes de patrulha e das sentinelas, bem como a localização dos militares com funções importantes como o comandante da operação e Estado Maior.

Como desvantagens, observaram-se um maior custo em relação ao sistema convencional e a necessidade de treinamento de uma equipe técnica para realizar a implantação e operação dos recursos computacionais adicionados. Outro aspecto que deve ser ressaltado é a necessidade de monitoramento constante do funcionamento dos recursos computacionais agregados, já que a segurança fica comprometida no caso de falhas técnicas.

Uma maneira de maximizar a eficiência do Sistema Ciber-Físico proposto é fazer com que esta solução seja amplamente reutilizável, de forma que a tropa seja tecnicamente apta a realizar a implantação e operação dos recursos computacionais agregados nos diferentes teatros de operações relativos à segurança de infra-estruturas críticas dentro do território nacional.

REFERÊNCIAS

[1] Beder, D. and Araújo, R.B. Towards “The Definition of a Context-Aware Exception Handling Mechanism”. Workshop On Exception Handling in Contemporary Software Systems. Co-Located With The Fifth Latin-American Symposium On Dependable Computing (LADC). April 25th - São José Dos Campos, São Paulo, Brazil. 2011.

[2] Beket, G. A. “Autonomous Robots: From Biological Inspiration to Implementation and Control”. Cambridge, USA: The MIT Press, 2005.

[3] Bossonaro, A. A. ; Vilela, Mateus A. ; Moraes, J. L. C. ; Prado, A. F. ; Araujo, Regina B. . An Integrated System to Support Critical Infrastructure Security. In: 1ª Brazilian Conference on Critical Embedded Systems, São Carlos. EPUSP, 2011. v. 1. p. 73-78.

[4] Bulusu, Nirupama and Jha, Sanjay. “Wireless Sensor Networks - A system perspective”. Artech House, London, England, 2005.

[5] Chen, J.a , Tan, R.a , Xing, G. “Fidelity-aware utilization control for Cyber-Physical Surveillance Systems”. Proceedings 31st Real-Time Systems Symposium. California, USA. 2010.

[6] Connell, J. H. “A hybrid architecture applied to robot navigation”. IEEE International Conference on Robotics and Automation (ICRA). Nice, France, 1992.

[7] Conte, G. and Doherty, P. An integrated UAV navigation system based on aerial image matching, IEEE Aerospace Conference, Big Sky, MT, USA, 2008.

[8] Gracias, N. "Mosaic-based Visual Navigation for AUV". PhD thesis, Instituto Superior Técnico, Lisbon, Portugal, 2008.

[9] Kaltenbrunner, M., Bovermann, T., Bencina, R., Costanza, E. “TUIO - A Protocol for Table Based Tangible User Interfaces”. Proceedings of the 6th International Workshop on Gesture in Human-Computer Interaction and Simulation, Vannes, France, 2005.

[10] Kelly, J., Saripalli, S. and Sukhatme, G. S. "Combined visual and inertial navigation for an UAV". 6th International Conference Field and Service Robotics (FSR’07), Chamonix, France, 2007.

[11] Kim, Sukun and Pakzad, Shamim and Culler, David E. and Demmel, James and Fenves, Gregory and Glaser, Steve and Turon, Martin. “Health monitoring of civil infrastructures using wireless sensor networks”. In Proceedings of IPSN, Cambridge, MA, USA, 2007.

[12] Lemmon, M.a , Poellabauer, C.b , Zhang, L.c , Zhou, X.d. “Introduction to the special issue on self-adaptive and self-organizing wireless networking systems”. ACM Transactions on Autonomous and Adaptive Systems. New York, USA. 2009.

[13] Levente Buttyan, Dennis Gessner, Alban Hessler, Peter Langendoerfer. Application of Wireless Sensor Networks in Critical Infrastructure Protection: Challenges and Design Options. IEEE Wireless Communications. 2010.

[14] Pessin, G. ; Hata, A. Y. ; Osório, F. S. ; Wolf, D. F, "Intelligent Control and Evolutionary Strategies Applied to Multirobotic Systems". IEEE International Conference on Industrial Technology - ICIT, p. 1427-1432, 2010.

[15] Prado, Neli R. S. Almeida; Pereira, Néocles Alves; Politano, Paulo Rogério. “Dificuldades para a adoção de RFID nas operações de uma cadeia de suprimentos”. XXVI ENEGEP, Fortaleza, CE, Brasil, 2006.

[16] Program for the Development and Implementation of the Command and Control Military System - PDI-SISMC2 (MD31-M-06), 3ª Ed/2008. Classified Document (in Portuguese).

[17] Rajkumar, Ragunathan (Raj) and Lee, Insup and Sha, Lui and Stankovic, John. Cyber-physical systems: the next computing revolution. Proceedings of the 47th Design Automation Conference. naheim, CA, USA. 2010.

[18] Ribeiro, J. Eduardo. "Middleware Services for Multi-Layered Wireless Sensor Networks". Master thesis. Federal Universit of São Carlos. São Carlos/SP, Brazil, 2010.

[19] Ribeiro, C., Costa, A., Romero, R. “Robôs móveis inteligentes: Princípios e técnicas”. Anais do XXI Congresso da Sociedade Brasileira de Computação – SBC. 2001.

[20] Romano, Vitor Ferreira. “Robótica Industrial”. São Paulo: Edgard Blucher, 2002.

[21] Santin, R., Kirner, C., Garbin, T. R., Dainese, C. A. “Ações interativas em Ambientes de Realidade Aumentada com ARToolKit”. Proceedings of the VII Symposium on Virtual Reality, SP, Brasil, 2004.

[22] Silva, Cosme R. M. et all. "Satélite Geoestacionário Brasileiro: Proposta de Modelo Operacional". Revista da Universidade da Força Aérea, volume 19, número 21, 2006.

[23] Stankovic, John A.; Abdelzaher, Tarek; et all. **"**Lightweight Detection and Classification for Wireless Sensor Networks in Realistic Environments". http://www.cs.virginia.edu/wsn/vigilnet/index.html, novembro, 2010.

[24] Trindade, O. Junior et all. "Sistema de Navegação e Controle de Missão do Projeto ARARA (Aeronaves de Reconhecimento Assistidas por Rádio e Autônomas)". In VI Workshop de Teses e Dissertações, São Carlos, SP, Brasil, 2001.

[25] Trindade, O. Junior ; Jorge, L. A. C. ; Aguiar, J. G. B. "Field of Dreams - Using UAVs for Precision Farming Unmanned Systems". Arlington, VA, USA, 2004, v.22, p. 35-39.

[26] Vlajic, N. and Stevanovic, D. "Sink mobility in wireless sensor networks: a (mis)match between theory and practice". Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing, 2009, pages 386–393.

[27] Welsh, Matt. "Lessons from the field derived from developing wireless sensor networks for monitoring active and hazardous volcanoes". In Communications of the ACM. vol. 53, n. 11, 2010.

[28] Weis, S. A. **"**Security and privacy in Radio-Frequency Identification Devices". Thesis (Master) – Department of Eletrical Engeneering and Computer Science, Massachesetts Institute of Technology, 2005.