HI tecnologia

Automação Industrial

Nota de Aplicação

Utilizando os recursos de segurança dos controladores HI

HI Tecnologia Indústria e Comércio Ltda.

Documento de acesso Público

Apresentação

Este documento foi elaborado pela **HI Tecnologia Indústria e Comércio Ltda.** Quaisquer dúvidas ou esclarecimentos sobre as informações contidas neste documento podem ser obtidas diretamente com o nosso departamento de suporte a clientes, através do telefone (19) 2139.1700 ou do email suporte@hitecnologia.com.br. Favor mencionar as informações a seguir para que possamos identificar os dados relativos a este documento.

Título documento:	Utilizando os recursos de segurança dos controladores HI
Referência do documento:	ENA.00050
Versão do documento:	1.02

HI Tecnologia Indústria e Comércio Ltda.

	Sede:	Av. Dr. Armando de Sales Oliveira, 445.
	Cidade:	Campinas – SP
	Fone:	+55 (19) 2139.1700
	CEP:	13076-015
	Portal Web:	www.hitecnologia.com.br
Contatos	Vendas:	vendas@hitecnologia.com.br
	Suporte Técnico:	suporte@hitecnologia.com.br
	Engenharia de Aplicação:	engenharia@hitecnologia.com.br
	FAQ:	faq.webhi.com.br
	Portal de documentação On line:	doc.hitecnologia.com.br
	Forum:	forum.hitecnologia.com.br

Índice

1 Abrangência do Documento 4
2 Introdução 5
3 Informação Copyright 5
4 Isenção de Responsabilidade 5
5 Sugestões 5
6 Abordagem de Segurança Adotada 5
6.1 Compatibilidade de Recurso 6
6.2 Segurança para os arquivos fonte do projeto 6
6.3 Segurança para o programa corrente do PLC 7
6.3.1 Reset do Controlador 7
6.3.2 Atualização de Firmware (*) 7
6.3.3 Seleção do modo Loader 7
6.3.4 Setup de Comunicação 7
6.3.5 Setup de Hardware 8
6.3.6 Leitura da Base de Dados 8
6.3.7 Escrita da Base de Dados 8
6.3.8 Eliminação do Programa Corrente (*) 8
6.3.9 Carga de Programa (*) 8
6.3.10 Pausa no Programa 8
7 Configuração dos Critérios de Segurança 8
7.1 Configuração da proteção no acesso aos arquivos do projetos 10
7.2 Configuração da proteção no acesso à aplicação do controlador 11
8 Recurso de reinicialização do equipamento 12
8.1 Transferindo o equipamento para o modo Loader 12
8.2 Eliminando o programa de aplicação através do modo Loader 13
8.3 Recarregando o Firmware do Equipamento 13
Controle do Documento 15
Considerações gerais 15

1 Abrangência do Documento

Este documento abrange os seguintes Controladores nas plataformas especificadas abaixo:

Equipamentos			Plataforma					Abrangência
Tipo	Família	Modelo	GI	GII	GII Duo	G3	G3S	√
Controladores	MCI02	MCI02	X					
		MCI02-QC	X					
	ZAP500	ZAP500/BX/BXH	X					
		ZTK500/501	X					
	ZAP900	eZAP900/901, ZAP900/901		X				√
		eZTK/ZTK900, ZAP900-BXH		X				√
	ZAP91X	ZAP910 / ZTK910				X		
		ZAP911				X		
		eZAP910 / eZTK910				X		
		eZAP911				X		
		ZAP910-BXH				X		
		ZAP910-S / ZTK910-S					X	
		ZAP911-S					X	
		eZAP910-S / eZTK910-S					X	
		eZAP9911-S					X	
		ZAP910-BXH-S					X	
	FLEX950	FLEX950-PLC		X				√
	P7C	CPU300			X			
		CPU301, PPU305				X		
		CPU302, PPU306					X	
	NEON	CPU400					X	
IHMs	MMI600	MMI600/601		X				
	MM650	MMI650		X				
	MMI800	MMI800		X				
	FLEX950	FLEX950-IHM		X				
	GTI100	GTI100-RS/GTI00-ET						

2 Introdução

Este documento tem por objetivo apresentar os recursos de controle de acesso e segurança, implementados e disponibilizados no ambiente SPDSW a partir da versão 2.0.00. Estes recursos abrangem desde o controle do acesso ao programa ladder criado, até o bloqueio de comandos e acesso à base de dados da aplicação ativa no controlador.

Parte destas novas funcionalidades está disponível apenas para a linha de equipamentos GII (ZAP900, ZAP901 etc...). Cada recurso abordado será identificado se está disponível para toda linha de equipamentos ou apenas para os produtos GII.

O documento é dividido nas seguintes seções:

- Abordagem de segurança adotada
- Configuração dos critérios de segurança
- Recurso de reinicialização do equipamento

3 Informação Copyright

4 Isenção de Responsabilidade

A utilização dos conceitos, exemplos e outros elementos deste documento é responsabilidade exclusiva do usuário. A HI Tecnologia Indústria e Comércio Ltda. não poderá ser responsabilizada por qualquer dano ou prejuízo decorrente da utilização das informações contidas neste documento.

5 Sugestões

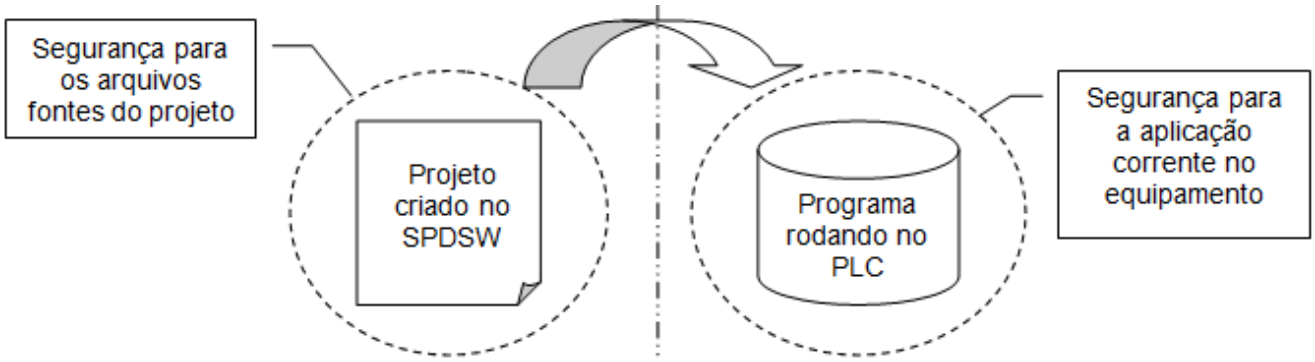
Sugestões são bem vindas. Por favor, envie seus comentários para suporte@hitecnologia.com.br
Novas versões deste documento podem ser liberadas sem aviso prévio. Caso tenha interesse neste conteúdo acesse o site da HI Tecnologia regularmente para verificar se existem atualizações liberadas deste documento.

6 Abordagem de Segurança Adotada

Nos sistemas de automação, existem situações onde um determinado programa agrega informações que são propriedade de um dado cliente e, portanto não devem ser disponibilizadas publicamente, devendo possuir acesso restrito a pessoas autorizadas. Paralelamente, existem casos em que, um programa carregado em um dado equipamento, não deve ser parado ou modificado, a não ser por uma pessoa qualificada para tal.

Para que um sistema de segurança seja eficiente neste contexto, é necessário que, tanto os arquivos dos programas desenvolvidos, quanto os equipamentos que estão executando os programas associados possuam recursos de proteção contra acesso não autorizado.

A partir da versão 2.0.00, o SPDSW incorpora uma abordagem de segurança que abrange tanto o projeto criado pelo usuário quanto a aplicação carregada em um dado equipamento, conforme indicado na figura a seguir:



6.1 Compatibilidade de Recurso

A tabela a seguir apresenta a compatibilidade dos recursos de proteção disponibilizados pelo SPDSW em função do ambiente de programação, dos equipamentos utilizados e das versões de firmware associadas.

	SPDSW	Equipamentos	Firmware
Proteção dos arquivos de projeto	2.0.00 ou superior	Todos	Todos
Proteção da aplicação do controlador	2.0.00 ou superior	Família ZAP900 e equipamentos GII	1.4.00 ou superior

6.2 Segurança para os arquivos fonte do projeto

Para este nível, o acesso a todos os arquivos do projeto associado pode ser controlado através de senha criptografada, permitindo restringir a visualização e alteração do programa e configurações do projeto. Quando esta proteção estiver ativada, o usuário do SPDSW ao carregar um projeto com proteção não poderá:

- Abrir o editor Ladder para projeto corrente;
- Abrir o depurador Ladder para projeto corrente;
- Abrir o módulo de configuração do equipamento para projeto corrente;
- Abrir o módulo de configuração da IHM para projeto corrente;
- Abrir o módulo de Setup do Programa de Aplicação;
- Abrir o módulo de Setup do Projeto;

- Salvar o projeto corrente;
- Imprimir o projeto corrente;
- Visualizar impressão do projeto corrente

Quando quaisquer das ações descritas acima forem ativadas pelo usuário, será solicitada uma senha para liberar o acesso a este recurso. Uma vez especificada a senha corretamente, toda funcionalidade estará disponível sem necessidade de especificar novamente a senha, até que o SPDSW seja encerrado ou um novo projeto seja carregado.

Este novo recurso pode ser utilizado a partir da versão 2.0.00 do SPDSW e se aplica a qualquer projeto, independentemente do modelo de PLC associado.

6.3 Segurança para o programa corrente do PLC

Quando o usuário estiver operando com equipamentos GII (Família ZAP900) e firmware de PLC com suporte para gerência de recursos de segurança (consultar item 2.1 - Compatibilidade do recurso) ou superior será possível proteger a aplicação carregada no equipamento de forma que, uma pessoa não habilitada não poderá remotamente modificar, eliminar e até mesmo monitorar a base de dados da aplicação corrente no equipamento. Os seguintes recursos podem ser liberados ou bloqueados seletivamente pelo usuário do projeto associado:

6.3.1 Reset do Controlador

Quando ativada esta proteção, o comando de Reset remoto do equipamento via o SPDSW estará condicionado à liberação prévia através de senha.

6.3.2 Atualização de Firmware (*)

Quando ativada esta proteção, a carga um novo firmware no equipamento conectado estará condicionado à liberação prévia através de senha.

6.3.3 Seleção do modo Loader

Quando ativada esta proteção, o comando de ativação do modo loader no equipamento conectado estará condicionado à liberação prévia através de senha.

6.3.4 Setup de Comunicação

Quando ativada esta proteção, o acesso à tela de configuração de comunicação do equipamento conectado estará condicionado à liberação prévia através de senha. Mesmo quando utilizadas versões anteriores do SPDSW para este acesso a escrita de uma nova configuração de comunicação no equipamento conectado não será possível sem liberação prévia.

6.3.5 Setup de Hardware

Quando ativada esta proteção, o acesso às telas de setup de hardware dos módulos de I/O (ex. tela de setup do módulo de I/O DXM510 do ZAP900) do equipamento conectado estará condicionada à liberação prévia através de senha. Desta forma, nenhuma alteração de parâmetros de setup dos módulos de hardware, (modo de operação da placa, ganhos das entradas, filtros etc..) será possível sem liberação prévia.

6.3.6 Leitura da Base de Dados

Quando ativada esta proteção, os comandos de leitura das variáveis do equipamento (R-Contatos, M-Memórias Inteiras e D-Memórias Reais) só serão possíveis após liberação através de senha.

6.3.7 Escrita da Base de Dados

Quando ativada esta proteção, os comandos de escrita das variáveis do equipamento (R-Contatos, M-Memórias Inteiras e D-Memórias Reais) só serão possíveis após liberação através de senha.

6.3.8 Eliminação do Programa Corrente (*)

Quando ativada esta proteção, o comando de eliminação da aplicação corrente no equipamento conectado estará condicionado àliberação prévia através de senha.

6.3.9 Carga de Programa (*)

Quando ativada esta proteção, o comando de carga de uma aplicação no equipamento conectado estará condicionado à liberação prévia através de senha.

6.3.10 Pausa no Programa

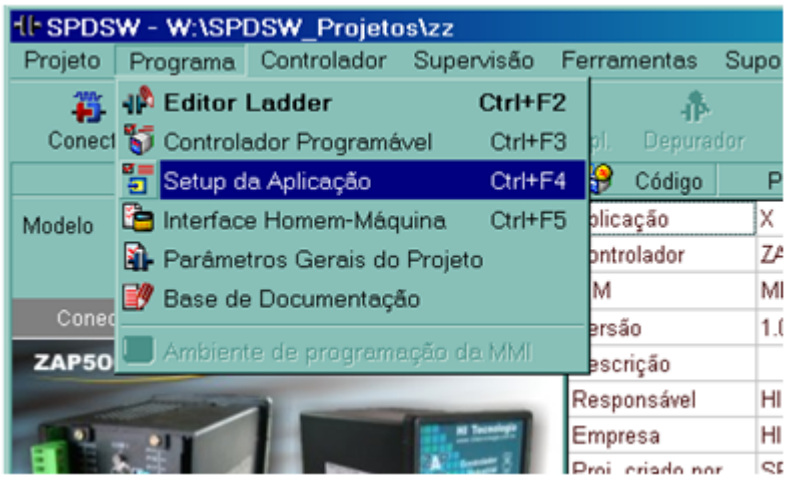
Quando ativada esta proteção, o comando de parar a execução da aplicação no equipamento conectado estará condicionado à liberação prévia através de senha.

(*) As opções de proteção, "Atualização de Firmware", "Carga de Programa" e "Eliminação de Programa" são habilitadas ou não de forma única.

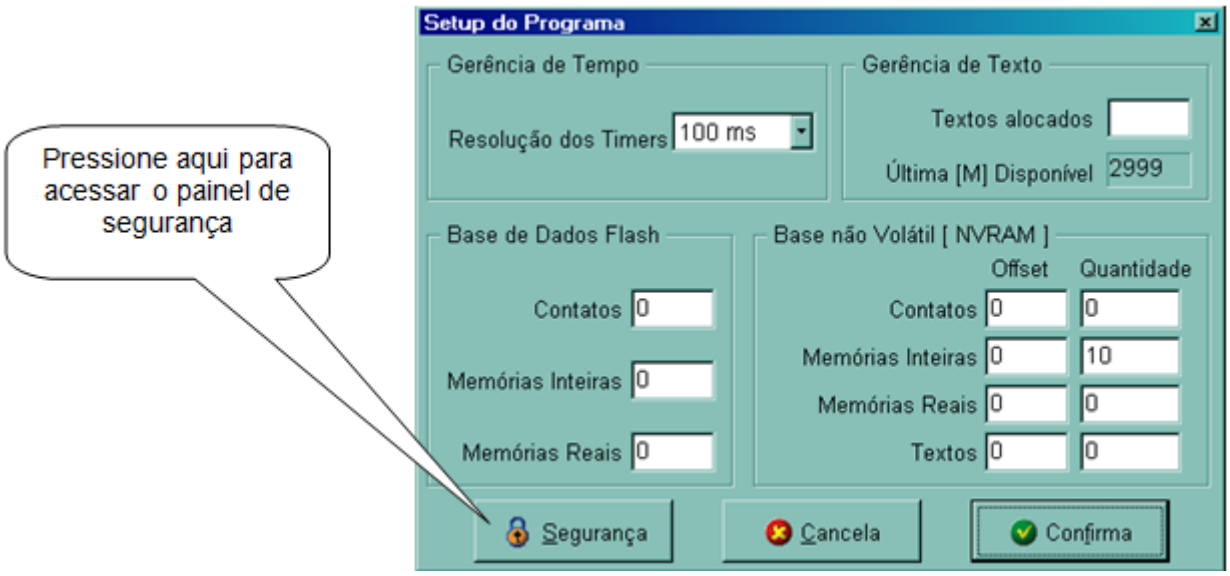
Confirmação dos critérios de segurança

7 Configuração dos Critérios de Segurança

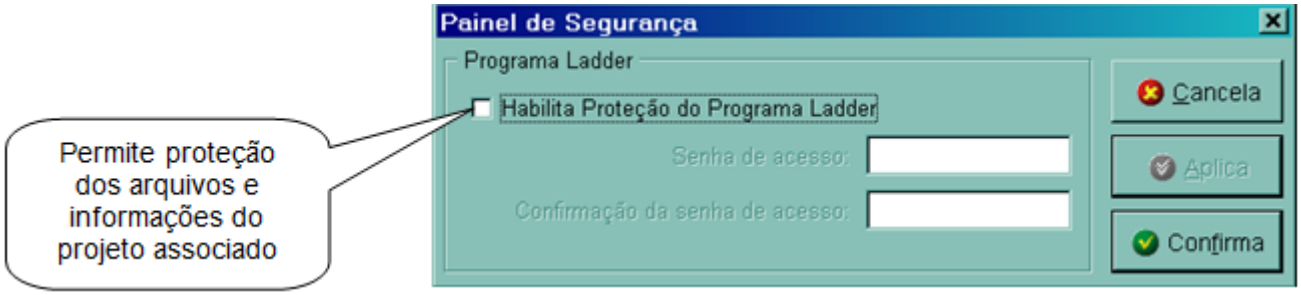
Para acesso a Tela de Proteção deve-se primeiramente carregar ou criar o projeto a ser protegido no SPDSW. Com o projeto carregado, ative a opção de "Setup da Aplicação" conforme indicado na figura a seguir:



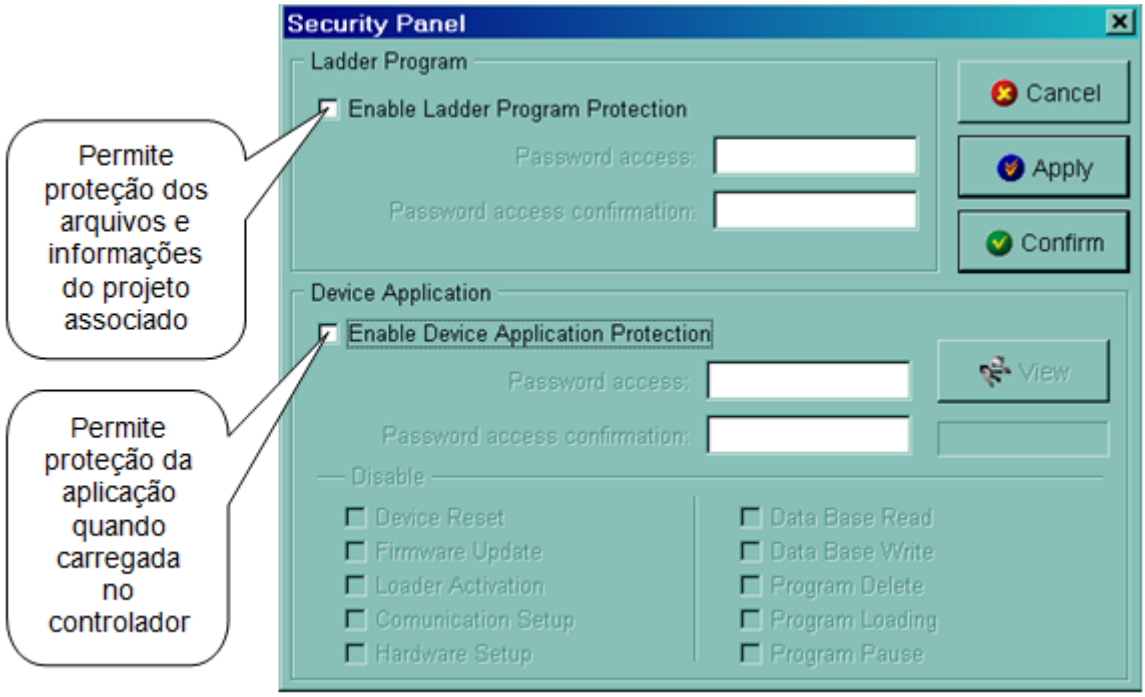
Ao selecionar está opção, será apresentada a tela a seguir:



Se o projeto corrente estiver associado a um equipamento da geração I, a seguinte tela será apresentada



Se o equipamento associado ao projeto corrente for da Geração II (ex. ZAP900), a tela a seguir será apresentada:



Tela de Segurança para equipamentos da Geração II

7.1 Configuração da proteção no acesso aos arquivos do projetos

Para ativar a proteção para acesso aos arquivos associados ao projeto carregado, clique no item "Habilita Proteção do Programa Ladder". Em seguida especifique uma senha de acesso de no máximo 10 dígitos e confirme a senha no campo logo abaixo. Pressione o botão Aplica para validar a configuração.

Atenção: Uma vez definida a senha de Proteção do Programa Ladder e confirmada através do botão "Confirma", todo acesso aos arquivos do projeto associado estarão condicionados a esta senha. **Portanto, se o usuário perder (esquecer) a senha especificada, não será mais possível visualizar, ou modificar o projeto corrente**.

Note que para acesso a esta tela de configuração será necessária a especificação da senha definida.

7.2 Configuração da proteção no acesso à aplicação do controlador

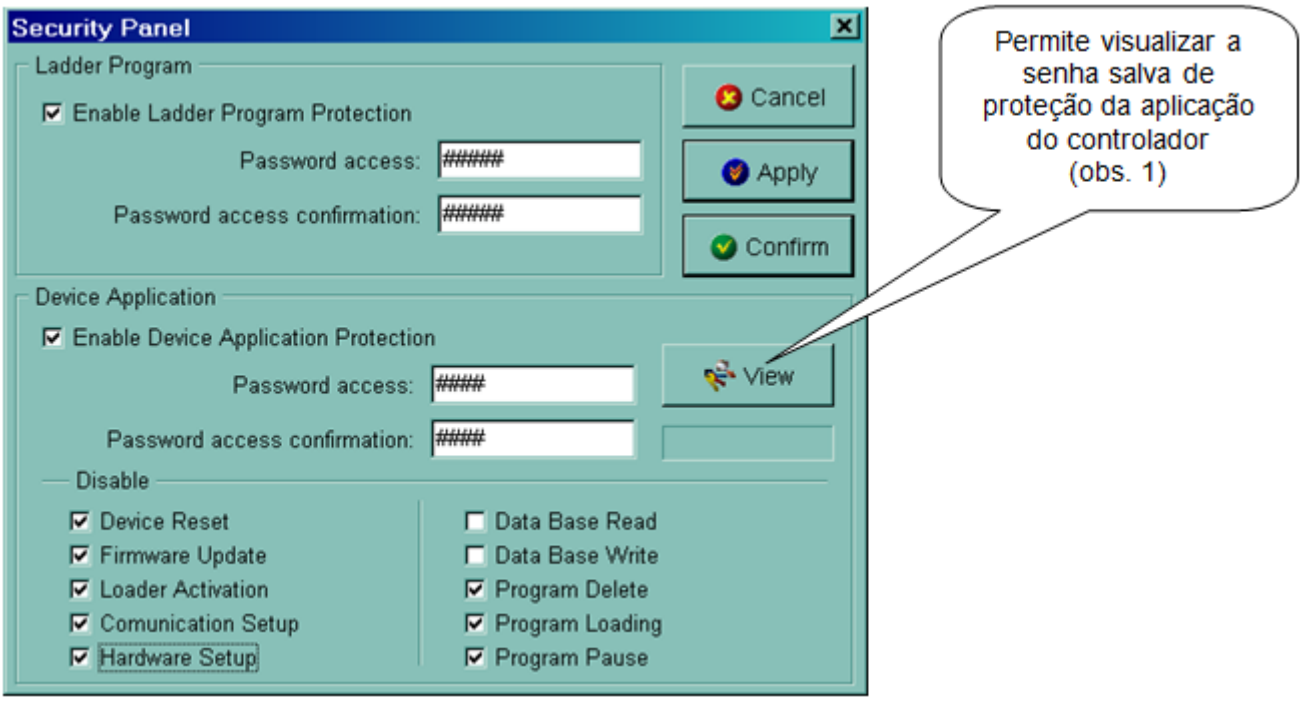
Para ativar a proteção da aplicação a ser carregada no controlador, clique no item "Habilita Proteção da Aplicação no Controlador". Em seguida, especifique uma senha de acesso de no máximo 10 dígitos e confirme a senha no campo logo abaixo. Quando for ativada pela primeira vez esta opção, serão selecionadas a proteções de alguns itens da lista apresentada. Selecione os itens da lista que devem ser protegidos com senha e pressione o botão "Aplica" para validar a configuração.

Uma vez definida a senha, esta será salva no projeto corrente. A próxima vez que o usuário compilar e carregar esta aplicação no controlador as proteções definidas serão ativadas.

Atenção: Uma vez definida a senha de Proteção da Aplicação do Controlador e carregada a aplicação no mesmo, todo comando que foi protegido estará condicionado a esta senha. Note que, se o usuário estiver utilizando uma versão anterior a 2.0.00 do SPDSW não será mais possível executar o comando protegido, uma vez que o ambiente antigo não disponibiliza recurso para especificação da senha de acesso para liberar o recurso em questão.
Portanto, se o usuário perder (esquecer) a senha especificada, não será mais possível executar o comando protegido.

OBS: Vide o item "Recurso de reinicialização do equipamento" para restaurar a funcionalidade do controlador no caso de perda da senha.

A tela a seguir apresenta uma condição típica onde foram especificadas senhas de Proteção do Programa Ladder e da Aplicação do Controlador.



Note que a senha apresentada neste campo pode não ser a mesma presente na aplicação do controlador, caso esta senha tenha sido previamente alterada e a aplicação não tenha sido carregada novamente.

8 Recurso de reinicialização do equipamento

Como mencionado anteriormente, quando utilizado o recurso de proteção da aplicação do controlador, o programa carregado no equipamento contém a senha que irá habilitar o recurso de comunicação protegido. Considere por exemplo que um dado programa foi carregado com senha de proteção da aplicação do controlador e ativou o recurso de carga / eliminação de programa e carga de firmware.

Nesta condição, para carregar qualquer nova aplicação (inclusive recarregar a mesma) ou atualizar o firmware do controlador será necessário que o usuário especifique a senha definida para liberar estes comandos. Se o usuário desconhece ou esqueceu a senha, o equipamento estará bloqueado para alterações. Remotamente não existe forma de recarregar ou reiniciar o equipamento se o usuário não possuir a senha de liberação do mesmo.

Nesta situação será necessário reinicializar o controlador, eliminando o programa corrente. Nesta condição, esta operação só pode ser realizada com o equipamento no modo Loader.

8.1 Transferindo o equipamento para o modo Loader

Para transferir o equipamento para o modo Loader execute os seguintes procedimentos:

Desligue o controlador;

Pressione o botão Loader indicado no equipamento;

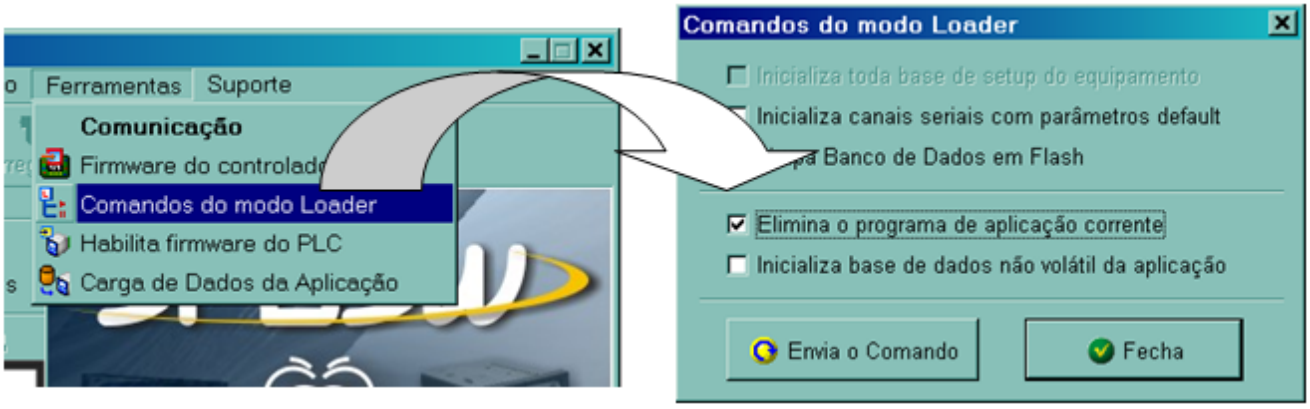
Ligue o controlador com o botão Loader pressionado. Após ligar, aguarde cerca de 2 segundos e libere o botão de loader. Confira através do Led de operação (3 piscadas) que o modo loader esta ativado.

Com o equipamento no modo Loader, ative o SPDSW através da porta COM1 do equipamento (no modo Loader apenas a porta de comunicação COM1 esta ativa). Confira esta condição através da indicação do firmware especificada no SPDSW conforme apresentado na figura a seguir.

Uma vez no modo Loader, pode-se eliminar o programa Ladder corrente através de um dos 2 procedimentos descritos a seguir.

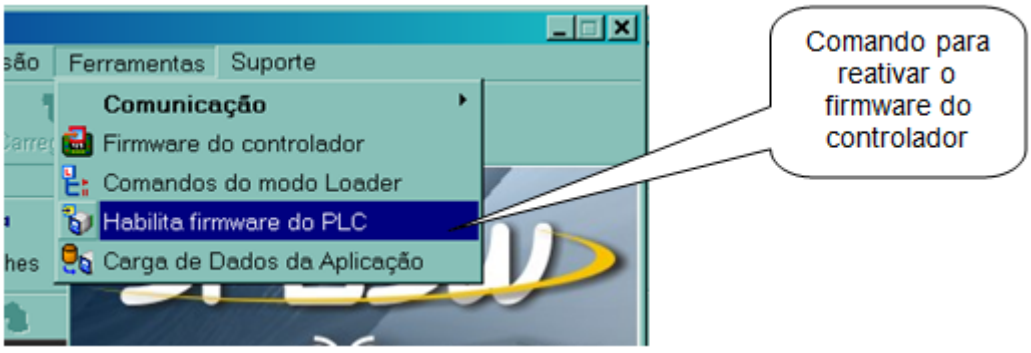
8.2 Eliminando o programa de aplicação através do modo Loader

Com o equipamento no modo Loader, selecione no menu principal a opção Ferramentas\Comandos do modo Loader (vide figura a seguir).



Na tela apresentada, marque o item "Elimina o programa de aplicação corrente" e pressione o botão "Envia o Comando". Uma mensagem de confirmação será exibida indicando que o comando foi realizado com sucesso.

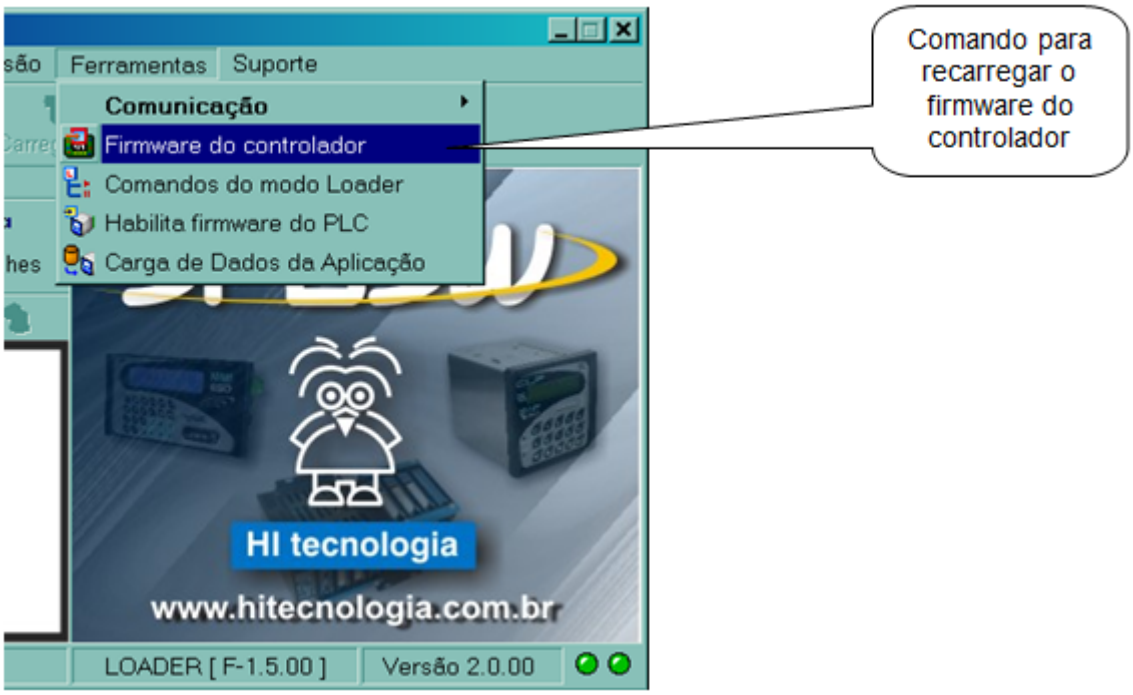
Feche a tela de comandos do modo Loader pressionando o botão "Fecha". Reative o firmware do controlador através da opção do menu Ferramentas/Habilita firmware do PLC conforme apresentado na figura a seguir.



Ao ser executado o comando, o equipamento deverá ativar o firmware de PLC novamente, porém sem programa de aplicação e, portanto, sem senha de proteção da aplicação.

8.3 Recarregando o Firmware do Equipamento

Uma segunda maneira de reativar a operação do equipamento quando a senha de proteção da aplicação foi perdida é efetuar o procedimento de carga de firmware do PLC. Sempre que um novo firmware é carregado, o programa de aplicação corrente é eliminado e, portanto, a senha de proteção é apagada



O problema é que, com a senha de proteção da aplicação ativada não é possível executar o comando de carga de firmware pelo SPDSW, pois a senha será solicitada para envio do comando. Para permitir a utilização deste comando nesta condição, deve-se primeiro ativar o modo Loader conforme descrito no item 4.1. Uma vez com o equipamento operando no modo Loader o comando de carga de firmware pode ser utilizado sem que seja necessária a especificação de uma senha de acesso.

No modo Loader selecione a opção do menu principal Ferramentas/Firmware do controlador. Será apresentada uma tela solicitando que o usuário especifique o arquivo de firmware a ser carregado. Selecione o arquivo (*.EFF) desejado e pressione o botão abrir.

O processo de carga de firmware será ativado e apresentado através de uma barra de progresso apresentada na parte inferior do SPDSW conforme indicado na figura seguinte.

Controle do Documento

Considerações gerais

1. Este documento é dinâmico, estando sujeito a revisões, comentários e sugestões. Toda e qualquer sugestão para seu aprimoramento deve ser encaminhada ao departamento de suporte ao cliente da **HI Tecnologia Indústria e Comércio Ltda.**, fornecendo os dados especificados na "Apresentação" deste documento.

2. Os direitos autorais deste documento são de propriedade da **HI Tecnologia Indústria e Comércio Ltda.**

Controle de Alterações do Documento

Data Liberação	Revisão	Descrição	Elaborado por	Revisado por	Aprovado por
05/01/2017	**1**	Documento revisado e migrado para o novo ambiente de documentação. Revisada a tabela de controle do documento para manter histórico dos responsáveis por elaboração, revisão e aprovação	N/a	Maria Villella	Isaias Ribeiro
16/01/2004	**0**	Documento Original	Hélio Almeida	Paulo Inazumi	Hélio Almeida