

# Contents

---

<b>Previously Published Parts of this Work</b>	<b>8</b>
<b>Introduction</b>	<b>14</b>
<b>I Background and Methods</b>	<b>17</b>
1 Structure and Methods for this Work	19
2 Preliminaries in Metrology	23
3 Synchronization Protocols and their Goals	29
4 Preliminaries in Information Security	38
5 Mathematical Model	42
6 Method for Formal Analysis and Verification	46
<b>II-A Security Measures for Two-Way Synchronization</b>	<b>51</b>
7 Preliminaries in Two-Way Synchronization	53
8 Security Design Guidelines (Two-Way)	55
9 Existing Security Designs (Two-Way)	59
10 Formal Security Analysis (Two-Way)	63
11 Practical Design Evaluation (Two-Way)	78
12 Formal Design Verification (Two-Way)	80
13 Discussion of Results (Two-Way)	93
<b>II-B Security Measures for One-Way Synchronization</b>	<b>97</b>
14 Preliminaries in One-Way Synchronization	99
15 Security Design Guidelines (One-Way)	102
16 Existing Security Designs (One-Way)	106
17 Formal Security Analysis (One-Way)	109

---

<b>18 Practical Design Evaluation (One-Way)</b>	<b>123</b>
<b>19 Formal Design Verification (One-Way)</b>	<b>135</b>
<b>20 Discussion of Results (One-Way)</b>	<b>151</b>
 <b>III Overarching Discussion</b>	 <b>155</b>
<b>21 Watchdogs and Guards</b>	<b>157</b>
<b>22 Provable Synchronization and Traceability</b>	<b>161</b>
<b>23 Outlook</b>	<b>165</b>
<b>Conclusion</b>	<b>170</b>
 <b>Glossary</b>	 <b>172</b>
<b>List of Figures</b>	<b>176</b>
<b>List of Tables</b>	<b>177</b>
<b>Bibliography</b>	<b>178</b>