OTIMIZAÇÃO DA COMUNICAÇÃO ENTRE CLP E ESTAÇÕES DE OPERAÇÕES COM REDUNDÂNCIA FÍSICA, ROTINAS DE WATCHDOG E HOT STANDBY

Ely Alves de Paula Júnior[1], Luís Augusto Mattos Mendes (Orientador)[2]

[1]Departamento de Ciência da Computação – Universidade Presidente Antônio Carlos (UNIPAC)
Campus Magnus – Barbacena – MG – Brasil

ely.junior@techely.com.br[1], luisaugustomendes@yahoo.com.br[2]

Resumo. *Atualmente, com o aumento de áreas automatizadas nas indústrias, o número de clientes OPC[1] que solicitam dados dos sistemas de automação segue a mesma tendência, assim este artigo apresenta otimizações físicas na estrutura da rede e algoritmos que validam a comunicação entre CLP's[2] e Estações de Operações chaveando a mesma em caso de falhas de comunicação para outro servidor OPC.*

Palavras-Chave: OPC; CLP; Redundância; Watchdog; Hot Standby.

1. Introdução

Historicamente o processo de automação industrial começa na década de 1920 com Henry Ford e sua linha de montagem de automóveis. Posteriormente, nos anos de 1960 assistimos ao desenvolvimento da microeletrônica, o que possibilitou o desenvolvimento dos CLP's.

Na década de 1990, encontram-se os novos sistemas de supervisão e controle, desenvolvidos especialmente com o objetivo de obter maior produtividade, qualidade e competitividade para esta nova realidade. Basicamente podem-se dividir sistemas de automação em duas funções básicas: controle e supervisão. Controle é a função ou requisitos pré estabelecidos nos CLP's que podem ou não ter a intervenção de sistemas externos para controlar atividades de processo produtivo. A função de Supervisão consiste na monitoração dos processos, através de interfaces sinóticas (formulários),

[1] (Protocolo OLE para Controle de Processo)[2]
[2] CLP's (Controladores Lógicos Programáveis)[1], que é um aparelho eletrônico digital que utiliza uma memória programável para armazenar internamente instruções e implementar funções específicas, tais como lógica, seqüenciamento, temporização, contagem e aritmética, controlando, vários tipos de máquinas ou processos, que substituíram os painéis de controle com [1] [2].

gráficos de tendências, relatórios diversos, dentre outros. Um sistema supervisório permite que sejam monitoradas e rastreadas informações de um processo produtivo ou instalação física. Tais informações são coletadas através de equipamentos de aquisição de dados e, em seguida, manipuladas, analisadas, armazenadas e, posteriormente, apresentadas ao usuário.

Estes sistemas também são conhecidos como SCADA (*Supervisory Control and Data Acquisition),* sistemas que utilizam software para monitorar e supervisionar variáveis e dispositivos de sistemas de controle conectados através de *drivers* (Aplicativos que fazem interface entre o CLP e os sistemas SCADA) específicos. Um sistema supervisório deve apresentar algumas funcionalidades básicas, entre elas destacam-se a visualização de dados, que consiste na apresentação das informações através de um HMI (*Human Machine Interface* – Sistema supervisório para operação e monitoramento de processos), geralmente acompanhados por animações, de modo a simular a evolução do estado dos dispositivos controlados na instalação industrial. Tolerância a falhas que para atingir níveis aceitáveis é usual a existência de informação redundante na rede e de máquinas *backups* nas instalações das indústrias de forma a permitir que sempre que se verifique uma falha num computador, o controle das operações seja transferido automaticamente para outro computador [2].

2. Cenário

O ambiente de rede se passa em uma indústria cimenteira composto por vários níveis. A Figura 1[3] representa graficamente este modelo de referência, diferenciando apenas na localização do Roteador que se encontra entre os níveis 3 e 4.

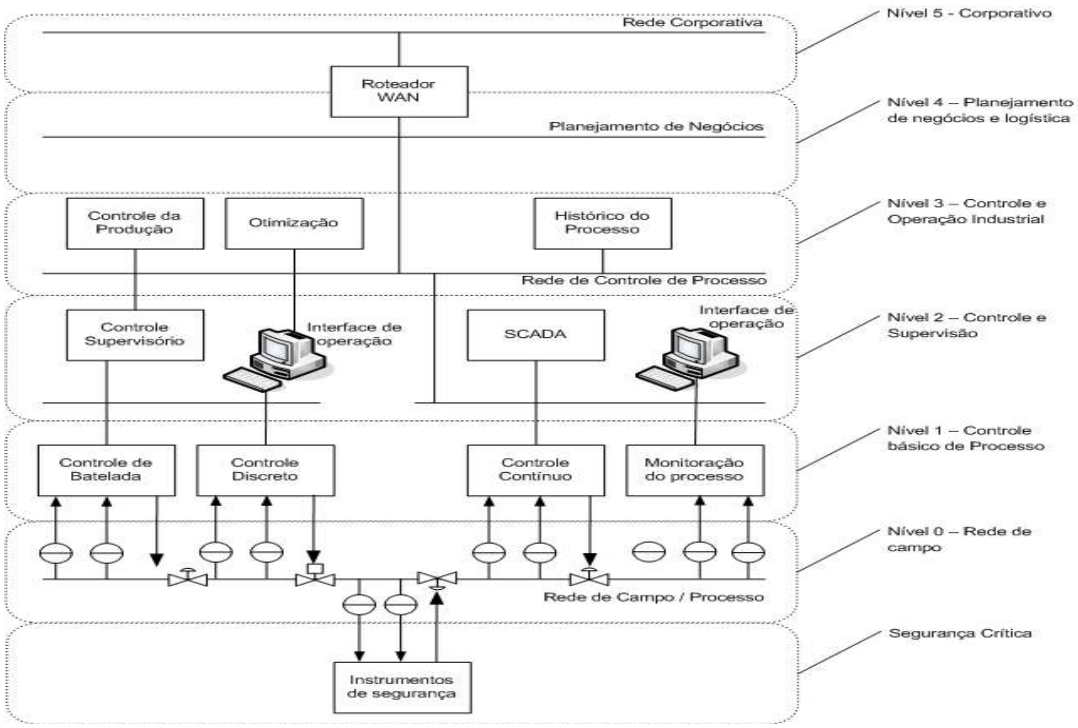


Figura 1. Modelo de referência geral

Os seis níveis de referência do modelo, como demonstrado na Figura 1, são descritos a seguir [3]:

Nível 5 – Corporativo.
Incluem os sistemas da corporação, como sistemas de gerenciamento, sistemas de correio eletrônico, intranet e outros.

Nível 4 – Administração
Este nível inclui sistemas de planejamento da produção, gerenciamento de manutenção e inspeção preditiva dentre outros.

Nível 3 – Operações de manufatura e controle.
Este nível inclui sistemas de planejamento detalhado de produção, dados históricos com longo período de armazenamento, otimização de custos e processos específicos, consolidação de relatórios e outros.

Nível 2 – Operação, controle e supervisão.
Neste nível são realizadas as funções de operação da planta de produção. Os sistemas deste nível são responsáveis por prover uma interface homem-máquina para o operador, gerar alarmes e alertas, funções de controle e supervisão e gerar dados históricos com curto período de armazenamento.

Nível 1 – Controle básico de processo.
Este nível inclui os equipamentos de controle e monitoração, que estão diretamente ligados aos sensores (instrumentos de medição de variáveis de processo) e elementos finais de controle do processo (válvulas de controle, motores elétricos e outros). Os equipamentos de controle são responsáveis por ler os dados dos sensores, executarem um algoritmo, enviar uma saída para o elemento final de controle.

Nível 0 – Rede de campo.
Este nível é também conhecido como chão de fábrica e inclui os vários tipos de sensores e elementos finais de controle que são diretamente conectados ao processo ou aos equipamentos de um processo industrial. Os sensores são responsáveis por medir a variável do processo (pressão, temperatura, nível, fluxo e outros) e enviar ao equipamento de controle.

O foco deste artigo será a rede industrial nível 1 e 2 dos sistemas de automação, onde serão propostas as melhorias. Estes dois níveis são compostos de 04 Servidores, 13 estações de operações e 38 CLP’s distribuídos conforme Figura 2.

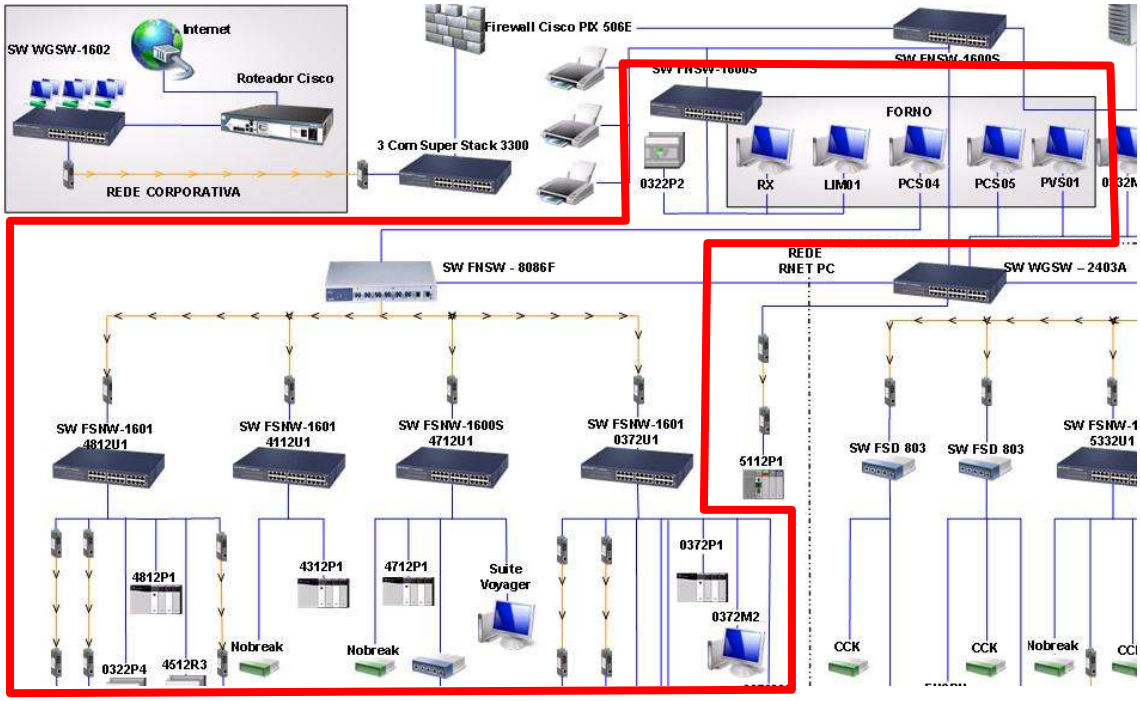


Figura 2. Diagrama parcial de Rede da Automação

Será delimitado o trabalho na rede industrial, especificamente nas estações de operações do forno, conforme destacado na Figura 2 onde temos um potencial de melhoria.

A topologia física implementada é a de estrela, formada através do switch principal Planet WGSW-2403A cascateados com outros 2 switches Planet FNSW-1600S, distribuindo acessos aos sub switches FNSW-1600S e FNSW-1601 através de links de fibra óptica provenientes de 2 switches ópticos Planet FNSW-8086F e conversores de mídia.

Os servidores da automação estão divididos em, um Controlador de Domínio com Microsoft Windows 2003 Server SP2, dois servidores de banco de dados com a plataforma do Microsoft Windows 2000 Server SP4 um com SQL Server 2000 e o segundo com *InSQL (Industrial Structured Query Language)* 9.0 da Wonderware e o último um servidor Web executando Microsoft Windows 2003 Server SP2 e um portal de relatórios web *SuiteVoyager*. O software SCADA utilizado nas HMI's é o *Intouch* da empresa *Wonderware* na versão 7.11 com uma aplicação dedicada ao forno com 30906 variáveis internas e externas com 1024 janelas de operações.

Essa aplicação é executada em quatro computadores industriais com Microsoft Windows 2000 Professional SP4 todas comunicando diretamente com os CLP's utilizando o protocolo OPC através de um servidor OPC chamado RSlinx V2.51 e um driver cliente OPCClient V 2.0.

3. Análise dos Problemas encontrados

Com o crescimento das áreas automatizadas nos últimos anos e com um número expressivo de novos equipamentos em rede, mais variáveis sendo requisitadas nos CLP's, ativos de rede sem características para ambientes industriais, excesso de pó, falta de redundância na rede, falta de rotinas de controle e monitoramento da comunicação,

foi percebido um aumento de erros de comunicação entre CLP's e Estações de Operações. Tempos de respostas que antes demoravam segundos, passaram a demorar minutos para se concretizarem, e até falhas nos processos produtivos, foram os principais motivos para o estudo de uma melhoria da estrutura física da rede e de um algoritmo de controle dessa comunicação.

Nos últimos dois anos foi constatado um aumento no número de falhas de comunicação considerável nos sistemas de automação do forno, como é mostrado na Figura 3 um gráfico pareto de falhas por CLP extraído do sistema de gerenciamento industrial *SAP (Serviços, Aplicações e Produtos em Processamento de Dados).*

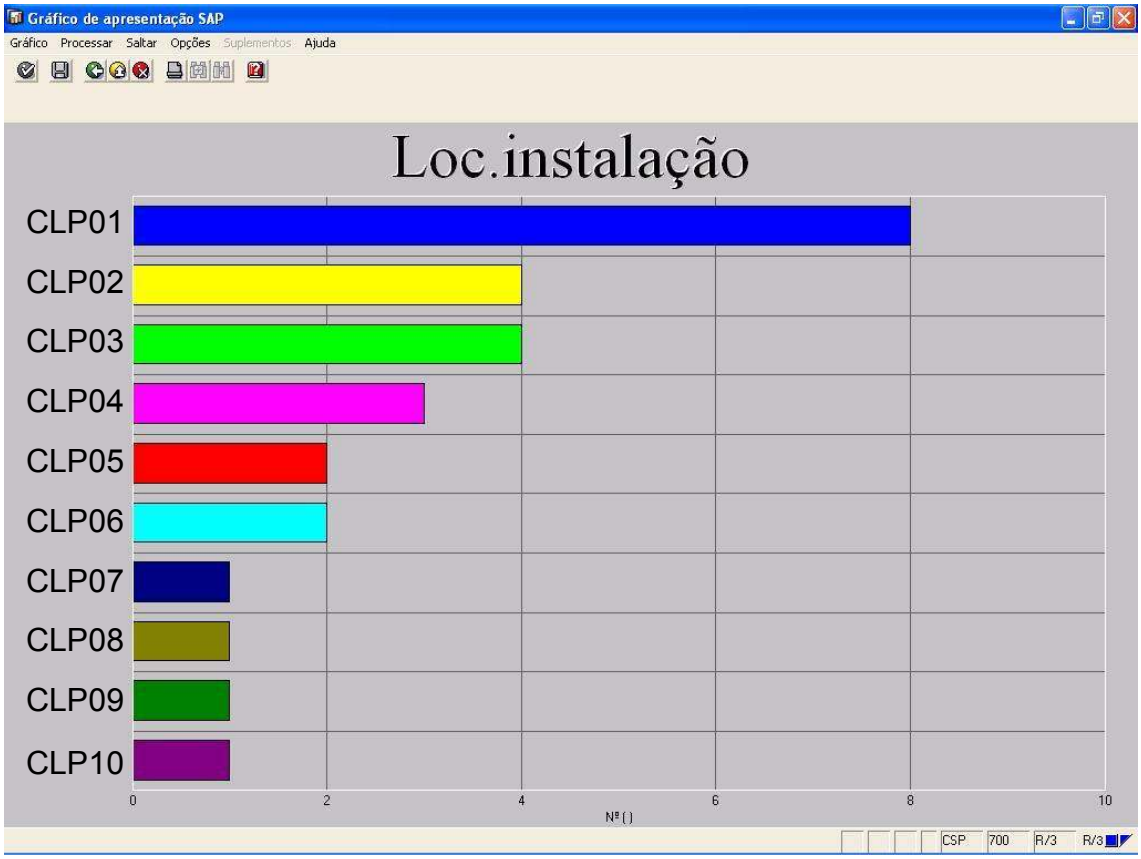
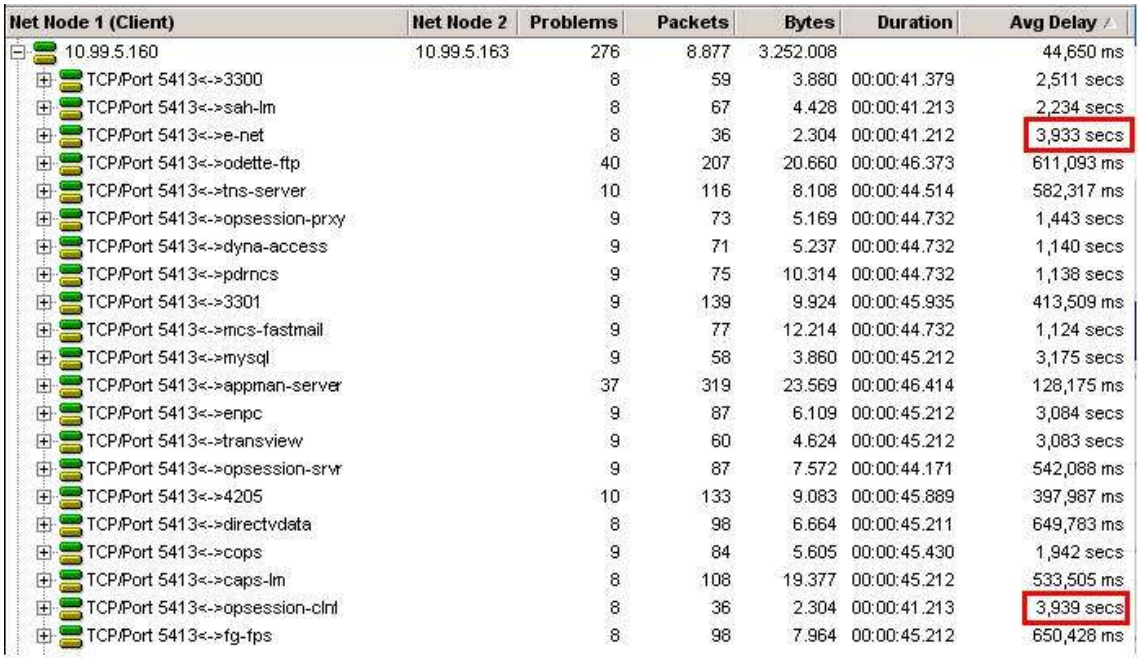


Figura 3. Pareto de Falhas por CLP SAP

Como mostra a barra azul no gráfico da Figura 3, o CLP01 parou 8 vezes por falhas, sendo a maioria delas relativa à perda de comunicação.

Através das estatísticas realizadas com um *Sniffer* (*Software ou Hardware* capaz de interceptar e registrar o tráfego de dados em uma rede de computadores) de rede *EtherPeek* na versão 4.2 através de espelhamento de todas as portas para a porta 15 do switch principal Planet WGSW-2403A, foi detectado em algumas portas erros de CRC *(Cyclic redundancy check)* [4]. Uma característica nos *Sniffer's* de rede é que ainda não possuem regras definidas para protocolos de redes industriais dificultando muitas das vezes o diagnóstico preciso do problema [4].



Net Node 1 (Client)	Net Node 2	Problems	Packets	Bytes	Duration	Avg Delay
10.99.5.160	10.99.5.163	276	8.877	3.252.008		44,650 ms
TCP/Port 5413<->3300		8	59	3.880	00:00:41.379	2,511 secs
TCP/Port 5413<->sah-lm		8	67	4.428	00:00:41.213	2,234 secs
TCP/Port 5413<->e-net		8	36	2.304	00:00:41.212	3,933 secs
TCP/Port 5413<->odette-ftp		40	207	20.660	00:00:46.373	611,093 ms
TCP/Port 5413<->tns-server		10	116	8.108	00:00:44.514	582,317 ms
TCP/Port 5413<->opsession-prxy		9	73	5.169	00:00:44.732	1,443 secs
TCP/Port 5413<->dyna-access		9	71	5.237	00:00:44.732	1,140 secs
TCP/Port 5413<->pdrncs		9	75	10.314	00:00:44.732	1,138 secs
TCP/Port 5413<->3301		9	139	9.924	00:00:45.935	413,509 ms
TCP/Port 5413<->mcs-fastmail		9	77	12.214	00:00:44.732	1,124 secs
TCP/Port 5413<->mysql		9	58	3.860	00:00:45.212	3,175 secs
TCP/Port 5413<->appman-server		37	319	23.569	00:00:46.414	128,175 ms
TCP/Port 5413<->enpc		9	87	6.109	00:00:45.212	3,084 secs
TCP/Port 5413<->transview		9	60	4.624	00:00:45.212	3,083 secs
TCP/Port 5413<->opsession-srvr		9	87	7.572	00:00:44.171	542,088 ms
TCP/Port 5413<->4205		10	133	9.083	00:00:45.889	397,987 ms
TCP/Port 5413<->directvdata		8	98	6.664	00:00:45.211	649,783 ms
TCP/Port 5413<->cops		9	84	5.605	00:00:45.430	1,942 secs
TCP/Port 5413<->caps-lm		8	108	19.377	00:00:45.212	533,505 ms
TCP/Port 5413<->opsession-clnt		8	36	2.304	00:00:41.213	3,939 secs
TCP/Port 5413<->fg-fps		8	98	7.964	00:00:45.212	650,428 ms

Figura 4. Tempo de latência elevado [4]

Através das várias portas de serviço abertas pode-se constatar que as mesmas possuem vários serviços em operação simultânea, elevando a taxa de processamento destas estações e aumentando, desta forma, o tempo de resposta das estações, como observado na Figura 4.

Fisicamente a Topologia da rede encontrada na automação é plana não possuindo um nível de hierarquia adequada, não há redundância na comunicação entre Estações de Operações e os CLP's, o switch principal Planet WGSW-2403A não possui características de um switch Core.

A velocidade da rede é 100Mbps tanto para Estações de Operações, para Uplinks, Servidores e CLP's. Não há utilização de tecnologia Gigabit para Estações de Operações, Uplinks e Servidores, o que pode degradar a performance de acordo com a utilização, criando gargalos.

4. Modificações sugeridas na estrutura de rede

Após um estudo da arquitetura da rede, notou-se que seria interessante fazer modificações na mesma, tais como passar a velocidade de comunicação entre os servidores e estações de operações para gigabit substituindo o switch principal, substituir ativos de redes por ativos com características industriais, criar uma redundância física garantindo duas rotas de comunicação caso o Planet WGSW-2403A entrasse em falha. Para isso seria necessário reposicionar uma das estações de operações e conectá-la diretamente no switch óptico FNSW-8086F conforme mostrado na Figura 5, com isso se ganha mais uma rota de comunicação com os CLP's da área do Forno. A segunda estação de operações permanece no switch principal.

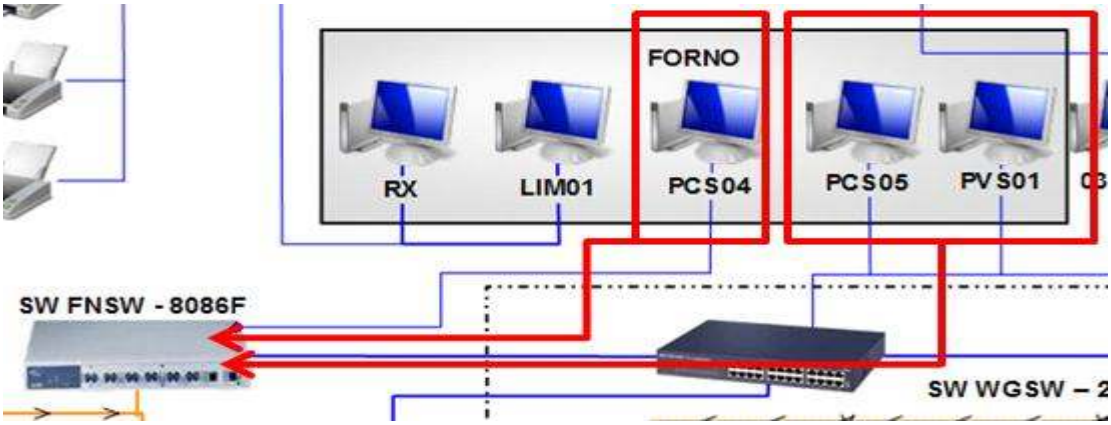


Figura 5. Redundância física de comunicação

Com as medidas propostas, pode-se observar uma maior disponibilidade nos sistemas de automação em caso de falhas no switch principal e por conseqüência ter um processo contínuo produtivo de uma indústria automatizada.

5. Rotinas de watchdog e hot standby

Com a implementação das rotinas sugeridas neste artigo, será menor o número de conexões abertas diretamente entre os CLP's e as estações de operações visto que as estações de operações clientes irão comunicar com a estação de operação servidora de dados e não mais com o CLP, diminuindo assim várias conexões com o CLP.

À medida que o número de clientes OPC aumenta na rede, nota-se um aumento no tempo de resposta entre o servidor OPC e o Cliente OPC. Criam-se dois algoritmos, o primeiro chamado de watchdog, que fica monitorando a comunicação com o servidor OPC preferencial e avisa quando o mesmo entra em falha. E o segundo chamado de Hot Standby, que faz o chaveamento do servidor preferencial OPC para o Servidor secundário OPC.

6. Rotina de watchdog (cão de guarda)

O objetivo deste algoritmo é verificar a cada minuto se a comunicação entre o cliente OPC e o servidor OPC com os CLP's está ativa. Na Figura 6 temos um exemplo de implementação do algoritmo de watchdog.

```
{Verifica dados do micro servidor AccessName HotStandBy}
IF TimeHotStandBy == TimeHotStandByAnt OR Falha_Com_Forno THEN
A_Micro_Fonte_CommOK = 0;
CALL DirecionaComm();
ELSE
A_Micro_Fonte_CommOK = 1;
TimeHotStandByAnt = TimeHotStandBy;
ENDIF;
```

Figura 6. Exemplo de implementação da rotina de watchdog.

O algoritmo recebe e guarda em uma variável interna do tipo inteira, um número relativo à data e hora do servidor OPC que é atualizado todo segundo. A cada minuto essas duas variáveis são comparadas e, caso em uma dessas comparações estes números aparecem iguais, significa que a comunicação foi interrompida. Neste momento é informado ao sistema que aconteceu uma falha, e será chamado um segundo algoritmo para chavear a comunicação, que será detalhada no próximo item.

7. Rotina de hot standby

Este algoritmo faz uma chamada no sistema e altera o nome do servidor de comunicação para o nome do servidor reserva, que passa a comunicar com os CLP's a partir deste novo servidor de comunicação.

Na Figura 7 temos um exemplo de implementação do algoritmo de hot standby.

```
{Quick function/DirecionaComm}
{SETA COMUNICACAO COM DRIVER LOCAL OU LEITURA POR OUTRO INTOUCH}
IF ((A_Nome_Micro <> "033-2M1-PCS-04") AND (A_Nome_Micro <> "033-2M1-PCS-05"))
THEN
   IF A_Micro_Fonte == "033-2M1-PCS-04" THEN {Preferencialmente é a 033-2M1-PCS-04}
      A_Micro_Fonte = "033-2M1-PCS-05";  {Muda para 033-2M1-PCS-05}
   ELSE
      A_Micro_Fonte = "033-2M1-PCS-04";  {Muda de 033-2M1-PCS-05 para 033-2M1-PCS-04}
   ENDIF;
   IOSetAccessName("Forno_R",A_Micro_Fonte,"OPCLINK","431_2P1_CLP1_R");
   IOSetAccessName("Forno_M",A_Micro_Fonte,"OPCLINK","431_2P1_CLP1_M");
   IOSetAccessName("Forno_L",A_Micro_Fonte,"OPCLINK","431_2P1_CLP1_L");
   CALL DebugMessage( "### Realizando o redirecionamento da comunicação - Forno ###");
   CALL DebugMessage( "DirecionaComm, A_Micro_Fonte  -> " + A_Micro_Fonte );
ENDIF;
      {*Seta tópico para resgate de WatchDog para Status}
      IOSetAccessName("Hot_StandBy", A_Micro_Fonte,"VIEW","TAGNAME");
```

Figura 7. Exemplo de implementação da rotina de hot standby.

Quando o algoritmo é chamado, o mesmo verifica se não um servidor de comunicação validado essa informação pelo seu nome, validado essa informação ele verifica com quem está comunicando atualmente e que possivelmente houve uma falha para então alterar a fonte de comunicação e direcionar a comunicação para o servidor de comunicação reserva.

8. Considerações finais

Através das alterações na estrutura da rede da automação principalmente a troca do switch principal por um switch industrial com a tecnologia gigabit e gerenciamento da rede, o reposicionamento das estações de operações criando uma redundância física e a implementação das rotinas sugeridas nos itens 6 e 7 são fundamentais para o sucesso na resolução do problema.

Outro ponto importante para garantir a comunicação eficaz entre os CLP's e as Estações de operações, é que se adquira um software de monitoramento contínuo da

rede, e que se faça este monitoramento para antecipar eventuais falhas na estrutura de rede.

Será necessária a contratação de empresa especializada em monitoração da rede para validar as melhorias aqui sugeridas depois de implementadas, com o uso de um *Sniffer* conforme feito na seção 3, para que seja possível medir os resultados obtidos com as modificações.

Como sugestão para melhoria em trabalhos futuros na gestão de ativos de rede é conveniente que se aumente a freqüência de inspeções em áreas onde o acúmulo de pó pode ser observado com maior freqüência para evitar problemas de perda de pacotes na comunicação.

9. Referências bibliográficas

[1] NEMA *National Electrical Manufacturers Association*. Disponível em: <http://www.nemabrasil.org.br/>. Acesso em: 5 de Abril de 2008.

[2] PINHEIRO, J.M.S. *Introdução às Redes de Supervisão e Controle*. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_redes_de_supervisao_e_controle.php> Acesso em: 05 de abril de 2008.

[3] BARBOSA, H.A. *Detenção de Intrusão em Redes de Automação Industrial*. Disponível em: <http://sergio.inf.ufes.br/files/Heber_Barbosa.especializacao.pdf>. Acesso em: 12 de abril de 2008.

[4] PUNGEDA, A. Alta Network. *Relatório de Análise de Rede 2007* 16p.