Safe and Unsafe Interfaces 5

This chapter defines MT-safety levels for functions and libraries.

Thread Safety	*page 103*
MT Interface Safety Levels	*page 105*
Async-Safe Functions	*page 107*
MT Safety Levels for Libraries	*page 107*

Thread Safety

Thread safety is the avoidance of *data races*—situations in which data are set to either correct or incorrect values depending upon the order in which multiple threads access and modify the data.

When no sharing is intended, give each thread a private copy of the data. When sharing is important, provide explicit synchronization to make certain that the program behaves deterministically.

A procedure is *thread safe* when it is logically correct when executed simultaneously by several threads. At a practical level, it is convenient to recognize three levels of safety.

- Unsafe
- Thread safe—Serializable
- Thread safe—MT-safe

An unsafe procedure can be made serializable by surrounding it with statements locking and unlocking a mutex. Code Example 5-1 shows first a nonthread-safe implementation of a simplified `fputs`().

Next is a serializable version of this routine with a single mutex protecting the procedure from concurrent execution problems. Actually, this is stronger synchronization than is necessary in this case. When two threads are calling `fputs`() to print to different files, one need not wait for the other—both can safely print at the same time.

The last version of the routine is *MT-safe*. It uses one lock for each file, allowing two threads to print to different files at the same time. So, a routine is *MT-safe* when it is thread safe and its execution does not negatively affect performance.

Code Example 5-1 Degrees of Thread Safety

```
/* not thread-safe */
fputs(const char *s, FILE *stream) {
    char *p;
    for (p=s; *p; p++)
        putc((int)*p, stream);
    }

/* serializable */
fputs(const char *s, FILE *stream) {
    static mutex_t mut;
    char *p;
    mutex_lock(&m);
    for (p=s; *p; p++)
        putc((int)*p, stream);

    mutex_unlock(&m);
}

/* MT-Safe */
mutex_t m[NFILE];
fputs(const char *s, FILE *stream) {
    static mutex_t mut;
    char *p;
    mutex_lock(&m[fileno(stream)]);
    for (p=s; *p; p++)
        putc((int)*p, stream);
    mutex_unlock(&m[fileno(stream)]0;
}
```

MT Interface Safety Levels

The *man Pages(3): Library Routines* use the following categories to describe how well an interface supports threads (these categories are explained more fully in the `Intro`(3) man page).

Safe	This code can be called from a multithreaded application.
Safe with exceptions	See the NOTES sections of the man pages for a description of the exceptions.
Unsafe	This interface is not safe to use with multithreaded applications unless the application arranges for only one thread at a time to execute within the library.
MT-Safe	This interface is fully prepared for multithreaded access in that it is both *safe* and it supports some concurrency.
MT-Safe with exceptions	See the NOTES sections in the *man Pages(3): Library Routines* for descriptions of the exceptions.
Async-Safe	This routine can safely be called from a signal handler. A thread that is executing an Async-Safe routine does not deadlock with itself when interrupted by a signal.

See the table in Appendix B, "MT Safety Levels: Library Interfaces," for a list of *safe* interfaces from the *man Pages(3): Library Routines*. If an interface from Section 3 is not in this table, it is probably unsafe (this does not include the Source Compatibility Library). Check the man page to be sure.

All functions described in the *man Pages(2): System Calls* are MT-Safe except for `vfork`(2).

Some functions have purposely not been made safe for the following reasons:

- Making the function MT-Safe would negatively affect the performance of single-threaded applications.
- The function has an Unsafe interface. For example, a function might return a pointer to a buffer in the stack. You can use reentrant counterparts for some of these functions. The reentrant function name is the original function name with "`_r`" appended.

Caution – There is no way to be certain that a function whose name does not end in "_r" is MT-Safe other than by checking its reference manual page. Use of a function identified as not MT-Safe must be protected by a synchronizing device or restricted to the initial thread.

Reentrant Functions for Unsafe Interfaces

For most functions with Unsafe interfaces, an MT-Safe version of the routine exists. The name of the new MT-Safe routine is always the name of the old Unsafe routine with "_r" appended. The following "_r" routines are supplied in the Solaris system:

Table 5-1 Reentrant Functions

asctime_r(3C)	ctermid_r(3S)	ctime_r(3C)
fgetgrent_r(3C)	fgetpwent_r(3C)	fgetspent_r(3C)
gamma_r(3M)	getgrgid_r(3C)	getgrnam_r(3C)
getlogin_r(3C)	getpwnam_r(3C)	getpwuid_r(3C)
getgrent_r(3C)	gethostbyaddr_r(3N)	gethostbyname_r(3N)
gethostent_r(3N)	getnetbyaddr_r(3N)	getnetbyname_r(3N)
getnetent_r(3N)	getprotobyname_r(3N)	getprotobynumber_r(3N)
getprotoent_r(3N)	getpwent_r(3C)	getrpcbyname_r(3N)
getrpcbynumber_r(3N)	getrpcent_r(3N)	getservbyname_r(3N)
getservbyport_r(3N)	getservent_r(3N)	getspent_r(3C)
getspnam_r(3C)	gmtime_r(3C)	lgamma_r(3M)
localtime_(3C)r	nis_sperror_r(3N)	rand_r(3C)
readdir_r(3C)	strtok_r(3C)	tmpnam_r(3C)
ttyname_r(3C)		

Async-Safe Functions

Functions that can safely be called from signal handlers are *Async-Safe*. The POSIX standard defines and lists Async-Safe functions (IEEE Std 1003.1-1990, 3.3.1.3 (3)(f), page 55). In addition to the POSIX Async-Safe functions, the following three functions from the threads library are also async safe.

- `sema_post`(3T)
- `thr_sigsetmask`(3T)
- `thr_kill`(3T)

MT Safety Levels for Libraries

All routines that can potentially be called by a thread from a multithreaded program should be MT-Safe.

This means that two or more activations of a routine must be able to *correctly* execute concurrently. So, every library interface that a multithreaded program uses must be MT-Safe.

Not all libraries are now MT-Safe. The commonly used libraries that are MT-Safe are listed in Table 5-2. Additional libraries will eventually be modified to be MT-Safe.

Table 5-2 Some MT-Safe Libraries

Library	Comments
`lib/libc`	`get*` interfaces that are not safe have threadsafe interfaces of the form `get*_r`
`lib/libdl_stubs`	(To support static switch compiling)
`lib/libintl`	
`lib/libm`	MT-Safe only when compiled for the shared library, but not MT-Safe when linked with the archived library
`lib/libmalloc`	
`lib/libmapmalloc`	
`lib/libnsl`	Including the TLI interface, XDR, RPC clients and servers, `netdir`, and `netselect`. `get`*XX*`by`*YY* interfaces are not safe, but have threadsafe interfaces of the form `getXXbyYY_r`

Table 5-2 Some MT-Safe Libraries

Library	Comments
`lib/libresolv`	(Thread-specific errno support)
`lib/libsocket`	
`lib/libw`	
`lib/nametoaddr`	
`libX11`	
`libC`	.

Unsafe Libraries

Routines in libraries that are not guaranteed to be MT-Safe can safely be called by multithreaded programs only when such calls are single-threaded.