SecureSMX®

User's Guide

Version 5.2

February 2024

by Ralph Moore

and

David Moore

Micro Digital

Micro Digital Associates, Inc.
(714) 437-7333
support@smxrtos.com
www.smxrtos.com

Table of Contents

PREFACE 1

CHAPTER 1 INTRODUCTION 3

1.1 How to Use This Manual 3
1.2 Partitioning 3
1.3 Advantages of Isolated Partitions 5
1.4 Hardware 5
1.5 Methodology 6
1.6 Security 6
1.6.1 The Increasing Need for Security 6
1.6.2 Protection Goals 6
1.6.3 What You Need 7
1.7 SecureSMX Snapshot 7
1.8 SecureSMX Licensing 8

CHAPTER 2 BACKGROUND 9

2.1 MMUs vs. MPUs 9
2.2 Cortex Micro Controller Units (MCUs) 10
2.2.1 Cortex-M 10
2.2.2 Cortex-v7M 11
2.2.3 Cortex-v8M 12

CHAPTER 3 GETTING STARTED 13

3.1 Legacy Code 13
3.2 New Code 14
3.3 References 14

CHAPTER 4 BASIC THEORY 17

4.1 Partitions and Tasks 17
4.1.1 What are Partitions? 17
4.1.2 Secure Boot 19
4.1.3 RTOS & System Services 19
4.1.4 The Vault 20
4.1.5 Mission Critical 20
4.1.6 utasks 20
4.1.7 ptasks 20
4.1.8 Parent and Child Tasks 20
4.2 MPU Control 22
4.2.1 Memory Protection Arrays and Tasks 22
4.2.2 MPU / MPA Relationship 23
4.2.3 Active Slots 24

4.2.4 Static Slots ... *25*
4.2.5 Auxiliary Slots ... *26*
4.2.6 MPU Slot Numbers & Region Overlaps ... *27*
4.2.7 Task Stack Slot ... *27*

4.3 MPA Templates ... 27

4.3.1 Creating and Loading MPAs ... *27*
4.3.2 Using Parent and Child Tasks ... *29*
4.3.3 Using v7M MPU Subregions ... *30*
4.3.4 Creating v7M MPA Templates ... *32*
4.3.5 Creating v8M MPA Templates ... *33*
4.3.6 Fast MPU Load ... *34*
4.3.7 Template Errors ... *34*
4.3.8 Standard Regions ... *35*

4.4 Linker Command File ... 35

4.4.1 First Sections ... *36*
4.4.2 Region Block Definitions ... *37*
4.4.3 Block Ordering ... *38*

4.5 Defining Sections ... 38

4.5.1 Command Line Switches ... *39*
4.5.2 Section Pragmas ... *39*
4.5.3 Template Macros ... *40*
4.5.4 String Literals ... *40*

4.6 Map Files ... 42

4.6.1 v7M ... *42*
4.6.2 v8M ... *44*
4.6.3 MpuMapper ... *45*

4.7 Regions ... 46

4.7.1 Insufficient MPU Slots ... *46*
4.7.2 Combined Regions ... *46*
4.7.3 Common Regions ... *48*
4.7.4 I/O Regions ... *48*
4.7.5 I/O Regions Using Subregions ... *49*

4.8 Interrupts and Exceptions ... 49

4.8.1 Priorities ... *49*
4.8.2 Enabling ISRs and Exception Handlers to Run ... *49*
4.8.3 Interrupts ... *50*
4.8.4 Writing ISRs ... *51*
4.8.5 Exceptions ... *52*

4.9 SVC API ... 53

4.9.1 SVC Calls ... *53*
4.9.2 SVC Call Mechanism ... *55*
4.9.3 Restricted Services ... *56*
4.9.4 Custom SSTs ... *57*
4.9.5 Partially Restricted Services ... *59*
4.9.6 Mixed Code Modules ... *59*

4.10 Processor Control ... 61

4.10.1 smx Task Switching ... *61*
4.10.2 From pmode to umode ... *61*

4.10.3 Memory Protection Arrays, MPAs ... *63*
4.10.4 What Good are ptasks? ... *64*
4.10.5 Hacking a ptask ... *65*

4.11 Dynamic Features ... 66

4.11.1 eheap and smx_Heap ... *66*
4.11.2 The Need for Multiple Heaps ... *67*
4.11.3 Allocating Heap Space ... *67*
4.11.4 Creating a Heap ... *68*
4.11.5 Heap Manager ... *69*
4.11.6 Task Stacks ... *70*
4.11.7 PSPLIM and MSPLIM ... *71*
4.11.8 Task Local Storage ... *72*
4.11.9 Dynamic Regions ... *72*
4.11.10 Protected Data Blocks ... *73*
4.11.11 Protected Messages ... *74*

4.12 Miscellaneous ... 75

4.12.1 Standard C Library Functions ... *75*
4.12.2 Partition Isolation ... *77*
4.12.3 HAL Code ... *77*

CHAPTER 5 PARTITION PORTALS ... 79

5.1 Introduction ... 79

5.1.1 Isolated Partitions ... *79*
5.1.2 Function Call APIs ... *79*
5.1.3 Partition Portals ... *80*

5.2 Protected Messages ... 80

5.2.1 pmsg Structure ... *80*
5.2.2 Sending pmsgs ... *81*
5.2.3 Receiving a pmsg ... *83*
5.2.4 Dual Slots for v8M ... *83*

5.3 Free Message Portal ... 84

5.3.1 Configurations ... *84*
5.3.2 Portal Creation ... *86*
5.3.3 Client Open ... *87*
5.3.4 Client Operation ... *88*
5.3.5 Server Operation ... *88*
5.3.6 Client Close ... *90*
5.3.7 Portal Deletion ... *91*
5.3.8 More Flexible Operation ... *91*

5.4 Tunnel Portal ... 92

5.4.1 Get pmsg (by client) ... *94*
5.4.2 Create Portal (by server) ... *95*
5.4.3 Open Portal (by client) ... *96*
5.4.4 Open Portal (by server) ... *96*
5.4.5 Send and Receive Data (by client and server) ... *97*
5.4.6 Close Portal (by client) ... *99*
5.4.7 Close Portal (by server) ... *99*
5.4.8 Delete Portal (by server) ... *99*

5.5 Shell Functions 100
5.5.1 Mapping Functions to Shell Functions 100
5.5.2 Creating a pmsg 101
5.5.3 Portal Server Operation 103
5.6 Sending Free Messages to Tunnel Portals 104
5.7 Other Portal Topics 107
5.7.1 Portal Access Delays 107
5.7.2 Portal Errors 107
5.7.3 Chained Portals 108
5.7.4 Server Callbacks 108
5.7.5 Who's The Boss? 108
5.7.6 Client Data 108
5.7.7 Window Portal 109
5.8 Console Portal 109
5.9 Middleware Portals 110
5.9.1 smxFS 111
5.9.2 smxNS 113
5.9.3 smxUSBD 114
5.9.4 smxUSBH 115
5.10 Portal Tips 117

CHAPTER 6 ADVANCED THEORY 119

6.1 System Services 119
6.1.1 System Calls from pmode 120
6.1.2 System Calls from umode 121
6.2 Critical Sections 123
6.2.1 SecureSMX Object Priorities 123
6.2.2 Interrupt Disabling and Masking in Tasks 125
6.2.3 Other Methods to Protect Critical Sections 126
6.3 Cache Control 126
6.4 Porting SecureSMX 126
6.4.1 To Another Toolchain 126
6.4.2 To Another RTOS 127
6.4.3 To Another Processor 127
6.5 Runtime Limiting 127
6.5.1 Guidelines 127
6.5.2 Approach 129
6.5.3 Enabling Runtime Limiting 130
6.5.4 Adaptive Time slicing 131
6.6 Tokens 131
6.6.1 General 131
6.6.2 Blocking Excessive Creates 132
6.6.3 Handle Verification 133
6.7 Safe LSRs 133
6.7.1 The ISR Problem 133
6.7.2 LSR Types and Operation 133

6.7.3 Performance 135
6.7.4 Resulting Security 135

CHAPTER 7 PARTITION DEMOS 137

7.1 Getting Started 137
7.2 Creating an Isolated Umode Partition Demo 137
7.2.0 pd0 138
7.2.1 pd1 139
7.2.2 pd2 141
7.2.3 pd3 145
7.2.4 pd4 147
7.2.5 pd5 151
7.2.6 pd6 151

CHAPTER 8 IMPLEMENTATION 153

8.1 Planning 153
8.1.1 Security Plan 153
8.1.2 Reliability Plan 154
8.1.3 When to Add MPU Support 154
8.2 Project Approach 155
8.2.1 Legacy Code 155
8.2.2 New Code 157
8.2.3 Iterative Process 157
8.2.4 Keeping a Log and Backups 158
8.3 Working Base 158
8.3.1 Getting Started 158
8.4 Partitions 158
8.4.1 Creating Partitions 158
8.4.2 Partition Overlap 159
8.4.3 Using Region Tails 159
8.4.4 Partition Updating 160
8.5 Templates & Regions 160
8.5.1 Creating Templates 160
8.5.2 Code and Data Regions 161
8.5.3 I/O Regions 161
8.5.4 Too Many I/O Regions 161
8.5.5 MPU Region Details 163
8.5.6 ucom_code Region 164
8.5.7 Using TLS to Reduce Regions 164
8.6 Using the Linker 165
8.6.1 Block in Block 165
8.6.2 Initialized Variables 166
8.7 Tasks 166
8.7.1 Creating ptasks 166
8.7.2 Converting from ptask to utask 166
8.7.3 Dealing with Restricted and New Services 167

8.7.4 Dealing with Shared Code and Data........167
8.7.5 Permanent ptasks........168
8.7.6 Using Child Tasks to Reduce Regions........168

8.8 Creating SVC Calls........170

8.9 Portals........170

8.9.1 Creating a Free Message Portal........170
8.9.2 Creating a Tunnel Portal........174
8.9.3 Tunnel Portal Client Shells and Server Cases for Most Calls........178
8.9.4 Tunnel Portal Data Block Transfers in Item Units........180
8.9.5 Data Block Transfer Considerations........181
8.9.6 Portal Configuration Settings........182

8.10 Miscellaneous........182

8.10.1 Heap Calls........182
8.10.2 Performance Measurements........183
8.10.3 Where Am I?........183
8.10.4 Event Buffer........183
8.10.5 Reset Vector........183
8.10.6 ISRs and LSRs........183
8.10.7 Critical Sections........184

8.11 Reducing Memory Waste for v7M........185

8.11.1 Using MpuPacker........185
8.11.2 Reducing Block Tails........186
8.11.3 Reducing Region Block Gaps........186
8.11.4 Using Plug Blocks........187
8.11.5 Reducing Region Block Sizes........188
8.11.6 Restructuring Regions........188
8.11.7 Handling Aligned Blocks within Aligned Blocks........188
8.11.8 Reducing code and data sizes........189
8.11.9 Conclusion........190

8.12 Prerelease Checklist........190

8.13 Design Tips........191

8.14 Measurements........192

8.14.1 Size........192
8.14.2 General Performance........192
8.14.3 Thumb Drive Performance........193
8.14.4 SD Card Performance........194
8.14.5 v7M Memory Waste........194

8.15 EWARM Tool Issues........195

CHAPTER 9 DEBUGGING........197

9.1 Using Configuration Constants........197

9.1.1 SMX_CFG_MPU........197
9.1.2 SMX_CFG_MPU_ENABLE........197
9.1.3 MP_MPA_DEV........197
9.1.4 SMX_CFG_PORTAL........197
9.1.5 SMX_CFG_RTLIM........198
9.1.6 SMX_CFG_SSCTR........198
9.1.7 SMX_CFG_TOKENS........198

9.2 Debugging Techniques 198

9.2.1 Keep a Debug Log 198

9.2.2 Buy a Tracing Tool 198

9.2.3 Finding MMFs 198

9.2.4 MMF Storms 199

9.2.5 Using Debugger Windows 199

9.2.6 The Handle Problem 200

9.2.7 Fixing an Easy MMF 200

9.2.8 Region Overlaps 201

9.2.9 Reversing Course 201

9.2.10 Portal Debugging 201

9.3 Using smxAware Security Features 202

9.3.1 MPU Display 202

9.3.2 MPA Displays 203

9.3.3 Tasks Display 204

9.3.4 Memory Map Window 204

9.3.5 Portal Events 204

9.4 Multitasking Issues 205

9.5 Pay Attention to Errors 205

9.6 Debug Tips 206

9.7 C-SPY Tool Issues 208

APPENDIX A.1 SECURESMX SERVICES 209

mp_FPortalClose 209

mp_FPortalCreate 210

mp_FPortalDelete 211

mp_FPortalOpen 211

mp_FPortalReceive 212

mp_FPortalSend 212

mp_FTPortalSend 213

mp_MPACreate 214

mp_MPACreateLSR 215

mp_MPASlotMove 216

mp_MPUSlotLoad 216

mp_MPUSlotSwap 217

mp_TPortalCall 218

mp_TPortalClose 219

mp_TPortalCreate 220

mp_TPortalDelete 220

mp_TportalOpen 221

mp_TPortalReceive 222

mp_TPortalSend 223

mp_TPortalServer 224

mp_RegionGetHeapR 226
mp_RegionGetHeapT 227
mp_RegionGetPoolR 227
mp_RegionGetPoolT 228
mp_RegionMakeR 229
mp_RegionMakeT 230

APPENDIX A.2 SMX PROTECTED BLOCK & MESSAGE SERVICES 231

smx_PBlockGetHeap 231
smx_PBlockGetPool 232
smx_PBlockMake 233
smx_PBlockRelHeap 234
smx_PBlockRelPool 234
smx_PMsgGetHeap 235
smx_PMsgGetPool 236
smx_PMsgMake 237
smx_PMsgReceive 238
smx_PMsgReceiveStop 239
smx_PMsgRel 240
smx_PMsgReply 241
smx_PMsgSend 242
smx_PMsgSendB 243

APPENDIX B: LINKER COMMAND FILES 245

v7M 245
v8M 248

APPENDIX C: GLOSSARY 253

APPENDIX D: SMX API LIMITATIONS 255

Table of Figures

FIGURE 1.1 NON-PARTITIONED SOFTWARE....4
FIGURE 1.2 PARTITIONED SOFTWARE....4
FIGURE 2.1 MPU OPERATION....11
FIGURE 4.1 PARTITIONS....17
FIGURE 4.2 SECURE BOOT AND STARTUP....19
FIGURE 4.3 PARENT AND CHILD TASKS....21
FIGURE 4.4 MPA TEMPLATES, MEMORY PROTECTION ARRAYS, AND TASKS....22
FIGURE 4.5 MPU / MPA ALIGNMENT....24
FIGURE 4.6 USING EXPANSION SLOTS....26
FIGURE 4.7 TEMPLATE LOADED INTO MPAS....28
FIGURE 4.8 USING V7M SUBREGION OVERLAYS....31
FIGURE 4.9 REGION WITH SUBREGION 5-7 DISABLES....37
FIGURE 4.10 MINIMAL INTERRUPT PROCESSING....50
FIGURE 4.11 TASK INTERRUPT PROCESSING....51
FIGURE 4.12 SYSTEM CALLS....55
FIGURE 4.13 MPA FOR PTASK....63
FIGURE 4.14 MPA FOR UTASK....64
FIGURE 4.15 DEDICATED HEAP FROM MAIN HEAP....68
FIGURE 5.1 DESIRED ISOLATION BETWEEN PARTITIONS....79
FIGURE 5.2 LOSS OF PARTITION ISOLATION....79
FIGURE 5.3 PARTITION ISOLATION USING FS PORTAL P....80
FIGURE 5.4 PROTECTED MESSAGE STRUCTURE....81
FIGURE 5.5 PMSG TRANSFER....82
FIGURE 5.6 FREE MESSAGE PROTOCOL CONFIGURATIONS....85
FIGURE 5.7 TUNNEL PORTAL....93
FIGURE 5.8 TUNNEL PORTAL OPERATION....94
FIGURE 5.9 MULTIBLOCK SEND....98
FIGURE 5.10 SHELL FUNCTIONS....100
FIGURE 5.11 PMSG FORMAT....101
FIGURE 5.12 SMXFS PORTAL....111
FIGURE 5.13 SMXFS AND SMXUSBH MASS STORAGE CHAINED PORTALS....112
FIGURE 5.14 SMXUSBD MASS STORAGE PORTAL....113
FIGURE 5.15 SMXNS TRANSPORT LAYER (HI/LO) PORTAL....113
FIGURE 5.16 SMXUSBD MOUSE PORTAL....114
FIGURE 5.17 SMXUSBD SERIAL PORTAL....115
FIGURE 5.18 SMXUSBH FTDI232 SERIAL PORTAL....116
FIGURE 6.1 SYSTEM CALL FROM PTASK....120
FIGURE 6.2 SYSTEM CALL FROM UMODE....121
FIGURE 6.3 SYSTEM HIERARCHY....123
FIGURE 6.4 RUNTIME LIMITING....129
FIGURE 6.5 TOKENS....131
FIGURE 8.1 CONVERTING PTASKS TO UTASKS....156