

E10-2010-35

A. Yu. Isupov

CAMAC SUBSYSTEM AND USER CONTEXT UTILITIES
IN *ngdp* FRAMEWORK

Исупов А. Ю.

E10-2010-35

Работа с САМАС и пользовательские утилиты режима задачи в инфраструктурной системе *ngdp*

Описаны продвинутые элементы инфраструктурной системы (framework) *ngdp*: работа с аппаратурой САМАС, «самотечные» варианты нод для систем сбора данных (DAQ) с соответствующей политикой, нода *ng_mm(4)* как альтернатива сокету *ng_socket(4)*, управляющая подсистема, утилиты режима задачи, представление событий для пакета ROOT, тестовые и отладочные ноды, возможные дополнения собственно пакета *netgraph(4)* и др. Таким образом, *ngdp* пригодна для построения относительно простых систем DAQ, обслуживающих САМАС.

Работа выполнена в Лаборатории физики высоких энергий им. В. И. Векслера и А. М. Балдина ОИЯИ.

Сообщение Объединенного института ядерных исследований. Дубна, 2010

Isupov A. Yu.

E10-2010-35

CAMAC Subsystem and User Context Utilities in *ngdp* Framework

The *ngdp* framework advanced topics are described. Namely we consider work with CAMAC hardware, «selfflow» nodes for the data acquisition systems with the As-Soon-As-Possible policy, *ng_mm(4)* as an alternative to *ng_socket(4)*, the control subsystem, user context utilities, events representation for the ROOT package, test and debug nodes, possible advancements for *netgraph(4)*, etc. It is shown that the *ngdp* is suitable for building lightweight DAQ systems to handle CAMAC.

The investigation has been performed at the Veksler and Baldin Laboratory of High Energy Physics, JINR.

Communication of the Joint Institute for Nuclear Research. Dubna, 2010

1. INTRODUCTION

The [1] paper describes only basic design solutions and key elements of the *ngdp* framework intended for the data acquisition (DAQ) systems building. However many topics have not been touched upon due to publishing limitations. So here we'll try to fill this gap and consider the items, which allow us to build some lightweight DAQ systems to work with CAMAC using *ngdp* elements. Also we'll describe some advanced topics like the control subsystem, *ng_mm(4)* node as an alternative method to communicate with *netgraph(4)* graph in the kernel from the user context, possible advancements for the *netgraph(4)* itself, test and debug nodes, etc.

Through the presented text the file and software package names are highlighted as *italic text*, C and other languages constructions — as `typewriter text`. Reference to the manual page named «qwerty» in the 9th section is printed as *qwerty(9)*, reference to the sections in this paper — as «Subsec.2.3.1». Note also verbal constructions like «*close(2)*d» and «mk*peer*ing», which means «closed by *close(2)*» and «peer making by mk*peer*». Subjects of substitution by actual values are enclosed in the angle brackets: <setup>, while optional parameters are given in the square brackets: [mod [group]]. All mentioned trademarks are properties of their respective owners.

2. ADVANCED TOPICS IMPLEMENTATION

2.1. *netgraph(4)* Additional, Patches and Improvements. The default maximal size of the *netgraph(4)* datagram can be too small to hold a packet with the event of some MB. Fortunately, all what we need is changing of OS tunables (kernel and *sysctl(8)* variables), so recompile of the kernel is not required.

At the moment of writing this paper we saw the following possible principal advancements for the existing *netgraph(4)* system:

- Generalization of the currently local scheme of the control messages addressing to be used remotely through the network. A special agent — *ng_sv(4)* (supervisor) node (see also Subsec.2.4.1) — is proposed to perform the remote control messages delivering. The *ng_sv(4)* is assumed to be launched on each involved computer. Also we should modify the control messages delivery mechanism in the *netgraph(4)* code to change its behaviour to be some analogue of the

«default gateway». This means that all control messages with locally unknown (effectively remote or wrong) addresses should be sent to the local *ng_sv(4)* node for the decision on further delivering. The remote delivery should use the connectionless (UDP) protocol, which allows communication with an arbitrary number of hosts through the only one *ng_ksocket(4)*. We have also introduced the `NG_MKREMOEMSG()` macro and patched the existing functions `ng_path_parse()`, `ng_path2noderef()` and macro `NG_MKRESPONSE()`. Affected files: *ng_base.c*, *ng_message.h*.

- Possibility to insert some node between the two already connected nodes. It is absent in the current *netgraph(4)* system, however it will be very useful for the *ng_filter(4)* node implementation. So we introduce the function:

```
int ng_insert(node_p, char *hook1, char *hook2, char *path1,
char *path2). Affected file: ng_base.c.
```

The following technical improvements in the form of the corresponding patches are available:

1. *ng_socket(4)* is patched against the crash on the netgraph datagram fragmented by TCP/IP. Affected file: *ng_socket.c*.

2. *ng_ksocket(4)* is patched for `NGM_KSOCKET_GETOPT` control message proper working. Affected file: *ng_ksocket.c*.

3. The *ngctl(8)* is improved in some aspects:

- Buffer for write command is increased to be large enough to hold the increased *netgraph(4)* datagram.

- Script variable `$?` is introduced. It is substituted by a path of the last node responding to *ngctl(8)* control message. `$?` is very useful for naming of new *ng_ksocket(4)* instance which appears after the `listen()`ing *ng_ksocket(4)* `accept()`s.

- `sleep` command is added to be used in scripts.

- A `MsgCmd()` reaction on the `EINPROGRESS` error from `NgSendAsciiMsg()` is changed. Now `MsgCmd()` waits for a response during the timeout instead of the immediately error return. This behaviour is needed to continue the script execution after *ng_ksocket(4)* `connect()`ing.

- New nonblocking function `NgSendAsciiMsg_nb()` used in the `MsgCmd()` is introduced. It is able to wait for ascii-to-binary conversion response up to timeout expiration instead of the infinite waiting in `NgSendAsciiMsg()` from *libnetgraph* library. The remote delivering scheme of the control messages needs this behaviour.

- The `MsgRead()` function is patched to support remote control messages delivering.

- `msg` command now understands the remote path specification (see Sub-sec.2.4.1) in the form: `node_name@IP_address:hook1.hook2`. Note, that the so-called generic control messages are still only local as well as the `mkpeer`,

shutdown, connect, rmhook, name, list, config, show, status, and types *ngctl(8)* commands based on them.

— The `dot` command implementation is refined in some aspects: output of disconnected nodes is eliminated; `fontsize` is enlarged by 2 pt for both the node and edge labels; explicit default fontname declaration (**Helvetica-Bold**) is added. Affected files: *main.c* , *msg.c* , *name.c* , *write.c* , *ngctl.h* .

4. Ascii-to-binary and binary-to-ascii conversion schemes are revised to handle the remote control messages delivering properly. Affected file: *ng_base.c* .

5. The `NgSendAsciiMsg()` and `NgDeliverMsg()` functions from the *libnetgraph* are patched to handle the remote control messages delivering properly. Affected file: *msg.c* .

Let us note that during modifications of the basic *netgraph(4)* system we try to limit ourselves by only absolutely necessary changes, as minimal as possible, in order to simplify maintenance at the future *netgraph(4)* version changes.

2.2. *ng_mm(4)* Node as an Alternative for *ng_socket(4)*. To allow a cheaper data injection into *netgraph(4)* system and their extraction from it than it is possible to do by means of the standard method using the socket mechanism provided by *ng_socket(4)* node, we implement the *ng_mm(4)* (for memory mapping) node type. It supplies two UNIX devices */dev/mmr<N>* and */dev/mmc<N>*, whose instances with different unit numbers *<N>* and minors belong to different node type instances. Both devices support *open(2)*, *close(2)*, *ioctl(2)*, *mmap(2)*, *select(2)/poll(2)* system calls like usual UNIX devices do*. When the user context process performs *mmap(2)* of this device it obtains a direct access to the packet circle buffer allocated in the kernel memory by *ng_mm(4)*. After that the process can read from the buffer of the so-called «raw» device */dev/mmr* and/or write to the buffer of the so-called «converted» device */dev/mmc*. To synchronize the process with the packets arrival in and departure from the buffers, the following *ioctl(2)* interface for these devices is provided (first three commands are for a raw device while the last three ones — for the converted device):

`MMGBUFRAW`, `size_t` argument — gets raw buffer size;

`MMGROFFT`, `size_t` argument — gets offset of the next packet ready to obtaining (process can be blocked up to the packet arrival);

`MMRDDONE`, without argument — says the packet reading done;

`MMGBUFCONV`, `size_t` argument — gets the converted buffer size;

`MMSSZGWOFFT`, `size_t` argument — sets the size of the packet to be written and gets the offset where it should be written;

`MMWRDONE`, without argument — says the packet writing done.

*Note, we do not support *read(2)* and *write(2)* because that contradicts to the main idea — to eliminate the memory copying overhead as a result of using *copyin(9)/copyout(9)*.

So the data flow through the *ng_mm(4)* as follows: the packets arrived on the in hook are either placed into the raw buffer or dropped, if the raw device was not opened; the process will be waken up, if it was blocked on MMGROFFT request; the oldest packet(s) will be discarded, if the buffer lacks of space; however if the process reads one of them, the newly arrived packet will be dropped. Immediately after the process reports the end of the packet placement into the converted buffer, this packet will be checked and, in case of approval, transmitted through the out hook. The packets arrived on the out hook are always dropped.

To simplify mkpeering in some situations, the *ng_mm(4)* node supports the creat hook, which can be removed after in or out hook appearing, however in or out hook can be used for mkpeering, too. If the process *open(2)*s the raw device only and is sure that it does not need the converted device (and vice versa, of course), then for security reasons the process can «catch» the converted device, so nobody (including this process itself) can open it before the raw device is *close(2)*d. The raw device should be *open(2)*ed with O_EXCL flag for catching the converted device (and vice versa).

Naturally, *ngget(1)* and *ngput(1)* utilities (see Sec. 2.5) with -A and -a options use the *ng_mm(4)*'s interface.

The *ng_mm(4)* node supports a generic set of *netgraph(4)* control messages as well as the following specific ones:

clrstats (clrostats) — clears the current statistics (numbers of data_packs, data_bytes, fails and drops) for the in (out) hook;

getistats (getostats) — returns the current statistics for the in (out) hook;

getclrstats (getclrostats) — returns the current statistics and clears it for the in (out) hook;

getdev <struct ng_mm_getdev> — returns the raw and converted device names with unit numbers as C-strings <rawname> and <convname>.

2.3. Nodes with ASAP Policy. The As-Soon-As-Possible variants of the *ng_fifo(4)*, *ng_em(4)* and *ng_pool(4)* nodes [1] named *ng_fifos(4)*, *ng_ems(4)* (*s* for *simple*) and *ng_bp(4)* (for *branch point* after *qdpb*'s terminology), are implemented to allow the building of lightweight DAQ systems, for example [2, 3]. Generally speaking, ASAP («selfflow») policy means that the data are processed immediately after obtaining and transmitted immediately when ready. Therefore all the transfers are done synchronously, if possible. Otherwise, for example, if the *rcvdata()* of the destination node is locked, the *netgraph(4)* bufferizes the data intermediately and retransmits them later invisibly for the nodes. So, a «primary push» from the data originator — an interrupt (IRQ) handler or some socket — is enough for a data packet to travel through the whole DAQ system. The «selfflow» behaviour allows us to avoid an execution stream (kernel thread) in design of the ASAP client nodes *ng_ems(4)*, *ng_bp(4)*. In contrast, a complex DAQ systems with LAZY policy [1] should have on each level at least one exe-

cution stream able to send requests to the bufferization server node *ng_fifo(4)* of the data upstream level.

ASAP client nodes allow only one hook named `output` simultaneously, so to multiply the output stream, we can use some of *ng_tee(4)*, *ng_one2many(4)*, or *ng_fifos(4)*. All ASAP nodes understand the generic *netgraph(4)* control messages.

2.3.1. *ng_fifos(4)*: simple «selfflow» queue. The *ng_fifos(4)* node is able to

- spawn `listen()`ing `ng_ksocket` at startup;
- spawn `accept()`ing `ng_ksocket(s)` at each connection request from the known host(s) / port(s) up to the configured maximum, and/or
- accept hook connection from the local `ng_socket(s)`;
- emit each data packet obtained on the `input` hook as soon as possible through all `accept()`ing `ng_ksocket(s)` and local `ng_socket(s)` currently connected;
- close `accept()`ing `ng_ksocket` at EOF notification obtaining or connection loss.

The *ng_fifos(4)* node supports the same hooks and specific set of control messages as *ng_fifo(4)* [1] with exclusion of `setconf`, `getconf`, `outtype`, `outpatt` coupled with omitted debugging ability to self-generate packets.

2.3.2. *ng_ems(4)*: event merger's «selfflow» implementation. The *ng_fifos(4)* node requires the corresponding clients, so *ng_ems(4)* instead of requests issuing is simply waiting for the data packets on the input channels. When the arrived packets follow one of the configured merging rule(s), they are merged. Such functionality does not require *kthread(9)* usage, however, it involves some complicated merging algorithm, too. Of course, `id` marks [1] are supported by *ng_ems(4)*, because they are even more useful here than in the *ng_em(4)* case, where, at least, the packet numbers usually are guaranteed to be as required. Note, however, that none of `id` marks is added by default in the node constructor, so at least `addid { name="num" }` control message should be sent to *ng_ems(4)* for it works as expected.

Using the approach described for *ng_em(4)* [1] we can compile the same *ng_ems(4)* source for both the kernel and user contexts. After strong debug sessions in the both contexts we are sure, that the *ng_ems(4)* algorithm implementation is working now.

The *ng_ems(4)* node supports the same hooks and specific set of control messages as *ng_em(4)* excluding `settimo` and `gettimo`. The following control messages have slightly different meanings:

`connect` — checks the already supplied input channels and input type entries configuration, removes the unused input channels (if any) and connects the unconnected yet `ng_defrag` subnodes to the upstream servers according to the current configuration;

`start <int64_t outpacks>` — starts packets accepting up to supplied `<outpacks>` output packets will be merged (`-1` means to accept infinitely);
`stop` — explicitly stops the packets accepting before the `<outpacks>` are merged.

2.3.3. *ng_bp(4) node as «selfflow» version of ng_pool(4)*. An ASAP version of *ng_pool(4)* node [1] named *ng_bp(4)* is able to

- launch the `ng_defrag` subnode at each configured input channel, this node in its turn launches the client `ng_ksocket` node, which `connect()`s to the upstream ASAP server corresponding to this channel;
- transmit all the packets, accepted in the input channel(s) according to the configured rules, through the output hook.

Each of the accepting rules is a `struct tbl` and contains the input packet type `<in_type>`, which is allowed to arrive through any configured input channel with the corresponding set bit (equals to 1) in mask `<mask>`. The `struct tbl` also contains the number `last_num` of the last obtained packet of type `<in_type>`. A specific input type value `-1` matches the arbitrary input type. After *ng_bp(4)*'s mkpeer'ing the only one rule with such wildcard input type and mask with all the bits set is defined. It is equivalent to obtaining `addcfg { in_type=-1 mask=-1 }` control message at the early startup. Note, that the input type comparison is done in the same order, in which the rules were added. So, the default wildcard rule will always match first. Thus, to establish the rule(s) with the nonwildcard input type, we should firstly remove the default rule — e.g., by `delcfg { in_type=-1 }`. However, the last wildcard rule with some restrictive mask, where only some bits are set, allows one to receipt packets of any type through only some input channels. The default *ng_bp(4)*'s state after the fresh startup allows the packets obtaining through any configured input channel.

The *ng_bp(4)* node supports the same hooks and specific set of control messages as *ng_pool(4)* excluding `settime`, `gettime`. The following control messages has slightly different meanings:

`addcfg <struct tbl>/delcfg <struct tbl>` — adds/deletes the input packet type configuration entry;
`getconf` — returns the full current configuration of the input packet types;
`connect` — connects `ng_defrag` subnodes to upstream servers according to the current configuration of the input channels;
`start/stop` — allows/denies packets obtaining through all the configured input channels.

2.4. Control Subsystem. According to a big DAQ system scheme from [1], the computers belonging to the SubEvB, EvB and pool levels are controled from computers of the DAQ Operator group. The FEM level is supervised from both the Slow Control group and FEM Control group. The machines belonging to all the groups (instead of levels) are autonomous. DAQ Operator group should be able to propagate changes in the *ngdp* system state very quickly. So the

corresponding software control subsystem, at least the slave side elements on the very busy SubEvB, EvB and pool level machines, should be implemented outside of preemptive scheduling. We have the following options to do so:

- in the kernel context as some *netgraph(4)* node type: *ng_sv(4)* (for supervisor);
- in the user context by programs with realtime priority for slave elements and with any priorities for master elements on the usually idle machines of the DAQ Operator group.

Note, that the user context realtime with the guaranteed response time is practically impossible under usual UNIX-like systems, so the last option can be unreachable. The *ng_sv(4)* option is more attractive also for the reasons of unification, startup schemes building and remote control messages implementation (see Sec. 2.1).

2.4.1. *ng_sv(4)* prototype. As a first step to *ng_sv(4)* node with the functionality, described in Sec. 2.1, we implement some prototype, which is able to

- spawn `bind()`ed `ng_ksocket` of UDP protocol at node startup and respawn it after shutting down accidentally;
- send/receive arbitrary remote control messages through this `ng_ksocket`;
- send a `test` remote control message to remote `ng_sv` node instance and respond to this message.

According to the control subsystem's requirements the *ng_sv(4)* is «permanent» (survive without hooks) node, around which a required *ngdp* graph could be built during the DAQ startup or automatically recreated after troubles.

The prototype supports the following specific control messages:

`bindaddr` <struct sockaddr> — sets own IP address to perform `bind()` in the same format as understood by the *ng_ksocket(4)* node;

`testsend` <char *ng_remote_path> — sends `test` remote control message according to the supplied remote path specification <ng_remote_path>.

The remote path specification extends the usual *netgraph(4)* absolute path specification in the following way: the nodename field before «:» now can contain an IP address after usual nodename itself and «@» sign. So, `src2@192.168.10.15:out1` specification means the peer node of the hook named `out1` of the node named `src2` on the computer with IP address `192.168.10.15`.

2.4.2. Control utilities. Some control utility could be implemented for each introduced *ngdp* node type. The utility can have a graphical user interface (GUI) to allow the end-user to be more comfortable than it is possible by using the *ngctl(8)* command string directly. The control utility should be aware of the control messages specific to the corresponding node type, as well as of the node type defaults, parameter ranges, etc. Of course, the preferred way to send control messages is to call *ngctl(8)* internally, however, the control utility could also use the *netgraph(3)* directly. The former approach similar to the one used by the supervisor *sv(1)* utility of the *qdpb* system, which simply provides GUI over

already existing command string tools. There is a wide assortment of toolkits for the X Window System [4,5], which allow one to implement any required GUI. Note, that the control utilities implementation is reasonable at some mature stage of the *ngdp* system, and it is beyond the scope of the present paper.

2.5. User Context Utilities. As was noted in [1], any user context utilities previously implemented for *qdpb* — *writer(1)* [6], *analyser(1)* [7], *statman(1)* [8], polarization calculators from polarimeter DAQ systems [9–11] — are still usable under *ngdp*, too, until they are recompiled to be aware of the redesigns mentioned in Sec.A.1. Here we consider only utilities introduced by *ngdp*. We describe neither the command string options nor the reaction on signals because the *ngdp* provides the manual pages for all the mentioned utilities. Note, that each utility exits 0 on success and > 0 if an error occurs, and has *-h* flag means to write the usage to the standard error output and exit successfully.

2.5.1. *ngget(1)*. The *ngget* is a utility for the packet stream extraction from *netgraph(4)*.

```
ngget [-f{<outfile>|-}] [-p{<pidfile>|-<template>XXXXX}] [-A|-a [-e]]
      [-l] [-d] [-r{<outrate>|-}] [-v]] <peername> <peerhook> [<name> [<hook>]]
ngget -m [-f{<outfile>|-}] [-p{<pidfile>|-<template>XXXXX}] [-A|-a [-e]]
      [-l] [-d] [-r{<outrate>|-}] [-v]] <peertype> <peerhook>
      [<peername> [<name> [<hook>]]]
```

The *ngget* reads messages from the *netgraph(4)* data socket, optionally de-fragments them into packets and writes the packets to the standard output. Thereof *ngget* is a service module to extract the packet stream from the kernel graph into the user context.

In the first synopsis form the *ngget* connects the hook named <hook> (or «in» if not supplied) of the newly created *ng_socket(4)* named <name> (or «ngget<PID>» if not supplied) to the hook <peerhook> of the already existing node <peername>.

In the second synopsis form the *ngget* connects hook <hook> of the newly created *ng_socket(4)* <name> to the hook <peerhook> of the node with type <peertype>, newly created by the *mkpeer* control message, and named as <peername>, if supplied.

2.5.2. *ngput(1)*. The *ngput* is a utility for the packet stream injection to *netgraph(4)*.

```
ngput [-l] [-d] [-c] [-p{<pidfile>|-<template>XXXXX}] [-A|-a [-e]]
      <peername> <peerhook> [<name> [<hook>]]
ngput -m [-l] [-d] [-c] [-p{<pidfile>|-<template>XXXXX}] [-A|-a [-e]]
      <peertype> <peerhook> [<peername> [<name> [<hook>]]]
```

The *ngput* reads the packets from the standard input and writes them to the *netgraph(4)* data socket. Thereof *ngput* is a service module to inject the packet stream from the user context into the kernel graph.

In the first synopsis form the *ngput* connects hook <hook> (or «out» if not supplied) of the newly created *ng_socket(4)* <name> (or «ngput<PID>» if not supplied) to the hook <peerhook> of the already existing node <peername>.

In the second synopsis form the *ngput* connects hook <hook> of the newly created *ng_socket(4)* <name> to the hook <peerhook> of the node with type <peertype>, newly created by the *mkpeer* control message, and named as <peername>, if supplied.

2.5.3. *b2r(1)* (*Binary-To-ROOT*) *converter*. The *b2r(1)* reads the data packets from the standard input and for each of them produces representation for the ROOT package [12]. The *b2r(1)* has three synopsis forms which correspond to the following ROOT events' transfer variants:

- to remote client process(es) by ROOT *TMessage* class through the usual socket pair*;
- to the local child process by *TBufferFile* through the *mmap(2)*ed memory or SysV IPC shared memory mechanisms synchronized by the SysV IPC semaphores;
- to the local process by the data packets of the special type, which encapsulate *fBuffer* of the *TBufferFile* with the stored ROOT event, through the standard output.

The *b2r(1)* avoids intermediate HDD storage, however, for flexibility reasons it is able optionally to store ROOT events as ROOT *TTree* with single *TBranch* into ROOT *TFile*, too. The *b2r.cxx* source is written in terms of the only one «high-level» ROOT class to reach the event content independence (see Sec. 3 for details). The object codes of the implementation as well as of ROOT dictionary generated by *rootcint(1)* of this class and possibly of other involved classes, should be linked (dynamically or statically) with the *b2r.o*.

```
b2r [-l] [-d] [-f{<outfile>|-}] [-s{<filesize>|-}] [-S{<splitlevel>|-}]
  [-p{<pidfile>|-<template>XXXXX}] [-a{<addr>[ ...]}] [-r{<outrate>|-}] [-v]]
b2r -b{<childname>} -f{<outfile>|-} [-p{<pidfile>|-<template>XXXXX}]
  [-r{<outrate>|-}] [-v]]
b2r -O [-m{<mmname>|-}] [-l] [-d] [-f{<outfile>|-}] [-r{<outrate>|-}] [-v]]
  [-s{<filesize>|-}] [-S{<splitlevel>|-}] [-p{<pidfile>|-<template>XXXXX}]
```

In the first synopsis form the *b2r* sends the produced ROOT events to all the clients, which have already requested registration on port 12340/tcp. The number of simultaneously registered clients is limited by the compiled-in value.

In the second synopsis form (the so-called batch or offline mode) the *b2r fork(2)s* and *exec(3)s* <childname> child process (usually *r2h(1)* in the batch mode, too) with the same -f, -r and -v options. The -d, -s, and -S options are ignored.

*Using ROOT *TServerSocket* / *TSocket* wrappers.

In the third synopsis form (the so-called output mode) the *b2r* transfers the produced packets with ROOT events into the standard output.

2.5.4. *r2h(1)* (*ROOT-To-Histogram(s)*) converter. One of possible *b2r(1)* clients is the *r2h(1)*, which fills some histograms from the event-by-event data. Like *b2r(1)* the *r2h(1)* is written in terms of the only one ROOT class and obtains the event's data through the interface provided by them (see Sec.3 for details), so it is event content independent, too. This means, the *r2h.o* should be linked in the same way as *b2r.o* (see Subsec.2.5.3). Also we implement the configuration and control protocol *r2h.conf(5)* for the runtime conversations between *r2h(1)* as server and its client(s). The *r2h(1)* startup configuration is performed from the file written in terms of this protocol (see Subsec.2.5.5).

```
r2h [-l] [-d] [-c{<cfgfile>|-}] [-f{<outfile>|-}] [-s{<saverate>|-}]
[-p{<pidfile>|-<template>XXXXX}] [-r{<outrate>|-} [-v]] [-a<addr>[ ...]]
[-A<addr>[ ...]] {[ -I [-P]]| [<peerhost> [<peerport>]]}
r2h -b<shkey> -f{<outfile>|-} [-l] [-c{<cfgfile>|-}] [-a<addr>[ ...]]
[-p{<pidfile>|-<template>XXXXX}] [-r{<outrate>|-} [-v]] [-A<addr>[ ...]]
```

In the first synopsis form the *r2h* reads ROOT TMessages from a server (f.e., *b2r(1)*) through ROOT TSocket connected to the port <peerport> (12340 by default) on the host <peerhost>; extracts event representation in the form of some compiled-in ROOT class from each TMessage obtained; fills some histograms configured by <cfgfile> file in the *r2h.conf(5)* format; sends the requested histogram(s) to the corresponding registered client(s) by TMessage(s); and optionally writes all the configured histograms to ROOT TFile <outfile>. The *r2h* is listen()ing on port 12341 for the client registration requests. The number of simultaneously registered clients is limited by the compiled-in value.

If the -I option is specified, *r2h* instead of TSocket reads the standard input for the data packets of some compiled-in type, each of them should contain a serialized ROOT event (f.e., produced by *b2r(1)* in the output mode). The *r2h* extracts this event using the ROOT TBufferFile with fBuffer, which points to the packet's body. With the -I option the <peerhost> and <peerport> arguments are ignored.

In the second synopsis form (the so-called batch or offline mode) the *r2h* extracts each ready ROOT event using the ROOT TBufferFile with fBuffer, which points to the shared memory region with key <shkey>, where the ROOT event was stored by *b2r(1)*. Other tasks are the same as in the first synopsis form. The memory synchronization is based on the SysV IPC semaphore mechanism. The -d, -s options and <peerhost>, <peerport> arguments are ignored.

2.5.5. *r2h.conf(5)*: control protocol for *r2h(1)*. The protocol for conversation between the histogram server *r2h(1)* and its client(s) is #defined in the *r2hproto.h* header as follows:

```

#define CMD_GET 10002
#define CMD_RESET 10003
#define CMD_DELETE 10004
#define CMD_BOOK1D 10005
#define CMD_BOOK2D 10006
#define CMD_RESETELL 10009
#define ACK_ERR 10010
#define ACK_OK 10011

#define CMD_QUIT 10012
#define CMD_LEAVE 10016
#define CMD_CONNECT 10017
#define ERR_NoSuchHist 1
#define ERR_UnknownCmd 2
#define ERR_PermDenied 3
#define ERR_ZipFailed 4

```

The `what()` field of the `ROOT TMessage` sent from the client to *r2h(1)* could contain any of `CMD_*` values, while the `TMessage` body should contain the command parameters in the C-string form. The *r2h(1)* can respond by

`ACK_ERR` with `UInt_t error` (can have any of `ERR_*` values) in the `TMessage` body;

`KMESS_OBJECT` with `TObject` of type `TH1F` or `TH2F*`; or

`ACK_OK` without the body.

`CMD_DELETE`, `CMD_BOOK1D` and `CMD_BOOK2D` commands have parameter(s) as described below for their counterparts `Delete`, `Book1d` and `Book2d` in the configuration language;

`CMD_GET` and `CMD_RESET` have a single histogram name parameter `hname`;

`CMD_RESETELL`, `CMD_QUIT` have no parameters;

`CMD_LEAVE` (if implemented) and `CMD_CONNECT` should be internal for client;

`Var`, `Add2var` and `Delvar` commands are currently internal for server.

Clients from the hosts specified for *r2h(1)* by `-A` option, have a permission to execute any `CMD_*` commands mentioned above (the so-called read-write access), while they from hosts specified by `-a` — only `CMD_GET` and `CMD_QUIT` (the so-called read-only access).

The configuration file in the *r2h.conf(5)* format consists of zero or more lines, delimited by the newline symbol. Lines could be the comment lines, empty lines, and configuration lines, where the newline symbol could be escaped by the backslash symbol to allow the line continuation. The lines, which in the first position contain the `<<#>>` (comment line) and newline (empty line) symbols, are ignored.

Other lines should be configuration lines. Configuration lines concatenated with all their continuations contain one or more fields, separated by space(s) or tab(s). The fields themselves should not contain space(s) or tab(s). The first field (command) of the configuration line is a C-string and represents the command name. The second (if any) and following field(s) are command parameters.

Note, that it is a client's responsibility to determine an actual `TObject`'s type. For example, that can be done by comparison of `type_info` of the obtained class (`TMessage::GetClass()->GetTypeInfo()`) with the type of each `TObject` recognized by the client (`TObject::Class()->GetTypeInfo()`).

Currently known commands are as follows:

`var` — declares the name `varname` of the variable which could be histogrammed in terms of the integer number triplet: channel `chan`, module `mod` and group of modules `group`. The event representation ROOT class used by ***r2h(1)*** should allow obtaining the variable's value by such triplet (see Sec. 3). The `var` has the following format:

`Var varname chan [mod [group]],` for example: `Var adc0 2 0 .`

`Add2var` — adds (yet another) triplet of channel `chan`, module `mod` and the group of modules `group` to the list of them belonging to the `varname` variable. So more than one detector channel could be united into the same histogram. The `Add2var` has the following format:

`Add2var varname chan [mod [group]],` for example: `Add2var adc0 3 1 .`

`Delvar` — removes the variable named `varname` and frees all the corresponding memory. Its format is as follows:

`Delvar varname,` for example: `Delvar adc0 .`

`Book1d` — declares ROOT TH1F histogram with name `hname`, id string `fullhname`, variable to be histogrammed `varnameX`, number of bins `chansX`, minimal `minX` and maximal `maxX` bins. The histogram should be filled at each event arrival. The `Book1d` has the following format:

`Book1d hname fullhname varnameX chansX minX maxX,` for example:

`Book1d adc0 ADC0 adc0 100 0 100 .`

`Book2d` — declares ROOT TH2F histogram with the name `hname`, id string `fullhname`, variables to be histogrammed `varnameX` and `varnameY`, number of bins `chansX` and `chansY`, minimal `minX`, `minY` and maximal `maxX`, `maxY` bins. The histogram should be filled at each event arrival. The `Book2d` has the following format:

`Book2d hname fullhname varnameX chansX minX maxX varnameY chansY minY maxY`

for example: `Book2d adc1_0 ADC1_0 adc1 200 0 200 adc0 300 0 300 .`

`Delete` — removes the histogram named `hname` and frees all the corresponding memory. Its format is as follows:

`Delete hname ,` for example: `Delete adc1_0 .`

The configuration lines failed to parse or be processed are ignored while file processing continues to the next line.

2.5.6. *histGUI(1): standalone client for r2h(1)* One of possible ***r2h(1)*** clients is ***histGUI(1)*** (for histograms viewer with ***GUI***), which requests histograms from the server and draws them. The protocol for the client-server conversations described in Subsec. 2.5.5 allows ***histGUI(1)*** to be independent on both ***r2h(1)*** internals and event representation ROOT class(es). So ***histGUI(1)*** depends on the standard ROOT classes only and could be compiled under any OS equipped with the ROOT package libraries.

`histGUI [-l] [-t<gui_sleep>] [<peerhost> [<peerport>]]`

The *histGUI* connects to histogram server (e.g., *r2h(I)*) on the port `<peerport>` (12341 by default) on the host `<peerhost>` through the ROOT `TSocket`, launches ROOT `TTimer` to do the required redraws, displays the own GUI window and enters the ROOT eventloop. After the user command obtaining (see Subsec. 2.5.5 for protocol description) the *histGUI* executes it or sends the corresponding request to the server side, obtains the response, and draws the histogram or reports the response error status in the output viewer area.

histGUI's GUI is designed to be self-explained. The main window contains at least «Exit» button, the command input field (`TGTextEntry`) and output viewer area (`TGTextView`). Single ROOT `TCanvas` is used to display all histograms after `Get` command, while after `Getcont` each histogram is drawn in the own `TCanvas` which disappears after `Stopall` or the corresponding `Stop`.

3. SCHEME OF EVENT REPRESENTATION BY ROOT CLASS(ES)

Let us formulate the *b2r(I)* and *r2h(I)* requirements to the interface to be provided by the ROOT class (or number of classes) intended to represent experimental events. Namely, the *b2r(I)* needs the following member functions:

- `int pack2r(packet *)` fills the class data members from the corresponding fields of the packet header and body, and should be aware of all (possibly more than one) the involved packet types;
- `void Clear()*` resets the class instance into the unfilled state same as appeared after constructor execution;
- `uint16_t Get_type()` returns the value of `type` data member equal to the type of the packet, from which the last proper filling of the class instance has been done;
- `TObject *GetTObject(uint16_t t)` returns the pointer (casted to `TObject pointer**` to be used in `TBufferFile::WriteObject()`) to the class instance, which represents the event of supplied type `t`;
- `char *GetName()` returns the C-string representation of the name of the class to be stored in ROOT `TTree` for using by `TTree::Branch()`;
- `void *GetAddr(void *addr)` returns the address of the pointer to the class instance to be stored in ROOT `TTree` for using by `TTree::Branch()`, where `addr` is the pointer to instance of the class known by *b2r(I)*;

*It is assumed that its calling is cheaper than the full class instance recreation by `delete` and `new`.

**The corresponding class should be derived from ROOT `TObject` base class to allow such cast.

- `bool need_write()` returns the true value, if the class instance is ready to be written into ROOT `TFile`, and the false value otherwise;
- (optionally) `TObject *Get_sp()` returns the pointer (casted to `TObject*` to be used in `TFile::WriteTObject()`) to the class instance to be stored in ROOT `TTree`.

The *r2h(1)* needs the following:

- `float Get_data(int chan, int mod, int group)` member function returns the value to be histogrammed, which identified by the integer number triplet: channel `chan`, module `mod` and the group of modules `group`;
- the ability to extract a class with this `Get_data()` member function from the obtained `TMessage` or `TBufferFile` class instances in the unambiguous way.

The sources of both *b2r(1)* and *r2h(1)* utilities are written to be event content independent, so each of them should know about only one class, however, these classes could be not necessarily the same.

In the simple cases, where we have the trigger data but not the data coupled with the accelerator cycle, a single class could satisfy all the above requirements, e.g. `class Ekeyaf` [2]. Even if we have many trigger types, the single class scheme is still suitable, if the trigger data contents do not differ essentially. However, for the experimental setups on the cyclic accelerators like Nuclotron (JINR, LHEP) we usually want to work with both: per event and per burst information. For this complicated case we propose the following approach.

The base class `B<setup>` inherits from ROOT `TObject` and provides at least `type` data member* and `Get_type()`, `Get_data()` member functions. Each event type representation class — e.g., `E<setup>` (trigger event types), `CB<setup>` (cycle begin event type), `CE<setup>` (cycle end event type) — is derived from `B<setup>` and provides at least the specific data members of the type and `Get_data()` member function. So `B<setup>::Get_data()` simply calls its counterparts from the event representer classes depending on the data member `B<setup>::type` value, while the *r2h(1)* simply does the so-called upcast (transforms the pointer to the obtained derived class into the pointer to `B<setup>` base class), and calls `B<setup>::Get_data()`.

To produce ROOT `TTree` with single `TBranch`, we provide `S<setup>` «container» class derived from ROOT `TObject` to be a single «leaf» object per branch. This class represents the whole accelerator cycle, thus, contains the following data members: cycle number `int cyc_num`; `TClonesArray *events` of trigger events and `int Nevs` quantity of them; and `CB<setup>`, `CE<setup>` pointers — as well as the member functions to store (`int Fill(int cyc, int Nev)`, `void AddEv(E<setup> *)`, `void AddCB(CB<setup> *)`, `void AddCE(CE<set`

*And, possibly, other data members are common for all event types, for example, represent the packet header fields `num`, `len`, `sec`, `usec`, etc.

up> *) and retrieve (int Get_cyc(), int Get_Nevs(), CB<setup> *GetCB(), CE<setup> *GetCE(), TClonesArray *Get_events()) the corresponding data members. The S<setup> also provides void Clear() member function.

After all we introduce the «metaclass» M<setup> derived from ROOT TObject, which contains uint16_t type of the event represented currently; the pointer to container S<setup> *sp; the instance of each known event representer E<setup> ev, CB<setup> cb, CE<setup> ce; and provides the full interface required by *b2r(1)*. Namely, Get_type() returns M<setup>::type value; GetTObject(t) — one of &ev, &cb, &ce depending on t supplied; GetName() returns name of S<setup>; Get_sp() and GetAddr() return sp and &sp with the required casts.

The most sophisticated job is done by pack2r() called once per each data packet arrival. The pack2r() assumes the data for each accelerator cycle are starting from the cycle begin packet (if any), contain zero or more trigger packet(s), and terminated by the cycle end packet. After each pack2r() return the event representer, corresponding to the type of the arrived packet, is ready to be sent to the *b2r(1)* registered client(s). After the cycle end packet processing by pack2r(), the S<setup> is ready to be stored into ROOT TFile and need_write() returns the true value, so *b2r(1)* writes ROOT TFile only if this condition is satisfied.

4. WORK WITH CAMAC HARDWARE

As was noted in [6], the *qdpb* framework uses the *camac* package [13] as the CAMAC subsystem implementation. The *ngdp* inherits this approach, so let us briefly explain the current design features of the *camac* package according to its manual pages. The code, which handles a specific CAMAC crate controller/computer interface card pair, is separated from the so-called CAMAC facility *camac(4)* in the OS kernel. This design allows us to add support for an arbitrary new CAMAC controller/adaptor pair very easily. The *camac(4)* supports the interface to software objects of two kinds, mentioned below as «CAMAC drivers» and «CAMAC modules». The CAMAC drivers (see *camac-drv(4)*) are kernel device drivers in the KLD module form, and work with some specific CAMAC hardware like CAMAC crate controllers. CAMAC modules (see *camacmod(9)*) are intended to handle interrupts from CAMAC hardware, and usually have a KLD module form, too (see below for details). The *camac(4)* realizes some abstraction level for CAMAC operations and therefore hides the CAMAC hardware specifics from the user and kernel contexts. Each CAMAC operation is performed at the CAMAC address, which uniquely represents the hardware correspondent of the operation. Drivers should be registered in the *camac(4)* before using. Driver registration consists of the branch number assignment to the named driver. The CAMAC driver can implement up to 4 methods: *subr()*, *setup()*, *conf()*, and *test()* (former is mandatory while others are

optional). The `subr()` function implements the CAMAC operations themselves, e.g. CCCZ — generates the dataway initialize (Z), CCCC — generates the crate clear (C), CFSA — performs a single CAMAC action, etc., and can be achieved from both contexts by the corresponding interfaces. The `setup()` function attaches the CAMAC module of the user provided interrupt handler to the CAMAC driver. The CAMAC module should be registered in the `camac(4)` before using and deregistered before unloading from the kernel. The CAMAC module can implement up to 4 methods: `hand()`, `oper()`, `conf()`, and `test()` (former is mandatory while others are optional). The `hand()` function is an interrupt handler itself and should address only one CAMAC driver, specified during the module configuration. The `oper()` function is a user interface to the module and can access CAMAC. The CAMAC module should also meet the requirements of `ng_camacsrc(4)` (see Sec. 4.1) to be able to inject the data into `ngdp` graph. Typically the CAMAC module sources are split to the number of files to isolate the hardware-dependent code parts. Namely, we define some macros — to initialize CAMAC, to recognize the trigger type, to perform read/reset CAMAC for each trigger type, etc., so `hand()` function can be written in the hardware independent manner. This macro set can be written «manually» for compact stable setups, or generated by means of configurable representation of the CAMAC hardware [14] for more extensive and/or changed from the run-to-run spectrometers.

4.1. `ng_camacsrc(4)`: `ngdp` CAMAC Interface. The `ng_camacsrc(4)` node type allows the data packets injection from a CAMAC interrupt handler into `netgraph(4)` as data messages. This means that we are able to use `ngdp` for building DAQ systems, which work with CAMAC, as well as to do some sophisticated testing of `ngdp` itself. This node supports the single hook output, which can be connected to, for example, the input hook of the `ng_fifos(4)` node (see Subsec. 2.3.1). The `ng_camacsrc(4)` sends the data packets in the interrupt handler context, where further data processing is undesirable. So the data should always be queued by `netgraph(4)` for later delivering to decouple from this context. Since by default the `netgraph(4)` delivers the data synchronously, we should set `HK_QUEUE` flag on the peer hook of the `ng_camacsrc(4)` output hook during the hooks connection.

The `ng_camacsrc(4)` provides the kernel-wide interface function* to send the data packet through the output hook, which returns 0 on success and error code otherwise. The function argument (`msh`) is the pointer to the instance of the node's private structure which belongs to the node instance, through whose output hook the interrupt handler wants to send the data. The `ng_camacsrc(4)` node declares its own version number in the `ng_camacsrc_ver.h` to allow the dependent KLD modules to declare such dependence and resolve `ng_camacsrc_send` symbol

*Prototyped as `int ng_camacsrc_send(camacsrc_p msh)`.

during the linkage into the kernel. In contrast, the *ng_camacsrc(4)* calls functions, provided by an interrupt handler, indirectly (by function pointers) to avoid cross-dependencies.

During processing of the `connect` control message (see below) the *ng_camacsrc(4)* obtains the corresponding function pointers* and calls the interrupt handler's `oper()` function with the following subfunction codes:

`NG_CAMACSRC_SETMSP` — provides `misp` address for the interrupt handler, and

`NG_CAMACSRC_GETBUF` — obtains the address of the ready packet buffer from it.

At receiving the `disconn` control message (see below) and during the shut-down sequence the *ng_camacsrc(4)* calls `oper()` with `NG_CAMACSRC_CLOSE` subfunction code to notify the interrupt handler about its own retirement.

So, the interrupt handler named `<camac_module>` should provide these three subfunction entries in its own `oper()` function realization. After the existing CAMAC interrupt handler implementations used in *qdpb* based DAQ systems it is also assumed, that the data produced in the packet form** — only to be able to get the data length from the known place in the data packet.

The described scheme allows us to use more than one instance of *ng_camacsrc(4)* nodes on the same computer, if we have more than one CAMAC driver and the corresponding CAMAC interrupt handler***.

In the *qdpb* system the control over `<camac_module>` CAMAC interrupt handler was done only by locally executed utility `<camac_module>oper(8)`, which calls `<camac_module>_oper()` with some required subfunction codes. This code set can be divided to «generic» (supported by approximately each CAMAC module) and «specific» (all others) parts. At least the following subfunction codes can be considered as «generic»: `INIT`, `FINISH`, `START`, `STOP`, `CNTCL`, `QUECL`. To allow cheaper and more flexible (in particular, remote) control over the CAMAC interrupt handler, the *ng_camacsrc(4)* understands a number of control messages (see below), whose arrival leads to performing each «generic» subfunction and even more. Note the same subfunctions can be easily implemented by the control packet mechanism, too.

The *ng_camacsrc(4)* node supports the following specific control messages:

`getclrstats` — returns the current statistics (numbers of `packets_out`, `bytes_out`, and `fails`) and clears it;

*These pointers are stored in the specific data structures of the CAMAC driver and the corresponding CAMAC module and can be found by known CAMAC driver name using the *camac(4)* interface.

**It will be very easy to move the packet encapsulation by `make_pack()` function (see *packet(9)*) into the generic *ng_camacsrc(4)* code.

***Possibly we can generalize this model to use more than one *ng_camacsrc(4)* instance with the same interrupt handler to separate the packet streams on the early stage or to enlarge the overall throughput.

`getstats/clrstats` — returns/clears the current statistics (the same values);
`connect <char *camac_driver_name>` — establishes a link with the CAMAC interrupt handler hosted on the CAMAC driver with name `<camac_driver_name>`;
`disconn` — breaks the link established by the `connect` control message;
`init, finish, start, stop, cntcl, quecl` — performs `<camac_module>_oper()` call with the corresponding subfunction codes, which lead to: CAMAC hardware initialization (`INIT`), CAMAC hardware preparation to power off (`FINISH`), data acquisition start (`START`) and stop (`STOP`), clean of the interrupt handler internal counters (`CNTCL`) and event buffers (`QUECL`);
`getmodstat/getmodconf` — returns some generic part of the internal statistic/configuration structure of the interrupt handler (`GETPSTAT/GETPCONF`).

5. CONCLUSIONS

The *ngdp* framework allows us to build full-sized modular distributed DAQ systems in a very efficient way with the minimal design and maintenance efforts due to the already implemented interface to CAMAC as well as binary-to-ROOT and ROOT-to-histogram conversion utilities. The proposed representation scheme of the experimental events for the ROOT package allows handling of many trigger types and data coupled with the accelerator cycle, and hides this complexity from the mentioned converters.

Acknowledgements. The author has a pleasure to thank K. I. Gritsaj for useful discussions and many years of *camac* package maintenance to fit into current OS FreeBSD releases, L. S. Zolin and V. E. Kovtun, who had need for DAQ systems and permit to implement them using *ngdp*, S. G. Reznikov — for cooperation during DAQ SPILL design and testing.

APPENDIX A

A.1. *qdpb* Inspired Entities and Imported Elements. As we have already written in [1], some *ngdp* ideas are inspired by *qdpb* design and some *qdpb* entities are imported and redesigned for *ngdp*, as described below.

- The packet implementation changes after *qdpb*:
 - the maximal packet size is enlarged up to 2048000 bytes;
 - the control and answer packets are introduced by separate `typedefs` because they should fit into single Ethernet frame to guarantee the nonfragmented delivery;
 - some functions (`defrag_pack()`, `merge_pack()` for kernel context, `recv_pack()` for user context) and macros (`CHECK_ID()`, `CHECK_CRC()`),

`CHECK_PACK()` in two versions for both contexts, `CHECK_NUM()` for kernel context) are added to *packet(3)*, while some existing entities are refined;

— *packet(3)* functions, originally implemented for the 32-bit `i386` (also known as `IA-32`)* and `HPPA` architectures, are ported to `AMD64/EM64T` architecture.

• The packet types support changes after *qdpb*:

— the packet type map as array of `type_attr` structures is introduced, that allows:

— the `NEVTYPES` constant (number of packet types known in the system) to be eliminated, because we always can count a number of entries in the packet type map;

— the all values of the packet type attributes (currently — the packet type itself (`u_short` value), the packet type name (C-string), the offset in arrays (for backward compatibility), the packet number counter (`u_long` value), and the permissions to split the datafile before, after or instead of this packet type writing) to be stored in the single place at the map initialization instead of being spread over the conversion functions of the packet type attributes; and

— this conversion functions for both contexts to be redesigned on the base of the linear search in the map as implemented currently (see *libsrc/pack_types.c*), or using fetch from the prefilled hash table of `type_attr` structures (see *test/thash.c* and Sec. A.3).

A.2. Packet Generator Nodes *ng_mysource(4)* and *ng_kthsource(4)*. The *ng_mysource(4)* node type is designed very close to *ng_source(4)* from the standard *netgraph(4)* distribution, however it produces *qdpb/ngdp* packets and is not coupled with the network interface. The node generates packets by the handler executed by *callout(9)* mechanism (timer kernel thread activated at each system clock interrupt), and accounts a size of the generated data in the both packet (`packets_out`) and byte (`bytes_out`) units, an elapsed astronomic time (`elapsed`) between the moments of the generation start and stop, a pure time (`pure`) of the data generation and emission, and a number of the occurred transfer failures (`fails`).

The *ng_mysource(4)* node supports only one hook named `output` simultaneously, however by default persists after such hook disconnection, so it can be reused by connecting `output` again, and should be unloaded explicitly by shutdown generic control message. The *ng_mysource(4)* can generate packets of only one type simultaneously, because it supports only one value for `type` and for `patt`. To overcome this limitation, the single hook named `input` is supported, and the data which arrived through it, are sent untouched through the `output`

*Note, that to the `i386` architecture the CPU types belong from `i386` itself through `i486` and `i586` up to `i686`, which includes Intel Pentium 4 and AMD K7.

hook (if any). This design allows us to link a number of *ng_mysource(4)* nodes with different configurations into a generation chain, which is able to imitate the multityped data produced by some real source (e.g., the CAMAC interrupt handler).

The *ng_mysource(4)* understands the generic set of control messages and the following specific control messages as well:

- start <int64_t num_of_packets> — starts the data generation;
- stop — stops the data generation explicitly before the <num_of_packets> generated;
- getclrstats — returns the current statistics (values of packets_out, bytes_out, elapsed, pure, and fails) and clears it;
- getstats/cclrstats — returns/clears the current statistics (the same values);
- setconf { packlen=<size> npack=<n> ticks=<m> pflag=<f> } — sets in according to the values of submitted struct *ng_mysource_conf* members:
 - length packlen of packets will be generated — to <size>,
 - number npack of packets will be produced per one generator function call — to <n>,
 - time interval ticks between two subsequent generator calls — to <m> ticks*,
 - packet header flags** pflag will be used for packets production — to <f>;
- getconf — returns the current setconf settings;
- settype <uint16_t type> — sets the generated packets type to <type>;
- setpatt <uint64_t patt> — sets the filling pattern <patt> for the packet bodies;
- fragile <uint8_t flag> — (re)sets the boolean <flag>, which requires to disconnect the input hook during the output one disconnection and to shutdown node without hooks, if true. This allows the easy shutdown of the whole generation chain of *ng_mysource(4)*s. However for freshly *mkpeered* node this <flag> by default is 0.

{get,clr,getclr}stats control messages can be submitted and will be processed during the data generation.

The *ng_kthsource(4)* node type preserves the described above functionality of the *ng_mysource(4)* node type in general, however, it uses the generic kernel thread *kthread(9)* mechanism instead of *callout(9)*. This thread is very much similar to a process in many aspects, however, it is not preempted by the scheduling

*Tick is the time interval between two subsequent system clock interrupts, usually 1/1000 s.

**After *qdpb* packet design the header flag field controls the valid timestamp and CRC presence in the header. Possible flag values are #defined in *ng_packet.h*. Note, that if pflag equal to zero is supplied, the header flags are set to default (F_TIME|F_CRC), while for -1 — to zero, that means to produce neither timestamp nor CRC. All other values are bitwise ANDed with F_MASK.

mechanism, so it generates packets as fast as possible. If the packets transfer failure occurs, our thread voluntarily participates in the scheduling: it *msleep(9)*s during `<delay>` timeout* (by default 0.1 s), and after that it continues the packets generation and transfer.

The *ng_kthsource(4)* supports the same hooks as the *ng_mysource(4)* and understands the same control messages set. The only exception is `setconf`, which submits `struct ng_kthsource_conf`, where instead of `ticks` a `delay` member is present. It means the time interval (in ticks) for *msleep(9)*ing after the packet transfer failure.

A.3. User Context Samples. To test and debug some aspects of *ngdp* nodes in the user context, we implement a number of program samples collected in the *test* directory:

tbuf_nNGO.c (queue disciplines for *ng_fifo(4)* buffer implementation),
thash.c (implementation of hash table of `struct type_attr` and `entrybyevtype()` function),
tthr_em.c (*ng_em(4)* model with control packets emission based on threads),
tems.c («selfflow» *ng_ems(4)* model without thread),
tthr_p.c (*ng_pool(4)* model with control packets emission based on threads),
tbp.c («selfflow» *ng_bp(4)* model without thread),
twrap.c (parser of some syntax suitable for configuration file),

as well as some user context program skeleton(s):

tthr.c (program with *pthread(3)*),
tmm.c (example of *ng_mm(4)* using),
tmmmap.c (parent/child data exchange through the mapped/shared memory with semaphore synchronization), etc.

REFERENCES

1. *Isupov A. Yu.* The *ngdp* Framework for Data Acquisition Systems. JINR Commun. E10-2010-34. Dubna, 2010. 20 p.
2. *Isupov A. Yu., Kovtun V. E., Foshchan A. G.* Implementation Trial of the DAQ System for the Compact Physics Setup on Base of the *ngdp* Framework (in Russian) // Book of Abstr. of 59 International Meeting on Nuclear Spectroscopy and Nuclear Structure (NUCLEUS-2009) «Fundamental Problems and Applications of Nuclear Physics: From Space to Nanotechnologies» Cheboksary, Russia, June 15–19, 2009. Saint-Petersburg, 2009. P. 346.
3. *Isupov A. Yu., Kovtun V. E., Foshchan A. G.* The Data Acquisition System for Multi-channel Spectrometer on Base of the *ngdp* Framework // Abstr. of Intern. Symposium on Exotic Nuclei (EXON-2009), Sochi, Russia, Sept. 28 – Oct. 2, 2009.

*Unfortunately, we have no means to *wakeup(9)* it in time, however a timeout value variation dependent on failures rate or etc., can be implemented in principle.

4. *Quercia V., O'Reilly T.* Volume Three: X Window System User's Guide. O'Reilly & Associates, 1990.
5. *Cutler E., Gilly D., O'Reilly T.* The X Window System in a Nutshell. 2nd ed. O'Reilly & Associates, 1992.
6. *Gritsaj K. I., Isupov A. Yu.* A Trial of Distributed Portable Data Acquisition and Processing System Implementation: the *qdpb* — Data Processing with Branchpoints. JINR Commun. E10-2001-116. Dubna, 2001. 19 p.
7. *Isupov A. Yu.* Software Utilities for Using on an Experimental Stand // Proc. of the Intern. Workshop «Relativistic Nuclear Physics: From Hundreds of MeV to TeV (RNP'2005)», Dubna, Russia, 2005. Dubna, 2006. P. 252–259.
8. *Isupov A. Yu.* SPHERE DAQ and Off-Line Systems: Implementation Based on the *qdpb* System // Proc. of the Intern. Workshop «Relativistic Nuclear Physics: From Hundreds of MeV to TeV (RNP'2003)», Stara Lesna, Slovakia, 2003. Dubna, 2003. P. 214–228.
9. *Isupov A. Yu.* DAQ System for High Energy Polarimeter at the LHE, JINR: Implementation Based on the *qdpb* (Data Processing with Branchpoints) System. JINR Commun. E10-2001-198. Dubna, 2001. 15 p.
10. *Anisimov Yu. S. et al.* Polarimeter for Nuclotron Internal Beam // Particles and Nuclei, Letters. 2004. V. 1. No. 1[118]. P. 68–79 (in Russian).
11. *Isupov A. Yu.* Data Acquisition Systems for the High Energy and Nuclotron Internal Target Polarimeters with Network Access to Polarization Calculation Results and Raw Data // Czech. J. Phys. Suppl. A. 2005. V. 55. P. A407–A414.
12. *Brun R., Rademakers F.* ROOT — An Object Oriented Data Analysis Framework // Proc. of the AIHENP'96 Workshop, Lausanne, Switzerland, 1996 // Nucl. Instrum. Meth. A. 1997. V. 389. P. 81–86.
13. *Gritsaj K. I., Olshevsky V. G.* Software Package for Work with CAMAC in Operating System FreeBSD. JINR Commun. P10-98-163. Dubna, 1998. 16 p. (in Russian).
14. *Isupov A. Yu.* Configurable Data and CAMAC Hardware Representations for Implementation of the SPHERE DAQ and Offline Systems. JINR Commun. E10-2001-199. Dubna, 2001. 16 p.

Received on March 16, 2010.

Корректор *Т. Е. Попеко*

Подписано в печать 18.05.2010.

Формат 60 × 90/16. Бумага офсетная. Печать офсетная.

Усл. печ. л. 1,68. Уч.-изд. л. 2,29. Тираж 290 экз. Заказ № 56993.

Издательский отдел Объединенного института ядерных исследований
141980, г. Дубна, Московская обл., ул. Жолио-Кюри, 6.

E-mail: publish@jinr.ru

www.jinr.ru/publish/