

OS SISTEMAS DE SEGURANÇA E A FALÁCIA DE “QUANTO MAIS REDUNDÂNCIA, MELHOR”

Paul Gruhn, PE, CFSE, L&M Engineering - pgruhn@ix.netcom.com, e
Vitor Finkel, Finkel Engenharia e Consultoria - vfinkel@attglobal.net

As emoções humanas podem ter uma força difícil de se confrontar. Por exemplo, todo mundo sabe que voar num avião é estatisticamente mais seguro do que dirigir um carro, mas isto não impede que muitos se apavorem com a simples idéia de voar. Muita gente já viu aquela charge de um rei medieval, em sua tenda de campanha, junto a uma batalha, dizendo a seu pajem para se livrar do vendedor que lhe procurava (“Estou muito ocupado para ser perturbado por um vendedor”), e o vendedor trazia a primeira metralhadora jamais fabricada. Há muita gente que não gosta de lidar com vendedores, embora estes muitas vezes realmente se disponham a resolver os problemas dos clientes.

De maneira semelhante, as pessoas pensam: “Se um é bom, dois é melhor, três deve ser ainda melhor; e, agora, já EXISTE O QUÁDRUPLO!”.

OS SISTEMAS TRIPLICADOS FORAM OS PRIMEIROS

Os sistemas TMR (Triple Modular Redundancy) foram desenvolvidos na década de 70 (pesquisa da NASA) e lançados comercialmente no início dos anos 80. A razão para a triplicação, na época, era bem simples. Os sistemas computadorizados tinham uma capacidade de diagnóstico bastante limitada. Se houvessem apenas dois sinais, e eles fossem divergentes, qual seria o certo? Como isso não podia ser determinado, implementaram os sistemas triplicados. Presume-se que o sinal do canal divergente está errado e é simplesmente desconsiderado na votação contra os outros dois. Esses sistemas ficaram muito populares em aplicações industriais, para os Sistemas de Segurança, inclusive os chamados sistemas de missão crítica, onde uma falha segura que derrubasse uma planta era quase tão inadmissível quanto uma falha perigosa, que podia permitir um acidente.

AÍ APARECEU O DUPLO

Durante os últimos doze anos, no entanto, foram lançados alguns sistemas redundantes *duplos* para controles críticos e aplicações em segurança. Os vendedores

desses sistemas diziam que eram equivalentes aos sistemas TMR, enquanto estes diziam que isto não era verdade. Alguns vendedores agora estão promovendo os sistemas redundantes quádruplos! Qual é o “melhor”? Qual é o “adequado” para sua aplicação? Em quem se deve acreditar e, mais importante ainda, *porque*? Como é que se toma esse tipo de decisão?

UMA PERSPECTIVA DE OUTRAS INDÚSTRIAS

Comparemos com a situação da aviação comercial. Não é preciso enfatizar como a segurança é levada a sério nesse ambiente. O Boeing 747 foi lançado por volta de 1970. Na época, era o maior jato comercial de passageiros, levando mais de 450 pessoas a bordo. A tecnologia disponível então limitava o tamanho do motor a uns 23.000 quilos de empuxo - O maior motor existente no mundo à época. Era preciso ter quatro desses motores para alcançar a potência necessária à decolagem. Considerando-se a confiabilidade dos motores naquele tempo, esse nível de redundância foi considerado adequado para vôos transatlânticos.



O tempo e a tecnologia evoluem. O Boeing 777 é hoje o maior jato bi-reator. Variantes do 777 com fuselagem um pouco mais comprida, e com envergadura maior, transportam um número equivalente de passageiros por distâncias semelhantes à de certas versões do 747. Algumas companhias aéreas estão substituindo os 747s por 777s. O motivo é o de sempre: *economia*. A tecnologia de hoje permite construir motores de até 50.000 quilos de empuxo (A indústria aprendeu muito sobre metalurgia e confiabilidade nestes últimos 30 anos). Para focar os motores a jato, o diâmetro da nacelle do 777 é pouca coisa maior do que o diâmetro do corpo de um 757, um avião que leva fileiras de seis passageiros lado a lado! Dois motores modernos conso-

mem menos combustível, são mais confiáveis e precisam de menos manutenção do que quatro motores mais antigos. Quando o 777 foi lançado, recebeu o certificado ETOPS (Extended Twin Engine Operations - operação estendida com dois motores), o que significa poder voar o avião até 3 horas consecutivas com um só motor, enquanto se dirige a um campo alternativo para pouso de emergência. Depois disso, o 777 já foi certificado para os mais longos vôos transatlânticos, além das exigências requeridas pelo ETOPS original.

COMO SE TOMAM ESSAS DECISÕES?

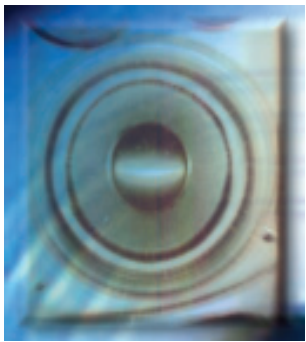
Os sistemas tecnicamente complexos, como aviões, reatores nucleares, refinarias e plantas químicas não são mais construídas baseados na intuição ou experiência empírica. Os riscos envolvidos em grandes sistemas técnicos modernos são simplesmente muito grandes para se aprender por tentativa e erro. Decisões desse tipo precisam envolver análises técnicas bem fundadas e julgamento baseado em boas práticas de engenharia. Por exemplo, imagine que você foi convidado para o vôo inaugural do primeiro Boeing 777. O Engenheiro Chefe da Boeing está presente e cumprimenta a todos apertando a mão, com um largo sorriso, congratulando-os por fazerem esse vôo pioneiro de um avião novo. Você, como bom e curioso Engenheiro que é, já percebeu que o avião têm só dois motores, enquanto os outros jumbos tinham sempre 3 ou 4. Naturalmente você pergunta ao Engenheiro Chefe: “Você pode me dizer como decidiu pelo tamanho e quantidade dos motores para este avião?”. Como você se sentiria se ele respondesse: “Bem... na verdade não estávamos muito certos... mas foi isto que um vendedor de motores nos recomendou”.

Você ainda pensaria em entrar nesse avião para fazer esse vôo?

Outra analogia vem dos alto-falantes para sistemas estereofônicos. Há algumas décadas bons falantes eram grandes e pesados, sem exceção. Um fabricante, a Bose, mudou isto. Usando ímãs de terras raras, ao invés da tradicional liga metálica Alnico, foi possível obter falantes mais leves,

mais baratos e eficientes, que soam tão bem ou melhor do que os de 20 anos atrás. Nós simplesmente aprendemos coisas novas nas últimas décadas.

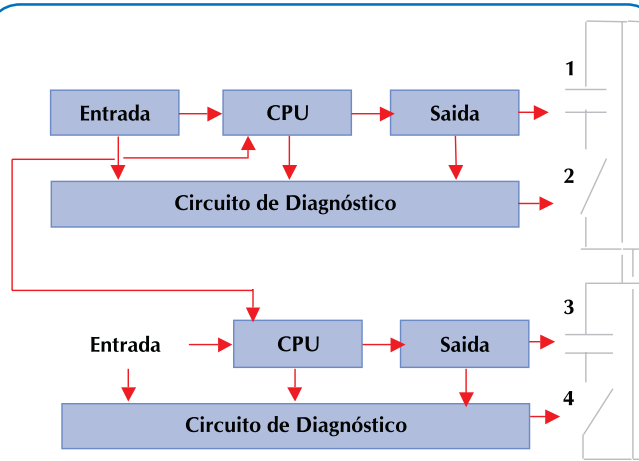
Nos sistemas de segurança também aprendemos coisas novas. Infelizmente muitas delas através do estudo de acidentes catastróficos, outras por meio do cálculo de probabilidades de falhas e do tipo das falhas: segura ou perigosa.



Hoje há sistemas redundantes duplos, para controles críticos e sistemas de segurança que usam diagnósticos avançados, com velocidade e software que não existiam há 25 anos. Esses sistemas não são do tipo com votação 1 de 2, onde se precisa de apenas um canal bom para iniciar um *shutdown*, nem 2 de 2, onde é preciso ter ambos canais bons para iniciar um *shutdown*, ou *hot-back-up*, onde apenas um canal está ativo, enquanto o outro assume em caso de falha do que estava ativo. A indústria tem chamado esses sistemas de 1 de 2D (de Diagnóstico). Essa terminologia foi empregada pela primeira vez por Bill Goble em 1992, em seu livro da ISA “Evaluating Control System Reliability” (Avaliando a Confiabilidade de Sistemas de Controle). Esses sistemas exigem ao menos duas falhas seguras simultâneas (por exemplo, falha desenergizando) para derrubar a unidade sem necessidade (a mesma coisa que um TMR), e duas falhas perigosas simultâneas (por exemplo, travada em posição energizada) para uma falha tipo não desliga em caso de necessidade (também a mesma coisa que um TMR). Os sistemas 1 de 2D também têm sido certificados por agências independentes de certificação, como a alemã TÜV (de reconhecimento mundial) e FM - Factory Mutual (americana). Mais uma vez, a indústria aprendeu algumas coisas nestas últimas décadas.

E AÍ APARECEU O QUÁDRUPLO!

Quando já existiam opções diferentes em número suficiente para complicar a decisão do usuário, alguns fornecedores de sistemas 1 de 2D lançaram o “quad”. Esses sistemas seriam melhores do que os 2 de 3 (TMR)? Porque “quad”? A resposta é bem simples. Quando um sistema de lógica de segurança falha, precisa ser reparado. Quanto tempo leva até ficar novamente em condições normais de uso, é chamado de “tempo de uso em degradação”, ou seja com segurança reduzida. Os primeiros sistemas 1 de 2D tinham restrições de só operar nessas condições por 72 horas (conforme seus relatórios de certificação). Os fornecedores de 2 de 3 (TMR) exploravam esse ponto fraco, seus sistemas poderiam operar em modo degradado por até 1500 horas. Os principais fatores que afetam esse tempo de operação em degradação são os níveis de Diagnósticos e de Redundâncias. Mudar radicalmente o diagnóstico de um sistema representa um trabalho extenso, caro e complicado, enquanto aumentar o nível da redundância (elo mais fraco desta corrente) não o é (relativamente falando). O elo mais fraco, neste caso, é o bloco do processador central. Os fabricantes simplesmente usam processadores redundantes em cada canal do sistema duplo, ou seja 4 processadores ao todo. Estes mesmos sistemas são fornecidos com canal de saída duplo (e, em vários casos, nem duplo, mas singelo).

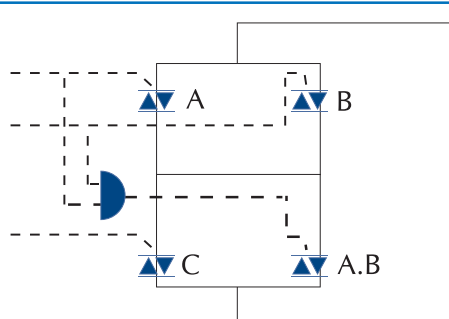


Arquitetura de um Sistema 2 de 4D.

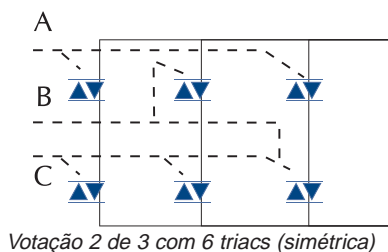
TODOS OS SISTEMAS PODEM SE VANGLORIAR DE SEREM QUÁDRUPLOS E, ALGUNS, ATÉ SÊXTUPLOS !

Todo vendedor pode se vangloriar de ter um sistema redundante quádruplo! Todos os vendedores de sistemas 2 de 3 (TMR) usam componentes quádruplos para fazer a votação em seus módulos de saída. Todos os fornecedores de sistemas 1 de 2D usam circuitos quádruplos semelhantes.

Isto não quer dizer que não haja nada de “errado” com os sistemas TMR, nem que os 1 de 2D ou 2 de 4D sejam “melhores” do que os TMR. O fato é que realmente os sistemas atingem performances equivalentes, embora geralmente os sistemas duplos custem menos.



Votação 2 de 3 com 4 triacs



Votação 2 de 3 com 6 triacs (simétrica)

E QUANDO VOCÊ PENSA QUE ACABOU...

Obviamente tudo o que foi mencionado até aqui se refere apenas à comparação de arquiteturas de sistemas de segurança com lógica programável, mas existem também sistemas lógicos pneumáticos; hidráulicos (ainda empregados em painéis de cabeça dos poços em plataformas de produção de petróleo); a relés (boa opção para sistemas de pequeno porte, ou como redundância de poucas entradas/saídas de segurança crítica em sistemas maiores; para sistemas de transportes, como trens e elevadores, etc.; e, ainda, são uma preferência para muitos sistemas projetados no Japão); e principalmente os sistemas de lógica fixa em estado sólido com falha segura, redundantes ou não, amplamente usados na Europa para níveis de segurança mais elevados (SIL-4) que, normalmente, não se consegue atingir com os sistemas programáveis. Ufa! Achemos que é só!



MAS, NO FINAL ...

Finalmente, na verdade, não importa muito qual a caixa de lógica é a “melhor”! Muitas são certificadas para uso em aplicações SIL 3 (Safety Integrity Level - O Nível de Integridade de Segurança; para os americanos o nível 3 é o mais elevado; os europeus usam até SIL 4, mais seguro ainda). Uma caixa de lógica certificada geralmente tem uma contribuição insignificante para a probabilidade de falha sob demanda (PFD) do sistema, como um todo. São os dispositivos de campo que representam o elo mais fraco dessa corrente na maioria dos sistemas modernos - um assunto que a maioria dos vendedores de caixas lógicas prefere ignorar, propositalmente.

Os fatores decisivos para a escolha do sistema a ser comprado realmente não mudaram. Pessoas compram de pessoas. Qual organização e pessoas mantém melhores relações com você? Quem lhe inspira mais confiança? Quem oferece a integração mais simples com o sistema de controle (interface-homem-máquina)? Quem pode lhe dar melhor assistência durante o projeto, instalação, testes e eventual manutenção corretiva? A sua licenciadora de tecnologia, o que recomenda? Discutir sobre as caixas de lógica não faz muito sentido. Qual é o melhor carro? Qual o melhor CLP? Qual o melhor telefone celular? A mulher mais bonita? ...■

NA INTERNET

PARA SABER MAIS SOBRE SISTEMAS DE SEGURANÇA NA WEB,
VISITE OS SITES RELACIONADOS ABAIXO.

ESTA BIBLIOGRAFIA FOI COMPILADA E COLETADA POR VITOR FINKEL.

<http://www.acutech-consulting.com> – *AcuTech - Safety Systems Consultants.*

<http://www.exida.com> – *Consultoria em avaliação de riscos (Ed Marzal, etc.).*

<http://www.exida.com/news.asp#top> – *Exida.com Industry News.*

<http://www.boilercontrol.com> – *Boiler Control information DCS, PLC, HMI (Ênfase em segurança).*

<http://www.control.com> – *Control Technology Corporation – (Lista de discussão “Automation”).*

<http://www.csa.ca/index.htm> – *CSA – Canadian Standards Association.*

<http://www.epa.gov/ceppo/whatnew.html> – *EPA – Chemical Preparedness and Prevention Office - CEPPPO.*

<http://www.gre.ac.uk/research/cms/fire> – *Fire safety Engineering Group.*

<http://www.ge.com/gemis/gefanuc> – *GE Fanuc.*

<http://www.saunalahti.fi/ility/FailureRates.html> – *Equipment and Instruments Failure Data.*

<http://www.cssinfo.com/info/din.html> – *DIN - CSS: Deutsches Institut fur Normung.*

<http://www.che.com/mag/ce3.htm> – *Chemical Engineering – Safety Database.*

<http://www.asse.org> – *ASSE – American Society of Safety Engineers.*

http://www.hima.com/hima_e/hima.html – *HIMA (Fornecedor Safety PLCs e Lógica Fixa Falha Segura).*

<http://www.ibp.org.br> – *IBP Site Map – Brazilian Petroleum Institute (Curso EC-50 da ISA).*

<http://www.plcopen.org/iecdocs.htm> – *IEC - International Electrotechnical Comission.*

<http://www.iec.ch> – *IEC - International Electrotechnical Comission (English).*

<http://sunnyday.mit.edu/accidents> – *Accident Reports.*

<ftp://ftp.cle.ab.com/stds/iec/sc65bwg7tf3/html/toc.htm> – *IEC – HT1131-3 - Table of Contents.*

http://www.iee.org.uk/PAB/CompSafe/scc_snip.htm – *IEE - PAB Preciis of safety.*

<http://www.isa.org> – *ISA (Curso EC-50 e livro Safety Shutdown Systems de Paul Gruhn).*

<http://www.isa.org/portals/safety> – *ISA Safety Portal.*

<http://www.isa.org/~safety/index.htm> – *ISA Safety Group (Division).*

<http://www.isadistrito4.org.br> – *ISA Distrito 4.*

<http://www.n-vision.com/lmeng> – *L&M Engineering Home Page (Consultoria do Paul Gruhn, programa CASSPack).*

<http://spice.mhv.net/~philmm/entrance.htm> – *PLC Tutor (Livro PLC - Básico).*

<http://www.plcs.net> – *PLC Tutor Teaches PLCs (Curso de PLC on-line gratuito - Muito bom).*

<http://www.pilzusa.com> – *Pilz Industrial Electronics LP (USA).*

<http://process-safety.tamu.edu> – *Mary Kay O'Connor Process Safety Center.*

<http://www.risk-solutions.com> – *Risk Solutions.*

<http://www.meadep.com> – *Meadep - Reliability Soft, Markov Chains, Reliability Block Diagrams.*

<http://www.trip-a-larm.com> – *Trip-a-larm (Sistema Shutdown Lógica Fixa + Papers do Phil Corso).*

<http://www.triconex.com> – *Triconex - Anthony Friederickson III. Ver também Angela Sanders em Premier Consultants.*

<http://www.icsplc.co.uk/index.htm> – *Triplex - (ICS England) – Sistemas Shutdown TMR.*

<http://icsweb.ics.org> – *ICS PLC->TMR.*

<http://www.thom.compuserve.com/safety.htm> – *GE Fanuc - Sistemas de Segurança.*

<http://www.tuvps.com/services/sfsafety/benefits/cert.htm> – *TÜV List of Certified Programmable Controllers.*

<http://www.tuvglobal.com> / <http://www.tuv-fs.com> – *TÜV Süddeuchland.*

<http://www.yokogawa.co.jp> / <http://www.yokogawa-iss.com> – *Yokogawa Japan.*

<http://www.yca.com> – *Yokogawa Corporation of America.*