

# EXTRAÇÃO DO PROTOCOLO DE COMUNICAÇÃO PARA O CONTROLE DE UM DISPOSITIVO ATRAVÉS DO MONITORAMENTO DOS SINAIS DA PORTA SERIAL (RS232)

SERENO H. R. S.

*Laboratório de Massa, Diretoria de Metrologia Científica e Industrial, Inmetro  
Av. Nossa Senhora das Graças, 50 Prédio 3, Xerém Duque de Caxias, RJ  
E-mail: [hrsereno@inmetro.gov.br](mailto:hrsereno@inmetro.gov.br)*

**Resumo** Para desenvolver um programa de controle alternativo ao programa original do fabricante de um dispositivo controlado via interface serial RS232 é necessário conhecer o protocolo de comunicação. Em alguns casos, em especial quando os dispositivos são relativamente antigos, o protocolo não está disponível. Este trabalho apresenta uma metodologia para a extração do protocolo de comunicação de um sistema automático balança-alternador de carga utilizado para a calibração de pesos-padrão de alta exatidão de até 10 kg.

**Abstract** – To develop a control program other than the original program of the manufacturer for a controlled device using the serial RS232 interface it is necessary to know the communication protocol. In some cases, specially when the devices are relatively old, the protocol is not available. This work presents a methodology for the extraction of the communication protocol of an automatic scale load - alternator system used for the calibration of high accuracy standard weights of up to 10 kg

**Palavras-chave** Protocolo de Comunicação, Porta Serial, Monitoramento, Balança, Alternador de Carga, Automação.

## Introdução

Com o objetivo de aprimorar o controle dos processos de pesagem realizados no Laboratório de Massa do Inmetro (LAMAS), os processos que utilizam softwares originais (fornecidos pelos fabricantes) das balanças e instrumentos auxiliares utilizados do laboratório estão sendo substituídos por softwares desenvolvidos pelo corpo técnico do LAMAS.

A ferramenta básica para desenvolvimento destes softwares é o protocolo de comunicação do equipamento, ou seja, as configurações e o formato dos comandos, a serem implementados via software, que permitam a comunicação com o equipamento e obter as informações para a realização do controle.

Durante o desenvolvimento do processo de coleta de informações para o desenvolvimento do software do sistema balança-alternador, usado para a calibração de pesos-padrão de alta exatidão até 10 kg, verificou-se que o manual de operação não apresentava as informações referentes ao protocolo de comunicação deste equipamento.

Desenvolveu-se então uma metodologia para extração e análise dos sinais existentes na comunicação via serial durante operação do sistema balança-alternador com o software do fabricante. Com estes dados foi possível a dedução de um protocolo de comunicação para o sistema e posterior implementação deste no desenvolvimento do software.

## Características sistema Balança-Alternador

O sistema é composto por uma balança comparadora modelo C10000S com capacidade de 10 kg e resolução de 0,1 mg marca SARTORIUS, com um alternador de carga da mesma marca modelo YLA-01C. Este consiste em um sistema que faz a troca dos pesos sobre o prato da balança com duas posições onde são colocados os padrões de massa (de um lado o padrão de referência e do outro o objeto a ser calibrado), um módulo de controle externo que permite o acionamento do alternador através um painel frontal e uma impressora para impressão dos comandos acionados neste painel. O alternador realiza ciclos de pesagens ABBA (Padrão – Objeto – Objeto – Padrão), cada comparação é composta pela repetição de vários ciclos de pesagem.

Pode ser acrescentado ao sistema uma estação climática marca LAMBRECHT modelo YAK02Y-0001 que faz a tomada dos dados de temperatura, umidade relativa e pressão atmosférica.

Ambos equipamentos, sistema balança-alternador e estação climática, tem portas RS232 (serial) para comunicação com o computador.

O sistema possui um software desenvolvido pelo fabricante em ambiente DOS que permite o trabalho em conjunto ou independente da estação climática. Porém, o software oferece algumas limitações como:

- a identificação do arquivo para armazenagem dos dados da comparação se limita a oito dígitos
- a impossibilidade da programação de séries consecutivas de pesagens.
- a impossibilidade de atualização do registro de medição pois o mesmo é gerado automaticamente pelo software

### Desenvolvimento do novo software de acionamento do sistema Balança-Alternador

Para o desenvolvimento do software do sistema, são seguidos os seguintes passos:

- Identificação do Protocolo
- Testes de Verificação
- Programação

#### 3.1 Identificação do Protocolo

O manual de operação do alternador de carga [1] não fornece orientações sobre os comandos de acionamento remoto e formato do código de resposta. O manual apresenta somente algumas informações sobre os comandos do painel frontal de operação do alternador.

Observando a opção de configuração do software fornecido pelo fabricante, obteve-se as informações sobre velocidade de comunicação, bits de dados, bits de parada e paridade.

Com isso, sabe-se as configurações da porta, mas não os comandos e o formato de recebimento dos dados na porta (o protocolo de comunicação).

Na primeira tentativa de se obter o protocolo foi feito contato com o representante do fabricante no Brasil. Esse informou que não havia informações sobre o protocolo em seus arquivos por se tratar de um equipamento antigo.

Na segunda tentativa, estimulado pela experiência de que os fabricantes mantêm o protocolo entre equipamentos de uma mesma linha, tentou-se buscar o protocolo de comunicação de algum alternador de carga “novo” para que pudesse tentar a comunicação com o equipamento do LAMAS.

Pesquisando em manuais dos alternadores da mesma linha disponíveis hoje no mercado[2] também não foram encontradas informações sobre o protocolo de comunicação.

Na terceira tentativa considerou-se a possibilidade de extração dos comandos e formato dos dados de resposta do sistema monitorando os sinais de comunicação durante a operação do mesmo.

### 3.2 Monitoramento do Sinal

#### 3.2.1 Monitoramento dos níveis de tensão

Com base nas informações de configuração da porta e sabendo-se que, segundo o padrão RS232,

nos pinos 2 e 3, do conector serial de 9 pinos, encontram-se respectivamente os dados recebidos e enviados [3],[4],[5], poder-se-ia então fazer o monitoramento dos níveis de tensão nesses pinos. Sabendo-se que os níveis de tensão que representam o estado lógico 0 (zero) são de +5V a +15V e os níveis de tensão que representam o estado lógico 1 (um) são de -5V a -15V (Fig. 1), usando-se um osciloscópio poder-se-ia extrair o protocolo fazendo as conversões dos sinais de tensão em sinais binários.

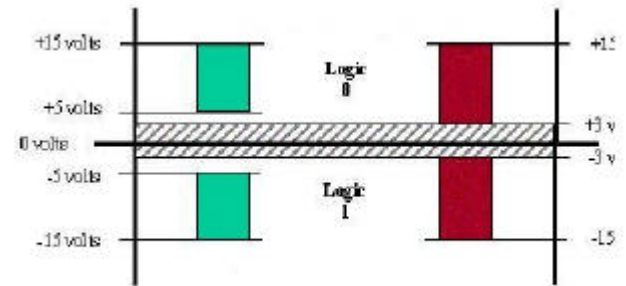


Fig.1. Níveis de tensão na serial

Porém, a necessidade de se fazer a análise do código binário embutido nos sinais inviabiliza, na prática, essa alternativa.

Conclui-se, então, que a alternativa viável seria análise do código ASCII embutido nos sinais.

#### 3.2.2 Monitoramento do sinal via software

Este monitoramento mostra-se mais eficiente pois o problema da dedução do protocolo fica reduzido à análise de código ASCII e não à códigos binários.

Para isso implementou-se a idéia de se fazer uma derivação no cabo de comunicação PC de controle / sistema balança-alternador Fig. 2 [6],[7],[8] que permitiria a apresentação na tela do código ASCII do tráfego de sinais entre estes dispositivos.

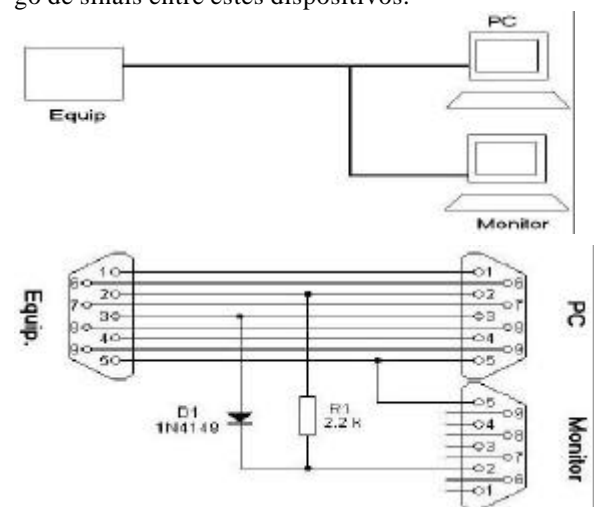


Fig. 2. Esquema ligação e cabo de monitoramento

No conector ligado ao computador de controle (PC) o pino 2 representa o sinal *Receive Data* ou Recebimento de Dados, o pino 3 o sinal *Transmitted Data* ou Transmissão de Dados e o pino 5 o sinal de terra.

No conector ligado ao sistema balança-alternador (Equip.) os pinos 2 e 3 tem sua representação invertida (condição original do cabo do equipamento).

Ambos conectores são ligados entre si pino a pino por um cabo de ligação com derivação como descrito abaixo.

Ao fio que une os pinos 2 do cabo de ligação conecta-se o pino 2 da serial do PC monitor através de uma resistência em série de 2,2 k $\Omega$ .

Conecta-se também ao fio que une os pinos 3 do cabo de ligação o pino 2 da serial do PC monitor através de um diodo (1N4148) segundo esquema mostrado na Fig. 2 (é importante colocar o diodo na posição indicada).

O pino 5 do cabo de ligação também conecta-se ao pino 5 da serial do PC monitor

A Fig.3 mostra o cabo construído segundo o esquema acima.

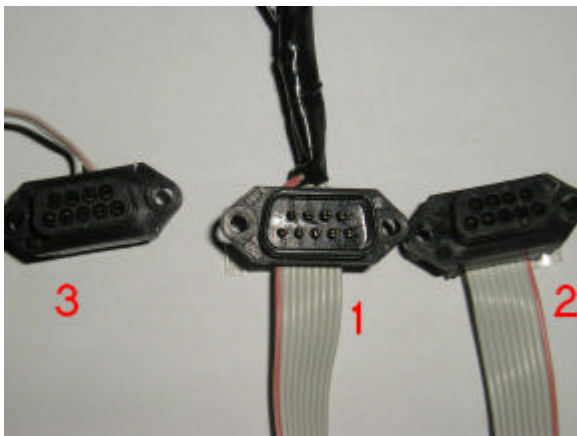


Fig. 3. Cabo construído

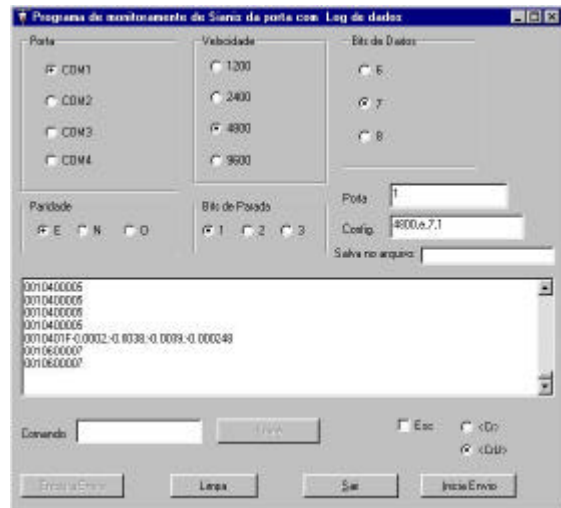
No cabo acima, o conector 1 (macho) é conectado ao cabo vindo do sistema balança-alternador, o conector 2 (fêmea) é conectado ao PC de controle com o programa do fabricante e o conector 3 (fêmea) é conectado ao PC monitor.

Para o monitoramento foi desenvolvido, também, um software em Visual Basic<sup>®</sup> (Fig. 4) que escrevesse em forma de código ASCII todos os dados trafegados na porta para a tela e para um arquivo texto.

Esse software permite também o envio de dados podendo ser utilizado em outras aplicações.

Foram executadas 30 séries de comparações (pesagens) com o objetivo de capturar os sinais de controle e ter-se condições de analisar uma quantidade de dados que permitisse deduzir com segurança os códigos de controle e formato dos códigos de resposta.

Fig. 4. Aplicação desenvolvida



### 3.3 Análise dos dados

Para deduzir o protocolo, além dos dados capturados é necessário contar como referência os respectivos valores indicados no display da balança para cada pesagem. Esses valores são apresentados, para cada série de comparações, em um registro de medição gerado pelo software do fabricante. Com esta informação é possível comparar as leituras das pesagens com os códigos ASCII capturados e deduzir os formatos de comunicação.

Para cada registro de medição o programa desenvolvido para esta aplicação gera um arquivo (.dat) com os códigos ASCII que trafegavam na porta durante o monitoramento. Cada arquivo contém aproximadamente 2500 linhas com códigos, onde alguns se repetiam.

Os códigos ASCII capturados no arquivo (.dat) apresentavam dois tipos distintos de seqüências:

- exclusivamente formadas de números de 10 e 11 caracteres

Ex.: 00502001137  
0010600007

- formadas por números e letras de 37 a 41 caracteres

Ex.:0010401B0.0009;0.0063;0.0065;0.00094  
B  
0010401B0.0010;-0.0015;-  
0.0016;0.00094B

Ambos tipos de seqüências são seguidas pelos caracteres 13 (CR – Carriage Return) e 10 (LF – Line Feed) não mostrados nos exemplos acima.

Analisando os códigos, identificou-se que as seqüências longas formadas por letras e números continham os valores de leitura correspondentes às pesagens indicados no registro de medição. Estes valores eram enviados todos em conjunto ao final do ciclo de pesagem e não após cada pesagem como em outros equipamentos.

Alguns códigos tinham uma sintaxe bem parecida mudando somente alguns dígitos, onde se deduziu

que o primeiro seria o comando de envio de dados e o segundo a resposta do sistema.

De posse dessas informações e com o programa anteriormente desenvolvido para o monitoramento, realizou-se vários testes de verificação.

### 3.4 Testes de Verificação

Analizando os códigos ASCII extraídos pode-se deduzir quais eram os códigos de acionamento e formato da resposta do sistema, podendo-se dessa forma iniciar os testes.

Durante os testes enviou-se, através do software utilizado no monitoramento, os comandos deduzidos e verificou-se a resposta do sistema. Caso a resposta fosse compatível com o esperado ter-se-ia a comunicação estabelecida e protocolo conhecido.

No primeiro teste enviou-se o código:

0010100000

obtendo-se como resposta do sistema o próprio código enviado, iniciando assim a comunicação. Após o recebimento do código anterior enviou-se o código:

00502001137

obtendo-se como resposta desta vez o código:

0050200007

e observou-se que o alternador de carga iniciou os movimentos de colocação e retirada dos pesos, dando início a uma rotina de movimentos programada em ROM no módulo de controle.

Com o objetivo de verificar se os resultados eram enviados automaticamente após o encerramento do ciclo de pesagens ou enviados em resposta a um comando de solicitação dos resultados, durante os movimentos do alternador de carga foi enviado várias vezes o código:

0010400005

sem resposta do sistema. Após a conclusão do último movimento de descarregamento do alternador de carga encerrando o ciclo de pesagens, enviou-se novamente o mesmo código, obtendo como resposta do sistema a sentença:

0010401B0.0009;0.0063;0.0065;0.00094B

contendo os valores das pesagens.

O último código enviado/recebido era sempre:

0010600007

verificou-se que o envio deste ao término das comparações habilitava o sistema para receber novos códigos (comandos). Este código foi enviado finalizando, então, o ciclo de comunicação.

Neste primeiro teste obteve-se sucesso na comunicação com sistema balança-alternador.

Efetando testes adicionais de maneira semelhante utilizando outros códigos também deduzidos confirmou-se a função pré-programada (ROM) de cada um deles, como mostrado na tabela 1:

**Tabela 1. Códigos Deduzidos**

<i>Código</i>	<i>Sentido</i>	<i>Função</i>
0010100000	PC-Sistema / Sistema-PC	Estabelece a comunicação
00502001137	PC-Sistema	Solicita a realização do 1º ciclo
0050200007	Sistema-PC	Resposta à solicitação
0010400005	PC-Sistema	Ciclo terminado
0010401X	Sistema-PC	Valores do ciclo
00503001136	PC-Sistema	Solicita a realização do próximo ciclo
0050300006	Sistema-PC	Resposta à solicitação
0010600007	PC-Sistema / Sistema-PC	Finaliza a comunicação

X - é uma letra qualquer seguida dos valores das pesagens

### 3.5 Programação

De posse do protocolo deduzido, o passo seguinte foi escolher a plataforma de programação e desenvolver o novo software de controle propriamente dito.

A plataforma escolhida foi o LabVIEW® pois é de fácil programação e todos os programas do laboratório estão migrando para ela.

O software desenvolvido, como desejado, apresenta as seguintes vantagens:

- possibilidade de programação de múltiplas séries de pesagens;
- análise de resultados a cada ciclo de pesagem;
- apresentação gráfica de resultados parciais;
- identificação do arquivo de uma forma mais clara;
- possibilidade de adicionar observações, referentes à comparação, ao registro de medição;
- autenticação do registro de medição;
- validação da entrada de dados.

O software está em fase final de teste para validação e implementação definitiva.

## Conclusão

A metodologia aplicada para extração do protocolo de comunicação foi efetiva permitindo o desenvolvimento de um novo programa de controle muito mais flexível do que o original.

Essa metodologia de extração poderia ser aplicada a outros dispositivos também controlados através da interface serial RS232 cujo protocolo de comunicação não esteja disponível.

Essa metodologia é de fácil aplicação e custo reduzido.

## Agradecimentos

Agradeço a Deus, minha família, em especial a meu irmão Gustavo, e ao apoio de todas as pessoas que contribuíram para a realização desse trabalho, aos colegas de laboratório, Fábio e Vivian, que me apoiaram e me incentivaram, ao Victor pela parceria no desenvolvimento deste trabalho e um agradecimento especial a minha namorada Livia e Rafael Oliveira.

## Referências Bibliográficas

[1] Sartorius YLA01C. Instrucciones de instalación y manejo.

[2] Sartorius Interface. Interface Description for Sartorius Balance and Scales

[3] Canzian, E. *MINICURSO Comunicação Serial - RS232*

[4] Seixas Filho, C. *Comunicação Serial*. Universidade Federal de Minas Gerais Departamento de Engenharia Eletrônica

[5] Oliveira, R. S. *SISTEMA AUTOMATIZADO PARA CALIBRAÇÃO DE TRANSDUTORES DE FORÇA*. Universidade do Estado do Rio de Janeiro, Monografia curso de especialização em Engenharia Mecatrônica, 2004

[6] <http://www.aggsoft.com/rs232-pinout-cable/serial-port-monitor-cable.htm>

[7] <http://www.lammertbies.nl/comm/cable/RS-232-spy-monitor.html>

[8] Müller M. *RS232 in-line data spy* Elektor Electronics, 10/2001 p. 60-63.