Grupo de Estudo de Sistemas de Informação e Telecomunicação para Sistemas Elétricos-GTL

Desenvolvimento de uma rede inteligente de sensores para monitoramento estrutural de barragens baseado na tecnologia IoT

LUIZ CARLOS MAGRINI[1]; PAULA SUEMI DANTAS KAYANO[1]; FERDINANDO CRISPINO[1]; EDVALDO FABIO CARNEIRO[2]; TATIANA PERES ARARIPE[2]; ANTONIO LUIZ CARMO SANTOS[2]
FDTE[1] ;CESP[2]

RESUMO

A evolução da tecnologia IoT (Internet of Things) propicia a integração de plataformas heterogêneas de hardware e software encontradas no Smart Grid, principalmente quando apresentam pouca potência computacional e baixo consumo de energia.

Este artigo apresenta um sistema de monitoramento de segurança das estruturas de barragens de usinas hidroelétricas, baseado no protocolo aberto XMPP (eXtensible Messaging and Presence Protocol) para a comunicação entre os diferentes sensores, quase em tempo real, confiável e segura entre os IEDs (Intelligent Electronic Devices), bem como com o SCADA. Os dados trafegam encapsulados no formato XML, utilizando a padronização definida pelo grupo do IEEE Sensei-IoT.

PALAVRAS-CHAVE

IoT (Internet of Things), XMPP, Monitoramento de segurança das estruturas de barragens, Internet das Coisas.

1.0 - INTRODUÇÃO

Em usinas hidrelétricas o monitoramento das estruturas das barragens e eclusas é costumeiramente realizado durante as fases, construtiva e operativa. Nas fases construtiva, formação do reservatório e operativa são instalados instrumentos de auscultação, em sessões estabelecidas pela projetista nas estruturas, visando o monitoramento dos valores e efeitos dos esforços atuantes, tais como: deslocamentos, tombamentos, elevação, etc.

Esse monitoramento periódico possibilita a detecção de problemas no seu estágio inicial, situação onde a atuação e reparos são usualmente mais simples e menos oneroso. Possibilita ainda o monitoramento da estabilidade estrutural de elementos com muitos anos de operação e que apresentam sinais de deterioração.

Os instrumentos de auscultação civis apresentam diferentes funcionalidades, como por exemplo, os extensômetros de haste (strain gages) que avaliam a deformação da estrutura perante as variações das tensões mecânicas ocasionadas por variações climáticas e hidrológicas. Outro instrumento muito importante é o piezômetro que possibilita o mapeamento das subpressões encontradas no local da sua instalação.

O medidor de vazão é outro instrumento encontrado com frequência nas barragens, e fornece medições das vazões de água percolada através das estruturas e fundações das barragens de concreto e de terra.

(*) R. Capitão Otávio Machado, 525 - CEP 04718-000, São Paulo, SP, – Brasil
Tel: (+55 11) 2975-3527 – Email: lc.magrini@live.com

Adaptando-se transdutores aos diferentes tipos de instrumentos civis existentes nas barragens, torna-se possível a utilização de equipamentos microprocessados ou IEDs (Intelligent Electronic Device) que digitalizam as medidas coletadas e as disponibilizam numa rede de comunicação de dados, formando um sistema distribuído. Esse sistema distribuído é composto de uma grande quantidade de IEDs geograficamente espalhados ao longo da região compreendida pela barragem de terra e pela barragem de concreto, formando uma arquitetura distribuída heterogênea, fracamente acoplada (loosely coupled), e constituída por diversas camadas de software (multitier).

O aparecimento do conceito de Internet of Things (IoT) barateou e viabilizou a interoperabilidade entre sensores, IEDs e SCADAs (Supervisory Control and Data Acquisition) comercializados por diferentes fabricantes fugindo das tecnologias proprietárias de chão de fábrica que dificultavam e encareciam a conectividade entre produtos de fabricantes e tecnologias diferentes. A adoção de arquiteturas abertas baseadas na Web democratiza o acesso à informação por meio de ferramentas que já são do conhecimento da maioria dos usuários, possibilitando assim o acesso às informações por todos os níveis empresariais. As abordagens atuais para IoT se concentram principalmente em protocolos de comunicação para integrar equipamentos com padrões de protocolo de Internet, considerando recursos limitados de computação e memória, bem como disponibilidade de largura de banda e energia restritas.

Num projeto desenvolvido em pareceria com a CESP - Companhia Energética de São Paulo, foi colocado em em operação um protótipo em escala reduzida de um sistema de monitoramento de segurança de barragens, onde sensores e transdutores são adaptados aos instrumentos civis existentes e que no seu estágio final irá se constituir num sistema distribuído com mais de dois mil instrumentos civis de auscultação, cujas informações devem ser periodicamente coletadas, processadas, e salvas em uma base de dados histórica.

A utilização de equipamentos aderentes a tecnologia IoT, por meio de suas versões industriais, também denominadas de IIoT (Industrial Internet of Things) barateou o custo dos equipamentos de aquisição e processamento local de dados, além de proporcionar protocolos de comunicação de dados que aproveitam os investimentos anteriores graças ao compartilhamento da infraestrutura de rede TCP/IP, tanto em cabos (fibra óptica ou par trançado), como também da comunicação sem fio (WiFi) alimentados por conjuntos de painel solar/baterias em locais remotos.

Nessa arquitetura identificam-se módulos de software instalados nos IEDs que desempenham o papel de produtores e que são responsáveis pela produção dos dados, enquanto que o software SCADA terá processos que irão consumir essa informação, utilizando-a em cálculos, transformações, atualização de telas e armazenamento-a em sistemas gerenciadores de banco de dados.

O desenvolvimento de módulos de software que efetuam a comunicação de dados entre os IEDs com processos produtores, que adquirem os dados dos sensores e efetuam um pré-tratamento e os processos do SCADA que irão consumir esses dados, pode ser facilitado através do uso de middlewares que abstraem os detalhes de comunicação de dados tornados mais evidentes em plataformas heterogêneas, minimizando dessa forma o tempo desenvolvimento.

2.0 - MIDDLEWARE

Num sistema computacional distribuído, tal qual uma rede de sensores inteligentes, onde o processamento é dividido em unidades lógicas residentes em IEDs distribuídos, a execução harmoniosa dos vários módulos de software irá produzir a funcionalidade desejada. Para tanto, há uma grande necessidade de comunicação entre IEDs que podem apresentar processos produtores e consumidores, e que pode ser suprida por uma camada de software intermediária entre o sistema operacional e o programa aplicativo, que é denominada de Middleware.

Middlewares padronizados facilitam a interoperabilidade entre softwares de fabricantes distintos, além de facilitar o desenvolvimento de novas aplicações e simplificar a integração com sistemas de legados.

A maioria dos middlewares desenvolvidos recentemente para ICT (Information and Communications Technology) seguem arquitetura baseada em serviços computacionais segundo o modelo SOA (Service Oriented Architecture). Essa arquitetura propõe a integração de módulos de software com características distintas através da adoção de serviços computacionais baseados em Web (ou Web Services) que trocam informações e comandos embutidos em arquivos XML. Essa arquitetura já é referendada pela norma IEC 61898 e também endossada pelo NIST (U.S. National Institute of Standards and Technology) através da proposta do modelo de referência “NIST Framework and Roadmap for Smart Grid Interoperability Standards, bem como pelo meta-modelo denominado de Smart Grid Architecture Models (SGAM) criado numa parceria entre o CEN (European Committee for Standardization), CENELEC (European Committee for Electrotechnical Standardization) and ETSI (European Telecommunications Standards Institute).

As necessidades de comunicação em um Smart Grid são complexas, em virtude da heterogeneidade de equipamentos, softwares e funções neles encontrados. Cabe ao middleware prover uma camada de abstração permitindo que se foque na lógica da aplicação ao invés de cuidar das inúmeras exceções e problemas de compatibilidade encontrados. Os middlewares podem ser classificados em: Remote Procedure Call (RPC) oriented Middleware, Transaction-Oriented Middleware (TOM), Object-Oriented/Component middleware (OOCM)

e Message-Oriented Middleware (MOM).

O middleware RPC oferece recursos para invocação de procedimentos remotos, sem haver necessidade de se preocupar com os detalhes de comunicação. Originalmente foi desenvolvido para chamadas de procedimento síncronas, ou seja, o processo consumidor fica aguardando o retorno da chamada para prosseguir sua execução, fazendo com que a aplicação tenha dificuldade para ser escalável e que também tenha pouca tolerância à falhas.

Os middlewares tipo Transaction-Oriented (TOM), foram inicialmente concebidos para acesso à banco de dados e tem recursos para comunicação síncrona. ou assíncrona. em sistemas distribuídos heterogêneos.

Por outro lado, o Object-Oriented/Component middleware (OOCM) foi desenvolvido como uma extensão do RPC para o modelo de programação orientado à objetos.

Já os middlewares tipo MOM - Message-Oriented Middleware - proporcionam recursos para troca de mensagens (ou message passing) em sistemas distribuídos incorporando recursos para comunicação síncrona ou assíncrona, além de um formato comum de transporte de dados, tornando-o adequado a aplicações fracamente acopladas e que necessitam de tratamento diferenciado de acordo com o seu nível de prioridade. Esse tipo de ferramenta pode ainda oferecer recursos apenas para message passing, onde os processos envolvidos devem ser definidos explicitamente sem mascarar a identidade dos participantes. Essa categoria de middleware pode ainda possibilitar a utilização de aplicativos voltados ao enfileiramento e armazenamento das mensagens (message queues) que respondem pela a persistência das mensagens até a sua entrega. Além disso, a comunicação assíncrona ocorre por meio de nomes lógicos que são resolvidos pelo software gerenciador da fila de mensagens. As mensagens da fila podem ser resgatadas em qualquer ordem e somente quando necessárias.

Para sistemas distribuídos heterogêneos e que necessitem alta disponibilidade, baixo consumo de energia (quando alimentados por painel solar/bateria) e elevado desempenho, tais como aplicações de Smart Grid e IoT o middleware orientado a mensagens é o mais indicado, pois desacopla os nós da rede facilitando que equipamentos com arquiteturas diferentes de hardware e software troquem mensagens entre si. Possibilita a troca de mensagens síncronas e assíncronas, transformação de formato de dados para se adequar às necessidades de diferentes aplicações remotas rodando em IEDs heterogêneos, suporte a diferentes níveis de prioridade e processamento paralelo de mensagens.

Além da comunicação ponto a ponto, há em situações que se têm diversos aplicativos produtores. Nesse caso algumas implementações adicionam o mecanismo publish-subscribe que efetua a distribuição de mensagens entre muitos produtores para muitos consumidores.

Dentre os padrões desenvolvidos para IoT podemos destacar: Message Queuing Telemetry Transport (MQTT) protocol, Data Distribution Service (DDS), eXtensible Messaging and Presence Protocol (XMPP) e Advanced Message Queuing Protocol (AMQP).

Alguns protocolos como CoAP (Constrained Application Protocol), Message Queuing Telemetry Transport (MQTT) e o Web Application Messaging Protocol (WAMP) possuem problemas de interoperabilidade entre redes heterogêneas para implantações de IoT em grande escala. Já o protocolo XMPP pode ser utilizado para resolver o problema da interoperabilidade entre redes heterogêneas, tornando possível a comunicação com redes de sensores, através de uma simples troca de mensagens de texto, que pode ser feita de qualquer local e com qualquer aparelho que tenha acesso à Internet.

O grupo de trabalho IEEE P21451 vem trabalhando no sentido definir uma arquitetura unificada de comunicação para redes de sensores inteligentes e adotou o XMPP como sendo o padrão internacional para Web semântica e M2M(Machine to Machine)/IoT.

3.0 - O PROTOCOLO XMPP

O protocolo eXtensible Messaging and Presence Protocol (XMPP), ou Jabber como ficou originalmente conhecido, é um protocolo aberto, extensível, baseado no formato XML para troca de dados em sistemas de mensagens instantâneas. Foi desenvolvido originalmente por solicitação do IETF (Internet Engineering Task Force, uma comunidade internacional de técnicos, agências, fabricantes, fornecedores, e pesquisadores, preocupados com a evolução da arquitetura da Internet e seu perfeito funcionamento, e atualmente descrita pela RFC 3160).

Esse protocolo segue a arquitetura cliente-servidor, mas pode ser configurado para outros modelos de comunicação por mensagem, tais como publish/subscribe, presence and status updates, alerts, feature negotiation, service Discovery.

Para a autenticação em aplicações que utilizam o protocolo XMPP é utilizado o protocolo SASL (Simple Authentication and Security Layer), o qual é baseado na troca de dados, da aplicação cliente/servidor, a fim de autenticação do cliente no servidor e estabelecer um nível elevado de segurança na comunicação entre ambos. O protocolo XMPP, também, utiliza o protocolo TLS (Transport Layer Security), o qual trabalha em conjunto com o protocolo de transporte TCP, para o envio de mensagens. Sendo que, o protocolo TLS é o responsável pela comunicação segura de informações, proporcionando privacidade, autenticidade e integridade às mesmas.

Diversas implementações open source para o XMPP, encontram-se disponíveis, tornando-o extremante viável, bem como devido a fatores como:

- Segurança: qualquer servidor XMPP pode ser isolado da rede pública (correndo, por exemplo, numa intranet de uma empresa). O núcleo das especificações XMPP inclui mecanismos de segurança robustos fazendo uso de Simple Authentication Security Layer (SASL) e Transport Layer Security (TLS).
- Baixo custo: por se tratar de uma ferramenta Open Source;
- Descentralizado: a arquitetura da rede XMPP é semelhante à do e-mail, permitindo que qualquer um possa correr o seu próprio servidor XMPP, tornando assim possível que indivíduos ou organizações possam tomar o controle absoluto das suas comunicações.
- Extensível: usando as capacidades do XML, qualquer um pode construir funcionalidades por cima do núcleo de protocolos. Com o objetivo de manter a interoperabilidade, extensões comuns são publicadas nas XEP. No entanto tal publicação não é necessária e as empresas podem manter as suas próprias extensões se assim o desejarem.
- Flexível: as aplicações XMPP, além de IM (Instant Messaging), incluem serviços como gestão de redes, organização de conteúdos, ferramentas de colaboração, transferência de arquivos, jogos, monitorizarão remota de sistemas entre outras.
- Diversificado: Existe um grande número de empresas e projetos open-source que usam o XMPP para construir e implementar serviços e aplicações que utilizam comunicação em tempo-real.

4.0 - ARQUITETURA DO SISTEMA DE MONITORAMENTO DE BARRAGENS

O sistema de monitoramento dos instrumentos civis instalados na usina hidroelétrica da CESP de Porto Primavera faz uso do protocolo de comunicação XMPP para a troca de mensagens entre os IEDs e seus respectivos transdutores e o sistema SCADA. Para tanto foram desenvolvidas aplicações tanto para o lado do software produtor (IEDs), quanto do lado do consumidor (SCADA).

O software desenvolvido na linguagem Python para os IEDs processa uma versão simplificada de um cliente open-source, de forma a transferir as informações coletadas após convertê-las em unidades de engenharia. Em seguida formata os dados no formato XML padronizado pelo grupo IEEE Senseio-IoT, e os envia para o software XMPP instalado no servidor. Nesse caso foram utilizadas as extensões do protocolo XMPP para IoT, tais como o XEP-0323 (IoT Sensor Data), XEP- 0325 (IoT Control) que padronizam o conteúdo e as tags do arquivo XML produzido. Para deixar o sistema mais flexível, foi incorporado no cliente um driver de comunicação para o protocolo ModBus/TCP de forma a possibilitar a integração com sensores legados, já que as informações recebidas por esse driver também são formatadas segundo o XML padrão e disponibilizadas para o SCADA.

Nessa arquitetura, no lado do software SCADA foi utilizado um software Servidor XMP para controlar e autenticar quais clientes XMPP podem trocar mensagens. Um módulo de software foi desenvolvido e agregado a esse servidor para efetuar o parse das informações formadas em XML e inseri-las no banco de dados, após terem sido passadas por um pré-processamento que efetua a sua validação por meio de uma análise de razoabilidade.

Como servidor XMPP foi utilizado o aplicativo Openfire que é um software aberto, desenvolvido pela comunidade Open Source denominado Igniterealtime, composta por usuários finais, desenvolvedores e provedores de serviços de todo o mundo.

Esse servidor XMPP terá uma configuração diferenciada que pode ser descrita pela utilização dos seguintes componentes:

- Componente XMPP–IoT: Responsável pelo envio e recebimento das mensagens XML entre clientes XMPP;
- Componente para BD: Responsável pela gravação dos dados recebidos do formato XML no banco de dados.

Um cliente XMPP instalado no IED pode ser descrito pela utilização dos seguintes componentes:

- Componente XMPP–IoT: Responsável pela envio e recebimento das mensagens XML entre clientes XMPP;
- Componente Modbus/TCP: Responsável pela integração com sensores legados.

No IED um cliente XMPP é instalado como um serviço de forma a prover um maior controle de execução do programa, principalmente em caso de reinicialização do sistema. Nesse mesmo IED será instalado também um segundo serviço que irá verificar periodicamente se o cliente XMPP residente está sendo executado e em caso contrário irá tomar as providencias necessárias para ativar esse serviço.

4.1 Formato das Mensagens

As mensagens trocadas entre os dispositivos que coletam as leituras dos instrumentos civis de auscultação da barragem seguem o formato estabelecido pelo Sensei/IoT group que é o primeiro esforço conjunto entre ISO, IEC e IEEE, conhecido como ISO/IEC/IEEE 21451-1-4 — Smart transducer interface for sensors, actuators and devices, e é considerado como o primeiro padrão de Web Semantica 3.0 para sensores. Esse formato é definido

com o auxílio da linguagem XML, tornando-o autodescritivo e de fácil interpretação pelos demais membros da rede.

A norma ISO/IEC/IEEE 21451-1-4, adota para identificação dos IEDs um endereço de 64 bits denominado de UUID(Universal Unique IDentifier), definido segundo a norma ISO 29161 - Automatic Identification for the Internet of Things.

A comunicação entre os clientes da rede XMP segue o modelo request-response (pergunta e resposta), sendo que o payload da mensagem é definido pelo XEP-0323 - Internet of Things - Sensor Data. Esse padrão já define as tags utilizadas para descrever as grandezas medidas e suas unidades, mas nem todos os tipos medidas realizadas pelos instrumentos civis de auscultação puderam ser encontradas, obrigando a uma extensão ao padrão original.

Na implementação desenvolvida todos os clientes XMPP são identificados através de JIDs (Ae558n222PPR @sicesp.com/km428) de forma única e permitindo disponibilizar na rede a sua localização e quais recursos possuem (XEP-0030). Cada cliente XMPP é responsável por iniciar uma conexão TCP/IP persistente com o servidor XMPP a qual o cliente XMPP pertence, fazendo assim com que o servidor saiba quais sensores estão online.

A seguir é apresentada uma mensagem típica a uma interrogação de dados a um instrumento de medição de recalque magnético de identificação km0428:

<message to="cesp_1@pc-i7/7516br8pdq" from=" Ae558n222PPR @sicesp.com/km428" xml:lang="en">
<fields xmlns="urn:xmpp:iot:sensordata" seqnr="1" done="true">
<node nodeId="km428">
<timestamp value="2018-07-18T16:53:07">
<numeric unit="C" automaticReadout="true" name="Temperatura" value="20.10376" momentary="true" />
<numeric unit="mm" automaticReadout="true" name="Leit_Placa1" value="0.76000" momentary="true" />
<numeric unit="mm" automaticReadout="true" name="Leit_Placa2" value="1.00061" momentary="true" />
<numeric unit="mm" automaticReadout="true" name="Leit_Placa3" value="2.50038" momentary="true" />
</timestamp></node></fields></message>

Nesse IED são adquiridas quatro medidas, sendo que uma delas é uma temperatura enquanto que as demais indicam a posição relativa da placa metálica enterrada na barragem de terra da usina hidroelétrica. Assim o campo identificado por “numeric unit” define a unidade de medida e value corresponde ao seu valor no instante identificado pela tag “timestamp value”.

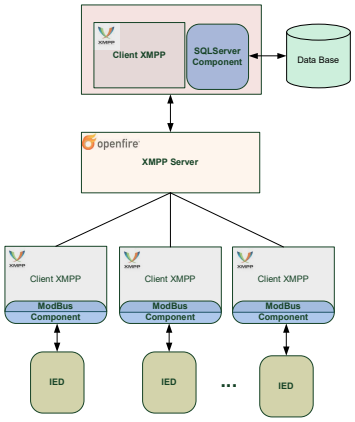
Nesta particular aplicação, cada IED poderá ter de um a seis portas de medidas, de modo que o payload (bits úteis da mensagem) não terá tamanho excessivo. Em aplicações onde o payload apresenta um tamanho que ocasione um impacto expressivo na rede de comunicação de dados, ele poderá ser comprimido através um formato de XML representado em binário, conforme definido no XEP -0322 - Efficient XML Interchange (EXI) Format.

4.2 Implementação e testes

A tecnologia XMPP utiliza arquitetura cliente-servidor descentralizada como utilizada na Word Wide Web e nas redes de emails. No desenvolvimento do sistema para as usinas da CESP foi usada uma arquitetura onde se identifica um servidor e diversos clientes. O servidor XMPP é responsável pelo gerenciamento, identificação dos clientes e do transporte dos dados. Todos os clientes XMPP podem solicitar e receber informações. Nesta implementação do sistema de monitoramento foi utilizada uma arquitetura onde apenas um cliente XMPP solicita as informações dos sensores para todos os demais clientes XMPP.

No diagrama da figura abaixo é apresentada a arquitetura do sistema de monitoramento.

Figura 1 - Arquitetura do sistema de monitoramento

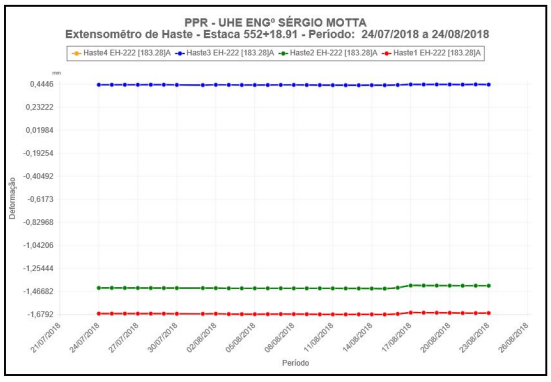


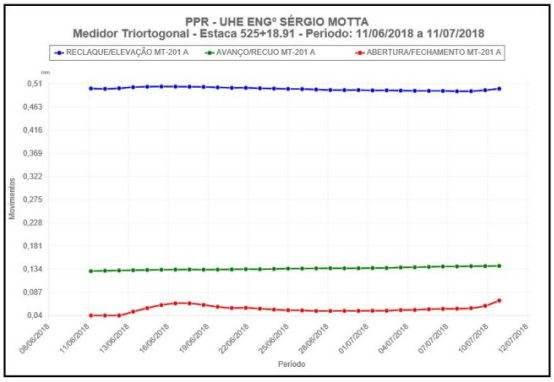
Os clientes XMPP conectados aos sensores podem coletar os dados dos sensores com diferentes protocolos de comunicação, sendo que para essa implementação foi utilizado o protocolo Modbus/TCP.

O cliente XMPP que solicita as informações aos demais Clientes XMPP, envia as informações para uma base de dados histórica. Para a base de dados pode ser utilizado diferentes sistemas gerenciadores de banco de dados (SGBD), bastando apenas utilizar o componente de conexão adequado para cada tipo de produto comercial. Nesta implementação foi utilizado o MS SQLServer.

Sensores LVDT (Linear Variable Differential Transformer) foram instalados nos instrumentos civis de auscultação, denominados Extensômetros de Haste e Medidores Triortogonais, em diferentes pontos da estrutura da barragem da usina, monitorando dessa forma o deslocamento estrutural da barragem. Esses sensores estão conectados a IEDs que se comunicam como clientes XMPP. Esses IEDs quando solicitados, efetuam a leitura dos valores de deslocamento produzidos pelos LVDT, convertendo os sinais elétricos em valores de engenharia e juntamente com dados de timestamp e unidade de medida os envia através do protocolo XMPP para o Cliente XMPP que solicitou a informação. O cliente XMPP que fez a solicitação dos dados, recebe e grava as informações recebidas no SGBD, integrado ao programa WEB de análise e gestão das informações de segurança da barragem da CESP, chamado SICESP.

A figura abaixo apresenta gráficos do sistema SICESP obtidos a partir dos dados do sistema de monitoramento para o instrumento EH e MT.





4.3 Trabalhos futuros:

Verificou-se ainda a possibilidade de implementações futuras de serviços como o de localização de sensores, a partir da extensão “XEP-0080 – User location” que permite o envio de mensagens contendo informações de localização dos sensores. Essa informação é bastante útil para o monitoramento de barragens onde os sensores se encontram espalhados entre diferentes níveis (cotas) da barragem. Além disso, outro serviço que poderia ser implementado é o de envio de comandos aos sensores. possibilitando realizar ajustes, configurações de escala e unidades, ou calibrações dos sensores, entre outros comandos.

5.0 - CONCLUSÃO

Foi apresentada a aplicação da aplicação do conceito de IoT num sistema de monitoramento da segurança da estrutura da barragem de uma usina hidroelétrica. Um piloto encontra-se instalado nas usina hidroelétricas

operadas pela CESP (Companhia Energética de São Paulo, Brazil) em Porto Primavera e Jaguarí, e faz uso do protocolo de comunicação XMPP para a troca de mensagens entre os IEDs e seus respectivos transdutores e o sistema SCADA.

Esse protocolo é um padrão internacional aberto, altamente escalável e extensível, podendo ser configurado para utilizar diferentes modelos de comunicação de dados, além de cliente/servidor. Possibilita também a interoperabilidade com protocolos legados, atende aos requisitos de segurança da informação, além de oferecer suporte à comunicação de tempo real. É apoiado pelo grupo de trabalho denominado Sensei/IoT, formado pelo ISO, IEC e IEEE por meio do grupo de trabalho XMPPI - XMPP Interface Working Group, formado pela IEEE Instrumentation and Measurement Society.

6.0 - RECONHECIMENTO

Este trabalho foi financiado pela CESP (Companhia Energética de São Paulo, Brasil), no âmbito do programa de P&D da ANEEL (Agência Nacional de Energia Elétrica).

7.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) M. Albano, L. L. Ferreira, L. M. Pinho, and A. R. Alkhawaja, “Message-oriented middleware for smart grids,” *Comput. Stand. Interfaces*, vol. 38, pp. 133–143, 2015.

(2) NIST Framework and Roadmap for Smart Grid Interoperability, Interoperability Standards, Release 3.0 (2014), Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, U.S. Department of Commerce. Online: https:// www.nist.gov/sites/default/files/documents/smartgrid/Draft-NIST-SG-Framework-3.pdf.

(3) Smart Grid Reference Architecture (SGAM), CEN/Cenelec/ETSI Smart Grid Coordination Group Std., Nov. 2012

(4) J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet Things J., vol. 4662, no. c, pp. 1–17, 2017.

(5) P. Saint-Andre, K. Smith, and R. Troncon, “XMPP - The Definitive Guide: Building Real-Time Applications with Jabber Technologies,” 2009.

(6) P. Waher, “XEP-0323: Internet of Things - Sensor Data,” 2013. [Online]. Available: https://xmpp.org/extensions/xep-0323.html.

8.0 - DADOS BIOGRÁFICOS

Luiz Carlos Magrini nasceu em São Paulo, Brasil, em 1954. Graduou-se pela Escola Politécnica da Universidade de São Paulo em 1977 (Engenharia Elétrica), onde também obteve os títulos de mestre e doutor na área de automação de sistemas elétricos. Trabalhou por 17 anos na Empresa Themag Engenharia Ltda nas áreas de planejamento de sistemas, automação de sistemas elétricos e automação industrial. Atualmente, é professor titular da UNIP e também atua como pesquisador e coordenador projetos pela FDTE - Fundação para o Desenvolvimento Tecnológico da Engenharia, nas áreas de Smart Grid e IoT, em pesquisas que envolvem supervisão e monitoramento de usinas, subestações e LTs, bem como em projetos envolvendo processamento de imagens, inteligência artificial, mineração de dados, e sensoriamento remoto.

Paula Suemi Dantas Kayano, graduou-se pela Escola Politécnica da Universidade de São Paulo em 1995. Obteve o título de Mestre em 1998 na mesma instituição. Trabalhou em projetos de monitoramento de navios na Marinha do Brasil e atuou em diversos projetos de automação e monitoramento de equipamentos na área de sistemas elétricos.

Ferdinando Crispino, graduado em Engenharia Elétrica pela Escola Politécnica da Universidade de São Paulo – (1999) e Mestre pela mesma instituição (2001) com ênfase em Energia e Automação Elétricas. Tem mais de 15 anos de experiência no desenvolvimento de projetos de P&D na área de automação e monitoramento de equipamentos de sistemas elétricos. Atualmente é Pesquisador da Fundação para o Desenvolvimento Tecnológico da Engenharia – FDTE, responsável por pesquisas no campo de desenvolvimento de sistemas inteligentes, IoT, e sistemas automação da geração, transmissão e distribuição de energia elétrica.

Edvaldo Carneiro, nascido em Itajubá no dia 01 de dezembro de 1959. Graduado pela Faculdade de Engenharia Civil de Itajubá (FECI) em 1983. Atualmente é supervisor da Divisão de Engenharia de Manutenção Civil e Segurança de Barragens da Companhia Energética de São Paulo.

Tatiana Peres Araripe Cappi, possui graduação em Engenharia Civil pela Universidade Estadual Paulista Júlio de Mesquita Filho em 2009. Atualmente é Engenheiro da Companhia Energética de São Paulo. Tem experiência na área de Engenharia Civil, com ênfase em Barragens, especializações em Segurança de Barragens e em Gerenciamento de Projetos – Práticas do PMI, assim como aperfeiçoamentos na área de patologias das construções.

Antonio Luiz Carmo dos Santos, possui graduação em Engenharia Civil pela Faculdade de Engenharia de São Paulo em 2009, em Tecnologia da Construção Civil Módulo Edifícios pela Faculdade de Tecnologia de São Paulo em 1998, em Tecnologia Civil - Movimento de Terra e Pavimentação pela Faculdade de Tecnologia de São Paulo em 2003 e em Tecnologia Civil Módulo Obras Hidráulicas pela Faculdade de Tecnologia de São Paulo em 2001. Possui experiência na área de Engenharia Civil e especialização em Gestão de Projetos de Sistemas Estruturais.