Grupo de Estudo de Operação de Sistemas Elétricos-GOP

Desenvolvimento e Utilização da Arquitetura OPC UA no Sistema Aberto de Gerenciamento de Energia - SAGE

RUY MAGALHÃES BRITTO(1); NIVALDO LAMBERT(2); AYRU L. OLIVEIRA FILHO(1); CEPEL(1);Cepel / PUC-Rio(2);

RESUMO

Neste trabalho descrevemos como o OPC UA foi inserido na arquitetura original do SAGE, considerando aspectos tais como a integração com a base de dados de tempo-real, a exposição do modelo de dados para acessos externos e integração com os mecanismos de autorização e autenticação.

A demanda para a integração de aplicações aos sistemas de tempo-real é crescente e envolve uma série de paradigmas, este trabalho apresenta uma alternativa padronizada, robusta e segura para tratar esse desafio, o OPC UA, um protocolo padrão de mercado para troca de dados na área de automação industrial e sistemas elétricos.

PALAVRAS-CHAVE

SAGE, OPC UA, INDÚSTRIA 4.0, IIoT – Industrial Internet of Things.

1.0 - INTRODUÇÃO

O OPC é um padrão de fato, desenvolvido pela OPC Foundation, para a troca de dados na área de automação industrial incluindo os sistemas elétricos. A especificação OPC UA (Open Platform Communications Unified Architecture), estendeu este padrão para uma arquitetura orientada a serviços (SOA – Service Oriented Architecture), que objetiva ser independente de plataforma, escalável, extensível.

De fato, esta nova arquitetura traz vários benefícios quando comparada com o padrão OPC original e tem tido grande aceitação entre os fabricantes de sistemas de automação e software afins, incorporando no seu conjunto de serviços recursos para:

a. Comunicação segura entre os sistemas, através do uso de certificados X509 (para segurança das mensagens), assinaturas e criptografia baseada em algoritmos padronizados como PKCS (Public Key Cryptography Standards), DSS (Digital Signature Standard) e AES (Advanced Encryption Standard).
b. Autenticação de usuários que se registram nos sistemas utilizando Username+passwords, WebServices Security Tokens ou Certificados X509 (específicos para identificação do programa de aplicação ou do usuário interativo).
c. Exportação e importação dos modelos de dados utilizados pelos sistemas que se comunicam, incluindo modelos proprietários, como os modelos SCADA e EMS do SAGE, modelos proprietários de outros fabricantes, e modelos padronizados, como o modelo CIM (Commom Information Model) definido na norma IEC 61970.

(*) CEPEL – Av. Horácio Macedo, n° 354 – Cidade Universitária, Rio de Janeiro – RJ - Brasil – CEP 21941-911
Tel: (+55 21) 2598-6422 – Email: rmb@cepel.br

O OPC UA foi formalizado como padrão internacional através da publicação da norma IEC 62541 tendo sido adotado como um dos protocolos padronizados para uso na Indústria 4.0 e também na IIoT (Industrial Internet of Things), a “Internet das Coisas aplicada na Indústria”.

Recentemente, o CEPEL empreendeu esforços para a implementação nativa do padrão OPC UA no sistema SAGE. Esta implementação abre novas fronteiras para a integração padronizada e segura de aplicativos, sistemas e fontes de dados aos sistemas de supervisão e controle suportados pelo SAGE.

Neste trabalho descrevemos como este padrão é inserido na arquitetura original do SAGE, considerando aspectos tais como a integração com a base de dados de tempo-real, a exposição do modelo de dados para acessos externos e a integração com os mecanismos de autorização e autenticação, dentre outros aspectos. De particular importância, também descrevemos como foram desenvolvidos e incorporados ao SAGE os mecanismos de segurança eletrônica especificados pelo OPC UA que enumeramos acima.

Agregadas ao módulo servidor e cliente OPC UA internos ao SAGE, apresentaremos com breve descrição as ferramentas:

a. SAGE_OPCUA Browser, ferramenta de navegação e exploração, após autenticação com grau de segurança adequado, permite uma visualização em *tree-view* de todo o modelo de dados disponibilizado pelo servidor e o monitoramento imediato dos itens escolhidos através de mecanismo assíncrono (subscribe e publish);
b. ADM_Certificados, uma ferramenta nos moldes de aplicações PKI (public key infrastructure), integrada ao mecanismo de autenticação e autorização do SAGE. Gerencia usuários e programas de aplicação que vão interagir com o sistema através do padrão OPC UA, atribuindo, alterando, validando ou revogando senhas, usuários e/ou certificados X509 para o acesso dos programas de aplicação ao sistema.

Dada a crescente aceitação do padrão OPC UA, diversos fabricantes disponibilizam, inclusive gratuitamente, kits de desenvolvimento e bibliotecas em várias linguagens e plataformas. Descrevemos brevemente as principais opções disponíveis e apresentaremos alguns protótipo de aplicativo desenvolvido sobre esta tecnologia.

2.0 - O SAGE

O SAGE foi concebido no início da década de 1990 como um projeto de pesquisa com o intuito de criar uma nova geração de centros de controle que representasse o estado da arte das tecnologias computacionais e das técnicas de operação em tempo real da época e, ao mesmo tempo, permitisse a constante incorporação de inovações, algoritmos e sistemas, frutos de novas pesquisas ao longo de seu desenvolvimento.

Em sua concepção original, o SAGE inovou ao propor novas bases para o desenvolvimento de sistemas de supervisão e controle (SSC). Os pilares desta nova concepção foram os conceitos de:

- Portabilidade: o SAGE foi concebido executar sobre diferentes plataformas de hardware e sistemas operacionais, já tendo suportado sistemas como Solaris, HP-UX, Alpha-Unix e Linux, sobre diferentes hardwares, como PCs, Itanium, workstations RISC (Sun, HP e DEC-Alpha) e servidores Intel Xeon, inclusive em redes heterogêneas. Hoje em dia, o segmento é marcado por diferentes distribuições Linux e por processadores Intel. Entretanto, o conceito original do SAGE permanece, estando este habilitado para suportar novas configurações de SO/HW sempre que adequado ou necessário.
- Expansibilidade: a base de tempo real do SAGE é originalmente distribuída, permitindo a evolução do sistema através adição de novas funcionalidades e do crescimento incremental de hardware.
- Modularidade: as diversas funções do SAGE são implementadas em módulos que podem ser inseridos, retirados ou alterados com mínima interferência nos demais.
- Interconectividade: o SAGE tem capacidade para receber e processar dados de múltiplos sistemas, de diferentes fabricantes e gerações tecnológicas, em diferentes protocolos, e de distribuir estes dados também para múltiplos sistemas distintos, permitindo convivência harmônica com diversos fabricantes e produtos existentes. Esta capacidade agora é expandida através do OPC UA, permitindo a troca de informações não somente de natureza SCADA com também qualquer dado modelado no sistema.
- Escalabilidade: o SAGE vem sendo utilizado para atender todos os níveis hierárquicos, desde uma pequena subestações (utilizando computadores de pequeno porte) até o Centro Nacional de Operação do Sistema - CNOS em Brasília, centro de maior nível hierárquico do Brasil. Esta característica otimiza, drasticamente, os investimentos na atualização do sistema e minimiza custos de treinamento.

Hoje, o desenvolvimento do SAGE busca atender às novas características do sistema elétrico tais como a crescente utilização de equipamentos de medição fasorial, a incorporação de equipamentos inteligentes ao sistema elétrico (smart-grids) e o tratamento de grandes volumes de informação consequente.

3.0 - O SERVIÇOS E PROTOCOLOS OPC UA

O OPC UA é um padrão independente de plataforma permitindo que vários tipos de sistemas e dispositivos se conectem no modo cliente servidor, através de vários tipos de redes, enviando mensagens definidas pela especificação, tanto através de serviços padronizados pela norma, como através de serviços (métodos) que podem ser definidos e implementados no sistema servidor. A norma OPC UA define serviços baseados em mecanismos modelados em solicitação/resposta (Request/Response) ou subscrição/publicação (Publishers e Subscribers), suportando comunicação robusta e segura garantindo a identidade dos aplicativos e resiste a ataques [4]. Nesses serviços, as informações são transmitidas usando tipos de dados definidos pelo fornecedor e definidos pela norma OPC UA, onde os servidores definem modelos de objetos que os Clientes podem descobrir dinamicamente.

Os servidores podem fornecer acesso a dados atuais e históricos, bem como a alarmes e eventos para notificar os clientes sobre alterações importantes. Através de serviços de uso obrigatório, os usuários e programas clientes devem se autenticar no servidor para que o referido acesso aos dados possa ser autorizado em função dos privilégios cadastrados para o usuário ou programa autenticado.

Os serviços definidos pela norma [5] são agrupados em conjuntos de serviços, sendo os principais implementados nativamente no SAGE apresentados a seguir. A Tabela 1 inclui os métodos específicos disponíveis em servidores SAGE OPC UA, assinalados com *, e os serviços ainda não implementados pelo SAGE no presente momento, assinalados com **.

Os serviços dos agrupamentos *SecureChannel Service Set* e *Session Service Set* serão abortados no item 5 deste artigo.

Tabela 1 – Serviços e Métodos OPC UA

SecureChanel Service Set • OpenSecureChannel • CloseSecureChannel	Method Service Set* • Consulta SQL à Base de tempo real* • Geração de Caso do Estimador de Estado* • Geração de CSV com Medidas Fasorias* • Consulta a Séries Históricas InfluxDB* • Obtenção de Lista de Alarmes* • Obtenção ou Ajuste de Papel do Usuário* • Consulta SQL à Base histórica Postgresql* • Ações de Entrada Manual em Objetos SCADA* • Carregamento em lote de Limites Cadastrais* • Obtenção de WEB Token de Autenticação*
Sesion Service Set • CreateSession • ActivateSession • CloseSession • Cancel	
NodeMangement Service Set** • AddNodes** • AddReferences** • DeleteNodes** • DeleteReferences**	
View Service Set • Browse • BrowseNext • TranslateBrowsePathsToNodesIds • UnregisteredNodes	MonitoredItem Service Set • CreateMonitoredItems • ModifyMonitoredItems • SetMonitoringMode • SetTriggering • DeleteMonitoredItems
QueryService Set • Querying Views • QueryFirst • QueryNext	Subscription Service Set • CreateSubscription • ModifySubscription • SetPublishMode • Publish • Republish • TransferSubscriptions • DeleteSubscriptions
Attribute Service Set • Read • Write • historyRead • HistoryUpdate	

Quanto aos protocolos, o OPC UA pode ser mapeado em uma variedade de protocolos de comunicação ao longo dos 7 níveis do modelo OSI / ISO, sendo que os dados trafegados podem ser codificados de várias maneiras para aumentar a portabilidade e a eficiência, conforme ilustrado no *stack* [1] de protocolos mostrados na Figura 1.

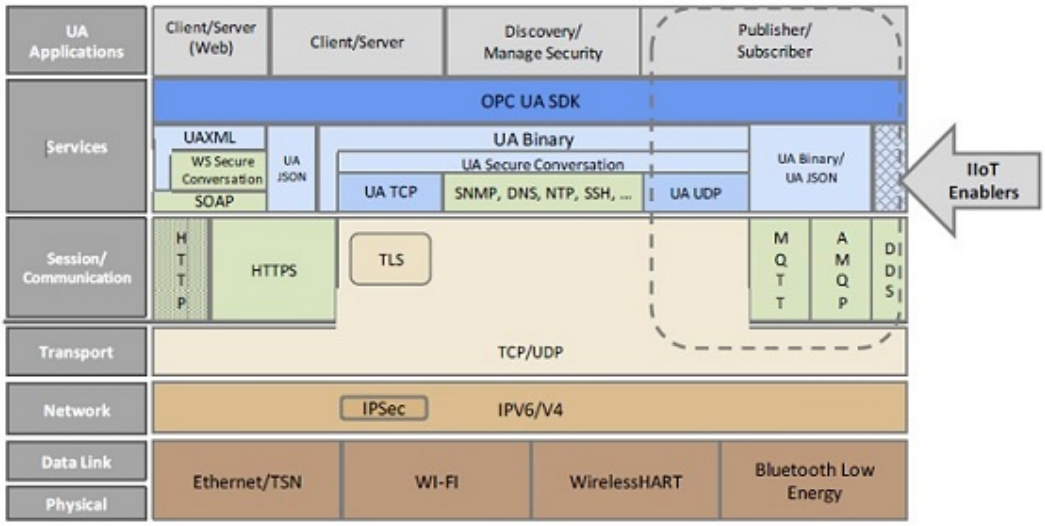

Figura 1 – Protocolos utilizados no OPC UA

Dessa forma, o OPC UA pode ser aplicável a diversos componentes, em todos os domínios industriais, visando à troca de informações entre sensores, atuadores, sistemas de controle, sistemas de fabricação e sistemas de planejamento conforme ilustrado na Figura 2.

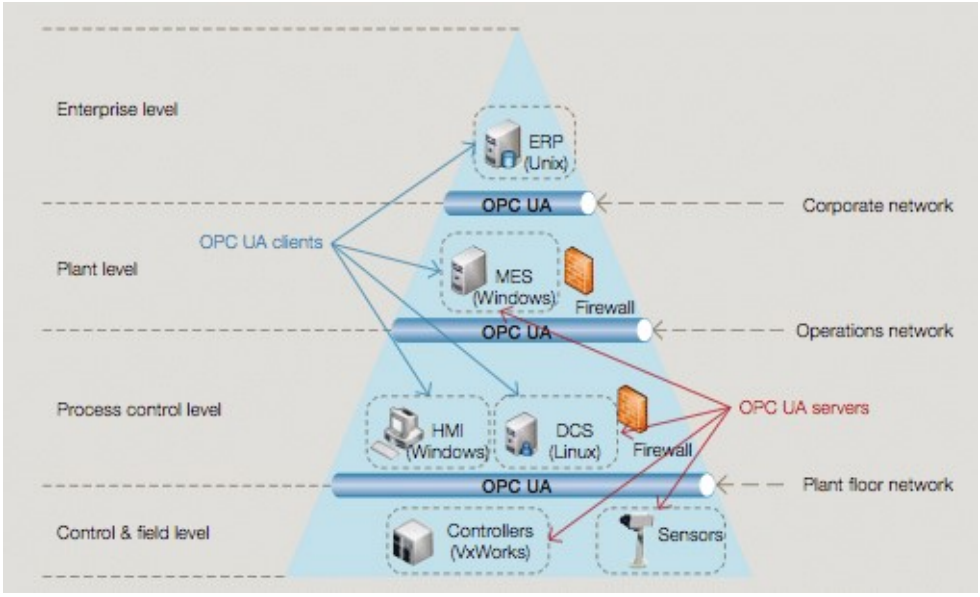

Figura 2 – Aplicação do OPC UA na pirâmide de automação

4.0 - ARQUITETURA SAGE – OPC UA

A implementação do OPC UA no SAGE é constituída de um módulo servidor (sOpcUA), um módulo cliente (cOpcUA), um aplicativo para administração de usuários do SAGE e certificados (Adm_Certificados), um servidor de autenticação com WebServices Tokens (serv_cgi_OpcUA), e um aplicativo de visualização *tree-view* da base de dados tempo-real e testador de serviços e métodos do SAGE (SageOpcUaBrowser), que é utilizado a partir de sistemas externos. A Figura 3 contextualiza esses módulos.

A Figura 4 também apresenta os diferentes perfis de aplicações desenvolvidas pelos usuários do SAGE, como por exemplo, aplicações servidoras de missão crítica com regime de funcionamento 7dias/24horas e que atendem os requisitos da Indústria 4.0, aplicações com requisitos de mobilidade para serem utilizadas em smartphones e tablets Android, e aplicações WEB de Interface de Usuário (UI).

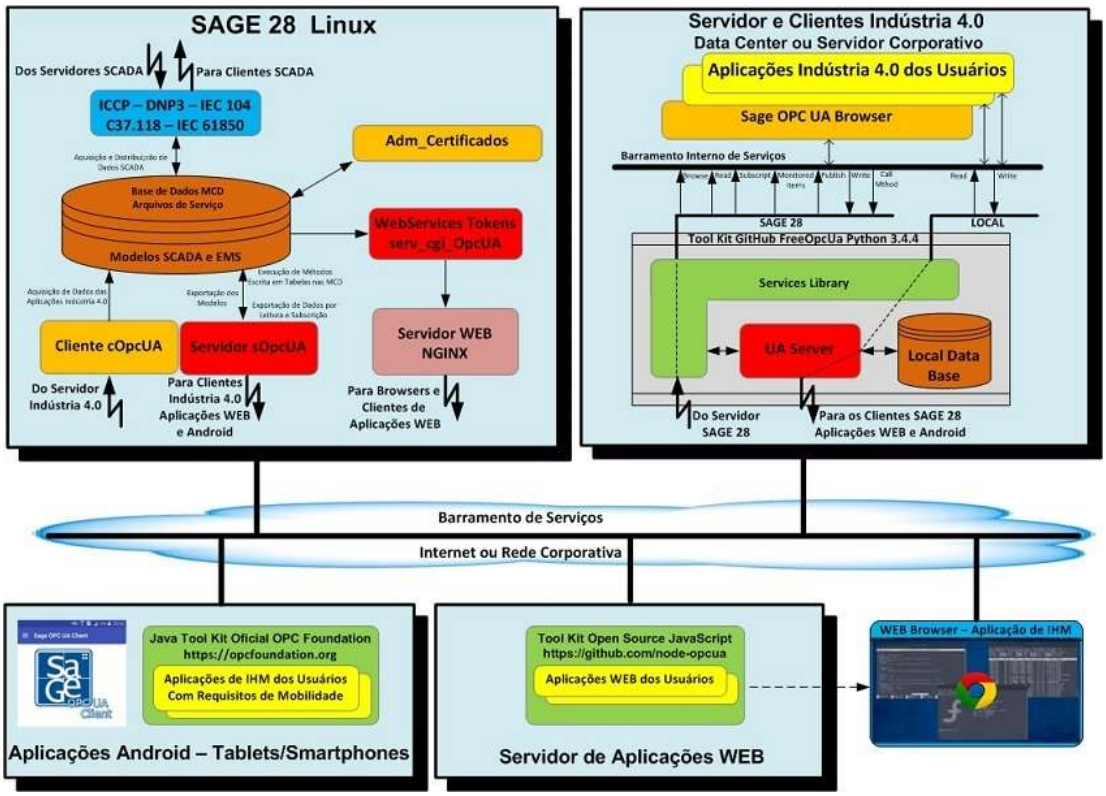

Figura 3 – Arquitetura OPC UA no SAGE

5.0 - A SEGURANÇA DO OPC UA

As questões relativas à segurança foram consideradas de fundamental importância na elaboração da norma OPC UA, que deu especial atenção a elas adotando técnicas consagradas e padrões de mercado, como criptografia ponto a ponto com assinatura digital e uso de certificados. [1]

Os algoritmos de segurança são aplicados em dois níveis da camada de protocolo: na camada de comunicação (Communication Layer) e na camada de aplicação (Application Layer), conforme ilustrado na Figura 4.

O Communication Layer é responsável por estabelecer um canal seguro (SecureChannel), garantindo a integridade das mensagens, confidencialidade e autenticação de instancias dos aplicativos.

O Application Layer é responsável por estabelecer uma seção segura (Secure Session) entre o Cliente e o Servidor, por meio de um usuário identificado e previamente cadastrado no sistema, com os devidos privilégios autorizados ou bloqueados para ele.

Todas as atividades no Application Layer trafegam em um Secure Channel, do qual os aplicativos dependem para uma comunicação segura. A Secure Session gerencia a autenticação e autorizações de usuário, com o cliente podendo se autenticar no sistema por meio de um determinado modo de identificação escolhido por ele, dentre um conjunto de opções regulamentados pela norma. Essa autenticação verificará a permissão daquele usuário para acesso aos recursos do sistema.

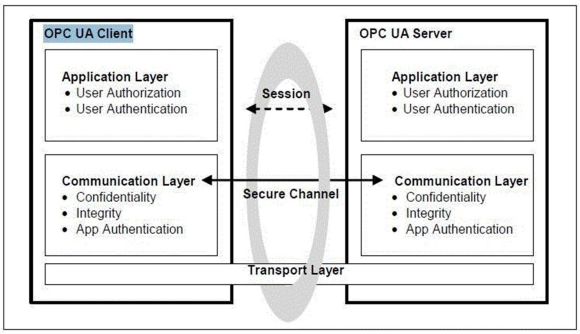

Figura 4 – Camadas de segurança do OPC UA

5.1 Secure Channel e Session

O Secure Channel é estabelecido entre o cliente e o servidor visando garantia da integridade das mensagens, a confidencialidade e autenticação de instancias dos aplicativos e a configuração da comunicação. O Secure Channel é baseado no uso de certificado X.509 podendo ser autoassinado ou emitido por uma autoridade de certificação (CA). Este certificado será o identificador entre a instância do aplicativo OPC UA cliente, e o servidor OPC UA. Nesta etapa ocorrem a troca e a validação de certificados entre o cliente e o servidor.

Posteriormente, sobre o Secure Channel, cliente e servidor estabelecem uma Session onde o cliente identificará o usuário que utilizará os demais serviços do sistema.

5.1.1 Abertura do Secure Channel

Antes de iniciar a criação / abertura do Secure Channel, o Cliente OPC UA deverá propor uma a política e um modo de segurança. A política de segurança é escolhida pelo cliente dentro de um conjunto de algoritmos disponíveis para a implementação dos mecanismos seguros para confidencialidade e integridade, como por exemplo, os algoritmos Basic128Rsa15, Basic256 e Basic256sha. Já o modo de segurança permite tanto assinatura digital e criptografia, apenas assinatura digital, ou nenhum deles.

O certificado e os Endpoints do servidor, (Endpoints, contém as políticas e modos de segurança implementados pelo servidor), são passados ao cliente por meio do serviço GetEndpoints, desta forma, o cliente pode avaliar a confiabilidade do certificado do servidor e escolher a política de segurança que ele considera adequada, permitindo assim que a criação do Secure Channel tenha sucesso, na próxima etapa, o cliente utiliza o serviço Open Secure Channel no qual ele passa o seu certificado, este, deverá ser considerado confiável pelo servidor para que o Secure Channel será estabelecido.

Ao fim desta etapa, é criada uma conexão lógica entre um único par cliente e servidor, que passam a utilizar um conjunto de chaves conhecidas apenas por eles para autenticar e criptografar mensagens enviadas através da rede. A Figura 5 - (a) ilustra o processo.

Após o estabelecimento do Secure Channel, o cliente começa a estabelecer uma sessão segura por meio dos serviços CreateSession, e ActivateSession. Durante esses serviços, são enviadas as credenciais do usuário para o servidor, que podem ser representadas por um certificado pessoal do usuário, por um par *username* e *password* ou por um Web Service Token. A Figura 5 - (b) ilustra este processo.

Figura 5 - (a) - Validação do certificado do cliente e servidor

Figura 5 - (b) - Autenticação e Autorização do usuário

5.2 Administração de certificados

Administrar os certificados disponíveis para o servidor OPC UA é uma tarefa que exige responsabilidade, pois, envolve questões de segurança do sistema, para suprir esta demanda, foi desenvolvido um programa nos moldes de uma ferramenta PKI (Public Key Infrastructure), ela permite o gerenciamento de todos os certificados utilizados pelo servidor OPC UA do SAGE.

Com uma interface simples e limpa é possível visualizar o estado de confiabilidade dos certificados, códigos de cores destacam os certificados confiáveis dos não confiáveis, permite também verificar e o prazo de validade, detectando certificados que estão por expirar e os que já expiraram. O programa está integrado ao mecanismo de autenticação e autorização do SAGE, visto que os certificados de usuário (SecureSession) tem estreita relação com os usuários do SAGE. A Figura 6 ilustra a tela principal da aplicação.

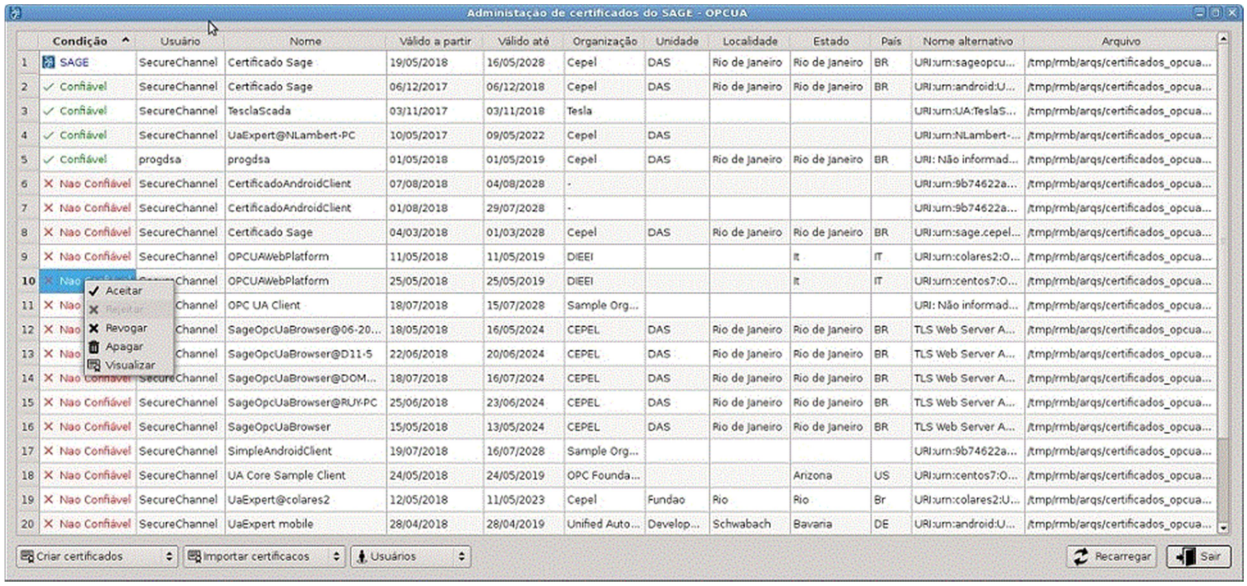

Figura 6 – Ferramenta para administração de certificados do OPC UA no SAGE

Funções:

- **Aceitação de certificado**: O servidor SAGE somente considera certificados marcados como confiáveis, que são movidos pela ferramenta para o diretório de certificados confiáveis.
- **Rejeição de certificado**: A ferramenta move o certificado para o diretório de certificados não confiáveis.
- **Revogação de certificado**: A ferramenta move o certificado para o diretório de certificados revogados.
- **Eliminação de certificado**: A fermenta remove o certificado dos diretórios do repositório.
- **Visualização de certificado**: A ferramenta exibe todos os atributos do certificado.
- **Criação e importação de certificados no formato X.509**: A ferramenta cria o certificado de conexão (SecureChannel) do servidor SAGE, cria ou importa os certificados de conexão (SecureChannel) de um cliente remoto e de usuário cadastrado no acesso legado do SAGE ou no acesso PAM.
- **Gerenciamento de usuários do sistema SAGE e suas autorizações**: A ferramenta atribui ou remove privilégios do acesso legado do SAGE e/ou papéis do acesso PAM.

6.0 - APLICAÇÕES OPC UA E KITS PARA DESENVOLVIMENTO

O OPC UA é um dos principais padrões adotados na Indústria 4.0 para integração entre sistemas e aplicações, o fator determinante para que esse patamar tenha sido atingido, deveu-se ao fato de estarem disponíveis no mercado inúmeros toolkits, comercializados ou gratuitos, desenvolvidos para diferentes linguagens de programação, que facilitam enormemente a integração nos padrões da Indústria 4.0. Ver Tabela 2

Tabela 2 – Ferramentas de Desenvolvimento OPC UA

Gratuitos	Comerciais
Java Toolkit official OPC Foundation (opcfoundation.org)	Unified Automation (unified-automation.com)
Python (github.com/FreeOpcUa)	Matrikon - Honeywell (matrikonopc.com)
C-ANSI e C++ (github.com/open62541)	Prosys OPC. (prosysopc.com)
JavaScript - App Web (github.com/node-opcua)	

No Cepel, a experiência de integrar ao SAGE aplicações desenvolvidas por outras empresas do setor elétrico, mostrou que, uma integração envolvendo troca de dados utilizando os serviços básicos e métodos do OPC UA, demandou poucos dias para ser realizada e sem nenhum esforço para a integração do protocolo entre o OPC UA do SAGE e o OPC UA do cliente. Empresas como Coelba, Cemig e ONS, desenvolveram aplicativos muito rapidamente e com muito pouca necessidade de suporte do Cepel. A Coelba, por exemplo, desenvolveu um protótipo para *self-healing* em sistemas de distribuição. Já o ONS desenvolveu um monitor de qualidade e estado dos enlaces de comunicação com agentes.

Em desenvolvimento no Cepel, destacamos os aplicativos SageOpcUaClient e SageOpcUaBrowser:

- SageOpcUaClient - Um protótipo de aplicativo Android sobre esta tecnologia, com aplicabilidades no âmbito gerencial e operacional, técnicos ou engenheiros de campo, farão uso deste aplicativo em atividades diárias no campo, permitindo um acompanhamento em tempo-real dos trabalhos a serem realizados. Ver Figura 7.

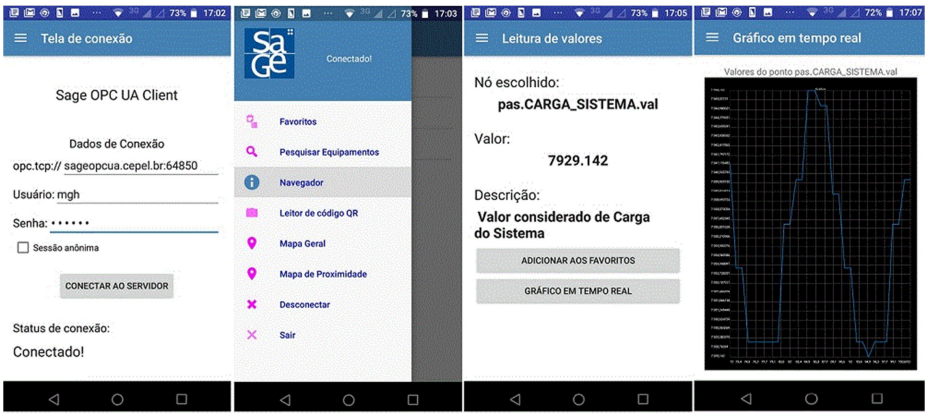

Figura 7 – Aplicativo android para navegação na base de dados e execução de serviços

- SageOpcUaBrowser – Um aplicativo Windows, que e a partir de sistemas externos, permite uma visualização em formato *tree-view* da base de dados tempo-real e a execução dos serviços implementados no servidor, como por exemplo a subscrição e/ou leitura de variáveis e execução de métodos. Ver Figura 8. Este aplicativo foi desenvolvido com o toolkit Python.

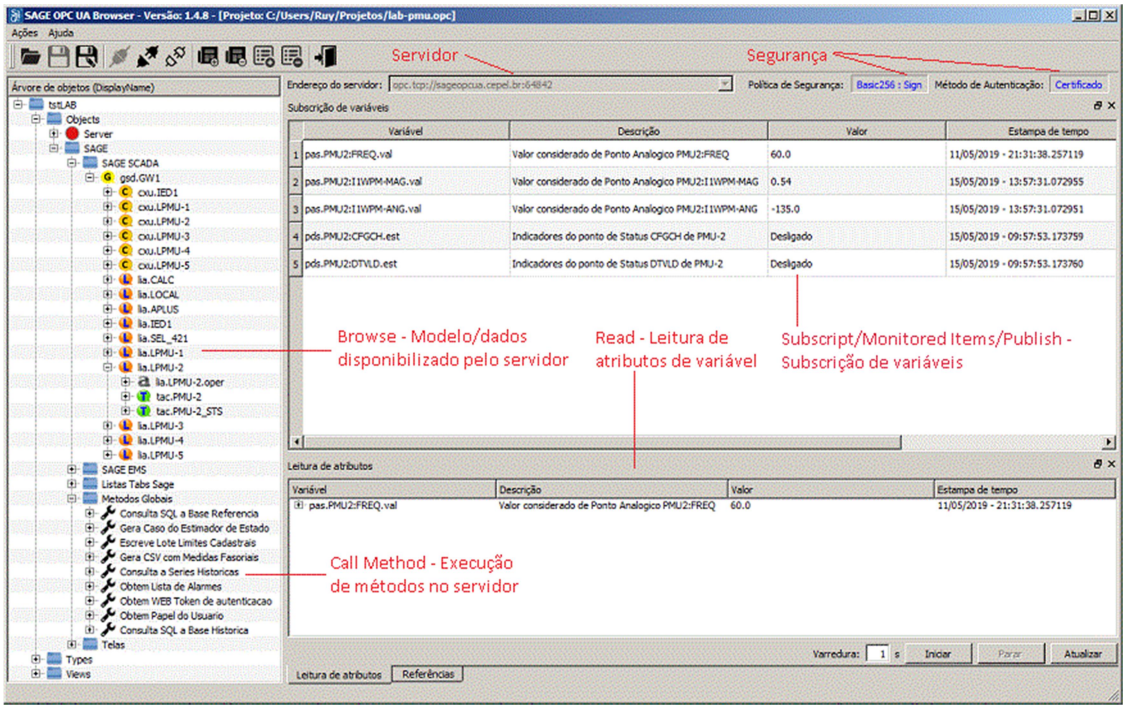

Figura 8 – Aplicativo Windows para navegação na base de dados e execução de serviços

7.0 - CONCLUSÃO

O OPC UA, hoje normatizado pela norma IEC 62541, vem ganhando grande adesão da indústria e é indicado como um dos padrões a serem utilizados na chamada indústria 4.0 ou IIoT (Industrial Internet of Things). Neste artigo, apresentamos o OPC UA não só como um protocolo de comunicação, mas também como uma opção de arquitetura orientada a serviços (SOA), como preconiza a própria OPC Foundation. Também apresentamos a integração desta tecnologia ao SAGE, feita de forma nativa como os demais protocolos disponíveis SAGE. As características de exposição de um modelo de dados completo, SCADA e EMS, o forte compromisso com os padrões de segurança eletrônica, juntamente com a exposição de métodos para acesso a funções específicas, faz com que esta tecnologia seja uma boa opção para a integração entre sistemas automação.

8.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) OPC Foundation: The Interoperability Standard for Industrial Automation™, “Introspective on Achieving Information Integration Interoperability in Process Automation“, March, 2006.

(2) OLIVEIRA FILHO, A. L., SANTOS, H. T., PEREIRA, L. A. C., LIMA, L. C., LAMBERT, N., CRUZ, D., SCHIO, G. R, GOMES, D. B., LAMEIRÃO, A. M. M. S., “Soluções para a Rede de Gerenciamento de Energia do ONS – REGER”, XXI SNPTEE, Florianópolis, SC, Brasil, 2011.

(3) COSTA, M. R., PEREIRA, L. A. C., ALVES, J. M. T., “A importância e a Evolução das Funções de Análise de Redes no Sistema de Supervisão e Controle”, VIII EDAO, Recife, PE, Março, 2005.

(4) OPC Foundation: “OPC Unified Architecture Specification Part 1: Overview and Concepts Release 1.04”, November, 2017

(5) OPC Foundation: “OPC Unified Architecture Specification Part 4: Services 1.04”, November, 2017

9.0 - DADOS BIOGRÁFICOS

Ruy Magalhães Britto graduou-se em Engenharia Elétrica pela Universidade Santa Úrsula (USU) em 1992, Curso de especialização em análise de sistemas pelo instituto brasileiro de pesquisa em informática (IBPI) em 1992, Curso de pós-graduação em engenharia de controle e automação industrial em 2005. É pesquisador do Departamento de Automação de Sistemas do Centro de Pesquisas de Energia Elétrica – CEPEL - desde 2006, atuando no desenvolvimento do sistema SAGE – Sistema Aberto de Gerenciamento de Energia, desenvolvido pelo CEPEL. Suas áreas de interesse para pesquisa incluem sistemas de supervisão e controle e protocolos de comunicação.

Ayru Leal de Oliveira Filho graduou-se em Engenharia Elétrica pela Universidade Federal de Juiz de Fora em 1987, concluiu o mestrado em Engenharia de Sistemas e Computação no Instituto Militar de Engenharia (IME/RJ) 1990 e o doutorado em Engenharia de Sistemas e Computação na Universidade Federal do Rio de Janeiro (COPPE/UFRJ) em 2000. É pesquisador do Centro de Pesquisas de Energia Elétrica desde 1988, atuando no desenvolvimento sistemas de suporte à operação em tempo-real de redes elétricas e no desenvolvimento de aplicações voltadas à supervisão e controle em tempo-real. Seus interesses incluem, ainda, banco de dados para operação de sistemas elétricos, sistemas distribuídos, protocolos de comunicação, e sistemas aplicados à operação.

Nivaldo Lambert atua em projetos na área de Sistemas de Comunicação de Dados e Controle de Processos de Tempo Real. Formado em Física pela UFRJ / FAHUPE, Brasil, sua experiência no CEPEL inclui a participação na concepção e desenvolvimento do SAGE nas áreas de Comunicação de Dados, Aquisição / Distribuição / Controle em Tempo Real, Suporte Computacional, e a implantação de sistemas SAGE em diversas instalações. Nivaldo é o autor das implementações nativas no SAGE dos protocolos DNP3, IEC-104/101, IEC-61850, ICCP, C37.118 e OPC UA, dentre outros.