

**ESCOLA POLITÉCNICA  
UNIVERSIDADE DE SÃO PAULO**

**ALEXANDRE FERRAZ BRITO**

**ESTUDO DE CASO DO SISTEMA DE TELECONTROLE DE ENERGIA**  
**Proposta de melhoria das Interfaces de Comunicação do Sistema de**  
**Telecontrole de Energia**

São Paulo

2016

**ESCOLA POLITÉCNICA  
UNIVERSIDADE DE SÃO PAULO**

**ALEXANDRE FERRAZ BRITO**

**ESTUDO DE CASO DO SISTEMA DE TELECONTROLE DE ENERGIA**

**Proposta de melhoria das Interfaces de Comunicação do Sistema de  
Telecontrole de Energia**

Dissertação apresentada à Escola  
Politécnica da Universidade de São  
Paulo para Conclusão do Curso de  
Especialização em Tecnologia Metro-  
Ferroviária.

São Paulo

2016

**ESCOLA POLITÉCNICA  
UNIVERSIDADE DE SÃO PAULO**

**ALEXANDRE FERRAZ BRITO**

**ESTUDO DE CASO DO SISTEMA DE TELECONTROLE DE ENERGIA**  
**Proposta de melhoria das Interfaces de Comunicação do Sistema de**  
**Telecontrole de Energia**

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para Conclusão do Curso de Especialização em Tecnologia Metro-Ferroviária.

Área de Concentração:  
Tecnologia Metro-Ferroviária

Orientador: Prof. Dr. João Batista Camargo Jr.

São Paulo

2016



## AGRADECIMENTOS

Na vida nenhuma batalha é vencida sozinha, temos muitas inspirações divinas que recebemos da graça de nosso bondoso Deus e seus colaboradores de luz. Tenho muita gratidão pela ajuda que venho recebendo e gostaria de retribuir o amor por todos ofertado com tanto carinho.

Deus Eterno, Pai Amado, que eu possa ser digno de receber suas bênçãos, agradeço a ti por mais esse caminho trilhado nessa fase de aprendizado, que todos os que participaram direta ou indiretamente dessa jornada possam ser agraciados com seu infinito amor e, portanto, agradeço:

A Escola Politécnica da Universidade de São Paulo, seu corpo docente, direção e administração, que possibilitaram as condições necessárias para o desenvolvimento do curso e conclusão do curso.

Aos professor Dr. João Batista Camargo, pela paciência e incentivo que tornaram possível a conclusão dessa monografia.

Aos amigos Nathalia e Robson que depositaram em mim confiança.

Aos meus pais Lourival (em memória) e Izabel, que com seu amor deram a oportunidade de minha existência.

Ao meu filho e minhas filhas por fazerem mais alegres os meus dias e serem minha motivação para vencer.

À minha querida e amada esposa Tatiane Damazio Brito pelo companheirismo, cumplicidade e todo o carinho que sempre teve por mim.

## RESUMO

A Companhia Paulista de Trens Metropolitanos é uma empresa de economia mista e busca a melhoria contínua no transporte público de forma a propiciar a mobilidade urbana com excelência, segurança e alcançar a sustentabilidade financeira.

Vários recursos tecnológicos foram adquiridos de forma a alcançar a melhoria desejada e ao mesmo tempo, diminuir os custos de operação. Uma dessas tecnologias, vem com a proposta de reduzir o tempo de resposta para o reestabelecimento das subestações de tração, cabines de seccionamento/paralelismo e domínios de Rede aérea, bem como, reduzir o custo com mão-de-obra especializada.

A medida que a utilização do Telecontrole de Energia vai sendo empregado, a necessidade de acompanhamento humano dentro das localidades deixa de ser necessária, porém, é imprescindível que estudos sejam realizados de forma a adequar essa nova realidade e prever a possibilidade de futuros problemas no emprego dessas novas tecnologias.

Essa monografia visa a realização de uma análise sistêmica e comportamental do Telecontrole de Energia, bem como, suas inúmeras interfaces no centro de controle operacional, alertando para possíveis problemas e sugerindo mudanças.

**Palavras Chaves:** Telecontrole de Energia, análise de riscos, análise sistêmica, análise de rede.

## ABSTRACT

The Companhia Paulista de Trens Metropolitanos (São Paulo's Metropolitan Train Company) is a mixed economy company that searches for continued improvements in public transportation, in order to provide urban mobility with excellence, safety and to attain financial sustainability.

Many technological resources were acquired in order to gain the desired progress and, at the same time, reduce the operation costs. One of these resources comes with the proposal of reducing the required time for the reestablishment of the traction substations, sectioning and parallelism booths, along with Air Network domains, while also reducing the costs of skilled manpower.

As the application of the Power Telecontrol is used, the need for human monitoring inside the locales is no longer necessary. However, it is essential that studies are carried out in order to adequate this new reality and to prevent the hazards of these new technologies.

This monograph aims to perform a systematic and behavioral investigations of the Power Telecontrol, as well as its interface inside the Operational Control Center, warning about potential problems and suggesting changes.

Keywords: Power Telecontrol, risk analysis, systemic analysis, network analysis.

## Sumário

1.	INTRODUÇÃO.....	9
2.	OBJETIVO.....	11
3.	JUSTIFICATIVA .....	11
4.	FUNDAMENTAÇÃO TEÓRICA .....	12
4.1.	CONCEITOS BÁSICOS .....	12
4.1.1.	SUBESTAÇÃO DE TRAÇÃO .....	12
4.1.2.	DISJUNTORES.....	13
4.1.3.	CHAVES SECCIONADORAS .....	13
4.1.4.	REDE AÉREA DE TRAÇÃO.....	14
4.1.5.	DEMAIS EQUIPAMENTOS .....	15
4.1.6.	CABINES .....	16
5.	TIPOS DE INTERVENÇÃO NO SISTEMA ELÉTRICO .....	17
5.1.	MANUTENÇÃO PROGRAMADA .....	17
5.2.	MANUTENÇÃO CORRETIVA .....	17
5.3.	NECESSIDADE OPERACIONAL .....	17
6.	CONTEXTO ATUAL .....	18
6.1.	CONFIGURAÇÃO FUNCIONAL DO TELECONTROLE DE ENERGIA (CCO) ..	20
7.	ANÁLISE DE RISCOS.....	21
7.1.	ANÁLISE DE RISCOS - APR .....	21
7.2.	ANÁLISE DE RISCOS - MATRIZ DE RISCOS .....	25
8.	ANÁLISE DE FALHAS NO SISTEMA DE ENERGIA .....	28
8.1.	ANÁLISE DE FALHAS DO SICOM .....	28
8.1.1.	FALHAS DO SISTEMA DE CONTROLE DE ENERGIA (SCE) .....	28
9.	ANÁLISE DO SISTEMA SCADA OASYS DNA.....	32
10.	ANÁLISE DO TRÁFEGO DE DADOS .....	37
11.	CONCLUSÃO .....	41
12.	BIBLIOGRAFIA.....	43



## 1. INTRODUÇÃO

A Companhia Paulista de Trens Metropolitanos - CPTM - teve sua origem na junção das empresas, FEPASA - Ferrovias Paulista S/A, Rede Ferroviária Federal e CBTU - Companhia Brasileira de Trens Urbanos, vindo a assumir os sistemas de trens da região metropolitana de São Paulo no ano de 1992, atendendo aproximadamente 800.000 usuários/dia. Anteriormente a esta data, cada empresa atuava de uma maneira segregada, utilizando tecnologias diversas e recebendo investimentos distintos.

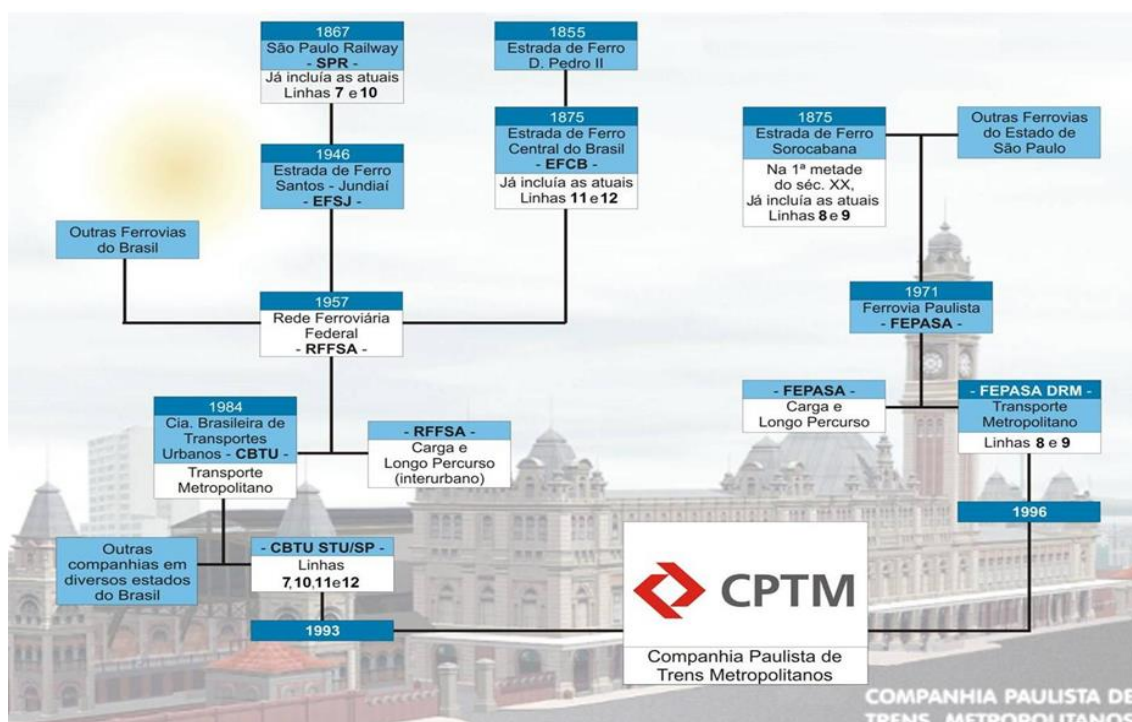


Figura 1 - História da CPTM

Atualmente são transportados pela CPTM cerca de 3 milhões de usuários diariamente. E diante deste contexto de alta e crescente demanda, houve a necessidade da criação do Plano de Expansão de São Paulo com o objetivo de proporcionar um serviço eficaz, de qualidade e seguro à população.

No início da Operação dirigida pela CPTM haviam três Centros de Controle Operacionais separados por pares de linhas (Linhas Rubi e Turquesa – 07/10; Linhas Diamante e Esmeralda – 08/09 e Linhas Coral e Safira – 11/12) que ficavam localizados respectivamente na Luz, Presidente Altino e Brás, o que dificultava a tomada de decisões pelas Gerências Operacionais e de Manutenção em casos de emergência.

Para aumentar a eficiência nas operações normais e situações emergenciais, controladas e supervisionadas a partir do CCO, foi decidido a centralização dos Centros de Controle e definido o Brás como o melhor local para esta estratégia.

Com o desenvolvimento tecnológico crescente, a necessidade de modernização para as aplicações e, até mesmo, substituição de recursos já existentes são cada vez mais frequentes. Para que a centralização dos CCO's fosse possível todos os equipamentos e informações de todas as Linhas Metropolitanas deveriam se concentrar agora em um único local físico e, para que isso fosse possível, foram instaladas diversas interfaces de comunicação entre os equipamentos de diferentes tecnologias para que pudessem oferecer rapidez e facilidade de controle e maior integração com os usuários.



Figura 2 - Mapa do Transporte Metropolitano

## **2. OBJETIVO**

O trabalho de Monografia a ser proposto tem como objetivo apresentar uma análise de falhas dos equipamentos instalados no Centro de Controle e que estão diretamente relacionados com o controle e supervisão do tráfego e energia, visando a identificação de pontos críticos que interferem na disponibilidade do Sistema de Controle de Tráfego Centralizado (SCTC) e do Sistema de Controle de Cabines e Subestações de Energia.

O estudo é composto por pesquisas dirigidas aos equipamentos e arquiteturas que os Centros de Controle de outras Ferrovias no mundo utilizam e, também, pesquisas sobre recursos tecnológicos existentes no mercado e que sejam compatíveis com as aplicações ferroviárias propondo melhorias para aumentar a eficiência e disponibilidade do CCO.

## **3. JUSTIFICATIVA**

Nesta parte do trabalho voltada ao Telecontrole de Energia, o Centro de Controle Operacional da CPTM é responsável por controlar as Subestações de Tração, Cabines Seccionadoras e seccionadoras de Rede Aérea ao longo da via por meio de infraestrutura de servidores, remotas, concentradores de dados, painéis sinóticos, gerenciadores, dentre outras miscelâneas, garantindo as condições operacionais de acordo com as necessidades da empresa.

Fazendo uma analogia ao corpo humano, o Sistema de Controle de Energia (SCE) é o coração que bombeia o sangue (trens) levando as substâncias (usuários) necessárias a vida (ferrovia) para todas as partes do corpo (estações), ou seja, sem o SCE não haveria circulação de trens via tração elétrica, sendo esse sistema essencial a continuidade dos trabalhos. Um problema nesse sistema pode significar a incapacidade de transportar usuários ao seu destino ou limitar a velocidade dos trens devido a uma paralisação total ou parcial do sistema. O tema do trabalho proposto foi devido a criticidade e impactos operacionais em decorrência da perda desse sistema.

## 4. FUNDAMENTAÇÃO TEÓRICA

### 4.1. CONCEITOS BÁSICOS

#### 4.1.1. SUBESTAÇÃO DE TRAÇÃO

A Subestação de Tração da CPTM é constituída por equipamentos destinados a transformar a tensão alternada de 88kv, fornecida pela concessionária de energia em uma tensão contínua de 3kv para alimentação da rede aérea de tração, 6.6KV, 4.4Kv e 13,2kV para a alimentação do sistema de sinalização e 220V para os equipamentos auxiliares da subestação. A Subestação de Tração tem como objetivo principal fornecer energia para os trens de forma confiável, econômica e ininterrupta.



*Figura 3 - Subestação Leopoldina*

Uma subestação de tração é basicamente composta por Disjuntores, Chaves seccionadoras, Transformadores de corrente e de potencial, transformadores principais, Retificadores, Ondulador, Transformadores de 6,6KV, Equipamentos de comando e proteção, etc.

#### **4.1.2. DISJUNTORES**

São equipamentos corta-circuitos, destinados a projeção da subestação, podendo ser abertos ou fechados. São dotados de câmara de extinção de arco voltaico, utiliza gás SF6 (hexafluoreto de enxofre) em 88Kv e sopro magnético em 3Kv podendo ser manobrados em carga.

O fechamento de um disjuntor somente pode ser executado através do COE ou do circuito de comando local. A abertura do mesmo, além do Telecontrole remoto e do controle local, também pode ser efetuada pelos reles de proteção, quando da ocorrência de alguma anormalidade no sistema, a qual é sinalizada no Painel Sinóptico e Console de Operação do COE (Console de Operação de Energia).

#### **4.1.3. CHAVES SECCIONADORAS**

Também são equipamentos corta-circuitos, porém não possuem dispositivo de extinção de arco voltaico, não podendo, portanto, serem manobrados em carga.

Nas subestações, a principal finalidade das chaves seccionadoras é a de isolar os demais equipamentos para a realização de manutenção. Podem ser bipolar ou monopolar:

- Seccionadora Bipolar - Presente em todos os disjuntores alimentadores das subestações e cabines, sua função é isolar a entrada e a saída de energia, proporcionando a segurança necessária para a atuação da manutenção corretiva emergencial ou para assegurar o desenergizamento no caso de intervalo programado, para a manutenção da Rede Aérea.
- Seccionadora Monopolar - Se divide em 2 grupos TAY's e Seccionadora de RA.
- ✓ TAY - Se apresentam sempre abertas, cuja função consiste em interligar as saídas independentes dos alimentadores na mesma Rede Aérea V1, V2, Vaux, V1s e V2s, evitando assim a diferença de potencial presente no GAP, causada pela distância e despacho de carga das SE's adjacentes no caso de religamento total ou parcial da SE ou falha em alimentador.
- ✓ Seccionadora de R.A. - São chaves seccionadoras que se apresentam sempre fechadas, cuja função consiste em seccionar a Rede Aérea em um trecho para evitar a perda total do sistema em situações de curto franco, queda de Rede aérea, etc.

#### 4.1.4. REDE AÉREA DE TRAÇÃO

É constituída de um cabo chamado mensageiro, que recebe a energia das subestações e de um ou dois outros cabos chamados de trolleys. O cabo mensageiro e os fios trolleys são interligados por alças metálicas chamadas suspensórios, que tem a finalidade de suportar mecanicamente os trolleys. Para garantir a transferência de energia do mensageiro para os fios trolleys, a cada 120 metros é executada uma ligação equipotencial entre os mesmos.

A rede aérea é seccionada junto às subestações adjacentes por chaves seccionadoras chamada “tays”, instaladas entre os alimentadores de uma mesma subestação.

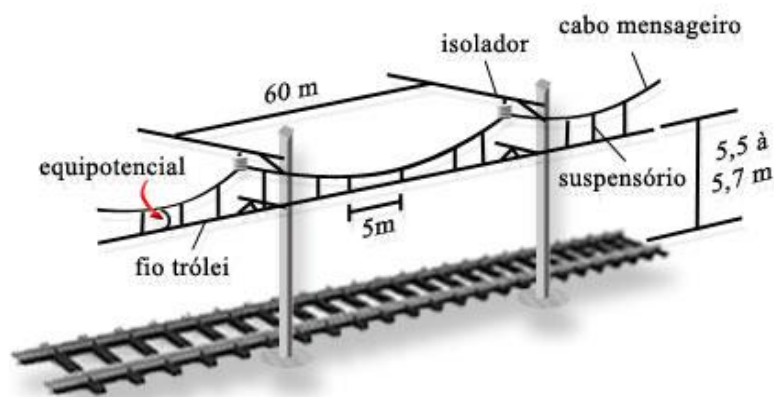


Figura 4 - Rede aérea de Tração

Ao longo da rede aérea, também estão instaladas outras chaves seccionadoras, com a finalidade de isolar estrategicamente seções da mesma, quando da necessidade de intervenção da manutenção ou da operação. Nos locais onde se localizam as chaves seccionadoras, os cabos da rede aérea são isolados pelos gaps a ar ou isoladores de seção.

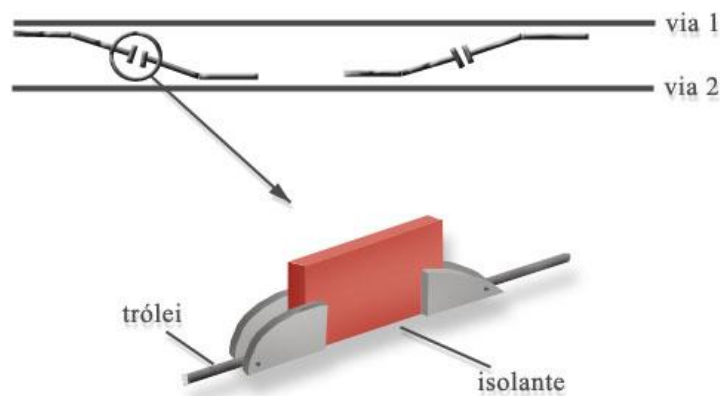


Figura 5 - Isolador de seção

Junto às chaves seccionadoras, são instalados os reles de tensão (Sensores de Energia) que indicam quando a tensão cai, sendo visualizada no COE através de sinalização luminosa e sonora.

#### 4.1.5. DEMAIS EQUIPAMENTOS

**Transformadores de Corrente e de Potencial:** São equipamentos destinados a reduzir a corrente e a tensão a níveis compatíveis à alimentação dos painéis de medição e dos reles de proteção.

**Transformadores Principais:** São destinados a transformar a tensão alternada de 88Kv, fornecida pela ELETROPAULO, em uma tensão alternada de 1,2Kv, que alimenta as entradas do retificador e do transformador de 6,6Kv.

**Retificadores:** São equipamentos destinados a transformar tensão e corrente alternada em tensão e corrente contínua. No caso das linhas 8 e 9, os retificadores das subestações de tração recebem uma tensão alternada entre fases de 1,2Kv e transforma em uma tensão contínua de 3Kv.

**Ondulador:** São destinados a inverter o fluxo de potência, isto é, recebem a potência gerada pela frenagem dos trens e a devolve à ELETROPAULO.

**Transformadores de 6,6kV:** Estes equipamentos estão destinados a alimentar o sistema de sinalização. São conectados no secundário dos transformadores principais, transformam a tensão de 1,2Kv em 6,6Kv e energizam a linha de transmissão de 6,6Kv.

**Equipamentos de Comando e Proteção:** As manobras de abertura e fechamento de disjuntores e chaves seccionadoras de alta tensão são efetuadas a distância. Os comandos são executados através de sensores (reles) que fazem a supervisão do



sistema. Caso ocorra alguma anormalidade, estando uma subestação a plena carga, o isolamento parcial ou total da mesma é efetuado através dos reles de proteção, que por meio de seus contatos provocam a abertura ou fechamento de um circuito elétrico, provocando a abertura de disjuntores.

#### **4.1.6. CABINES**

Podem ser de seccionamento e/ou de paralelismo. Tem a finalidade de diminuir a queda de tensão ao longo da rede aérea de tração e também de seccionar a mesma, em caso de anormalidade, reduzindo o trecho inoperante.



*Figura 6 - Cabine de PAL*

São constituídas de um disjuntor e duas chaves seccionadoras ou de mais de um disjuntor e chaves seccionadoras.



## **5. TIPOS DE INTERVENÇÃO NO SISTEMA ELÉTRICO**

Existem basicamente três situações em que ocorre intervenção no sistema elétrico:

- Manutenção Programada
- Manutenção Corretiva
- Necessidade Operacional

### **5.1. MANUTENÇÃO PROGRAMADA**

É realizada quando houver programação previamente definida pela Operação e Manutenção, nas reuniões de acesso, objetivando uma intervenção no sistema.

### **5.2. MANUTENÇÃO CORRETIVA**

É realizada quando houver avaria em um determinado sistema ou parte dele, que necessite da intervenção da equipe do reestabelecimento.

### **5.3. NECESSIDADE OPERACIONAL**

Ocorre quando houver a necessidade do CCO alterar a configuração normal do sistema, para possibilitar, por tempo determinado, a melhor circulação de trens ou para atender a situações de teste no sistema ou parte dele.

## 6. CONTEXTO ATUAL

O Sistema de Telecontrole de energia existente no centro de Controle Operacional (CCO) apresenta todas as indicações de estados dos objetos controláveis (Disjuntores e Seccionadoras), bem como, das possíveis falhas ou condições adversas que impeçam o seu perfeito acionamento.

Essas indicações são apresentadas através dos consoles de operação, engenharia, supervisão e Vídeo Wall (figura 3) instalados e dedicados para propósitos específicos.

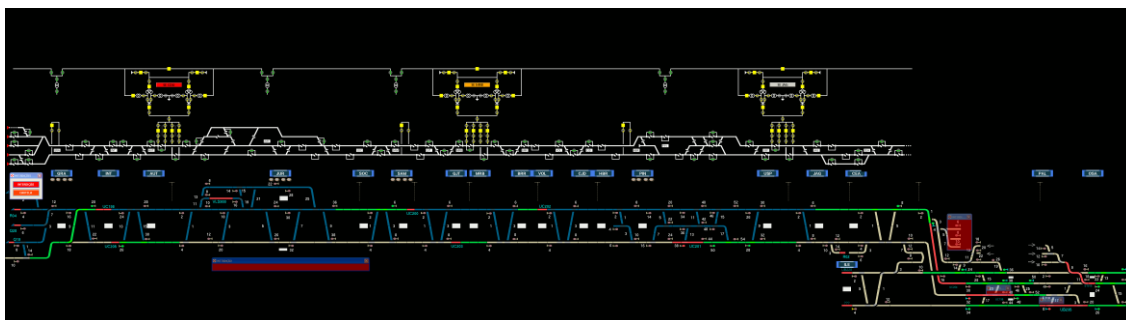


Figura 7 - Vídeo Wall linha 9

Na sequência (figura 4), é mostrada a arquitetura do sistema atual, sendo 2 servidores, 3 consoles operacionais, 1 console de supervisão, 1 console de Engenharia/Manutenção, Vídeo Wall, Gerenciador de imagem e Switch, equipamentos esses que são responsáveis pelo Telecontrole de 24 subestações de tração, 20 cabines de seccionamento e todas as seccionadoras de rede aérea (sem quantidade exata).

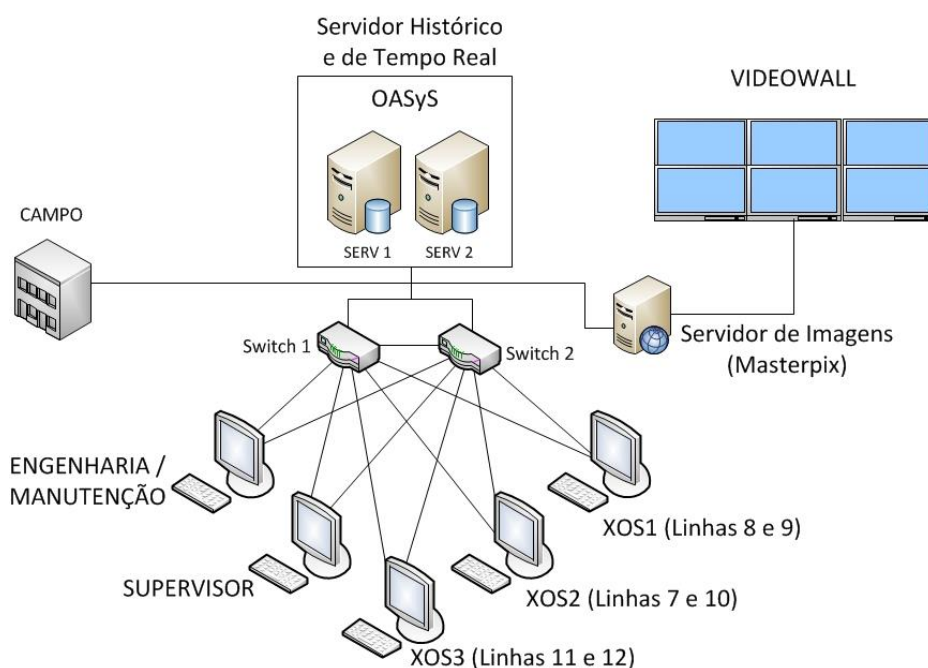


Figura 8 - Configuração do Centro de Controle (TELVENT, p.10)

A seguir são representados os sistemas que compõem a arquitetura do sistema de Telecontrole no campo (figura 5).

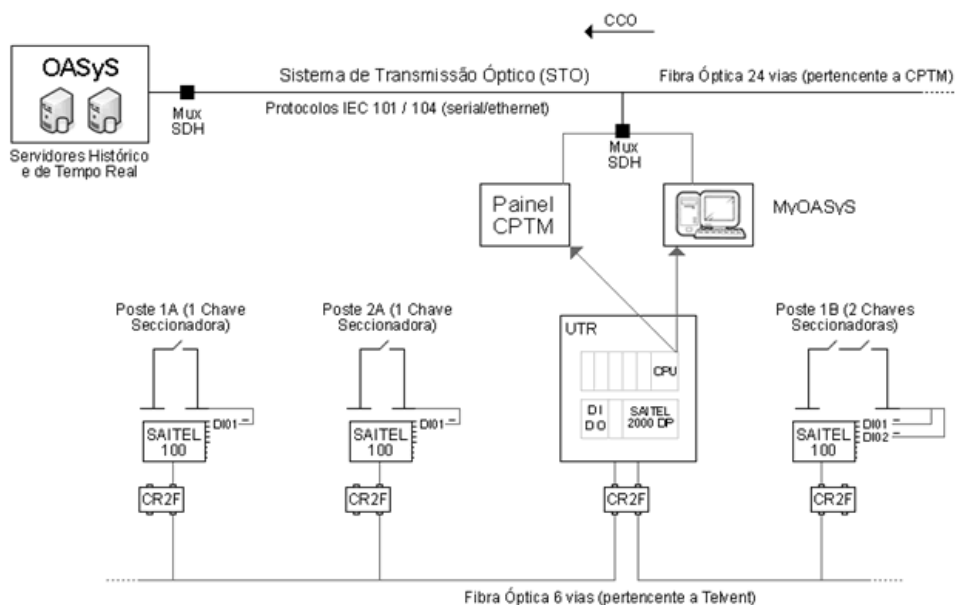


Figura 9 - Configuração dos sistemas no campo (TELVENT, p.11)

Através da fibra óptica um pacote de dados é transmitido do CCO para os equipamentos do campo, ao passar pelo CR2F o sinal de luz é convertido em bits, enviando para a UTR as informações necessárias para o comando de uma seccionadora ou disjuntor de uma subestação, cabine ou rede aérea, através do controlador SAI TEL 100 (no poste da rede aérea) ou SAI TEL 2000DP (dentro da subestação ou cabine de seccionamento e paralelismo) uma requisição de abertura ou fechamento.

Atualmente temos 5 subestações, 9 cabines e dois domínios de Rede Aérea entregues pelo sistema de Telecontrole OASYS. Além disso, tem-se 4 subestações, 4 cabines e 4 domínios de Rede Aérea controladas pelo sistema Jeumont Schneider (sistema antigo) para a operação conforme mapa a seguir.

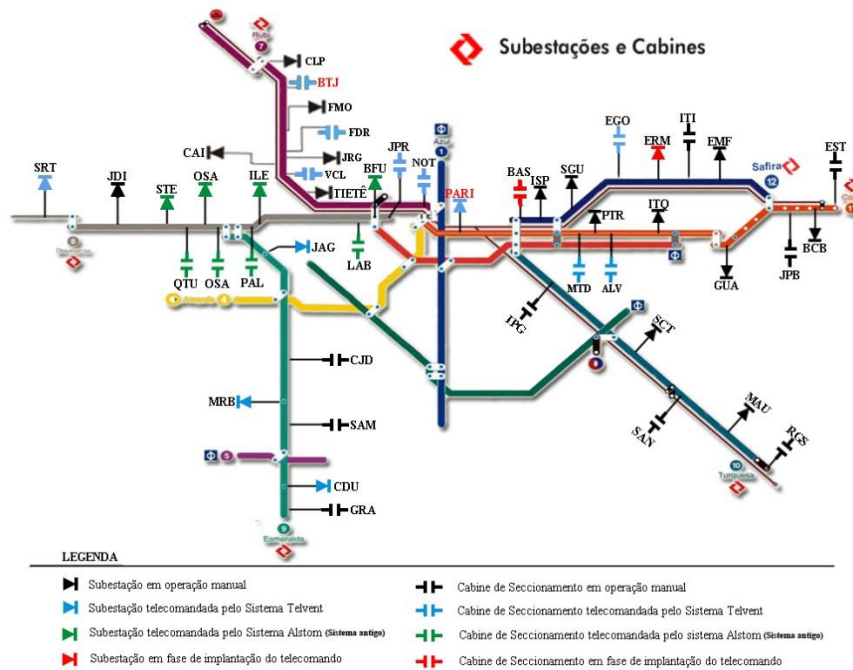


Figura 10 Diagrama simplificado das Subestações e Cabines

## 6.1. CONFIGURAÇÃO FUNCIONAL DO TELECONTROLE DE ENERGIA (CCO)

A configuração do Telecontrole de Energia, consiste em um conjunto de equipamentos interligados de modo a fornecer recursos ininterruptos para o acionamento remoto das seccionadoras, disjuntores e contatores de uma subestação ou cabine, bem como, receber as informações de anormalidades, proteções atuadas e automatismos a partir do centro de controle operacional (CCO) com o auxílio de interfaces gráficas para a representação dos objetos supervisionados.

O processo básico de atuação visa a interação do controlador com o equipamento em campo, onde o controlador envia um comando, recebe uma indicação de comando realizado automaticamente ou manualmente e toma as decisões necessárias para manter os equipamentos disponíveis para a circulação dos trens em situações normais ou degradadas.

## **7. ANÁLISE DE RISCOS**

Segundo EGOSHI (análise de riscos, p.10), risco é a possibilidade de ocorrer perda ou ganho dentro dos valores humanos. No mundo dos negócios o risco é convertido em mais ou menos dinheiro dependendo da conscientização sobre o sistema ou processo em relação a severidade, vulnerabilidade, impacto e grau de controle.

No âmbito de negócios, antes de se concretizar uma perda pressentimos o perigo e antes de se concretizar um ganho pressentimos uma oportunidade. A análise de riscos então, é definida por EGOSHI (análise de riscos, p.12) como sendo o procedimento técnico e administrativo utilizado para reduzir o risco de ocorrer perda parcial (prejuízo) ou total (falência) de uma empresa, podendo ajudar na criação do plano de continuidade de negócios ou para o planejamento estratégico da organização.

A análise de riscos (EGOSHI, p.13) constitui-se num método visando identificar e avaliar sistemas de forma qualitativa e quantitativa, identificando os riscos que a atividade representa para todo o sistema envolvido. A etapa da Análise de Risco que será utilizada denomina-se APR - Análise Preliminar de Risco (BARROS), que consiste em identificar eventos perigosos, causas e consequências em uma estrutura, procedimento, projeto, organização ou sistema e, dessa forma, decidir medidas de controle de forma preliminar. Dentro dessa análise é feita uma avaliação qualitativa dos riscos de forma a priorizar os itens mais críticos do sistema a ser estudado, sendo que o grau de risco é determinado através da Matriz de Riscos do sistema.

### **7.1. ANÁLISE DE RISCOS - APR**

O risco em um sistema Ferroviário pode acarretar em perigo de vida, desastres, vandalismos durante uma falta de energia ou avaria de trem dentre tantos outros.

Essa análise é feita identificando-se a Severidade, Vulnerabilidade, Impacto e o Grau de Controle que a empresa tem sobre o risco a serem considerados em cada aspecto. O resultado dessa análise é a identificação de cenários de degradação do sistema, suas frequências esperadas e a magnitude da ocorrência para a empresa e sociedade.

Na tabela a seguir foram consideradas ameaças que já ocorreram ou que poderiam ocorrer dependendo de fatores internos ou externos ao sistema.

Tabela 1 - Análise Preliminar de Riscos

Tabela Qualitativa de Riscos - Console de Energia (1 - 4)						
Item	Ameaça	Severidade	Vulnerabilidade	Impacto	Controle	Risco
A	Inconsistência dos Dados	3	3	1	2	4,5
B	Falha de Comunicação	2	3	1	2	3
C	Queda do Sistema	3	3	1	2	4,5
D	Falha de Armazenamento (Histórico)	2	3	1	3	2
E	Falha na IHM	2	3	1	2	3
F	Erro de Envio de Comando (Controlador)	3	3	2	2	9
G	Falta de Energia da Concessionária	4	4	2	1	32
H	Perda de 1 Servidor	1	3	1	2	1,5
I	Perda de 2 Servidores	3	3	1	2	4,5
J	Perda do Vídeo Wall	1	2	1	2	1
K	Perda de 1 Subestação	2	2	1	2	2
L	Falta de Operador na SE	1	1	1	4	0,25
M	Falta de Operador na SE + Perda do Sistema	3	3	1	2	4,5
N	Falta de Operador na SE + Perda do Sistema + Desarmes em Cascata	4	3	2	1	24

Os parâmetros abaixo foram descritos de forma a contemplar a análise sobre o sistema do Telecontrole de Energia. Cada ameaça foi tratada com os questionamentos a seguir.

Como exemplo, será feita a análise para o item k (Perda de 1 subestação).

**Severidade (Quanto prejudica?):** A perda de uma subestação deve ser evitada (Severidade = 2), pois, na sua ausência as subestações adjacentes assumem a demanda de energia, ou seja, sua utilidade para o sistema pode ser transferida sem problemas para outra subestação.

**Vulnerabilidade (Pode ser atacado?):** Uma subestação está sempre protegida com agentes de segurança, possui gradis de proteção e atende às normas da NR10 quanto a segurança dos equipamentos e pessoas. A subestação é de difícil acesso ao público externo, é acessada por pouquíssimas pessoas (engenharia e manutenção de subestações), não podendo ser atacada por intervenção humana ou do meio ambiente. Sendo assim uma vulnerabilidade dificilmente explorável (Vulnerabilidade = 2).

**Impacto (Custos para recuperação?):** A perda de uma subestação não compromete a imagem da empresa e normalmente ocorre por surtos de energia podendo gerar multas por excesso de demanda em situações esporádicas. A manutenção preventiva sendo acionada gera custos com recurso humano e os trens na região terão a tensão de entrada de linha reduzida, porém, sem acarretar danos ou desligamento de disjuntores dos trens por subtensão. Dessa forma entende-se que o impacto é baixo (Impacto = 1).

Controle (O que eu posso fazer se ocorrer algo errado?): Na perda de uma subestação existem procedimentos (ações mitigatórias) para a correção e a supressão da falta da mesma dentro do sistema. Todas as subestações possuem chaves seccionadoras de paralelismo para isolar os trechos na ocorrência de surtos de energia e possuem disjuntores ligados em um barramento único e posicionados de forma a não deixar esses trechos com diferença de potencial (condição que favorece o arco voltaico na passagem do trem pelo GAP (vão da rede aérea) e gera desgaste de equipamentos). Na falta da subestação, medidas mitigatórias devem ser realizadas pela operação via acesso remoto ou manual, como a interligação das chaves seccionadoras de paralelismo nesses trechos, diminuição de trens, criação de loop, acionamento da equipe de manutenção, etc., portanto o controle deve ser mitigado (Controle = 2).

$$\text{Considerando-se que: } Risco = \frac{\text{Severidade} * \text{Vulnerabilidade} * \text{Impacto}}{\text{Grau de Controle}}$$

O risco para a operação de perder uma subestação é igual a 2 conforme figura 7.

K	Perda de 1 Subestação	2	2	1	2	2
---	-----------------------	---	---	---	---	---

Figura 11 - Análise de Riscos da perda de 1 subestação

As tabelas a seguir mostram as justificativas para cada um dos itens.

Severidade		Justificativa
1	Aceitável	A ameaça é aceitável ou o custo de mitigação/gestão é mais alto que o impacto da ameaça
2	Evitar	Ameaça deve ser evitada ou transferida.
3	Impedir	Ameaça deve ser impedida ou prevenida.
4	Anular	Ameaça deve ser completamente anulada.

Vulnerabilidade		Justificativa
1	Nula ou Baixíssima	Processo/produto patenteado, marca registrada, patrimônio tangível. Versão de software não vulnerável ou serviço vulnerável não habilitado. Processo altamente controlado.
2	Difícilmente explorável	Provas de conceito, falha teórica de projeto, acessado por poucos ou nenhum custodiante – apenas proprietário, maior interessado, pode explorar.
3	Explorável	Vulnerabilidade plena e comprovada, mas depende de processos intencionais para efetivação, processo com muitos custodiantes que dependem de ter acesso para realizar seu trabalho. Processo volátil.
4	Altamente explorável	Métodos prontos e conhecidos de exploração; muitas vezes automáticos, processos que todos têm acesso, acesso descontrolado, custodiantes não documentados. Processo altamente volátil ou usualmente descontinuado/substituído.

<b>Impacto</b>		<b>Justificativa</b>
<b>1</b>	Baixo	Gera custos/gastos adicionais baixos (multas e afins). Diminui um pouco a receita líquida (elevação de impostos e afins). Atrasa entregas. Sobrecarrega recurso humano.
<b>2</b>	Alto	Perda de diferencial de mercado. Comprometimento de imagem da organização.
<b>3</b>	Crítico	Gera prejuízo financeiro. Impede aquisição de novas receitas/contratos.
<b>4</b>	Altamente Crítico	Compromete receita recorrente.

<b>Controle</b>		<b>Justificativa</b>
<b>1</b>	Não há	Medida de segurança/controle.
<b>2</b>	Mitigação	Procedimentos para amenizar ou eliminar a ocorrência dos riscos impactantes no projeto.
<b>3</b>	Correção / Nulidade	Plena ameaça.
<b>4</b>	Pró-ação	Ação crítica que antecipa medidas preventivas para a resolução de problemas, valendo-se dos desafios que se apresentam para compor soluções criativas, efetivas e sustentáveis.



## 7.2. ANÁLISE DE RISCOS - MATRIZ DE RISCOS

Com a análise preliminar de riscos é possível criar a matriz de riscos e dessa forma visualizar quais são os itens mais impactantes no sistema e necessitam de cuidados específicos ou quais itens devem ser mitigados para que não haja a evolução de um problema maior. A tabela é desenvolvida posicionando as letras na matriz de acordo com o resultado obtido. Conforme o exemplo da Perda de 1 subestação que resultou em risco = 2 na análise de riscos, desenvolvemos a matriz abaixo de forma a copiar a letra K (Perda de 1 subestação) dentro do campo respectivo onde a multiplicação dos números das linhas pelos números das colunas resulte em 2 e portanto coloca-se na coordenada 1;2 (linha, coluna) da matriz.

Tabela 2 - Matriz de Riscos

Matriz de Risco Qualitativo		Impacto Resultante						
		1	2		3		4	
Severidade	4							GN
	3	BE	A	C	F			
	2	D			M	I		
	1	HLJ	K					

LEGENDA	
<b>VERMELHO</b>	Controle depende de terceiros ou sequência de eventos, causa prejuízo financeiro e perda significativa da imagem da empresa
<b>LARANJA</b>	Gera custo de manutenção, prejuízo na operação, necessário mitigar
<b>AMARELO</b>	Gera custo de manutenção com pequeno ou nulo prejuízo a operação, eventos esporádicos
<b>VERDE</b>	Pouco ou nenhum reflexo no sistema

Todos os controles precisam de um plano de ação, seja a utilização de um sobressalente, o acionamento da equipe de prontidão, a utilização de dualidade, etc. Na análise de falha humana, devem ser utilizados recursos visando diminuir a chance de erro do operador, ou seja, comandos errados devem ser proibidos pelo sistema.

Tabela 3 - Análise qualitativa de Riscos em Ordem Decrescente

Tabela Qualitativa de Riscos - Console de Energia		
Item	Ameaça	Risco
<b>G</b>	Falta de Energia da Concessionária	32
<b>N</b>	Falta de Operador na SE + Perda do Sistema + Desarmes em Cascata	24
<b>F</b>	Erro de Envio de Comando (Controlador)	9
<b>A</b>	Inconsistência de dados	4,5
<b>C</b>	Queda do Sistema	4,5
<b>I</b>	Perda de 2 Servidores	4,5
<b>M</b>	Falta de Operador na SE + Perda do Sistema	4,5
<b>B</b>	Falha de Comunicação	3
<b>E</b>	Falha na IHM	3
<b>D</b>	Falha de Armazenamento (Histórico)	2
<b>K</b>	Perda de 1 Subestação	2
<b>H</b>	Perda de 1 Servidor	1,5
<b>J</b>	Perda do Vídeo Wall	1
<b>L</b>	Falta de Operador na SE	0,25

Baseado na abordagem qualitativa na análise de risco, conforme apresentado na tabela 3, foi possível identificar os 3 processos mais impactantes no Telecontrole de Energia em ordem de risco.

- G - Falta de Energia da Concessionária
- M - Falta de Operador na SE + Perda do Sistema + Desarmes em Cascata
- F - Erro de Envio de Comando (Controlador)

A condição de falta de Energia por qualquer motivo nos trens, gera índices de vandalismos, acidentes e tumultos devido ao não funcionamento do ar condicionado dentro dos trens e demais equipamentos de segurança. Um trem sem ar condicionado durante 2 minutos de paralisação, causa falta de ar, pânico e consequente indisposições nos usuários do sistema. A falta de energia foi um dos agentes causadores do acidente de Perus do dia 28 de julho de 2000 e que a partir dessa data corroborou para a criação de várias medidas mitigatórias para evitar novos acidentes.

Conforme a figura acima, o item “G - Falta de Energia da Concessionária” é o item mais crítico do sistema, não tem nenhum controle pela empresa e quando ocorre causa grandes transtornos e perda significativa da imagem da empresa. Desta forma trata-se de um item a ser mitigado, ou seja, é possível reduzir o impacto causado por esse problema com ações contingenciais e emergenciais, como o acionamento do PAESE (Plano de Atendimento entre Empresas de Transporte em Situação de Emergência), a evacuação e fechamento de estações, desembarques controlados na via férrea, etc.

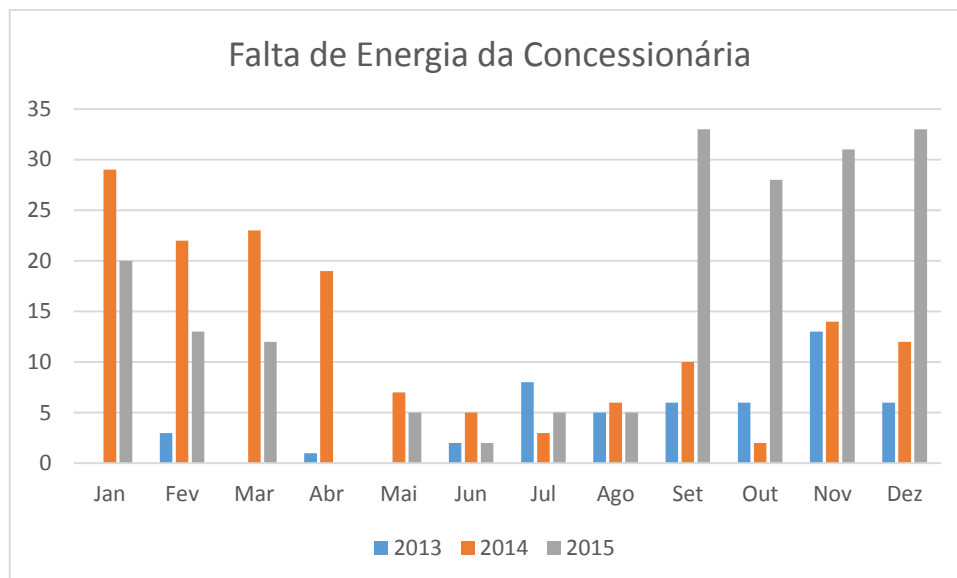


Figura 12 - Falta de Energia da Concessionária

O item “M - Perda do Sistema” que é um dos gargalos identificados, consiste em qualquer problema que de alguma forma impeça o funcionamento total do sistema, podendo ser:

- Perda de 2 servidores
- Perda de 2 switches
- Perda total do meio físico

Os servidores devem trabalhar de forma redundante e transparente, sendo que na perda de um servidor o outro deve assumir imediatamente todos os serviços do outro e para tanto o mesmo deve ter uma atenção especial sendo ele o pulmão do sistema.

O item “F - Erro de Envio de Comando” deve ser tratado, de preferência, via os sistemas de intertravamento de campo, porém, é possível também, em algumas situações, serem tratados via software do centro, evitando que qualquer comando identificado conceitualmente como errado sequer seja enviado ao campo.

Os efeitos de problemas decorrentes apenas da falha no sistema de energia não são considerados críticos, visto que existem outros métodos de controle.

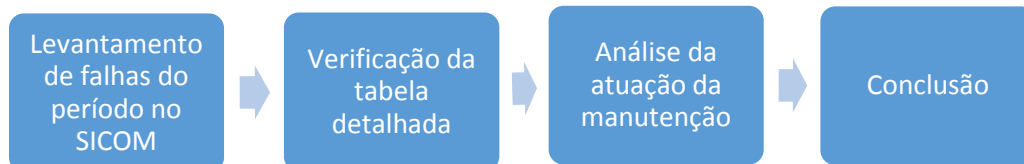
## 8. ANÁLISE DE FALHAS NO SISTEMA DE ENERGIA

### 8.1. ANÁLISE DE FALHAS DO SICOM

O SICOM (LAVORENTE, p.1) é o Sistema informatizado com acesso controlado e disponibilizado em rede de dados, onde são armazenadas informações sobre ocorrências operacionais e falhas, integrando as áreas de Operação, Manutenção e Segurança Operacional. É um sistema integrado de Controle da Operação e Manutenção e possui a funcionalidade de realizar o acompanhamento de todo o processo de abertura de falhas ou ocorrências via cadastro no sistema e possibilitando a consulta e realização de relatórios detalhados de todas as falhas, pendências e ocorrências dos equipamentos ou sistemas da CPTM.

Nesse documento foram realizados levantamentos no período de 01/01/2014 a 06/10/2015 conforme itens a seguir.

Para esse levantamento foi realizada a análise das falhas dos registros tabelados e detalhados constando a SAF (Solicitação de Abertura de Falha), FALHA, SSM (Solicitação do Serviço de Manutenção) e OSM (Ordem de Serviço de Manutenção).



*Figura 13 - SEQUÊNCIA DE ANÁLISE DO SISTEMA*

#### 8.1.1. FALHAS DO SISTEMA DE CONTROLE DE ENERGIA (SCE)

Dentro do SCE (onde o Telecontrole está incluso) existem diversos tipos de falhas como as descritas no Grupo de Sistema na tabela abaixo, porém, como o intuito do trabalho visa a comunicação dos sistemas do Telecontrole de Energia, serão utilizados os parâmetros do Telecontrole de Campo e Centro para o estudo. A análise desses parâmetros deve considerar ainda os itens que se referem a perda parcial ou total do Telecontrole em determinada localidade.

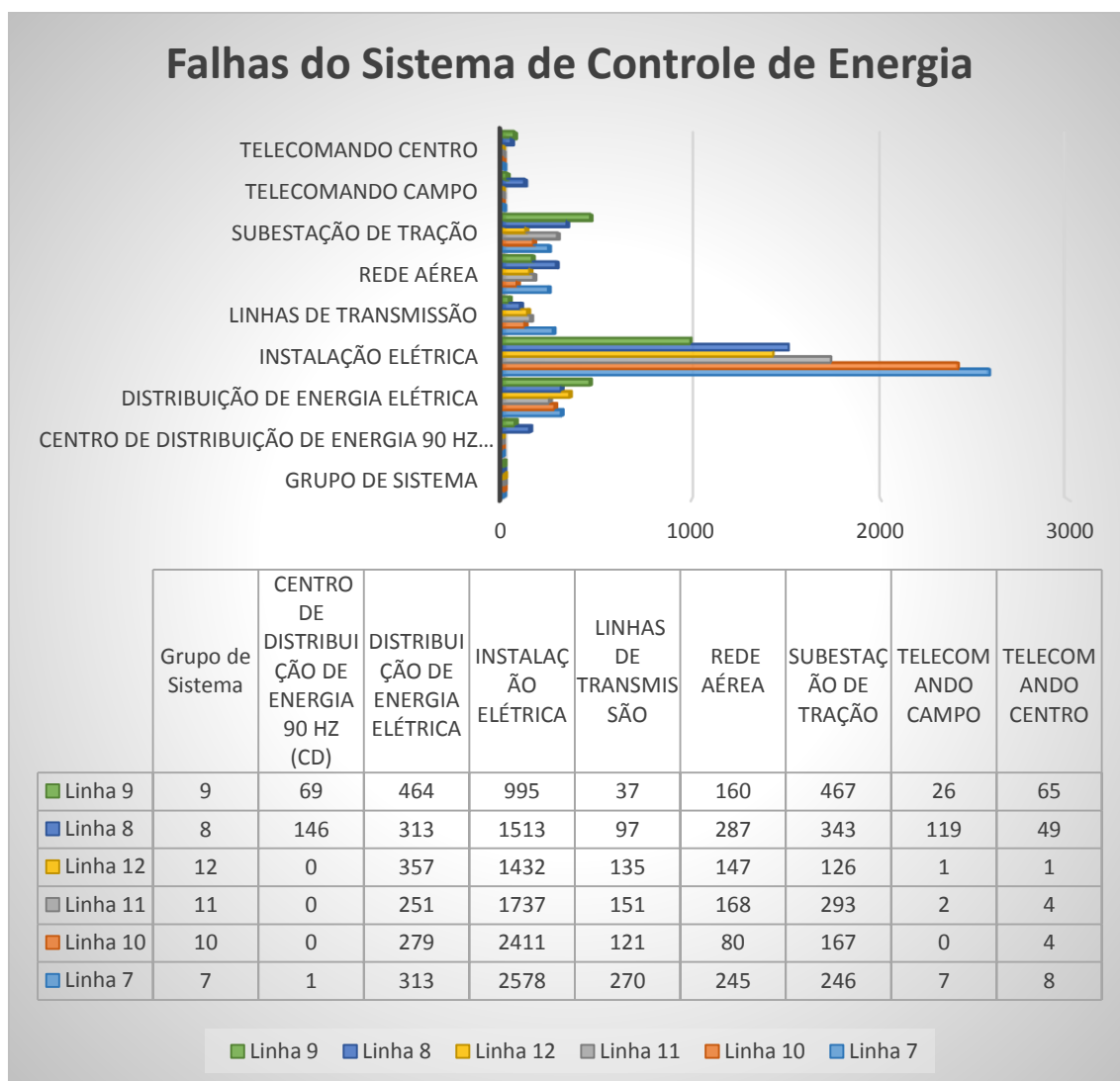


Figura 14 - Sistema de Controle de Energia – Período de 01/01/2014 à 06/10/2015

Observando o comportamento da figura 10, o Telecontrole nas linhas 7, 10, 11 e 12 possuem poucas falhas e isso é justificado pela recente implantação do Telecontrole nessas linhas (agosto 2015). Por outro lado, o Telecontrole da 8 possui um índice muito alto de falhas o que se justifica pela presença do Telecontrole antigo (Jeumont) ainda ser utilizado em pelo menos 60% das instalações e que está sendo substituído gradativamente.

Expandindo o relatório do “Telecontrole de campo” temos uma nova tabela conforme os dados a seguir.

*Tabela 4 – Quantidade de Falhas por Agente Causador – Telecontrole de Campo*

Agente Causador	7	10	11	12	8	9	Total
ATUAÇÃO DE PROTEÇÃO	3	0	0	0	10	10	23
CONCESSIONÁRIA SERVIÇOS PÚBLICOS / EQUIP. DE TERCEIROS	0	0	0	0	2	0	2
DESCARGA ATMOSFÉRICA	0	0	0	0	5	0	5
EFEITOS CLIMÁTICOS / ALAGAMENTO	0	0	0	0	2	0	2
ERRO NO PROCESSAMENTO	0	0	0	1	1	4	6
GRUPO DE SISTEMAS DIFERENTE	4	0	1	0	3	1	9
IMPREVISÍVEL E CIRCUNSTANCIAL	0	0	0	0	9	1	10
NÃO CARACTERIZA FALHA	0	0	0	0	4	0	4
NÃO IDENTIFICADO	0	0	0	0	29	2	31
PROJETO / EXECUÇÃO PELO FORNECEDOR	0	0	0	0	3	2	5
PRÓPRIO DO EQUIPAMENTO	0	0	0	0	46	6	52
TÉRMINO DA VIDA ÚTIL	0	0	0	0	2	0	2
<b>Total Liberadas por Linha</b>	7	0	1	1	116	26	151
<b>Total Geradas por Linha</b>	7	0	2	1	119	26	155

Como esperado a linha 8 é a única que sofre, devido ao término da vida útil dos equipamentos.

Expandindo o relatório do Telecontrole de centro temos uma nova tabela conforme os dados a seguir.

*Tabela 5 - Quantidade de Falhas por Agente Causador - Telecontrole de Campo*

	Linhas						
Agente Causador	7	10	11	12	8	9	Total
ATUAÇÃO DE PROTEÇÃO	1	0	1	0	2	8	12
CONCESSIONÁRIA SERVIÇOS PÚBLICOS / EQUIP. DE TERCEIROS	0	0	0	0	4	5	9
ERRO NO PROCESSAMENTO	5	2	2	1	5	22	37
GRUPO DE SISTEMAS DIFERENTE	0	0	0	0	12	7	19
IMPREVISÍVEL E CIRCUNSTANCIAL	0	0	1	0	1	3	5
NÃO IDENTIFICADO	0	0	0	0	14	5	19
PROJETO / EXECUÇÃO PELO FORNECEDOR	0	1	0	0	0	10	11
PRÓPRIO DO EQUIPAMENTO	2	1	0	0	5	3	11
<b>Total Liberadas por Linha</b>	8	4	4	1	43	63	123
<b>Total Geradas por Linha</b>	8	4	4	1	49	65	131

Analisando as falhas anteriores individualmente verifica-se que as falhas abertas pelos controladores muitas vezes caracterizam uma falha de comunicação segundo informações e relatórios de atuação da equipe de manutenção na OSM (Ordem de Serviço de Manutenção).

Conforme os itens dos agentes causadores não existem filtros de problemas de comunicação de dados e, dessa forma, foi necessária uma análise mais profunda, e também, a consulta a outra fonte de dados.

## 9. ANÁLISE DO SISTEMA SCADA OASYS DNA

O Sistema SCADA - Supervisory Control And Data Acquisition (Supervisão, Controle e Aquisição de Dados) é o conjunto de subsistemas que monitoram pontos e dispositivos, através de uma interface gráfica de software que interligado com uma base de dados proporciona o controle dos equipamentos de automação à distância e à aquisição de dados proveniente de Unidades Terminais Remotas (UTR), ou seja, fornece a visualização e controle dos objetos telecomandáveis em campo, diagnosticando, ajustando parâmetros, enviando e recebendo comandos via Sistema de Transmissão Ótica (STO).

O sistema OASYS DNA possui 3 subsistemas básicos para seu funcionamento, sendo eles o serviço de Histórico (Historical), Tempo Real (Real Time) e XOS (eXtended Operator Station).

O sistema de Tempo Real possui um conjunto de processos que recebem dados das remotas, checam as condições dos alarmes, convertem os valores, manejam os dispositivos de forma a assegurar o espaço de armazenamento para informações instantâneas e permitir aos operadores executar comandos sobre os dispositivos de campo.

A XOS é a estação de trabalho, que através de um conjunto de telas e listas, permite ao operador realizar as atividades de visualização e controle de forma cômoda e segura. Em outros sistemas o mesmo subsistema pode ser encontrado como IHM (Interface Homem Máquina).

O serviço de Histórico é responsável pela gravação de tudo que acontece no sistema, seja evento espontâneo ou forçado (manualmente ou remotamente), sendo esses causados pelos sistemas de proteção ou por pessoas habilitadas no decorrer de um intervalo programado, falha ou de necessidade operacional, permitindo a criação de relatórios e curvas de tendência, podendo essas informações serem consultadas a qualquer momento através do “Sumário de Eventos”, nosso próximo objeto de estudo. A verificação do SICOM trouxe problemas em que a manutenção precisou atuar de forma incisiva para a restauração do problema, porém, o sistema também identifica possíveis problemas na saúde do sistema e que, se não verificado atentamente, pode passar despercebido e causar problemas maiores se não devidamente tratados. Conforme análise de riscos do sistema, um dos gargalos do sistema está ligado aos servidores em função da maneira como foram concebidos. Realizando o levantamento



dos eventos de falhas nos sistemas críticos dos servidores foram obtidas as seguintes tabelas.

*Obs. Foram desconsideradas: alterações manuais do estado dos servidores mesmo no intuito de normalizar o sistema; registros duplicados do mesmo dia; determinadas falhas ocorrem centenas de vezes em um determinado período. Neste caso, quando ocorre uma falha do sistema, enquanto o sistema não é normalizado o mesmo fica tentando a comunicação ou o reestabelecimento e diante disso a mesma informação da queda de um serviço pode aparecer várias vezes não significando um novo evento.*

Tabela 6 – Relatório de Eventos – Dados de alteração dos Serviços

20/02/2015
O serviço Historical em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço Historical em CPTMRTS2 se alterou de HOT a FAIL.
25/02/2015
O serviço Historical em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço Historical em CPTMRTS2 se alterou de STANDBY a FAIL.
O serviço RCS em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço RCS em CPTMRTS2 se alterou de STANDBY a FAIL.
O serviço RealTime em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço RealTime em CPTMRTS2 se alterou de STANDBY a FAIL.
27/02/2015
O serviço Historical em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço RCS em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço RealTime em CPTMRTS1 se alterou de STANDBY a FAIL.
30/08/2015
O serviço Historical em CPTMRTS1 se alterou de HOT a FAIL.
31/08/2015
O serviço Historical em CPTMRTS2 se alterou de STANDBY a FAIL.
O serviço RealTime em CPTMRTS2 se alterou de STANDBY a FAIL.
03/09/2015
O serviço Historical em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço Historical em CPTMRTS2 se alterou de STANDBY a FAIL.
O serviço RCS em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço RealTime em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço RealTime em CPTMRTS2 se alterou de STANDBY a FAIL.
04/09/2015
O serviço Historical em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço RCS em CPTMRTS1 se alterou de HOT a FAIL.
O serviço RCS em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço RealTime em CPTMRTS1 se alterou de STANDBY a FAIL.
O serviço RealTime em CPTMRTS2 se alterou de STANDBY a FAIL.

08/09/2015
<b>O serviço RealTime em CPTMRTS1 se alterou de STANDBY a FAIL.</b>
<b>O serviço RealTime em CPTMRTS2 se alterou de STANDBY a FAIL.</b>
09/09/2015
<b>O serviço Historical em CPTMRTS2 se alterou de STANDBY a FAIL.</b>
16/09/2015
<b>O serviço RealTime em CPTMRTS1 se alterou de STANDBY a FAIL.</b>
<b>O serviço RealTime em CPTMRTS2 se alterou de STANDBY a FAIL.</b>
17/09/2015
<b>O serviço Historical em CPTMRTS2 se alterou de STANDBY a FAIL.</b>
25/09/2015
<b>O serviço Historical em CPTMRTS1 se alterou de HOT a FAIL.</b>
<b>O serviço Historical em CPTMRTS2 se alterou de HOT a FAIL.</b>
<b>O serviço RCS em CPTMRTS1 se alterou de HOT a FAIL.</b>
<b>O serviço RealTime em CPTMRTS1 se alterou de HOT a FAIL.</b>
<b>O serviço RealTime em CPTMRTS1 se alterou de STANDBY a FAIL.</b>
29/09/2015
<b>O serviço RealTime em CPTMRTS2 se alterou de HOT a FAIL.</b>

Para essa análise foi considerado que se um servidor, por algum motivo, passou do estado HOT a FAIL ou STANDBY a FAIL, algum problema ocorreu e, portanto, deve ser considerado e analisado. A perda de ambos os servidores é considerada quando os serviços de “real time” estão paralisados em ambos os servidores, o que ocorre nesse período (01/01/2015 à 05/10/2015) por 6 vezes e que é considerado crítico para o sistema conforme análise de riscos. A perda do histórico em ambos os servidores significa que a informação das manobras e eventos serão perdidas durante esse período e a perda do RCS (Remote Client Service) indica que todos os consoles remotos não funcionarão (Console Supervisão e Vídeo Wall das 6 linhas).

De forma a verificar e confrontar os dados acima foram levantados os logs do sistema contendo os serviços de Real Time, Historical e RCS nos servidores 1 e 2 e representado na tabela a seguir.

A pesquisa sobre os logs de eventos identifica quantas vezes os serviços críticos saíram do estado de HOT ou STANDBY e passaram a FAIL deixando o sistema com degradação parcial ou total.

Nessas tabelas (Tabela 1 e 2) é perceptível que com a entrada das novas localidades em agosto, houve aumento considerável do índice de falhas referentes aos servidores do Telecontrole de Energia.

Tabela 7 - Sumário de Eventos – 05/10/2015

Problemas nos Servidores (Ano 2015) - logs	SVR1			SVR2		
	REALTIME	HISTORICAL	RCS	REALTIME	HISTORICAL	RCS
20/02/2015		X			X	
25/02/2015	X	X	X	X	X	X
27/02/2015	X	X	X			
30/08/2015		X				
31/08/2015				X	X	
03/09/2015	X	X	X	X	X	
04/09/2015	X	X	X	X		X
08/09/2015	X			X		
09/09/2015					X	
16/09/2015	X			X		
17/09/2015					X	
25/09/2015	X	X	X	X	X	
29/09/2015				X		

Tabela 8 - Log de Eventos – 05/10/2015

Problemas nos Servidores (Ano 2015) - logs	SVR1			SVR2		
	REALTIME	HISTORICAL	RCS	REALTIME	HISTORICAL	RCS
04/02/2015	X	X	X			
10/03/2015	X	X	X	X	X	X
03/09/2015	X	X	X	X	X	X
04/09/2015	X		X	X	X	X
16/09/2015	X			X	X	X
17/09/2015	X	X	X	X	X	X
25/09/2015	X			X	X	X
26/09/2015	X					
29/09/2015	X	X	X	X		

Dentro do período foram constatados 7 dias com perda total dos servidores (realtime dos SVR1 e SVR2) e que, em conjunto com a falta de operadores nas localidades e existência de desarmes em cascatas, poderia causar sérios transtornos à circulação de trens.

Atualmente para guarnecer uma localidade e fornecer alta disponibilidade (24X7) são necessárias 8 pessoas distribuídas em regime de escala. O sistema estando em funcionamento pleno terá 44 localidades operacionais somente pelo sistema OASYS e, em caso de pane nos sistemas críticos, serão necessárias imediatamente 88 pessoas

para substituir completamente as funcionalidades do sistema e garantir assim a continuidade do negócio.

Com a identificação de problemas periódicos foi necessário a análise das informações que trafegam na rede em relação à capacidade do sistema.

## 10. ANÁLISE DO TRÁFEGO DE DADOS

Para a análise do tráfego foi utilizado o analisador de protocolos desenvolvido para o Telecontrole de Energia (DNA SWANA – Software Protocol Analyzer) e que possui uma interface amigável para a verificação de até 5 localidades ao mesmo tempo.

Dentre os protocolos desenvolvidos para Sistema estão:

Modbus RTU/TCP; DNP Serial/TCP; IEC 101, 103, 104, 61850; Modbus Enron; OPC Client/Server; BACnet; Fisher ROC; Actaris; Instromet; British Gas, entre outros.

Com o Software Protocol Analyzer é possível verificar o que está saindo e chegando de um determinado ponto na rede. O sistema foi moldado para identificar uma Pergunta (Q: Query) e uma Resposta (R: Response) em valores hexadecimal (base16), octal (base 8) e decimal (base10).

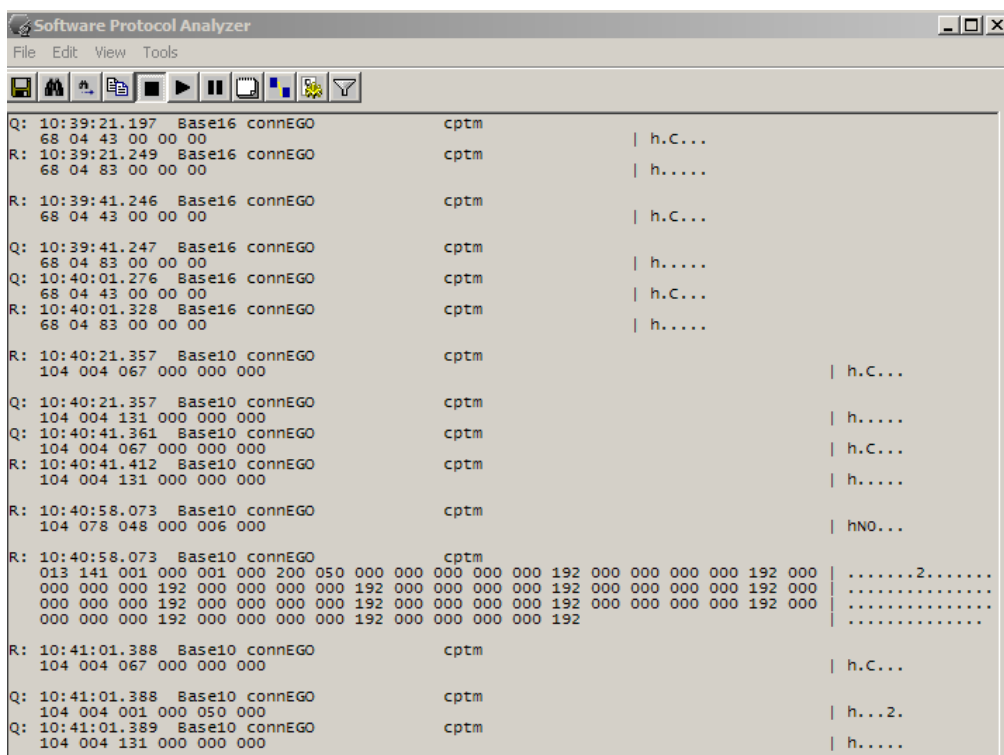


Figura 15 - Analisador de protocolo - DNA SWANA

A análise realizada foi a quantitativa conforme figura a seguir.

1CSBTJ.log	11/01/2016 10:31	Documento de Te...	4 KB
2CSALV.log	11/01/2016 10:34	Documento de Te...	5 KB
3SECDU.log	11/01/2016 10:37	Documento de Te...	477 KB
4CSEGO.log	11/01/2016 10:41	Documento de Te...	3 KB
5CSFDR.log	11/01/2016 10:45	Documento de Te...	5 KB
6SEJAG.log	11/01/2016 10:48	Documento de Te...	355 KB
7CSJPR.log	11/01/2016 10:51	Documento de Te...	80 KB
8SEMRB.log	11/01/2016 10:53	Documento de Te...	264 KB
9CSMTD.log	11/01/2016 10:56	Documento de Te...	4 KB
10CSNOT.log	11/01/2016 10:59	Documento de Te...	189 KB
11CSVCL.log	11/01/2016 11:02	Documento de Te...	5 KB

Figura 16 - Quantidade de Bytes transmitidos

A análise foi realizada durante 2 minutos de amostragem em cada localidade no intuito de verificar a quantidade de Bytes transmitidos e recebidos (Nota-se que não haviam comandos sendo enviados). Os protocolos utilizados nessas cabines e subestações são o IEC101 e ICE104 (Não são utilizados os protocolos Modbus e OPC relacionado na base de dados abaixo).

Table / Record	Name
IEC101 (18)	
IEC101: CS_GRA	CS_GRA
IEC101: CS_JUR	CS_JUR
IEC101: CS_PIN	CS_PIN
IEC101: CS_SAM	CS_SAM
IEC101: ES_AUT	ES_AUT
IEC101: ES_BRR	ES_BRR
IEC101: ES_CEA	ES_CEA
IEC101: ES_GJT	ES_GJT
IEC101: ES_GRA	ES_GRA
IEC101: ES_JUR	ES_JUR
IEC101: ES_PIN	ES_PIN
IEC101: ES_SAM	ES_SAM
IEC101: ES_VOL	ES_VOL
IEC101: SE_CDU	SE_CDU
IEC101: SE_CJD	SE_CJD
IEC101: SE_JAG	SE_JAG
IEC101: SE_MRB	SE_MRB
IEC101: SE_SOC	SE_SOC
IEC104	
Modbus	
OPC	

Figura 17 - Protocolo IEC101

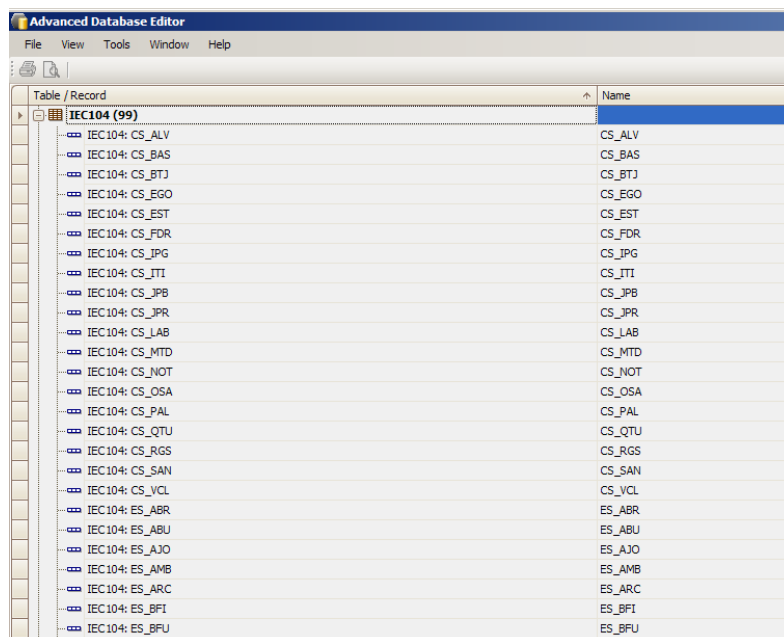


Table / Record	Name
IEC 104: CS_ALV	CS_ALV
IEC 104: CS_BAS	CS_BAS
IEC 104: CS_BTJ	CS_BTJ
IEC 104: CS_EGO	CS_EGO
IEC 104: CS_EST	CS_EST
IEC 104: CS_FDR	CS_FDR
IEC 104: CS_IPG	CS_IPG
IEC 104: CS_ITI	CS_ITI
IEC 104: CS_JPB	CS_JPB
IEC 104: CS_JPR	CS_JPR
IEC 104: CS_LAB	CS_LAB
IEC 104: CS_MTD	CS_MTD
IEC 104: CS_NOT	CS_NOT
IEC 104: CS_OSA	CS_OSA
IEC 104: CS_PAL	CS_PAL
IEC 104: CS_QTU	CS_QTU
IEC 104: CS_RGS	CS_RGS
IEC 104: CS_SAN	CS_SAN
IEC 104: CS_VCL	CS_VCL
IEC 104: ES_ABR	ES_ABR
IEC 104: ES_ABU	ES_ABU
IEC 104: ES_AJO	ES_AJO
IEC 104: ES_AMB	ES_AMB
IEC 104: ES_ARC	ES_ARC
IEC 104: ES_BFI	ES_BFI
IEC 104: ES_BFU	ES_BFU

Figura 18 - Protocolo 104

Para a análise foi realizada a divisão entre cabines, subestações e protocolos para que todos os dados sigam os mesmos critérios, tendo em vista que uma subestação possui muito mais pontos do que uma cabine.

Tabela 9 - Análise de Subestações (IEC101)

Subestações (IEC101)	Tempo duração da análise	Quantidade de pontos	Quantidade de Bytes
<b>SE CDU – Cidade Dutra</b>	2 min	341	477KB
<b>SE MRB – Morumbi</b>	2 min	341	264KB
<b>SE JAG – Jaguaré</b>	2 min	341	355KB

Verificando a maior diferença (SE CDU e SE MRB), temos cerca de 213KB (218.112 caracteres) de diferença entre a comunicação da SE CDU e a SE MRB, valor esse que em um dia se transforma em 153MB e em um mês 4,59GB (Nota-se que o tráfego não é armazenado e sim os logs de eventos, que registram as alterações de estado).

Na verificação a seguir notam-se duas anomalias (CS JPR - Linha 8 e CS NOT - Linha 7), sendo que as demais seguem um padrão relativamente parecido e aceitável em relação a quantidade de dados trocados entre o campo e o centro dentre equipamentos em equivalentes condições.

*Tabela 10 - Análise de Cabines de Seccionamento (IEC104)*

<b>CABINES DE SECCIONAMENTO (IEC104)</b>	<b>Tempo duração da análise</b>	<b>Quantidade de pontos</b>	<b>Quantidade de Bytes</b>
<b>CS BTJ - Botujuru</b>	2 min	153	4KB
<b>CS ALV - Artur Alvim</b>	2 min	97	5KB
<b>CS EGO - Eng. Goulart</b>	2 min	115	3KB
<b>CS FDR - Franco da Rocha</b>	2 min	153	5KB
<b>CS JPR - Júlio Prestes</b>	2 min	146	80KB
<b>CS MTD - Vila Matilde</b>	2 min	107	4KB
<b>CS NOT - Nothman</b>	2 min	196	189KB
<b>CS VCL - Vila Clarice</b>	2 min	176	5KB

Verificado a quantidade de pontos por localidade nota-se que a CS NOT possui mais pontos do que as demais, porém, não justificaria a enorme troca de informações no mesmo intervalo de tempo. Nesse caso, e conforme análise anterior das subestações, verificamos que a maior diferença está entre as Cabines Seccionadoras de EGO e NOT com 196kB (190464 Caracteres), que calculado em um dia obtemos 141MB e em um mês 4.2GB de diferença de Bytes enviados.

Conclui-se que devesse adequar a quantidade de perguntas e respostas, num determinado período, de todo o sistema de forma a padronizar a troca de informações e detectar alterações de estado.



## 11. CONCLUSÃO

A média de usuários transportados pela CPTM vem aumentando e junto com esse aumento, cresce também a necessidade de garantir a disponibilidade e confiabilidade do sistema a parâmetros aceitáveis e de forma a dar continuidade aos serviços prestados.

Diante dessa necessidade, a proposta dessa monografia foi mostrar situações de riscos e falhas ainda não mensuradas, de forma a antecipar problemas que poderão ocorrer em consequência do tempo de exposição dos equipamentos do Telecontrole de Energia às circunstâncias de riscos avaliadas. Com isso foi realizado um estudo de forma a identificar quais problemas podem causar perdas significativas para a empresa, qualificando e contabilizando dados gerenciáveis dos sistemas. Através desse estudo foi possível identificar que a perda de ambos os servidores pode oferecer prejuízos financeiros para a empresa se não tratados devidamente, sendo necessário o estudo de um plano de continuidade de negócios efetivo.

Devido ao Telecontrole de Energia ser um sistema relativamente novo, ainda não foram considerados e explorados os itens desse sistema de forma a possibilitar o desenvolvimento de um relatório gerencial de manutenção apropriado, que possa auxiliar a tomada de decisões de forma rápida e segura pela equipe de Engenharia de Manutenção. Esse aspecto indica, portanto, que o SICOM precisa ser remodelado de forma a atender essa necessidade, melhorando assim a análise e auditorias dos sistemas. Por meio dessa melhoria, será possível o estudo adequado do comportamento das falhas do sistema de Telecontrole de Energia de forma a realizar uma manutenção preditiva de forma satisfatória.

O estudo realizado, também foi capaz de elencar quais restrições seriam mais impactantes para o sistema. Dessa forma, as atenções foram direcionadas para os Servidores, onde foram analisadas as falhas no SICOM, relatório de eventos do sistema OASYS DNA, Logs dos Servidores do Sistema de Telecontrole de Energia e análise do tráfego da rede com o DNA SWANA. Essa análise permitiu levantar os problemas existentes e o comportamento do sistema.

De acordo com a análise realizada, os sistemas essenciais precisam melhorar sua disponibilidade e, dessa forma, será necessário a realização de serviços como limpeza lógica, avaliação do tempo de vida útil dos equipamentos, bem como, a substituição de equipamentos obsoletos e remodelagem da arquitetura existente. Conforme descrito no contexto atual, os equipamentos de centro estão todos dispostos em apenas um local

e, para garantir a continuidade dos serviços, é recomendado a criação de um site backup com os equipamentos básicos necessários dispostos de forma que o sistema possa continuar a ser monitorado e controlado em situações críticas, como a perda do centro de controle em casos de agentes externos à empresa. Dessa forma não será necessário um número grande de pessoas para guarnecer as localidades essenciais durante uma queda dos servidores do centro de controle ou a necessidade de manutenção nos equipamentos do centro de controle operacional. Com o site Backup um funcionário treinado e habilitado poderá acessar o sistema e dar continuidade aos serviços necessários sem perdas.

Foi também constatado divergências na quantidade de Bytes transmitidos entre as localidades (Subestações e Cabines de Seccionamento e paralelismo) durante a análise do tráfego de rede. Contudo os parâmetros devem ser estudados e alinhados de forma a encontrar um ponto ideal em que as mensagens sejam enviadas em um tempo que não onere a rede e que não impacte no tempo de resposta de eventuais transições ou sinalizações dos equipamentos de campo. Assim será evitado o mascaramento de dados, ou seja, um tempo de resposta muito pequeno pode criar um gargalo quanto a capacidade de transporte da rede. Por outro lado, um tempo de resposta muito grande pode ocultar falhas na entrega de pacotes ou mesmo vir a atrapalhar na interpretação do sistema pelo operador mascarando problemas.

## 12. BIBLIOGRAFIA

EGOSHI, Koiti. **Análise de Riscos**. São Paulo, out. 2008 (Apostila)

BARROS, Sergio Silveira de. **Análise de Riscos**. Instituto Federal do Paraná. Rede e-Tec Brasil, nov.2011 Disponível em:

[http://ead.ifap.edu.br/netsys/public/livros/LIVROS%20SEGURAN%C3%87A%20DO%20TRABALHO/M%C3%B3dulo%20III/16%20An%C3%A1lise%20de%20Riscos/Livro\\_An%C3%A1lise%20de%20Riscos.pdf](http://ead.ifap.edu.br/netsys/public/livros/LIVROS%20SEGURAN%C3%87A%20DO%20TRABALHO/M%C3%B3dulo%20III/16%20An%C3%A1lise%20de%20Riscos/Livro_An%C3%A1lise%20de%20Riscos.pdf). Acessado em 20 de janeiro de 2016.

LAVORENTE, José Luiz; JORDANI, José Henrique; Travassos, José Carlos. SICOM - Sistema Integrado de Controle de Operação e Manutenção. Norma de Serviço NS.DO/031 VS.4, out. 2013. Acessado em 15 dez 2015.

TELVENT. **Manual de Operação do SCADA OASYS das Linhas 7, 8, 9, 10, 11 e 12 da CPTM**, Disponível em:

[http://webcptm/Operacao/PortalSeg\\_APP/Adm/files/CCO%20TRINAMENTO%20Apostila%20OASYS.pdf](http://webcptm/Operacao/PortalSeg_APP/Adm/files/CCO%20TRINAMENTO%20Apostila%20OASYS.pdf). Acessado em 25 de novembro de 2015.

BRITO, Alexandre Ferraz. Apostila de Treinamento CCTI Módulo IV. São Paulo, Fev. 2012

Disponível em: <http://intranet/operacao/CCO/Treinamento/Apostilas/COE.pdf>