XX SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

Versão 1.0
XXX.YY
22 a 25 Novembro de 2009
Recife - PE

GRUPO - V

GRUPO DE ESTUDO DE PROTEÇÃO, MEDIÇÃO, CONTROLE E AUTOMAÇÃO DE SISTEMA DE POTENCIA -GPC

AVALIAÇÃO DE DESEMPENHO DE SEGURANÇA CIBERNÉTICA NO PROTOCOLO IEC-61850 ATRAVÉS DE ANALISE DE FLUXO UTILIZANDO O CONCEITO DE PICOM (PIECE OF COMMUNICATION)

Ubiratan Alves do Carmo (*)
COMPAHIA HIDRO ELETRICA DO SÃO FRANCISCO

RESUMO

Hoje em dia, grandes empresas - particularmente aquelas cuja atividade envolve infra-estrutura crítica como geradoras de energia, telecomunicações, água e esgoto, transporte coletivo, óleo e gás - enfrentam desafios na área de segurança de suas redes. De um lado, existe a ameaça real do terrorismo cibernético e de falhas de segurança involuntárias e/ou maliciosas. No outro lado, existe a pressão para melhorar o desempenho financeiro das empresas através da integração fácil das operações.

Alguns autores consideram que a única solução para estes problemas é voltar a operar como antigamente, onde as redes e os sistemas ficavam totalmente isolados do resto do mundo. Outros autores discordam desse ponto de vista e rebatem dizendo que se a meta é diminuir a ineficiência e auxiliar o processo produtivo, é essencial estar "conectado" com o mundo [01].

A implementação de técnica de segurança nos protocolos industriais significa na garantia da integridade e confiabilidade das mensagens. Integridade de mensagem significa que a mensagem chega ao seu destino sem modificações ou substituição não autorizadas durante sua jornada. O uso de métodos de autenticação e criptografia elimina este tipo de problema. O uso da criptografia demanda um enorme poder computacional e pode comprometer o requisito de tempo de quatro milissegundos para transmissão das mensagens de sistemas críticos.

O foco deste trabalho é analisar o impacto do uso do conceito de certificado para mensagens do protocolo IEC-61850 especificado na norma IEC-62531-6 utilizando o conceito de analise de fluxo de mensagens na rede utilizando o conceito de PICOM - *Piece of Information of Communication*

PALAVRAS-CHAVE

IEC 61850, Segurança, Certificado de Mensagens, PICOM, Analise de Fluxo

1.0 - INTRODUÇÃO

A necessidade de proteção dos sistemas críticos de um ataque cibernético é uma realidade esta cada vez mais presente nos dias atuais. As redes de computadores e dispositivos eletrônicos inteligentes que se assemelham aos computadores pessoais já são elemento encontrado em abundancia nos sistemas de automação e controle dos sistemas críticos. Por outro lado a necessidade de difundir as informações por diversos setores das empresas leva um numero crescente de redes interligadas. No caso das grandes empresas de energia elétrica já existe uma infaestrutura de rede de comunicação própria que atende a demanda corporativa e dos dados do processo de geração e transmissão de energia elétrica. No passado os sistemas de controle tinham sua segurança garantida

(*) CHESF – DOMC, Rua 15 de março n˚ 50 – sala B 205 - Anexo B – CEP 99.999-999 Recife, PE, – Brasil
Tel: (+55 81) 3229-4171 – Fax: (+55 81) 3229-4243 – Email: uacarmo@chesf.gov.br

pelo o isolamento. As arquiteturas destes sistemas eram constituídas de um computador com sistema operacional privado que rodava o aplicativo do sistema de controle e aquisição de dados - SCADA que se comunicavam em uma forma hierárquica com as unidades terminais remotas – UTR. Esta comunicação era de forma serial e utilizando uma infraestrutura de comunicações própria. O conhecimento destes sistemas era compartilhado por poucos especialistas dos fabricantes e das empresas de energia elétrica. Atualmente os aplicativos SCADA rodam em sistemas operacionais de uso geral tais como: Windows e linux e usam redes TCP/IP que são conhecidos por toda comunidade de hackers e curiosos e que podem utilizar todo arsenal de ferramentas de invasão e de elementos maliciosos já conhecido e praticado nas redes de gestão corporativa. Dentro deste contexto e do estado de conflito que mundo esta passando que tem como conseqüência atos de terrorismo já conhecido por todos. Neste contexto existe a necessidade de se conhecer as vulnerabilidade e eliminar as ameaças dos sistemas críticos com a finalidade de evitar situações de ameaças catastróficas para a humanidade. Várias entidades votadas à questão segurança e de normatização estão desenvolvendo normas e critérios para segurança dos sistemas críticos nos países do primeiro mundo.

No cenário da evolução tecnológica dos SAS esta em desenvolvimento e em implantação o protocolo IEC 61850 que é um novo protocolo de comunicações de dados que tem como principal propósito resolver a questão de interoperabilidade entre IEDs de diversos fabricantes instalados nos sistemas de automação de subestações – SAS. Este protocolo tambem trata a questão da padronização dos dados através do modelo de orientação a objeto de nome padronizado e de funções denominadas de nós lógicos – LN que são manipulados por serviços abstratos [2]. Apesar de este protocolo resolver diversas questões da área de comunicação dos SAS ele não trata e nem padroniza a questão da segurança destes sistemas.

O IEC esta elaborando a norma IEC 62351 que trata a questão da segurança para protocolos de comunicação de automação. Em particular a parte seis desta norma trata a segurança no protocolo IEC 61850 utilizando técnica de assinatura digital das mensagens. O acréscimo de mecanisno de segurança tanto na confiabilidade quanto na garantia da integridade das mensagens consome poder computacional dos processadores dos IEDs. A segurança na area de gestão ja foi estudas e implantadas varias técnicas de segurança nos sistemas e aplicativos dos sistemas desta área. Os bancos fazem operações envolvendo elevadas cifras de forma automática utilizando redes de computares TCP/IP. As mesmas técnicas de segurança dos sistemas bancário podem ser aplicadas nos SAS. Então qual é o problema ? O problema é o requisito de tempo necessário para operar em tempo real dos sistemas críticos. No caso dos SAS o tempo necessário para transmitir uma mensagem critica é de 4 milissegundos. Neste caso o processador do IED ainda não possui memória e nem capacidade computacional suficiente para calcular os algoritmos de criptografia necessários para garantir a integridade e confiabilidade das mensagens.

Os fluxos de dados nas redes dos SAS são afetados principalmente pela topologia da rede, da distribuição do LN nos IEDS e do tipo de falta no sistema elétrico [03]. Um bom projeto de SAS deve considerar todos estes requisitos e a capacidade de ampliação deste sistema de forma que o mesmo seja escalavel, quando do projeto da arquitetura de rede deste sistema. Estudos do modelo de trafego de forma que elimine os engarrafamentos que ocasionam atrasos de forma que a vazão atenda ao requisito de tempo necessários dos SAS, no estado atual do projeto e de futuras ampliações do mesmo. A inclusão de mecanismos de segurança degrada a performance destes sistemas e a arquitetura de rede necessita ser cuidadosamente estudada de forma a garantir a performance dos requisitos de tempo dos mesmos.

O objetivo deste artigo é mostrar a solução de segurança proposta pela norma IEC e avaliar o impacto desta solução nos requisitos de tempo, utilizando como modelo uma subestação do tipo T2-2. O item 2.0 deste artigo dará uma pequena introdução no conceito de PICOM, apresentaremos a solução proposta de segurança da norma IEC 62531, o cenário de teste e os resultados encontrados e finalmente no item seguinte as conclusões.

2.0 - INTRODUÇÃO AO PICOM

Neste item abordaremos o conceito de PICOM e os seus requisitos básicos, a norma IEC 62531 apresenta a solução de assinatura digital para as mensagens criticas do protocolo IEC 61850, também apresentamos um caso de calculo de fluxo em uma subestação de transmissão do tipo T2-2 com uma discussão dos resultados encontrados.

2.1 Abordagem sobre *Piece of Information of Communication* - PICOM

O sistema de comunicações de subestação é utilizado para realizar varias funções dentro do modelo de comunicação do protocolo IEC 61850. As Funções são divididas em nós lógicos. A comunicação entre todos os nós lógicos constrói a malha de comunicação entre os IEDs. Os nós lógicos realizam a troca de informação

através de conexões lógicas. Neste modelo a comunicação pode ser decomposta em objetos que trocam de informações.

A troca de dados pode ser representada por pedaços de informação denominada de PICOM. Este pedaço de informação de comunicação não é um procedimento real de comunicação e nem um formato de transmissão de dados [03]. O PICOM é uma descrição abstrata de comunicação sob o ponto de vista de requisitos de desempenho de comunicação e de informação. A troca de dados convencional é focada na organização e no formato dos dados. O protocolo IEC 61850 tem como principio a orientação ao objeto e a troca de dos dados é voltada para os dados e objetos. Neste protocolo a troca de informação é considerada sob o ponto de vista de função, portanto o processo de troca de dados leva em consideração o emissor e o receptor dos dados, atributos de dados da transmissão, requisitos de tempo, precisão da troca de dados e como o dado que chega ao seu destino (integridade e confiabilidade). O PICOM descreve a troca de dados sendo independente dos dispositivos físicos e não representa estruturas e formatos dos dados que são transmitidos na rede dos SAS [02].
A parte cinco da norma IEC 61850 define PICOM como a descrição da troca de informação com atributos de comunicação entre dois nós lógicos. O conceito de PiCOM foi introduzido pelo grupo de trabalho 34.03 do Cigré através da brochura 180.

Os principais componentes ou atributos do PICOM são sumarizados a seguir:

- Dados - significa o conteúdo das informações e as identificações necessárias a função;
- Tipo – descreve a estrutura de dados se é um valor analógico ou um valor binário se é um valor simples ou um conjunto de dados;
- Desempenho – significa o possível tempo de transmissão, integridades dos dados e o método ou causa da transmissão;
- Caminho – contem a função lógica da fonte e a função lógica do destino.

2.1.1. Requisitos de Desempenho das Mensagens

A comunicação entre os nós lógicos é realizada através de milhares de pedaços de comunicação (PICOMs). É provável que exista similaridade entre vários PICOMs. Por exemplo todos PICOM que descrevem trip da proteção, alem de praticamente possuir a mesma fonte tem mais ou menos requisitos de comunicação idênticos [03]. A classificação de PICOM permitirá uma visão geral dos requisitos e o suporte a um forte modelo e uma definição do desempenho das solicitações das mensagens.

O tempo de transmissão das mensagens é composto do tempo gasto no trajeto do canal e os tempos de manipulação dos dados em ambos os terminais. A contagem de tempo é iniciada no momento que o transmissor coloca os dados na pilha de transmissão e o receptor retira os dados na pilha de recepção. A inclusão de algoritmos de segurança com o intuito de proteger as mensagens aumenta o tempo de manipulação de dados o que compromete o requisito de tempo de quatro milissegundos exigidos pelos SAS. A Figura 01 ilustra os tempos de transferências de dados no protocolo IEC 61850.

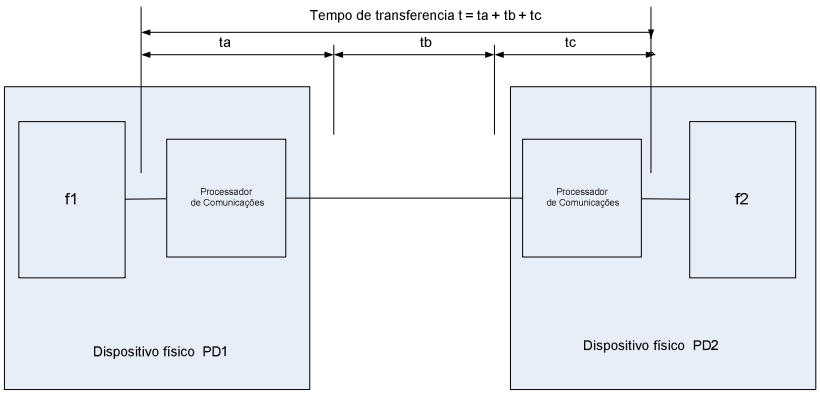

FIGURA 1 – Definição dos tempos de transferência de dados do IEC 61850

2.1.2 Tipos de Mensagens e Classes de Desempenho

Para atender a diferentes requisitos das subestações os tipos de mensagens são classificados por classes de desempenho. Existem dois grupos diferentes de classe de desempenho, um para proteção e controle e outro para medição e qualidade de energia. As classes de desempenho são definidas baseadas nas necessidades da funcionalidade portanto, estas classes independem do tamanho da subestação. A tabela 1 ilustra as classes de desempenho do protocolo IEC 61850.

Tabela 1 – Classes de Desempenho associadas ao PICOM

Controle e proteção	P1	Aplica-se tipicamente aos Bays de distribuição ou Bays de baixo requisito
	P2	Bays de transmissão ou qualquer outro Bay especificado pelo usuário
	P3	Aplica-se aos Bays de transmissão onde é necessário um desempenho elevado.
Medição e Qualidade de Energia	M1	Medidores de classe 0.5 e 0.2 e resposta em freqüência até o 5º harmônicos
	M2	Medidores de classe 0.5 e resposta de freqüência até o 13 º harmônico
	M3	Medidores de classe 0.2 e resposta de freqüência até o 40 º harmônico

As mensagens no contexto do PICOM são especificadas por tipo. Existem sete Tipos de mensagem e são denominadas de Tipo 1, ..., Tipo7.

- Tipo 1 – mensagens rápidas, o conteúdo deste tipo de mensagem pode ser um simples código binário contendo dados, comandos ou mensagens simples. Este tipo de mensagem é subdividido em mensagem de tipo 1A e tipo 1B;

    - Mensagem tipo 1A Trip – é a mensagem mais importante no ambiente de subestação e por conseqüência é a mensagem que tem a maior exigência de requisitos. As mensagens de inter-travamento, intertrip e discriminação de lógica também tem o mesmo requisito. Para a classe de desempenho P1 o tempo total de transmissão da mensagem é da ordem de meio ciclo sendo que o tempo de 10 ms foi adotado como referencia. Nas classes de desempenho P2 e P3 o tempo total de transmissão é da ordem de um quarto de ciclo e valor de 3 ms é adotado como referencia.

    - Mensagem do tipo 1B (demais mensagens) – este tipo de mensagem também é importante para outras funções nos sistemas de automação de subestação mas demanda um requisito de tempo menos rígido. Para as classes de desempenho P1 o tempo total de transmissão tem como referencia o valor de 100 ms. Para as classes de desempenho do tipo P2 e P3 o tempo total de transmissão da mensagem é de um ciclo e o valor 20 ms é definido como referencia.

- Tipo 2 – mensagens com velocidade média – são mensagens importantes para o SAS mas que tem menos exigência de requisito de tempo. O IED deve ter o seu próprio relógio interno e colocar um tarja de tempo nos dados que será transmitido. O requisito de tempo para este tipo de mensagem é de 100 ms.

- Tipo 3 – mensagem de baixa velocidade – são mensagens com um determinado grau de complexidade e que necessita do uso de tarja de tempo associada. Podemos citar como o exemplo mensagens de funções de autocontrole, transmissão de registros de eventos, leitura ou mudanças de *set points* e de apresentação de dados. Alarmes, manipulação de eventos e medidas de grandezas não elétricas (por exemplo temperaturas) também utilizam este tipo de mensagem. É considerado como referencia do tempo total de transmissão para este tipo de mensagem o valor de 500 ms.

- Tipo 4 – mensagem de dados brutos – este tipo de mensagem inclui saída de dados de transdutores e transformadores para instrumentos eletrônicos – TES. Estes dados são formados por um fluxo de dados

sincronizados continuo fornecido por um IED intercalado por dados de outro IED. A tabela 02 ilustra os requisitos de tempo definido para este tipo de dados.

Tabela 2 – Dados brutos para proteção e controle

Tipo de Dados	Classe	Tempo de transmissão (mseg) Definido por tempo de trip	Resolução (Bits) Amplitude	Taxa (Amostra/seg) Fequencia
Tensão	P1	10,0	13	480
Corrente			13	
Tensão	P2	3,0	16	960
Corrente			16	
Tensão	P3	3,0	16	1920
Corrente			18	
Tensão	M1	Classe 0.5 (IEC 62053-22) Classe 0.2 (IEC 60044-8) Até to 5º harmônico	12	1500
Corrente			14	
Tensão	M2	Classe 0.2 (IEC 62053-22) Classe 0.1 (IEC 60044-8) Até to 13º harmônico	14	4000
Corrente			16	
Tensão	M3	Classe 0.1 Não está definido pelo IEC Até to 40º harmônico	16	12000
Corrente			18	

- Tipo 5 – transferência de arquivos – este tipo de dados tem como finalidade transferência de arquivo de dados volumosos. Por exemplo, dados de oscilográfia, dados de informação genérica e dados de configuração. Estes dados são divididos em blocos de comprimento limitado, para permitir outras atividades na rede. O comprimento típico do bloco é de 512 bits.

- Tipo 6 – mensagens de sincronização de tempo. Este tipo de mensagem e usada para sincronizar o relógio interno dos IEDs nos SAS. Dependendo da aplicação. Por exemplo, tarja de tempo de eventos ou exatidão de amostragem de dados brutos diferentes níveis de exatidão são requisitados. No caso para tarja de tempo de eventos o valor de referencia é de 1ms e de 0,1 ms para traja de tempo de cruzamento pelo zero e suporte a verificação de sincronismo (*synchrocheck*).

- Tipo 7 – mensagens de comando. Este tipo de mensagens é usado para realizar ordem de controle emitida por interface homem maquina (IHM) local ou remota. Estas mensagens são baseadas nas mensagens de tipo 3 acrescidas de procedimento de verificação de controle de acesso. Este tipo de mensagem também pode ser emitido no nível de controle de bay dos SAS e neste caso podem ser consideradas mensagens de tipo 1.

3.0 - SEGURANÇA CIBERNETICA EM SISTEMAS DE AUTOMAÇÃO DE SUBESTAÇÃO.

As arquiteturas dos SAS utilizam as redes de computadores como o principal meio de transporte dos dados necessários para execução das funções de proteção, automação e controle de uma subestação. Os reles de proteção e controle (IEDs) têm sua arquitetura interna cada vez mais próxima da arquitetura de computadores utilizados para a informática pessoal e corporativa. Este fato permite que todo arsenal já desenvolvido para atividades maliciosas podem ser usados para invadir, interceptar, mascarar, negar serviço aos SAS. Os conflitos mundiais são fatos que ninguém pode negar e interesses escusos de indivíduos com a finalidade de demonstrar insatisfação pessoal, espionagem e terrorismo podem submeter os SAS a ataques de segurança cibernética. Órgãos governamentais, instituições de normatização e pesquisas, fabricantes e a comunidade de automação em geral vêm desenvolvendo esforços para criar políticas, normas e padrões voltados para proteção de sistemas de automação de serviços considerados de funções críticas para humanidade.

Técnicas de criptografia e todos os mecanismos de proteção contra ataques cibernéticos desenvolvidos para a informática pessoal e de gestão ainda não podem ser utilizados na área de SAS decorrente aos requisitos de tempos necessários para execução das funções destes sistemas. Uma autenticação bancaria pode levar alguns segundos para ser realizada e é considerada aceitável. Nos SAS operações de segundo são totalmente fora de propósito conforme já foi ilustrado no item dois deste artigo.

A implementação de mecanismo de segurança nas mensagens já é do convívio de todos. A inclusão do bit de paridade é uma forma rudimentar de oferecer segurança nas mensagens. Para garantir os fundamentos básicos de segurança como a confiabilidade, não repudio e integridade das mensagens são necessários algoritmos e técnicas mais elaboradas. O principio básico é criar uma chave de segurança de forma que sua quebra leve um tempo que praticamente seja impossível dentro do limite de tempo necessário para o sucesso da atividade maliciosa.

A norma IEC 61850 não regulamenta a questão da segurança para este protocolo e para resolver esta questão o IEC esta emitindo a norma IEC 62531 sobre segurança de dados e comunicação. A parte seis, “Segurança para o *Profiles* IEC 61850”, trata especificamente o protocolo IEC 61850 . Esta norma cobre todos os *profiles* da IEC 61850-7-2 que não são baseados em TCP/IP, GOOSE, GSSE e SMV. Esta parte define que na implementação de segurança nas mensagens GOOSE e SMV define estender o frame ethernet para incluir assinatura digital nas mensagens GOOSE e de valores amostrados *(Sample Value*). A inclusão de uma extensão nestas mensagens provoca o aumento do seu tempo de transmissão. O tempo total de transmissão destas mensagens deve levar em consideração o tempo de transmissão da mensagem propriamente dito, o tempo de calculo de criptografia da assinatura digital na transmissão incluindo na recepção o tempo gasto pelo algoritmo de calculo da validação da assinatura digital incluindo o tempo gasto na decriptografia. O aumento do tempo total provoca uma queda no desempenho no atendimento do requisito do tempo ilustrado na tabela 02 necessário para as mensagens GOOSE e SV. A figura 02 ilustra a unidade de dados de protocolo – PDU do GOOSE com seu campo de informação estendido.

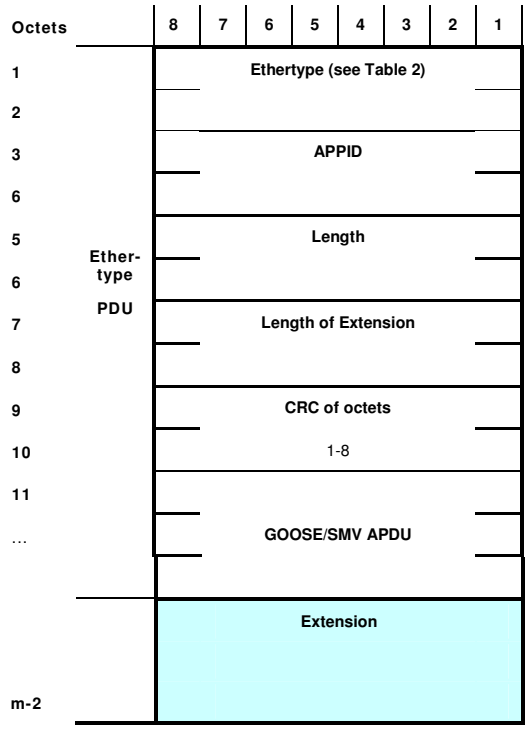

FIGURA 2 – Detalhe da extensão da unidade de dados PDU da mensagem GOOSE

4.0 - CENARIO DE CALCULO DOS FLUXOS DE DADOS UTILIZANDO O PICOM.

O cenário de calculo escolhido foi o mesmo cenário de falta de uma subestação do tipo T2-2 ilustrada

como exemplo na norma IEC 61850-5. A escolha deste cenário foi decorrente que no exemplo desta parte da norma já existem valores de desempenho para as mensagens diante de uma falta sem levar em consideração a extensão dos PDUs das mensagens GOOSE. Estes valores servem como valores referenciais para o calculo do fluxo realizado neste artigo. A figura 03 ilustra o cenário do tipo T2-2

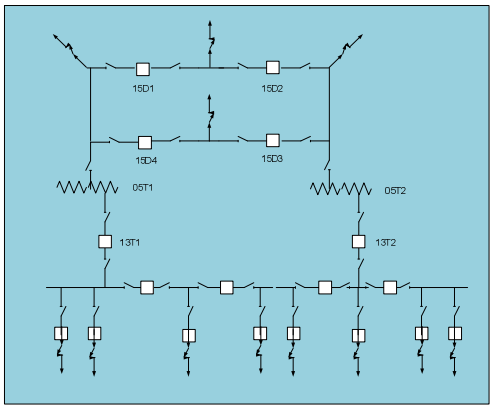

FIGURA 3 – Subestação de transmissão tipo T2-2

O cenário de calculo apresenta uma subestação de transmissão de 345 kV / 138 kV, seu arranjo é formado por dois transformadores de 345/138 kV, quatro linhas de 345 kV e oito alimentadores de 138 kV. As linhas de transmissão são formadas por quatro torres que suportam duas linhas de 138 kV e uma linha de 345 kV. As proteções das linhas de 345 kV são formadas por dois sistemas de proteção constituídos de dois reles microprocessado as linhas de 138 kV são formadas por um único sistema de proteção constituído de dois reles microprocessados. A arquitetura da rede de IEDS considerou uma única rede para interligar todos os IEDs dos sistemas de proteção deste cenário. Na simulação considerou-se a queda simultânea de duas torres das linhas de transmissão ocasionando a falta em duas linhas de 345 kV e quatro de 138 kV.

O calculo dos fluxos de dados é realizado dividindo-se o comprimento da mensagem pelo requisito de tempo definido na IEC 61850-5 e na brochura nº 180 do WG 34.03 do Cigré. O fluxo de dados foi calculado para o cenário de falta descrito acima e considerou que todas as mensagens iniciaram no mesmo instante t0. Também não foi considerado a utilização dos bits de prioridades no quadro ethernet. O numero total de IEDs na rede para atender os sistemas de proteção das linhas sob falta são de 47 IEDs. A figura 04 ilustra um fragmento da planilha que mostra as mensagens emitidas e o fluxo de dados no momento da falta para a situação ponto a ponto e multicast.

PICOM		PEER to PEER						MULTICAST					
		SOURCE	SINK	Extender	SLV	TIME(ms)	FLOW(bytes/seg)	SOURCE	SINK	Extender	SLV	TIME(ms)	FLOW (bytes/seg)
Line 1 345 kV System 1 Relay1	Trip Breaker X1	PLDIS	CSW	200	1	1	201000	SOBRO	SIBRO	200	2	1	202000
	Initiate Auto Reclose X1	PLDIS	RARU	200	1	1000	201						
	Initiate Breaker Fail Protection X1	Pxxx	RBFP	200	1	1	201000						
	Trip Breaker X2	PLDIS	CSW	200	1	1	201000						
	Initiate Breaker Fail Protection X2	Pxxx	RBFP	200	1	1	201000						
	Trip 138kV Transformer Breaker	PLDIS	CSW	200	1	1	201000						
	Initiate Breaker Fail Protect Transf BrKr	Pxxx	RBFP	200	1	1	201000						
	Stop Block on DCR or Start PTT on PTT Comm Channels (System 1 only)	PLDIS		200	1	10	20100						
	Send DTT on DTT Comm Channel	PLDIS		200	1	5	40200						

FIGURA 4 – Mensagens PiCOM emitidas no momento da falta e o fluxo de dados produzidos

Este artigo não considerou uma técnica ou algoritmo de proteção especifico e sim a aplicação de redundância no

quadro ethernet através da extensão do seu tamanho original até o valor de 200 bytes por mensagens a figura 05 ilustra o fluxo total da rede calculado para a falta definida no cenário considerando o uso de troca de informação ponto a ponto e multicast.

Security			
Byte	Flow Peer to Peer	Flow Multicast	%
0	62,312.00	76,000.00	21.97%
20	1,308,552.00	836,000.00	-36.11%
40	2,554,792.00	1,596,000.00	-37.53%
60	3,801,032.00	2,356,000.00	-38.02%
80	5,047,272.00	3,116,000.00	-38.26%
100	6,293,512.00	3,876,000.00	-38.41%
120	7,539,752.00	4,636,000.00	-38.51%
140	8,785,992.00	5,396,000.00	-38.58%
160	10,032,232.00	6,156,000.00	-38.64%
180	11,278,472.00	6,916,000.00	-38.68%
200	12,524,712.00	7,676,000.00	-38.71%

FIGURA 5 – Total de fluxo na rede para a falta considerando a queda em duas torres consideradas no cenário

5.0 - CONCLUSÃO

O uso do PICOM permite a possibilidade de realizar uma avaliação do fluxo total na rede para um determinado cenário de falta independente da tecnologia de rede aplicada ou de seu modelo das camadas associadas ao modelo. O PICOM não calcula vazão e nem retardos na rede, mas possibilita tirar conclusões de que uma rede que opera no limite ou na capacidade superior de sua banda provavelmente terá problemas de engarrafamentos e retardos. Na figura 05 podemos observar que para o tipo de falta especificado no cenário qualquer tipo de algoritimo de proteção ou criptografia que aplicar uma extensão de 200 bytes supera a capacidade de rede 10 megabits/seg.

A norma 62531 sugere o uso da assinatura digital para garantir a integridade e confiabilidade das mensagens GOOSE e SMV. A aplicação do conceito de *message digests* é bastante interessante tendo em vista que podemos comprimir uma mensagem de comprimento elevado em apenas 160 bits (vinte bytes) de forma que a extensão do PDU do GOOSE será acrescido apenas deste valor o que compromete menos o desempenho da rede.

O uso de mecanismo de proteção das mensagens é necessário para garantir a integridade e confiabilidade das mesmas de forma a proteger os sistemas críticos de possíveis ataques terroristas. As arquiteturas de rede devem levar em consideração a degradação dos tempos de transmissão decorrente à inclusão das proteções das mensagens. Substituído o formato das mensagens GOOSE e SMV pelo PICOM é possível realizar analise dinâmica em simuladores de redes de forma a se realizar analise de atrasos e engarrafamento na rede ficando este fato como sugestão do autor para futuro trabalhos.

6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) Carmo, Ubiratan; att All; Segurança da Informação em Redes de Controle e Automação. Simpósio de Automação de Sistemas Elétricos, 2007. 8 p.

(2) IEC-61850; part 5: Communication networks and systems in substations - Communication requirements for functions and device models, First edition 2003-5.

(3) WG 34.03 Cigré brochrure 180; Communication Requirements in Terms of Data Flow within Substations. February 2001.

7.0 - DADOS BIOGRÁFICOS

Ubiratan Alves Carmo. Graduado Engenharia Elétrica - 1979, Mestre em Ciência da Computação - 2003 pela Universidade Federal de Pernambuco, Especialista em Telecomunicações pela Universidade Federal Fluminense - 2005. Gerente da Divisão de Medição e Controle de Processo da Companhia Hidro Elétrica do São Francisco.