

Projeto SEAL - Sistema Especialista em Análise de Logs

Tema: Sistemas de Controle, Automação e Proteção

Autores: Ruã Luz Barbosa

Co-Autores: Leonardo Felipe Moreira, Alan Marques Ribeiro, Antonio Assumpção Viotti Flores

Empresa: Cemig Geração e Transmissão

Resumo

A operação remota das subestações da transmissão pelo Centro de Operação do Sistema (COS) exige que as informações das instalações tenham alta disponibilidade, de maneira que permita a operação do Sistema Interligado Nacional (SIN) pelo centro. Para isso, é necessária uma alta disponibilidade da infraestrutura que permite que esses dados sejam coletados dos equipamentos das instalações e disponibilizados aos equipamentos do centro. As equipes de manutenção devem trabalhar para manter essa infraestrutura e, em caso de falhas, identificá-las e corrigi-las de forma rápida e segura.

O Projeto SEAL foi idealizado para uma melhor análise das falhas de comunicação que impactam a teleassistência pelo centro de operação. A implantação do projeto nas instalações permite o monitoramento da comunicação entre a subestação e o COS para uma análise a nível de protocolo através de um analisador de rede, o Wireshark. Os logs de comunicação coletados permitem a identificação de falhas que passam despercebidas pelas equipes de operação, falhas que são reestabelecidas sem nenhuma ação, mas que podem ocorrer de maneira intermitente, impactando no indicador que mede a disponibilidade de comunicação das subestações.

1. Introdução

O modelo de operação das subestações da transmissão adotado pela CEMIG GT é o modelo teleassistido. Atualmente 100% das instalações da transmissão já são operadas dessa forma e essas instalações devem atender a critérios de disponibilidade definidos no submódulo 2.16 dos procedimentos de rede do ONS. A disponibilidade é medida através do indicador TELEASST, definido no módulo 9.6 dos procedimentos de rede, que indica o desempenho da teleassistência de uma instalação sem observar a assistência local. O indicador mede o percentual do tempo em que a instalação esteve teleassistida. O tempo de indisponibilidade é caracterizado pela indisponibilidade programada sem assistência local ou indisponibilidade não programada da telesupervisão ou telecontrole. O requisito mínimo do indicador TELEASST é de 99,90% para as instalações não estratégicas e de 99,95% para as instalações estratégicas.

A indisponibilidade de supervisão e controle de uma instalação pode ser causada por problemas na infraestrutura do Centro de Operação do Sistema (COS), na infraestrutura do sistema de telecomuni-

cações ou na infraestrutura da subestação. Esses problemas podem estar relacionados a travamentos, desligamentos acidentais ou falha na alimentação de equipamentos como conversores, remotas, switches, roteadores ou multiplexadores, por exemplo. As falhas também podem ser devido a desconexões ou rompimentos de cabos de rede ou fibras ópticas, ou, até mesmo, falhas devido a parametrização incorreta de equipamentos.

Após verificada a indisponibilidade de uma instalação, as equipes de manutenção da subestação, do sistema de telecomunicações e do COS são acionadas para que eles possam analisar, identificar e corrigir a falha. Algumas falhas podem ser facilmente identificadas pela equipe de manutenção através da verificação de um equipamento desligado, leds que indicam travamento ou ausência de conectividade em portas de rede. Outras falhas, no entanto, podem não serem fáceis de identificar, como falhas que ocorrem devido a perda de pacotes, ou falhas que normalizam antes mesmo de as equipes de manutenção realizarem o atendimento e fazerem uma inspeção visual, dificultando a identificação de qual equipamento falhou e qual a causa raiz. Para estes casos faz-se necessária a implementação de um monitoramento contínuo e que gerem dados para uma análise histórica pelas equipes de manutenção.

A comunicação entre o COS e a remota nas subestações da transmissão ocorre utilizando o protocolo IEC 60870-5-104 ou IEC 60870-5-101. Sendo o primeiro em padrão Ethernet e o segundo em padrão serial. As mensagens no protocolo IEC-101 são encapsuladas em pacotes TCP por um terminal server, instalado na subestação. A remota, já em protocolo IEC-104, ou o terminal server são conectados em switches do sistema de telecomunicações para que as mensagens cheguem ao centro de operação, seja por canais de enlace de fibra óptica, via ondas de rádio ou via satélite. Tendo o switch da rede operativa como porta de entrada do sistema de telecomunicações, as informações entre centro e instalação trafegam em pacotes TCP, possibilitando a utilização um analisador de protocolos, instalado nesse switch, para capturar todo o tráfego da comunicação e registrá-los em logs.

2. Desenvolvimento

O Projeto SEAL surgiu da necessidade de identificar, principalmente, a causa de falhas de comunicação que, além de curtas, normalizam sem nenhuma ação das equipes de manutenção. Essas falhas, em alguns casos, são classificadas como indeterminadas não sendo possível dizer se foi originada devido a problemas na infraestrutura da subestação, do sistema de telecomunicações ou do centro de operação, dificultando a proposição de ações de correções e melhorias por nenhuma das equipes de manutenção.

A arquitetura do projeto, conforme mostrada na Figura 1, consiste em instalar um servidor Linux com o software Wireshark (analisador de protocolos) nas subestações. Esse servidor é conectado aos switches do sistema de telecomunicações (switches DTI). Devido à redundância, a comunicação pode ocorrer tanto pelo Switch 1 quanto pelo Switch 2. Esses switches são conectados a remotas, terminal server ou a switches da rede de automação (switches AT). A porta de comunicação com a remota ou terminal server é espelhada em outra porta do switch e, nessa porta espelhada, é conectada a máquina do SEAL para a realização do monitoramento. A partir desse espelhamento o Wireshark captura e interpreta os pacotes de comunicação recebidos e enviados pela remota. Os logs dessa comunicação são salvos no servidor em arquivos, sendo cada arquivo gerado com seis horas de dados e excluídos do HD da máquina após 30 dias.

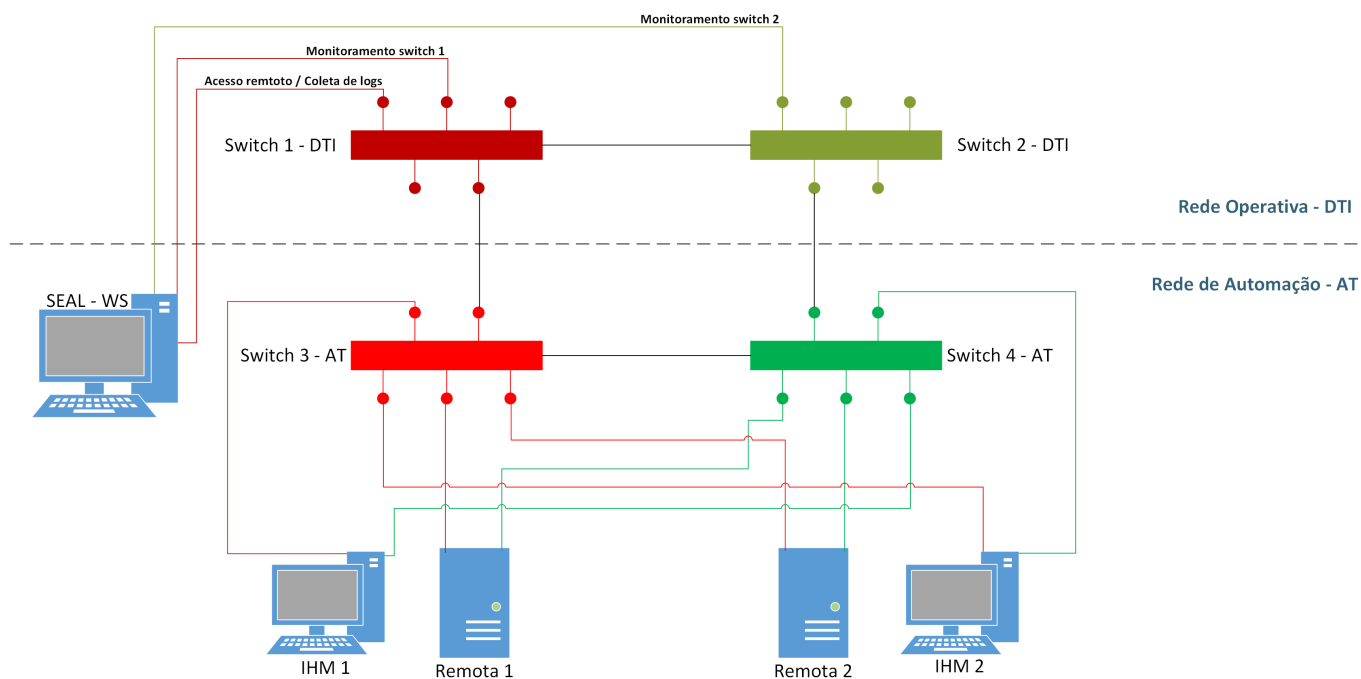


Figura 1 - Arquitetura básica do Projeto SEAL

A coleta dos logs do servidor do SEAL pode ser feita, através da rede operativa, a partir do acesso remoto a essa máquina por uma porta de rede dedicada. Esse acesso, atualmente, é feito por uma máquina, geralmente a IHM, dentro da própria subestação. Futuramente o acesso remoto poderá ser expandido para qualquer lugar que tenha um ponto da rede operativa, facilitando o acesso e análise pela equipe de engenharia da manutenção.

A partir da análise dos logs é possível visualizar os pacotes capturados pelo sistema de monitoramento, que mostram tanto os pacotes de comunicação como pacotes de outros serviços, como mostrado na Figura 2. Nesses pacotes é possível identificar o protocolo utilizado, o IP do equipamento que envia a mensagem e para qual IP ela está sendo enviada.

Além de visualizar as mensagens do protocolo IEC-101/IEC-104, protocolo de comunicação entre a subestação e o COS, é possível identificar mensagens de outros protocolos que trafegam na rede, como o protocolo ICMP, que é utilizado para monitorar a conectividade das remotas pelo sistema de monitoramento da DTI e COS (PRTG e Zabbix, respectivamente), o protocolo RSTP, que define as rotas das mensagens de maneira a evitar loops, quando habilitado, o protocolo ARP, que identifica o endereço MAC dos equipamentos na rede quando uma comunicação é iniciada. Devido à complexidade das redes Ethernet, não apenas a integridade e a dinâmica das mensagens 101 ou 104 devem ser entendidas e analisadas, mas também das mensagens quem impactam o desempenho da própria rede, pois uma falha nesses serviços podem ser a causa raiz da falha de comunicação.

Para uma análise efetiva dos logs é necessário um bom entendimento dos protocolos, entendendo como ocorre a inicialização da comunicação e, após a comunicação estabelecida, como os dados são requisitados pelo SAGE do COS e enviados pela remota da instalação. A partir do entendimento da dinâmica, é possível identificar as falhas no processo de comunicação, como mensagens que deveriam estar presentes e não estão, mensagens corrompidas, para então se estabelecer a causa dela e então propor soluções.

NO.	PC - TIME	PROTOCOLO	IP SOURCE	IP DESTINATION	SOURCE PORT	DESTINATION PORT	CASDU	PONTO	TYPEID	VALOR	CAUSETX	QUALID
98730	2024-09-10 20:00:20,512708763	IEC 60870-5 ASDU	10.209.25.70	10.208.67.141	2404	43808	12	30.07	M_ME_NA_1	0,08	Spont	Valid
98731	2024-09-10 20:00:20,514715407	TCP	10.208.67.141	10.209.25.70	43808	2404						
98732	2024-09-10 20:00:20,520453929	HSRIPv2	10.209.25.5	224.0.0.102	1985	1985						
98733	2024-09-10 20:00:20,729572801	DNP 3.0	10.209.25.70	10.209.25.170	20000	20000						
98734	2024-09-10 20:00:20,729805346	ARP	Cisco_c4:d5:c6	Broadcast								
98735	2024-09-10 20:00:20,750066468	ARP	Cisco_b4:90:e6	Broadcast								
98736	2024-09-10 20:00:21,317230996	IEC 60870-5 ASDU	10.209.25.70	10.208.67.141	2404	43808	12	30.05	M_ME_NA_1	0,43	Spont	Valid
98737	2024-09-10 20:00:21,319227256	TCP	10.208.67.141	10.209.25.70	43808	2404						
98738	2024-09-10 20:00:21,518360254	IEC 60870-5 ASDU	10.209.25.70	10.208.67.141	2404	43808	12	30.08	M_ME_NA_1	0,02	Spont	Valid
98739	2024-09-10 20:00:21,520359714	TCP	10.208.67.141	10.209.25.70	43808	2404						
98740	2024-09-10 20:00:21,734238943	DNP 3.0	10.209.25.70	10.209.25.170	20000	20000						
98741	2024-09-10 20:00:21,734480567	ARP	Cisco_c4:d5:c6	Broadcast								
98742	2024-09-10 20:00:22,328127675	IEC 60870-5 ASDU	10.209.25.70	10.208.67.141	2404	43808	12	30009	M_ME_NA_1	0	Spont	Valid
98743	2024-09-10 20:00:22,330377247	TCP	10.208.67.141	10.209.25.70	43808	2404						
98744	2024-09-10 20:00:22,750113607	DNP 3.0	10.209.25.70	10.209.25.170	20000	20000						
98745	2024-09-10 20:00:22,750352775	ARP	Cisco_c4:d5:c6	Broadcast								


```

Frame 98730: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface bond0, id 0
Ethernet II, Src: Harris_fe:fe:37 (00:00:c3:fe:fe:37), Dst: Cisco_9f:f0:0a (00:00:0c:9f:f0:0a)
Internet Protocol Version 4, Src: 10.209.25.70, Dst: 10.208.67.141
Transmission Control Protocol, Src Port: 2404, Dst Port: 43808, Seq: 528667, Ack: 40553, Len: 30
IEC 60870-5-104: -> I (2776,1110)
IEC 60870-5-101/104 ASDU: ASDU=12 M_ME_NA_1 Spont IOA[3]=30205,... 'measured value, normalized value'
  TypeId: M_ME_NA_1 (9)
  0... .... = SQ: False
  .000 0011 = NumIx: 3
  ..00 0011 = CauseTx: Spont (3)
  .0... .... = Negative: False
  0... .... = Test: False
  OA: 0
  Addr: 12
  IOA: 30205

```

Figura 2 - Pacotes capturados pelo Wireshark

O monitoramento dos protocolos IEC-101 e IEC-104, além de permitir a verificação da integridade da comunicação da instalação com o centro, é possível também verificar os pontos de supervisão e controle, verificando, por exemplo, se os pontos estão de fato sendo distribuídos além de possibilitar a visualização da qualidade, estampa de tempo e tipo do ponto. Esse monitoramento pode ser útil na etapa de comissionamento de uma subestação, ajudando a identificar erros de parametrizações que impedem os pontos de serem distribuídos pela remota ou aquisitados pelo COS.

Embora idealizado para a análise e identificação de falhas de comunicação da remota com o COS, o monitoramento pode também ser implementado na rede de aquisição da remota, monitorando a comunicação desta com os IEDs de supervisão e controle, que utilizam protocolos como o DNP3.0 e MMS, e a comunicação entre os IEDs, que utilizam o protocolo GOOSE. A análise dessa comunicação pode ajudar a entender falhas de supervisão e controle de vãos específicos.

2.2. Aplicação do Projeto SEAL

O Projeto SEAL já foi implantado em mais da metade das subestações da CEMIG GT e, em alguns casos, já foi possível realizar o diagnóstico das falhas e corrigi-las. Nas subestações implantadas a coleta de logs ainda só é possível por um acesso remoto feito na instalação. Quando necessário coletar os logs, a equipe de operação local é acionada para que os logs sejam coletados e enviados à engenharia da manutenção.

Através da análise dos logs foi constatada a presença, na SE Pimenta, de um loop na rede da subestação que derrubava a comunicação da remota com o COS. Na Figura 3 é possível verificar o aumento no tráfego de dados na rede de comunicação com o COS ocasionando na sua sobrecarga e, consequentemente, na sua queda. A curva em azul mostra os pacotes cujo endereço IP de origem é o IP do SAGE do COS e a curva em vermelho mostra os pacotes cujo endereço IP de origem é o IP da remota. Esse aumento no

tráfego é uma característica de loop. Após identificado, foi feita a correção na parametrização dos switches da rede de automação para que os loops fossem bloqueados.

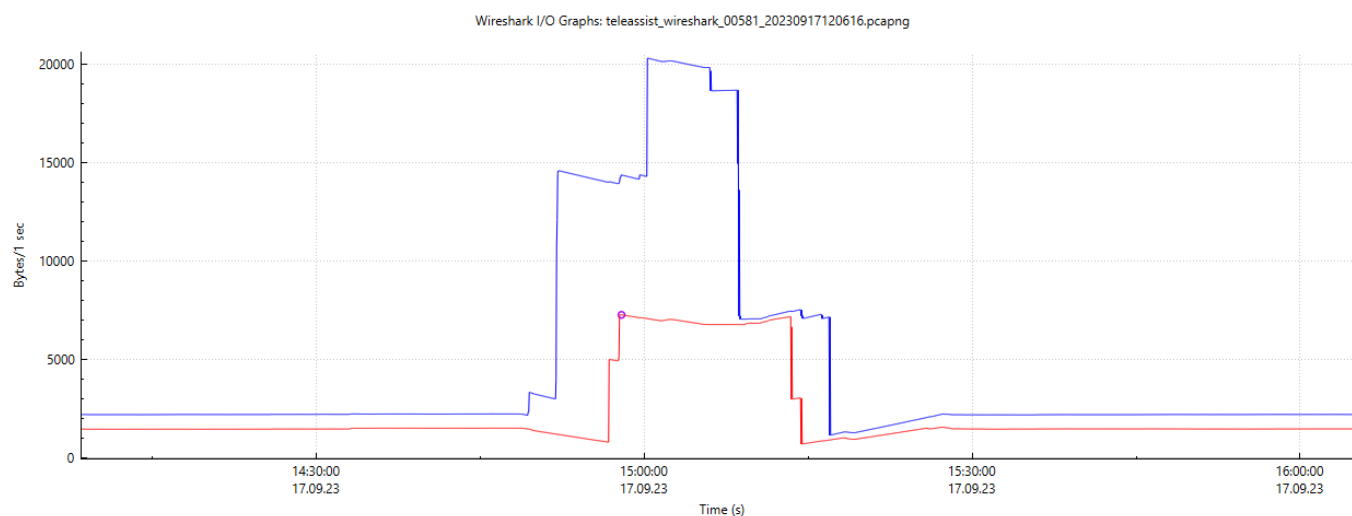


Figura 3 - Tráfego na rede da SE Pimenta durante um loop

Na SE Montes Claros 2 a utilização do analisador de protocolos possibilitou identificar uma falha em um equipamento de telecomunicações. Nos logs coletados durante as falhas de comunicação percebeu-se, de fato, que não estava havendo trocas de pacotes do protocolo IEC-104 entre a remota e o COS. Porém, embora a comunicação com o COS estivesse em falha, a comunicação da remota com a IHM local da SE estava íntegra, descartando assim uma possível falha daquele equipamento. A comunicação da remota com a IHM ocorre em protocolo DNP3.0 Ethernet pela mesma porta de comunicação com o COS. Assim, como o SEAL monitora essa porta, o monitoramento ocorre para ambas as comunicações. Após mais análises percebeu-se que outros protocolos que deveriam estar trafegando na rede, referente ao gerenciamento e monitoramento do sistema de telecomunicações (PRTG e ZABBIX), também pararam de trafegar, indicando que o problema estivesse na infraestrutura de telecomunicações. A equipe de manutenção da DTI foi acionada e foi constatado que o switch de telecomunicação estava com defeito em um dos módulos, sendo necessária sua substituição.

Na SE Várzea da Palma 1 a análise do tráfego permitiu verificar a integridade da infraestrutura do COS e do sistema de telecomunicações, uma vez que foi possível identificar a chegada, no switch da subestação, dos pacotes enviados pelo SAGE do COS. Porém não foi identificada nenhuma resposta da remota. Foram identificadas também as tentativas de comunicação da IHM com a remota, também sem nenhuma resposta desta. Assim, como as solicitações dos mestres das comunicações (SAGE e IHM) chegavam íntegros, mas sem nenhum retorno da remota, concluiu-se que esta que estava com problema. A partir dessa identificação as equipes de proteção, controle e automação da transmissão iniciaram um trabalho de busca de melhorias com o objetivo de otimizar o desempenho do equipamento. As melhorias aplicadas na subestação foram estendidas a outras subestações com remotas do mesmo modelo e que apresentavam o mesmo tipo de falha.

O monitoramento da comunicação na SE Barão de Cocais 3 permitiu identificar um intenso tráfego de dados entre a remota e o COS, a maior parte desse tráfego era desnecessária (solicitações de classe 2 sendo enviadas com alta frequência). Devido a um baixo desempenho da remota, a alta frequência dessas solicitações colocava a teleassistência em risco devido ao travamento do sistema. Além dos ajustes de

configuração para otimização do canal foram feitas várias intervenções a nível de hardware a fim de melhorar a qualidade da comunicação, dando uma sobrevida ao sistema até a sua substituição.

3. Conclusão

O monitoramento contínuo e a análise dos logs gerado pelo analisador de protocolos é de grande importância para falhas intermitentes e curtas. São falhas que, a princípio, geram pouco impacto na teleassistência, porém, de maneira acumulada ao longo do ano, podem afetar o indicador. Como o retorno da comunicação ocorre sem nenhuma intervenção da manutenção para identificação, fica difícil definir ações para correção. Os logs ajudarão a entender o que aconteceu durante a falha para que as medidas corretivas sejam tomadas.

O Projeto SEAL além de ajudar na identificação de falhas permitirá o melhor entendimento da dinâmica da comunicação entre a subestação e o centro de operação. Além das melhorias na infraestrutura já planejadas, como instalação de equipamentos mais modernos, redundantes e melhoria de canais, o melhor entendimento da comunicação a nível de protocolo poderá direcionar as equipes envolvidas em como melhor configurar os equipamentos, softwares e realizar ajustes finos em parâmetros para obter uma comunicação mais eficiente. Uma comunicação mais eficiente e robusta apresentará uma melhor performance, diminuindo os impactos que sua falha causa no indicador TELEASST e, conseqüentemente, evitando o custo de uma operação local ininterrupta em caso de mal desempenho do indicador.

A coleta dos logs pode ser feita diretamente do servidor pela equipe mantenedora da subestação e os logs enviados para a engenharia da manutenção para análise. É possível também a conexão dessas máquinas na rede operativa de forma que a coleta possa ser feita remotamente pela engenharia, acelerando o tempo de análise, desde que o link de comunicação da subestação suporte esse acesso sem competir e trazer riscos para a comunicação da remota com o centro.

A análise dos logs gerados ainda é feita pela equipe de engenharia de manutenção. Porém, através da exportação dos dados do Wireshark será possível o desenvolvimento de uma aplicação em que a análise possa ser feita de maneira automática, trazendo um ganho no tempo de análise tendo em vista que a quantidade de pacotes gerados nos logs é grande, podendo evoluir para um monitoramento em tempo real.

4. Referências bibliográficas

Procedimentos de Rede do ONS: Submódulo 2.16 – Requisitos mínimos para subestações e seus equipamentos

Procedimentos de Rede do ONS: Submódulo 9.6 – Indicadores de desempenho dos sistemas de supervisão e controle e dos serviços de telecomunicações