

A Pesquisa sobre OPC e OPC-UA

Sobre o padrão, desenvolvimentos e investigações

Schwarz Computer
Technology Segurança MH
Universidade de Kassel
Kassel, Alemanha
m.schwarz@uni-kassel.de

Börscsök J.
Programação de Computadores Arquitetura und Sistema
Universidade de Kassel
Kassel, Alemanha
j.boercoek@uni-kassel.de

Abstrato - Em 1996, um novo padrão foi anunciado que deve servir como uma interface de software para dados processo de troca e para resolver o problema com os dados do processo de troca usando diferentes protocolos industriais e sistemas de comunicação. A história de sucesso começou desde então, com alguns padrões adicionais, como o padrão de alarmes e eventos usando a abordagem OPC e algumas revisões e novas edições. Dez anos mais tarde, uma nova abordagem foi criada que unificou todas as normas existentes e também estava preocupado com por exemplo, interoperabilidade, segurança e sistemas baseados na web. Detalhes Este papel os diferentes padrões OPC, tenta responder à pergunta por que este padrão é importante para as indústrias e as universidades e onde a pesquisa e desenvolvimento utilizando esses padrões atual.

Palavras-chave - OLE for Process Control, OPC, Arquitetura unificada, OPC-UA, Colaboração Produtividade Abertura

EU. INTRODUÇÃO

Em meados da década de 1980 indústrias e universidades começaram a investigar, desenvolver e estabelecer redes, protocolos e sistemas de ônibus [8], [9], [30]. Dentro de alguns anos existem mais de 50 sistemas de bus diferentes [30], alguns tornaram-se sistemas de comunicação universais em indústrias, alguns são usados em algumas áreas específicas e alguns desapareceram. Por exemplo, *Profibus* e seus derivados são frequentemente utilizados em indústrias de processo, *PROSSO*-ônibus é usado principalmente em carros e redes de escritório são muitas vezes baseadas em Ethernet. Em um sistema de diferentes dispositivos têm para trocar informações como um

Interface homem-máquina (HMI) e Controle de Supervisão e Aquisição de Dados (SCADA)

do sistema; aqueles que recolher, analisar e exibir dados de vários dispositivos que usam diferentes protocolos e redes [14]. Esta tarefa torna-se não-trivial e propenso a falhas. Para cada dispositivo um controlador de software tem de ser fornecida pelo dispositivo de companhia, um esquema é mostrado na Fig

1. Mudanças na especificação do protocolo resultaram em comunicações com defeito e ajustes tiveram que ser feitos, que era demorado e caro [30]. Por um lado isso manteve concorrentes afastado por outro lado, era difícil entrar em novas áreas.

Em 1995, empresas como Fisher-Rosemount, Intellution, Tecnologia Intuitiva, Opto22, Rockwell e outros formaram uma força-tarefa para encontrar uma solução para este problema [8], [9], [11], [14]. Dentro de alguns meses um novo padrão foi estabelecido, que

descreve a arquitetura de software cliente-servidor para coletar dados de processo reais de dispositivos para passá-las por exemplo, para sistemas SCADA. A primeira especificação foi lançado em agosto de 1996 como o *OPC-DA 1.0 (Data Access)* eo OPC Foundation foi fundada para continuar, manter e comercializar os padrões.

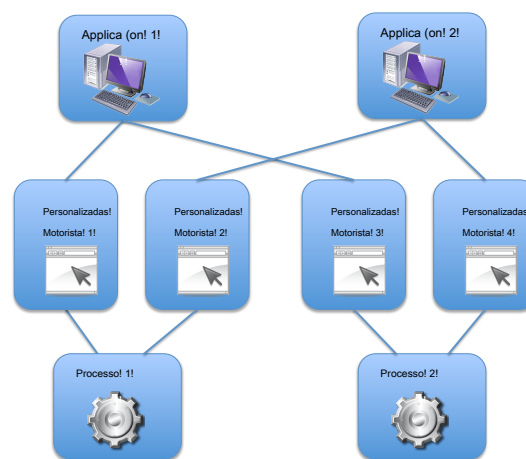


Fig. 1: uma comunicação sem OPC

O nome original do OPC representava **OLE para P ROCESSO C ontrol**, como a arquitetura cliente-servidor foi baseado em OLE da Microsoft (Object Linking and Embedding), uma tecnologia para desenvolver estruturas de objetos orientada, que mais tarde foi combinado em COM (Component Object Model) e DCOM

(Distributed componente Objeto Modelo) [3], [8], [9], [11]. Para basear a arquitetura cliente-servidor em componentes da Microsoft foi, provavelmente, uma das razões para o sucesso gigante da OPC [3], [11]. Diversas normas diferentes seguido e será detalhada na próxima seção.

Embora OPC é aceito em indústrias e tem sido amplamente utilizado em muitas aplicações, alguns aspectos negativos surgiu [3], [8], [9], [14] durante os anos. OPC operando em outros sistemas operativos tais como o Linux tinha o problema de que a funcionalidade COM / DCOM teve de ser emulado para ser utilizada que tem causado muitos problemas [14]. Em meados de 1990, os aspectos de segurança não estavam a ser visto como um grande problema e deve ser tratado pelo sistema operacional [2], [3]. Este tem sido indicado como um pressuposto errado, uma especificação separada sobre

segurança foi lançado em 2000, mas teve virtual nenhum efeito sobre o mercado [3].

Dados pertencentes a outro, mas foram fornecidos por diferentes arquiteturas de servidores OPC não poderiam ser agrupados. Por exemplo, o processo gerado um alarme, pois o valor do processo foi maior quando permitido, então o alarme foi fornecida pela *Alarme e Evento (A & E)* servidor, o valor atual processo pelo *Data de acesso (DA)* servidor) e que a informação não pode ser montada junto [3], [8], [9], [11], [14].

Embora, as diferentes arquiteturas cliente-servidor OPC especialmente *DA* e *AE* foram e ainda são altamente aceito em indústrias de processo e automação, em 2006, foi a vez de uma nova etapa para criar um novo conceito que combina os diferentes padrões separados em um, que usa um espaço de endereço para todas as arquiteturas OPC cliente-servidor diferentes em vez de cada arquitetura de um espaço de endereço separado. O novo padrão também integra aspectos de segurança e características de confiança como a tolerância a falhas, redundância, de interoperabilidade e utiliza tecnologias baseadas na Web [8], [9], [11], [14].

Com o novo nome padrão *Arquitetura Unificada-OPC* (OPC-UA) anunciou em 2006 e uma revisão com as peças adicionais do padrão em 2009, as versões OPC anteriores foram renomeados em *OPC Classic*, como muitas empresas e fabricantes ainda fornecer e desenvolver muitas arquiteturas e sistemas [11], [14] OPC.

A Fundação OPC também foi uma raiz diferente com o novo padrão OPC-UA [11] em comparação com o *OPC Classic*. o *OPC clássico* é um padrão de-facto aceite no processo e indústria de automação mas não foi aprovado como um padrão como o IEC 61508 [7] ou IEC 61131 [6]. Portanto, a Fundação OPC se envolveu a organização IEC em um estágio inicial e em fevereiro de 2010 as duas primeiras partes da especificação OPC-UA tornou-se também um padrão IEC, outras partes seguiram e seguirão. O padrão OPC-UA é, desde então, também disponível como IEC 62541 [11], [3], [14]. Além disso, a sigla OPC (OLE for Process Control) começaram a transformar-se em *Abertura, Produtividade Colaboração*.

Além disso, a fundação OPC começaram a cooperar com os outros, um exemplo é o PLCopen [29] para desenvolver um modelo comum para as variáveis do processo de troca.

Após a história do OPC padrão de fato (Classic OPC) eo padrão OPC-UA (IEC62541) tem sido mais ou menos detalhada, o esboço do papel restante é o seguinte: Seção 2 irá descrever as diferentes especificações da

OPC Classic. Seção 3 irá detalhar a principal inovação do OPC-UA. Seção 4 irá apresentar um estudo sobre investigação em curso e as investigações usando ou melhorar OPC e OPC-UA. Seção 5 vai tirar algumas conclusões.

II. CLASSIC OPC

Esta seção descreve as diferentes especificações OPC que são resumidos sob a égide de *OPC Classic*. Todos têm em comum que eles são baseados na arquitetura cliente-servidor. Eles são definições das interfaces comuns que permitam

aplicações que utilizam cliente OPC e servidor OPC para a troca de dados, eventos e informações com dispositivos como mostrado na figura abaixo [33].

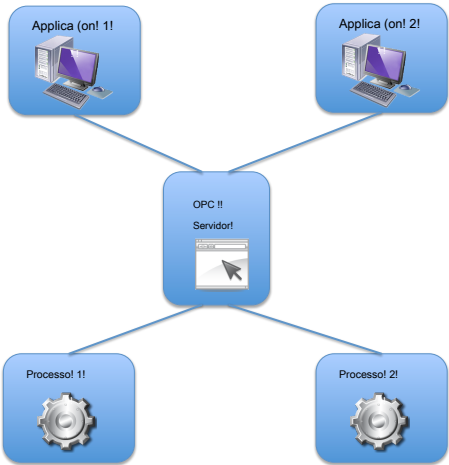


Fig. 2: A comunicação através de OPC

UMA. Acesso a Dados (DA) Especificação

A especificação de *Acesso de Dados OPC* foi o primeiro foi publicado em 1996 e foi o ponto de partida da fundação OPC [8], [9], [11], [14]. A versão atual é 3.0 publicado em 2003 [22]. O padrão de fato propõe uma arquitetura cliente-servidor para troca de dados de processo em tempo real em um formato especificado, como mostra a Tabela 1.

Tabela 1: Itens OPC e Atributos

Variável	Atributo
Valor do processo	Valor
carimbo de tempo	Data / Hora
Confiabilidade	Boa / unknown / bad

o *A DINAMARCA* servidor pode normalmente lidar com vários clientes e eles podem reservar itens necessários que consistem dos três atributos apresentados acima. Quando o dispositivo em si não é capaz de fornecer qualquer carimbo de tempo, em seguida, o servidor tem que fornecê-la. Se o link para o dispositivo é desligado, em seguida, o servidor pode indicar isso com uma bandeira confiabilidade eo cliente pode reagir sobre este fato [22].

B. Alarmes e Eventos (A & E) Especificação

o *A & E* especificação [19] define uma interface para servidor e os clientes para trocar informações sobre alarmes, eventos e suas confirmações. O servidor recebe processo informações de dispositivos e analisa-os e fornece os eventos resultantes ou alarmes com as informações necessárias. É importante que o *A & E* servidor avalia basicamente os mesmos valores de processo como o *DA* servidor, mas para obter as informações do ex alarme e o valor atual processo dois servidores são necessários, o *DA* e a *A & E* servidor eo cliente tem de ser ligado a ambos.

C. Acesso a dados históricos (HDA) Especificação

o **Histórico Data Access [24]** especificação pode ser visto como uma extensão da **Data de acesso** especificação. Trata-se de dados do processo, mas não com dados em tempo real e os efeitos do presente especificação diferente. Os dados do processo são armazenados e podem ser acedidas quer como dados brutos ou dados agregados. Do armazenados, dados passados (historical), tendências, características, valores médios, mínimos, etc. máximo dentro de um intervalo de tempo especificado pode ser calculado e enviado para o cliente. O objetivo desta arquitetura cliente-servidor é mais para usar os dados passados para, por exemplo otimização de um processo ou avaliar a qualidade dos produtos [8], [9], [11], [24], [33].

D. comandos Especificação

Às vezes, não é suficiente para ler e escrever valores de dados ou para se informar sobre um evento que ocorreu, mas inicia comandos a serem executados para controlar ou configurar um dispositivo ou sistema ou para iniciar uma recarga programa. Portanto, o **comandos** especificação foi criado para proporcionar uma interface para executar comandos definidos [3], [21].

E. Dados XML especificação de acesso

o **Acesso a dados XML** especificação baseia-se na **OPC** **Data de acesso** especificação mas usa XML e web-services sem qualquer comunicação COM / DCOM, de modo que a independência de plataforma pode ser alcançado [8], [9], [11], [14], [26]. No entanto, o padrão pode ser visto como o antecessor do OPC-UA, mas foram liberados tarde demais. Clientes, fabricantes e desenvolvedores estavam esperando por OPC-UA e não interessados no desenvolvimento de uma arquitetura cliente-servidor que seria logo ultrapassado pela nova especificação OPC-UA [11], [14].

F. Data Exchange (DX) Especificação

O objetivo desta especificação é para usar novamente a interface DA para a troca de dados, mas entre os servidores. É uma comunicação horizontal por exemplo para formular uma estratégia de servidor back-up ou redundante. Outra possibilidade seria a de incorporar um cliente no servidor que comunica com o segundo servidor e vice-versa, que é mostrada na figura abaixo [11], [14], [23].

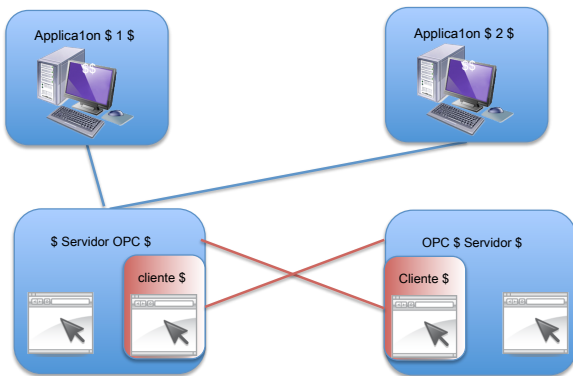


Fig. 3: a comunicação do servidor OPC utilizando um cliente inerente

G. Especificação de lote

o **OPC formada** especificação [8], [9], [11], [20], [33] não é uma interface inteiramente novo, em vez de uma extensão para o **Data de acesso** especificação para o caso especial de processos descontínuos. UMA

processo descontínuo consiste de diferentes fórmulas e receitas para fabricar ou produzir produtos. Dentro da execução dos lotes, os dispositivos têm de se comunicar e trocar informações. Dados de inscrição é enviado e relatório de informação é recebido. Produtos para processamento em lote tem de ser fabricado de acordo com o IEC [8] 61512-1, [9], [11], [33]. Isto inclui a visualização, a geração de relatórios, sistemas de controle de sequência e equipamento. Entre esses componentes e produtos,

informação sobre as propriedades do equipamentos, condições de trabalho atuais, dados históricos e substâncias, volumes e capacidade do lote devem ser trocadas. O OPC suprimentos especificação interoperabilidade entre diferentes componentes, equipamento e sistema das indústrias de processamento em lote. Portanto, esta especificação não descreve uma solução para os problemas de regulação do lote, mas soluções de diferentes fabricantes, em um ambiente heterogêneo [8], [9], [11], [25], [33].

H. Resumo

Até agora, as diferentes especificações do padrão de fato ter sido detalhado e pode ser graficamente apresentada como segue:

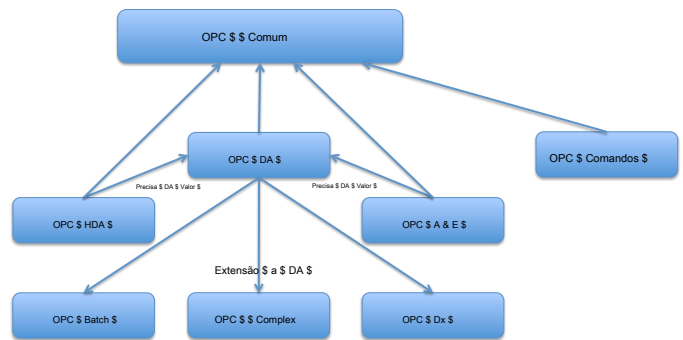


Fig. 4: Relação das diferentes especificações OPC

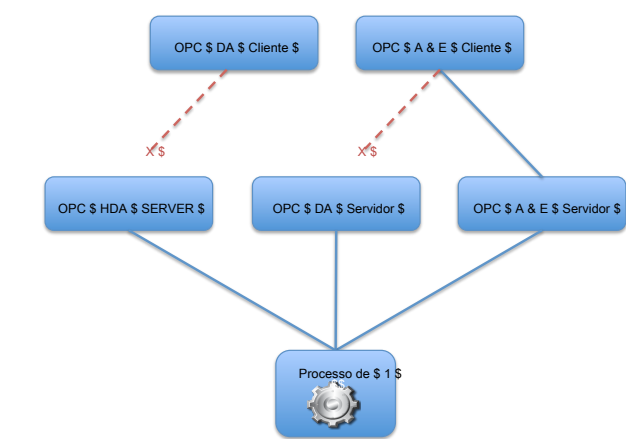
Nem todas as especificações são mostrados na figura acima, mas **demonstra quão importante é o OPC DA especificação é, o que é também uma** indicação por várias revisões existe desta especificação e por isso que as outras não foram alteradas que muito.

As próximas seção lida com a nova especificação OPC, que é também um padrão IEC, e não um padrão de-facto como o OPC clássico.

III. OPC U NIFIED UMA BORDAGEM

OPC clássico (que foi o estado da arte em sua aparência) tem sido amplamente aceito em indústrias de automação e processos e ainda é um padrão de fato. As diferentes especificações detalhadas na seção anterior eram necessárias e resultou de demandas de indústrias. Depois de cerca de 10 anos após a primeira especificação foi libertado, um novo padrão combinado surgiu. Isto foi necessário como os diferentes padrões individuais definidas diferentes espaços de endereço e aqueles que não podem ser fundidas em conjunto, mesmo se foi utilizada a mesma variável com os seus valores agregados, o cenário é mostrada na figura abaixo [3], [11]. Segurança e interoperabilidade não foram problemas no momento em que o primeiro padrão de-facto foi lançado; isso foi

assumido que esta deve ser tratada pelo sistema operativo, o qual foi um erro [2]. sistemas baseados na Web e XML estavam nas de meados de 1990 sem problemas.



comunicação OPC apenas dentro da mesma especificação possível: Fig.5

Um grande passo foi unificar todos os espaços de endereços diferentes para um que o servidor OPC-UA fornece um serviço para o objeto a ser acessado pelo cliente. O padrão caracteriza o objecto como variáveis, eventos e métodos como se mostra na figura abaixo.

variáveis estão relacionados à **OPC-DA** e **OPC-HDA** e **eventos** para **OPC-A & E** e **Métodos** para **OPC-Comandos**, quando seria em comparação com o **Clássico OPC** [3], [11].



Fig. 6: modelo objecto OPC -ua

UMA. Segurança

Como mencionado anteriormente, a segurança é um objetivo que tem sido subestimada no passado [1] e quando foi reconhecida como um problema grave, então a especificação de segurança foi anunciada tarde demais para ser aceita e adotada em indústrias. Uma solução é túnel as informações do cliente para o servidor [10], [16], [18], [33].

OPC-UA Segurança é considerado em duas fases diferentes da comunicação, uma é a camada de aplicação a um outro está no nível de comunicação. A camada de aplicação tem de lidar com a autenticação de usuário e autorização do usuário. Um canal seguro é fornecida na camada de comunicação, que é usada pela camada de aplicação para passar a data a partir do cliente para o servidor. A camada de comunicação inclui confidencialidade, integridade e aplicação de autenticação [3], [11], [27].

A autenticação do usuário é identificar um ex cliente, fornecendo uma senha, um certificado X.509v3 ou um símbolo WS-Security [3], [11], [27].

autorização do usuário [3], [11], [27] define os direitos individuais para aceder a determinados serviços ou negação de determinados serviços. A especificação em si não indica como o usuário deve legítimos os seus direitos, mas oferece a possibilidade de que isso pode ser implementado e aplicado.

A confidencialidade é para garantir a transmissão dos dados a partir do servidor para o cliente, portanto, a solicitação e as respostas têm de ser criptografado [3], [11], [27] para que outros não podem ler facilmente a informação que foi enviada.

A integridade é para garantir que a mensagem não é alterado durante a transmissão. As assinaturas podem ser usados para garantir que o cliente recebeu a idêntica informações que o servidor tinha enviado [3], [11], [27].

Também no nível superior, nível do aplicativo, o aplicativo cliente e servidor deve identificá-los, usando certificados, o que deve ser feito durante o tempo em que está estabelecido o canal seguro. Portanto, o aplicativo pode decidir aceitar ou rejeitar o pedido e respostas [3], [11], [27].

A Figura 7 mostra um esquema de segurança o OPC, onde a autenticação aplicação é feita através de um canal seguro, quando é estabelecida.

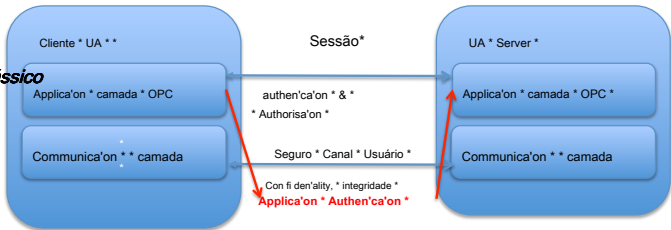


Fig. 7: modelo de segurança para o OPC UA

B. Pilha comunicação

A transmissão de dados pode ser feito de três maneiras diferentes; esses são: Native binário, web-services XML e SOAP / HTTP com binário. A figura abaixo mostra as três maneiras diferentes.

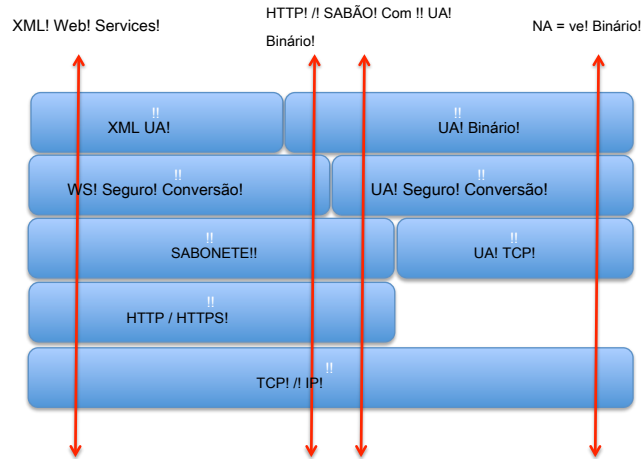


Fig. 8: pilha de comunicação

Com esta comunicação empilhar a abordagem OPC-UA fornece uma camada de interoperabilidade que dependem de nenhum sistema operativo específica ou protocolo de [3], [11], [28].

Ambos, UA-XML e UA-Binary são assegurar e transmitir os pedidos e respostas. Enquanto o UA-XML depende de esquemas de codificação para Web Services, a UA-binário em formatos binários, conforme especificado no OPC-UA part 6 [28] para a comunicação de alta velocidade ou sistemas embarcados, onde comunicação usando XML exigiria uma grande quantidade de recursos como memória e poder de CPU, que é muitas vezes demasiado para dispositivos embarcados. usa a conversão de segurança, quer protocolos padrão utilizadas pelos Serviços Web Security ou a versão binária definido na parte da especificação 6 para uma comunicação de alto desempenho em sistemas embarcados, as mesmas duas maneiras diferentes são fornecidos para os mecanismos de transporte. Também uma mistura de dois a XML e binário é possível [3], [11], [28].

IV. SURVEY E INVESTIGATIONS

Esta seção descreve alguns interessante e relevante on- indo áreas de pesquisa sobre OPC e OPC-UA. A primeira parte trata com o OPC clássico, a segunda parte concentra-se em OPC-UA.

UMA. OPC clássico

Existem poucos trabalhos introdutórios interessantes, como o papel, Mai Filho & Myeong-Jae Yi [34] ou por Liu et al. [13], que descreve os pontos de vista e as tarefas do OPC clássica e a arquitetura unificada. A primeira proporciona um resumo interessante dos diferentes especificações e os problemas a serem resolvidos na segunda descreve o desenvolvimento de um sistema de OPC para ser utilizado no sistema de controlo distribuído (DCS).

OPC clássico não teve muito interesse em comunidades de pesquisa; parecia que isso mudou, quando OPC tornou-se interessante para ser conectado à Internet. Um desenvolvimento e investigação é usando uma arquitetura OPC distribuído por controlo remoto e monitorização [32]. As comunicações dos diferentes processos locais estão usando PLCs e servidores OPC para monitorar e controlar os processos em um PC local. Além disso, uma comunicação baseada na Web foi adicionada em uma tal maneira que as diferentes estações de controlo através da Internet pode controlar remotamente esses processos. Os autores negligenciado a interface DCOM e desenvolveu uma interface da Internet, que é um banco de dados em um servidor web para trocar o (dados de processo e passado) atual, que pode ser visto como uma adoção de OPC-UA sem utilizar esta norma [32] .

Existem vários papéis, que o uso de OPC-XML para suas investigações. A primeira investigação [36] usa um servidor OPC-XML- DA para transmitir os dados do processo através da Internet para ser usado por exemplo, para aplicações de gestão de produção e empresariais, tais como MES (Manufacturing Execution Systems) ERP (Enterprise Resource Planning) CMMS (Manutenção Computadorizado Sistemas de gestão) e outros. O servidor XML OPC- herda uma arquitetura OPC-Complex-Data de ler, enviar e escrever complexos e vários tipos de dados, tais como elementos abstratos, inteiro ou cordas. Além disso, os autores propõem um método que utiliza XML para fins de segurança, pois esta é

uma questão importante, quando a comunicação é feita através da Internet [36].

Em outra pesquisa [38], um procedimento é descrito que utiliza um servidor OPC XML-DA e traduzir os dados em uma mensagem compatível SOAP que pode ser transmitida através da Internet. Este método pode ser interpretado como um método OPC-UA mapeado sobre clássico OPC.

B. OPC Arquitetura unificada

OPC é um novo e combinando tecnologia, construída em uma arquitetura cliente e servidor comprovada [11], [14], [35]. Mudar para uma nova tecnologia não é uma tarefa trivial, especialmente em indústrias. Cliente que usa OPC clássico pode não ser interessado em mudar a tecnologia, pelo menos não completamente ao mesmo tempo. Os sistemas existentes têm de ser incluído sem uma reinstalação completa. As diferentes maneiras de envolver os clientes OPC e servidores antigos, em um novo quadro compatível OPC-UA tem sido investigado e descrito [3], [4], [11]. Em tal forma, aqueles podem ser utilizados e acedido por sistemas OPC-UA.

OPC-UA não só é desenvolvido para a comunicação com aplicativos de gerenciamento de produção e empresariais, mas também para PLCs e dispositivos de processo. Numa aplicação, os autores demonstram que OPC-UA ANSI C pilha pode ser movido para um sistema embarcado com não-janelas com base sistema operativo [5].

Uma aplicação bem sucedida utilizando OPC-UA com MODBUS é apresentada pelos autores de [37], em que uma estratégia é descrita para controlar e monitorizar um grande sistema de ar condicionado. Este artigo demonstra como multilateral UPC-UA pode ser usado, com diferentes protocolos de comunicação.

OPC-UA não é apenas uma arquitetura cliente-servidor para indústrias de automação e de processo. A investigação por Maka et al. [15] demonstra o uso multilateral. O objeto estrutura orientada é desenvolvido para um sistema de informação para dar aos clientes usando verdadeira transporte público

informações e para fornecer para o viajante a via ótima e para identificar problemas, por exemplo, que um barramento é retardada ou para determinar a taxa de utilização corrente [15].

Questões relativas à segurança são importantes, como instalações de automação de processo e deve ser operado com PCs e software padrão. Portanto, as questões que são discutidas nas tecnologias de informação de área (TI) estão se tornando problemas em indústrias de processo e automação também. Existem várias investigações sobre este tema.

OPC-UA tem um modelo de segurança incluído como descrito na seção anterior; no entanto, como afirmou isso pode não ser suficiente para defender todas as ameaças [31], que são conhecidos por ataques na Internet e para a web-services. Nesta investigação [31] uma estratégia de segurança é apresentado e built-in estratégia de segurança OPC-UA. Um módulo foi proposto que pode ser configurado para os diferentes níveis de exigências de segurança.

Ao usar XML Web-services OPC-UA para a transferência de dados do processo, em seguida, navegador web seria uma possibilidade interessante para monitorar e exibir os dados [1]. No entanto, o navegador da Web, o que aceitar e usa a funcionalidade XML também para operar recursos de segurança, a fim de ser aceito em indústrias. A cifra e decifrar algoritmos têm para executar

funções matemáticas complexas, que não era a intenção original de XML. Os autores métodos presentes em JavaScript para melhorar e superar esta situação [1].

Os restantes dois documentos mostram que OPC-UA também recebe atenção de outras organizações. Tal como mencionado na secção anterior, a base OPC coopera com PLCopen. No primeiro artigo [17] é descrito um método para traduzir IEC 61131-3 modelos de software para o modelo de informação de OPC-UA. Mais uma vez, XML é a chave para esta conversão. Este trabalho também demonstra que OPC-UA tornou-se muito mais do que uma especificação de cliente-servidor simples.

O último documento mostra que o modelo OPC-UA pode ser usado como um modelo alternativo para o IEC 61850 para *Inteligente Automação Grid*. Os resultados apresentados pelos autores [12] proporcionam várias vantagens, também em segurança e de comunicações e mostra a capacidade de utilização da especificação OPC-UA.

V. C ONCLUSÕES

Este artigo fornece uma introdução ao *OPC (OLE para o controlo do processo)* e *OPC Unified Architecture*. O significado da sigla OPC mudou nos últimos anos para *Abertura, produtividade, colaboração*. interessante e investigações importantes e pesquisa utilizando e reforçando o OPC foram apresentados. A nova especificação OPC-UA também se tornou um padrão internacional - IEC 62541 e atrai pesquisa e diferentes organizações como a PLCopen. As investigações recolhidos e brevemente descritos mostram que OPC-UA não é apenas uma área para indústrias, mas deixar um monte de espaço para a academia, bem como, tais como segurança, sistemas embarcados ou aplicações interessantes.

R EFERÊNCIAS

[1] Braune A., Henning S., Hegler S., Avaliação de OPC UA segura Comunicação em aplicativos de navegador Web. (2008). A Conferência IEEE Internacional sobre Informática Industrial (Indin 2008) Daejeon, Coreia. [2] Burke T. OPC UA constrói em segurança funções. www.automationworld.com/feature-2642 [3] Hannelius T. Integração de Sistemas de Informação Industriais com OPC UA - Uma referência Java à Implementação Tese de Mestrado, Universidade de Tecnologia de Tampere, 2009. [4] Hannelius T. Salmenperä M., Kuikka S. (2008) Roteiro a adopção OPC UA. A Conferência IEEE Internacional sobre Informática Industrial (Indin 2008) Daejeon, Coreia. [5] Hannelius T., M. Shroff, Tuominen P. Incorporação de OPC Unified Architectura [6] IEC 61131-3 (2003) programáveis controllers- parte 3: Linguagens de programação, Electrotécnica Internacional Comissão [7] IEC / EN 61508 (2010). Norma: 61508 Segurança funcional de elétrico eletrônico programável sistemas de segurança Part1-PEÇA7 eletrônico, Genebra [8] Iwanitz F., J. Lange OPC, Grundlagen, und implementação Anwendung. (OPC Fundamentals, Implementação e Aplicações) 2.ed. Hüthig 2002 [9] Iwanitz F., J. Lange, fundamentos OPC, implementação e aplicação. 3ed. Heidelberg: Hüthig de 2006

[10] Kondor R. OPC Tunneling dados aumenta a disponibilidade, Matrikon, Inc. 2007 [11] Lange J., Burke TJ, Iwanitz F., von OPC de acesso a dados bis Unified Architectura. 4 Ed. Berlin, VDE-Verl., 2010 [12] Lehnhoff S., Mahnke W., Rohjans S., Usilar M., (2011), IEC 61850 com base OPC UA Comunicação - O Futuro da Smart Grid Automation. 17ª Conferência Computação Systems, Estocolmo na Suécia. [13] Liu T. Cai G. Peng X., design de software OPC Server no DCS. Proceedings of the 4, 2009ª Conferência Internacional sobre Computer Sciencne e Educação de 2009. [14] Mahnke W., Leitner S.-H., Damm M. OPC Unified Architecture, Springer Verlag Berlin Heidelberg, 2009 [15] Maka A., Cupek R., J. Rosner OPC UA orientada a objectos para Modelo Sistema de Transporte Público. UKSim 5ª Simpósio Europeu sobre Computação Modelagem e Simulação 2011.IEE Computer Society [16] Michaud A. Criando Arquiteturas OPC seguros, Matrikon, Inc. de 2007 [17] Miyazawa I., M. Murakami, Mutsukuma T., K. Fukushima, Maruyama Y., Matsumoto M., Kawamoto J., Yamashita E., OPC UA Information Model, troca de dados, segurança e segurança para IEC 61131-3. Conferência SICE Anual de 2011, Waseda Universidade de Tóquio, Japão. [18] Murphy E. OPC Segurança - Melhor prevenir que remediar. Matrikon Inc. de 2006 [19] OPC Foundation, OPC AE 1,1 Especificação, 2002 [20] OPC Foundation, OPC Lote Interface Specification, 2002 [21] OPC Foundation, OPC Comandos 1.00 Especificação de 2004 Draft [22] OPC Foundation, OPC DA 3.00 Especificação de 2003 [23] OPC Foundation, OPC DX 1,00 Especificação, 2003 [24] OPC Foundation, OPC HDA 1,0 Especificação, 2003 [25] OPC -Foundation OPC Overview OPC - fundação 1998 [26] OPC Foundation, OPC XMLDA 1.01 Especificação de 2004 [27] OPC Foundation, OPC Unified Architecture Specification Parte 2 Modelo de Segurança, Version1.01 fevereiro 2009 [28] OPC Foundation, OPC Unified Architecture Specification Parte 6 Mapeamentos, Version1.01 fevereiro 2009 [29] PLCopen, OPC UA Information Model para IEC 61131-3, http://www.plcopen.org/pages/tc4_communication/index.htm (Visitou 09.2013) [30] Reissenweber B. Feldbussysteme, 1998 [31] Renjie Huang, Feng Liu, Dongbo Pan, Research on OPC UA Segurança. 2010. 5ª Conferência IEEE em Eletrônica e aplicações industriais [32] Sahin C., Bolat ED Desenvolvimento de controle remoto e monitoramento de web-based sistema distribuído de OPC. Padrões e interfaces de computador 31, 2009, pp. 984-993 [33] Schwarz MH, Börcösk J., Adiantamentos de OPC Client Server Arquiteturas para estratégias de manutenção - uma área de pesquisa e desenvolvimento não apenas para indústrias. Transações WSEAS em Sistemas e Controle no.3 vol. 3 2008. pp 195-207 [34] Filho M. Yi M.-J. Um Estudo sobre OPC Especificações: Perspectiva e Desafios. INFOST 2010 Proceedings. 2010 [35] Stopper M., orientados Servie Katalinic B. Aspectos projeto de arquitetura de OPC UA para aplicações industriais. Proceedings da multiconferência internacional de cientistas de Computação 2009 Vo II Imecs 2009, Hong-Kong. [36] Tan VV, Yoo D.-S. e Yi M.-J. Desenho e Implementação de Web Serviços usando OPC XML-DA e OPC Data Complexo para automação e sistemas de controle. (2006). Proceedings of the 6ª IEEE Conferência Internacional sobre Informática e Tecnologia da Informação. (CIT06) [37] Tu, NTT, Thang HQ (2013) Projeto e Desenvolvimento da Air Sistema de Condicionamento usando OPC UA Especificações e protocolo Modbus. IEEE 8ª Conferência sobre Eletrônica e aplicações industriais [38] Yin Y., Zhou B. A Análise e Pesquisa da OPC XML-DA Server. Energia Procedia 16 (2012) (seleção de 2012 Conferência Internacional sobre Energia do Futuro, Meio Ambiente e Materiais) pp. 1535-1540