MPC

MULTI PROJECT CHIP GRUPPE
BADEN-WÜRTTEMBERG

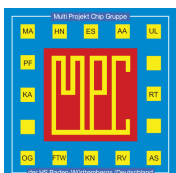Cooperating Organisation
Solid-State Circuit Society Chapter
IEEE German Section

Inhaltsverzeichnis

Tagungsband zum Workshop der Multiprojekt-Chip-Gruppe Baden-Württemberg

Die Inhalte der einzelnen Beiträge dieses Tagungsbandes liegen in der Verantwortung der jeweiligen Autoren.

Diesen Workshopband und alle bisherigen Bände finden Sie im Internet unter:
http://www.mpc-gruppe.de/de/workshopbaende.html

35 Jahre MPC-Gruppe – Eine Zeitreise

Gerhard Forster

Zusammenfassung—Die Multiprojekt-Chip-Gruppe (MPC-Gruppe), ein Verbund von 13 Fachhochschulen in Baden-Württemberg, die sich mit dem Entwurf Integrierter Schaltungen befassen, wurde im Jahr 1988 gegründet. Anlässlich des 35. Jahrestages wirft dieser Beitrag einen Blick zurück auf die Entstehungsgeschichte und die erzielten Ergebnisse. Er beleuchtet darüber hinaus die aktuelle Entwicklung des globalen Halbleitermarkts und versucht, daraus Antworten auf Fragen der Zukunft der MPC-Gruppe abzuleiten.

Schlüsselwörter—Multi-Projekt-Chip-Gruppe, Entstehungsgeschichte, Mikroelektronik, Chip-Entwurf.

I. Einleitung

Mikroelektronik ist heute allgegenwärtig und bestimmt in hohem Maße die weitere Entwicklung unserer Informationsgesellschaft. Ihre globale Bedeutung wird inzwischen auch von führenden Vertretern großer Volkswirtschaften hervorgehoben. So betonte Margrethe Vestager, Executive Vice President der EU anlässlich einer Ansprache am 8. Juni 2023: „Microchips are the backbone of innovation and of Europe's industrial competitiveness in a digital world" [1]. In den vergangenen Jahrzehnten wurde dies nicht immer so deutlich formuliert. Umso höher sind die Bemühungen der ehemaligen Professoren Schmidt und Führer zu bewerten, im Jahre 1988 einen Verbund der baden-württembergischen Fachhochschulen zu begründen, der die Einführung der Mikroelektronik in die Lehre zum Ziel hatte. So entstand die MPC-Gruppe mit 13 Fachhochschulen, die, gefördert durch das Land Baden-Württemberg, in die Lage versetzt wurden, nicht nur Grundlagen zu lehren, sondern mit neuester Entwurfstechnologie und weltweitem Zugang zu Halbleitertechnologien komplette Chip-Designs umzusetzen. Abbildung 1 zeigt beispielhaft das Ergebnis einer solchen Arbeit, einen 10 bit-A/D-Umsetzer als typisches Standard-Produkt [2], dargestellt im Größenvergleich.

35 Jahre sind mehr als eine Menschheitsgeneration, und so stellt sich die Frage: Ist das, was sich die Gründer der MPC-Gruppe gedacht hatten, heute überhaupt noch zeitgemäß? Oder profitieren wir einfach heute noch davon, dass damals gerade mal Finanzmittel verfügbar waren? Dieser Beitrag soll darauf Antworten geben und zeigen, dass der Weg auch damals nicht einfach war. Nach einem Blick auf die Situation der

Gerhard Forster, gerhard.forster@thu.de, Technische Hochschule Ulm, Prittwitzstraße 10, 89075 Ulm.
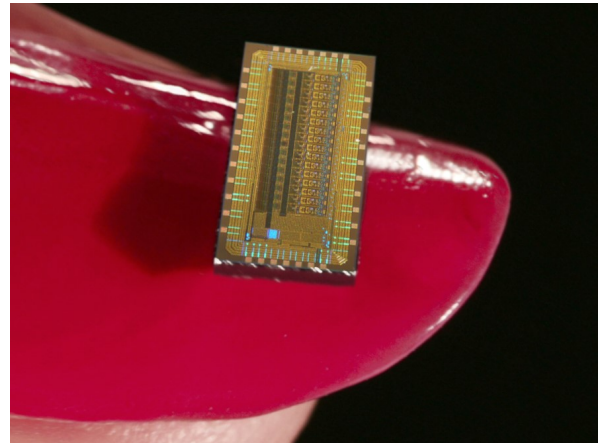
Abbildung 1. Chipfoto eines 10-Bit-A/D-Umsetzers (Sukzessiv-Approximationsverfahren) in $0.35\,\mu\mathrm{m}$ CMOS-Technologie im Größenvergleich mit einem kleinen Fingernagel. Die Chipfläche beträgt $3,8 \times 1.9\,\mathrm{mm}^2$.

Halbleiterelektronik vor 1980 wird der Entstehungsprozess der MPC-Gruppe kurz nachgezeichnet. Mit Daten und Fakten wird ihre Entwicklung über die Jahre gezeigt. Zum Schluss soll die aktuelle Situation beleuchtet werden mit dem Versuch, daraus einen Ausblick auf die weiteren Chancen der MPC-Gruppe abzuleiten.

II. Halbleiterelektronik vor 1980

Begonnen hatte alles 1958, also 10 Jahre nach der Erfindung des Transistors durch Shockley, Bardeen und Brattain, mit einem Patent von Jack Kilby, Texas Instruments, der Transistor, Widerstand und Kondensator erstmals auf gleichem Halbleitermaterial, damals noch Germanium, realisierte [3]. Bereits ein Jahr später erschien ein Patent von Robert Noyce, Mitbegründer von Fairchild, das allgemein als Nachweis für den ersten Chip in Si-Planartechnologie gilt [4]. Dieses Patent war auch Grundlage für den ersten Integrierten Schaltkreis, ein S/R-Flipflop in RTL-Logik, der von Fairchild ab 1961 kommerziell vertrieben wurde. Er markierte den Beginn der kommerziellen Erfolgsstory und läutete die atemberaubende Entwicklung ein, die bereits 1965 Gordon Moore, ebenfalls Mitbegründer von Fairchild und später Intel, zu der Projektion veranlasste, die später als „Moore'sches Gesetz" in die Geschichtsbücher eingehen sollte.

In Deutschland war der Elektronikmarkt, zumindest bis ins Jahr 1975, noch fest in der Hand von renommierten Unternehmen wie AEG-Telefunken, Bosch,

SEL oder Siemens, aber auch von bedeutenden Mittelständlern wie Grundig, mit typischen Produkten für die Telekommunikation (Telefon, Funknetze), die Unterhaltungselektronik (Fernsehen, HiFi) und die Verteidigungstechnik. Der Schaltungsentwurf erfolgte häufig noch experimentell auf dem Breadboard, gestützt auf Transistor-Datenbücher im Analogen oder das allgegenwärtige „TTL-Kochbuch" im Digitalen [5]. Wissensbasis waren die Grundlagenkenntnisse aus der Hochschule, ergänzt um Kenntnisse in Boole'scher Algebra und Halbleiterelektronik, meist beschränkt auf den Transistor als linearen Vierpol. Die großen Unternehmen verfügten allerdings bereits über „Großrechner", in der Regel Eigenprodukte, die sie selbst auf den Markt brachten, wie z.B. den TR 440 von AEG-Telefunken [6]. Mit unternehmenseigenen Programmen, geschrieben in Fortran, waren damit bereits Logikanalyse und vereinfachte Simulation analoger Schaltungen möglich. Schaltplaneingabe und Simulatorsteuerung erfolgten aber noch mit Lochkarten. Damit war kaum mehr als ein Rechnerlauf am Tag möglich und die Produktivität entsprechend gering.

Noch bis um das Jahr 1980 stand Deutschland unter dem Einfluss der Ölkrise 1973/74, die einen Anstieg der Ausgaben für die Energieimporte auf das $2^{1}/_{2}$-fache binnen eines Jahres auslöste. Dies führte erstmals nach der Währungsreform zu Inflation, gefolgt von Arbeitskämpfen und Lohnerhöhungen über der Produktivitätssteigerung. Die weiteren Folgen waren mangelnde Wettbewerbsfähigkeit, wirtschaftliche Rezession und schließlich beängstigende Arbeitslosenzahlen (1975 nahezu 5%, 1985 über 9%) [7]. Dies also waren die technischen und wirtschaftlichen Randbedingungen vor Gründung der MPC-Gruppe.

III. Entstehung der MPC-Gruppe

Reiner Hartenstein, Professor an der Universität Kaiserslautern, hielt nach seiner Rückkehr von einer Gast-Professur 1981 an der CU Berkeley einen denkwürdigen Vortrag anlässlich eines Institutsjubiläums in Karlsruhe. Er berichtete von der rasanten Entwicklung der Mikroelektronik im Silicon Valley und sah die Gefahr, dass wir in Deutschland von der sich abzeichnenden VLSI-Revolution komplett abgehängt werden. Um dem zu begegnen, mahnte er dringend an, die Mikroelektronik in der Lehre der Elektrotechnik und Informatik zu verankern. Es gelang ihm daraufhin, ein großes BMBF-Projekt, das Projekt E.I.S. (Entwurf Integrierter Schaltungen) auf den Weg zu bringen. Ziel dieses Projekts mit der Laufzeit von 1983 bis 1987 war die Einführung der Mikroelektronik in der akademischen Lehre, insbesondere die Durchsetzung einer neuen Disziplin „Entwurf Integrierter Schaltungen", auch unter Loslösung von der Mikroelektronik-Technologie. Dieses Konzept geht auf Carver Mead, Professor am CalTech zurück [8]. Mitglieder des Projekts, Vorläufer des mächtigen EU-Projekts Eurochip,

waren 20 Universitäten. Mitglied wurde allerdings auch eine Fachhochschule, die FH Furtwangen mit Prof. Schmidt. Ihm schlossen sich 1984 die Kollegen Prof. Führer von der FH Ulm und Prof. Kampe von der FH Esslingen an, wenn auch ohne Mittelzuteilung [9]. Damit waren neben den Universitäten drei Fachhochschulen, alle aus Baden-Württemberg, unter den Mitgliedern. Dies war Anlass für das MWK in Baden-Württemberg, Anfang 1985 in Furtwangen anzufragen, inwieweit die Hartenstein-Thesen auch an den hiesigen Fachhochschulen umgesetzt werden könnten, und es war der erste Meilenstein hin zur MPC-Gruppe. Aber es sollten noch viele Meilensteine folgen.

Am 08.05.1985 fand auf die Bitte der FH Furtwangen hin ein Gespräch im MWK über den Strukturwandel durch die Mikroelektronik und die daraus resultierenden Anforderungen an die Lehre statt. Prof. Schmidt legte am 26.05.1985 ein Konzept vor, das die Einrichtung eines Modellstudiengangs Mikroelektronik in Furtwangen unter Einbezug der anderen Fachhochschulen in Forschung und Lehre zum Inhalt hatte. Die Erörterung des Konzepts fand am 21.11.1985 im MWK statt. Seitens des Ministeriums wurde Zustimmung signalisiert, allerdings unter der Voraussetzung der finanziellen Beteiligung des Bundes am Studiengang. Am 11.07.1986 fand ein Meeting der Kollegen aus Furtwangen, Ulm, Esslingen, Aalen, Offenburg und Mannheim statt, das die Bildung eines Verbundes der Hochschulen unter Einbezug lokaler Halbleiterhersteller zum Ziel hatte. Das Institut für Mikroelektronik Stuttgart (IMS) hatte digitale Multiprojekt-Chips in Aussicht gestellt (Digital-Array CMOS 3 μm), AEG-Telefunken analoge Multiprojekt-Chips (Bipolar-Array). Das Konzept wurde am 22.10.1986 im MWK vorgestellt und am 20.11.1986 wurde der Verbund konstituiert mit Prof. Schmidt als Vorsitzendem. Bereits im Jahr darauf wurden erste Entwürfe mit IMS wie auch mit AEG-Telefunken realisiert, und so fanden am 01.12.1987 abschließende Gespräche im Ministerium statt. Hier wurde auch erstmals der Name „Multi-Projekt-Chip-Verbund" benannt. Doch am 21.12.1987 sagte der Bund die Beteiligung am Modellstudiengang in Furtwangen ab! Der Studiengang war aber wesentlicher Teil des Konzepts. Damit war das ganze Konzept im Grunde gescheitert, und das Projekt E.I.S. lief zum Jahresende aus.

Um die drohende Depression abzuwenden, wurde intensiv nach Lösungen gesucht. Schließlich erklärte sich das MWK Anfang 1988 bereit, auch den Bundesanteil für Furtwangen zu übernehmen, und so konnten verbleibende Fragen zu Finanzierung, Verwaltung und Nachweisen (Workshops) geklärt werden. Die „MPC-Gruppe" ging an den Start mit Prof. Schmidt als erstem Sprecher. Die Fachhochschulen Aalen, Albstadt-Sigmaringen, Konstanz, Pforzheim und Reutlingen schlossen sich sogleich an; die übrigen Fachhochschulen sollten bald folgen. Die MPC-Gruppe

war also alles andere als ein Selbstläufer und der Erfolg nur wenigen zu verdanken. Es sind insbesondere die Herren Guntermann vom MWK sowie Schmidt und Führer seitens der Hochschulen, die mit Mut, Weitsicht und unermüdlichem Einsatz zum Entstehen beigetragen haben.

IV. DATEN UND FAKTEN

Von entscheidender Bedeutung für eine nachhaltige Entwicklung der Gruppe waren die erfolgreichen Verhandlungen über die Mittelausstattung gleich zu Beginn. In einer ersten Investitionsrunde, beginnend 1988, konnten alle Mitgliedshochschulen im Rahmen von HBFG-Anträgen mit professioneller Rechnerhardware ausgestattet werden. Es handelte sich dabei um neuartige Grafik-Workstations der Fa. Apollo (Massachusetts), ergänzt um Peripheriegeräte und bauliche Infrastruktur (z.B. Raumklimatisierung). Prof. Führer hatte hierzu ein Rahmendokument ausgearbeitet, das die übrigen Hochschulen als Vorlage für ihre individuellen Anträge nutzen konnten. Es folgte eine zweite Runde ab 1994 mit neuen, leistungsfähigeren Workstations der Fa. HP, die inzwischen Apollo übernommen hatte. Die beiden Runden hatten ein Investitionsvolumen von jeweils ca. 5 Mio. DM. Ab 2002 schloss sich noch eine dritte Runde mit einem Investitionsumfang von 1,3 Mio. EUR an, bei der erstmals auf ein Client-Server-Konzept der Fa. HP umgestellt werden konnte. Weitere Großgeräteanträge kamen leider nicht mehr zustande, und so war danach erfolgreiches Arbeiten vor allem dem Verfall der Rechnerpreise zu verdanken. Ganz entscheidend aber war die erfolgreiche Beantragung gleich zu Beginn der laufenden Mittel für Hardware (Wartung) und Software (Lizenzen) sowie Chipfertigung. Somit beläuft sich die Gesamtförderung bis heute (inflationsbereinigt) auf über 15 Mio. EUR. Die Mittel werden nach wie vor von der Haushaltsstelle der THU bewirtschaftet.

Natürlich kamen die HBFG-Mittel nicht einfach als warmer Regen über die Fachbereiche, denn die Beantragung setzte den Willen der Hochschulen zu beträchtlichen Eingriffen in das Curriculum voraus. Es war also nicht selbstverständlich, dass die Professorinnen und Professoren im Fakultätsrat den Vorhaben zustimmten, wenn sie gleichzeitig selbst zurückstecken mussten. Letztlich wurden aber doch die Chancen gesehen. Zum einen bestand die Möglichkeit zur Einrichtung neuer Labors mit professioneller Rechnerausstattung und Chipmesstechnik. Hierbei kam uns nicht zuletzt die starke Verhandlungsposition zugute. Zum anderen eröffnete sich dank professioneller CAD-Software der Technologiezugang zu professionellen Halbleitertechnologien weltweit über Eurochip/Europractice. Die Ausstattung ließ damit kaum Wünsche offen; allein der oft unterkritische Mittelbau begrenzte an einzelnen Hochschulen teilweise deren effizienten Einsatz.

Zu Beginn ging es darum, eigenes Tool-Wissen durch den Besuch von Lehrgängen, außerhalb oder auch im Hause mit eingeladenen Dozenten, aufzubauen. Später wurden eigene Lehrgänge entwickelt, so dass die ganze Gruppe vom Spezialwissen einzelner Kollegen profitieren konnte. Die Themen deckten ein breites Spektrum ab, vom Systementwurf mittels Matlab, SystemC und VHDL über Analog-Simulation, Layoutentwurf und Layoutverifikation bis zum Tape Out. Ein besonderes Augenmerk lag in der Einrichtung durchgängiger Entwurfspfade ausgehend von HDL bis hin zum Mixed-Signal-Chip. Dieses Know-how öffnete schließlich auch zahlreiche Türen in die Industrie. Tausende Absolventinnen und Absolventen konnten von dieser Qualifikation als Entwicklungsingenieur profitieren.

Sichtbarstes Zeichen der in der MPC-Gruppe gebündelten Kompetenzen sind nach wie vor die Workshops und die in den Tagungsbänden veröffentlichten Arbeiten. Erschienen zunächst eher theoretische oder auch technologiegetriebene Beiträge, gefolgt von Beiträgen zum Digital-Design, so verlagerte sich der Schwerpunkt ab der Jahrtausendwende zunehmend auf den Systementwurf mit FPGA, der heute grob ein Drittel der Aktivitäten ausmacht. Am kontinuierlichsten sind bis heute die Analog- und Mixed-Signal-Beiträge, die ebenfalls ein gutes Drittel der Publikationen einnehmen, häufig mit konkreten Chip-Entwürfen. Unter Einbezug einfacherer Studien und Redesigns wurden über 100 Chip-Entwürfe auch gefertigt. Darunter befindet sich eine ganze Reihe abgeschlossener Projekte (in den Workshop-Bänden veröffentlicht) mit funktionsfähig getesteten ASICs, wie z.B.

- Laderegler für Solarsysteme
- Smart-Power-IC für den Betrieb von Stromsparlampen
- CMOS-Leistungsverstärker für niedrige Versorgungsspannungen
- Low Frequency Continuous Phase Differential Quadrature Phase Shift Keying Front End
- Prozessorkern Sirius-Janus
- Mixed-Signal SoC for Biomedical Applications
- MMIC-Phasenschieber für den Einsatz in phasengesteuerten Arrayantennen im C-Band
- High-speed Multiplexer/Demultiplexer-IC
- Tiefpassfilter 3. und 8. Ordnung
- Laser-Radar für ein bildgebendes Verfahren
- Verstärkerkette für die Infrarot-Spektralanalyse
- Ultra-Low-Power-Verstärker mit Energy-Harvesting-Versorgung
- High-Side-Gatetreiber mit Ladungspumpe
- Hoch-Volt-Interface für 230 V-Netzbetrieb von ICs
- Hocheffizienter resonanter Spannungswandler bis 30 V

Die Expertise im Entwurf Integrierter Schaltungen ermöglichte auch die Herausgabe eines Handbuchs

Abbildung 2. Gruppenfoto aus dem Jahr 2013 anlässlich des 25-jährigen Jubiläums der MPC-Gruppe und des 50. Workshops in Konstanz.

[10] und weiterer fachspezifischer Lehrbücher und nicht zuletzt die Möglichkeit zum Aufbau internationaler Kontakte beim Besuch von Tagungen und Institutionen. Bereits 1990 erfolgte die erste Auslandsreise ins Silicon Valley, gefolgt von Reisen 1991 nach San Diego und 2001 nach Kyoto. Mehrfach gab es Reisen zur europäischen DATE-Konferenz und zur ISSCC in San Francisco. Daraus resultierten wiederum interessante Beiträge auf unseren Workshops von namhaften Referenten. Besonders hervorzuheben ist der Jubiläumsworkshop anlässlich des 25-jährigen Bestehens der MPC-Gruppe in Konstanz (Abbildung 2) mit Beiträgen von Carl Das (IMEC Leuven) [11], Etienne Sicard (INSA Toulouse) [12] und Andrei Vladimirescu (CU Berkeley) [13]. Zu diesem Jubiläum wurde auch eine Festschrift herausgegeben [14].

35 Jahre bedeuten naturgemäß Wandel in der Mitgliedschaft. So wurde der Stab des MPC-Sprechers (heute: Vorstandsvorsitzender) wiederholt weitergegeben: 1988 von Prof. Dr. Schmid an Prof. Führer, 1996 an Prof. Dr. Jansen, 2013 an Prof. Dr. Giehl und 2022 an Prof. Dr. Hennig. 35 Jahre bringen aber auch mit sich, dass die MPC-Gruppe inzwischen vier Kollegen für immer verloren hat: Prof. Dr. Nielinger, Prof. Dr. Albert, Prof. Führer und Prof. Dr. Paul.

V. Aktuelle Situation

Beim Blick auf die Investitionen und die in den Workshopbänden behandelten Themen der vergangenen Jahre erkennt man deutliche Veränderungen und eine merkliche Abwendung von Mikroelektronik und Hardware-Design. Die Vorzeichen waren bereits vor der Jahrtausendwende erkennbar: Zunehmende Verlagerung der Produktionsstätten nach Fernost und in der Folge massive Reduktion der Fördermittel für die Mikroelektronik. Dies beschleunigte den Rückgang der Studierendenzahlen, insbesondere im Bereich der Elektro- und Informationstechnik, denn Studierende der Ingenieurwissenschaften wollen wissen, wo die zukünftigen Arbeitsplätze liegen, und die Geschichte lehrt uns, dass die Entwicklung noch immer der Produktion folgen musste. Da half auch unser stetiger Hinweis auf die enorme Hebelwirkung der Mikroelektronik nur bedingt, auch nicht der Hinweis darauf, dass Mikroelektronik nicht nur viele Innovationen ermöglicht, sondern dass umgekehrt existenzgefährdende Abhängigkeiten entstehen könnten, wenn wir die Technologie zunehmend aus der Hand geben. Die MPC-Gruppe musste sich dieser Entwicklung letztlich anpassen durch Konzentration auf den digitalen Systementwurf mit FPGA oder auf spezielle Themen im Analog-Design. Im Übrigen versuchte sie, zumindest ihre Sichtbarkeit zu erhöhen. Seit 2001 ist die MPC-Gruppe Mitglied der deutschen Sektion des IEEE SSCS (Solid-State-Circuits Society). Im Jahr 2008 wurden die Tagungsbände an den internationalen Standard der IEEE-Proceedings angepasst. Seitdem erscheinen sie in einem professionellen Design und durchlaufen einen Peer-Review-Prozess. Weiterhin wurden diverse Poster für die Verbesserung der Außenwirkung entwickelt. Innerhalb der (Fach-)Hochschullandschaft wurde damit der Status zweifellos gefestigt, aber die globale Entwicklung der Mikroelektronik und der Halbleitermärkte wird weiterhin eine Herausforderung bleiben.

Noch um das Jahr 1990 war Europa sowohl in Entwicklung als auch Produktion auf den Gebieten Halbleiterspeicher (DRAM, EEPROM), Prozessoren (High Performance Computing, Mobile Communication) und Mixed-Signal-Chips (HF, Power) maßgeblich engagiert, allerdings war zu dieser Zeit das weltweite Produktionsvolumen noch vergleichsweise gering. Bereits um 2000 wurden die technologie-getriebenen Speicher hauptsächlich in Asien produziert, während immerhin bei den Prozessoren die USA in Entwicklung und Produktion noch unangefochten den Weltmarkt anführten. Inzwischen hat sich die Halbleitertechnologie, vor allem durch das in Taiwan eingeführte Foundry-Konzept, so weit fortentwickelt, dass inzwischen TSMC als Technologieführer gilt und selbst Intel bestimmte High-End-Produkte dort fertigen lässt. Damit liegt der weltweite Halbleiter-Produktionsanteil in Europa bereits unter 10% und auch in den USA bereits nur noch bei 12%, obwohl über 50% aller Chips in den USA entwickelt werden. Der Produktionsanteil in Asien liegt hingegen über 70%, vor allem in Taiwan, und Taiwan besitzt mit TSMC die Technologieführerschaft. Dies hatte sich eigentlich China zum Ziel gesetzt, das seit 2014 enorme Fördermittel ausgegeben hat. Erklärtes kurzfristiges Ziel ist die Steigerung der Eigenproduktion auf 70% bis 2030 [15]. Hierzu sind derzeit über 40 neue Fabs im Bau.

Diese Entwicklung, verbunden mit der angesichts der politischen Lage bedrohlichen wirtschaftlichen und sicherheitstechnischen Abhängigkeit, hat inzwischen zu einem Umdenken im Westen geführt. Die USA haben inzwischen Lieferbeschränkungen für China ausgesprochen. China darf keine Chips neuester Technologie von TSMC beziehen und wird von neuester EDA und Fabrikationstechnologie (z.B. EUV) ausgeschlossen. Darüber hinaus wurde der Chips Act mit einem Fördervolumen von 52 Mrd. $ (plus 24 Mrd. $ Steuernachlässe) beschlossen. Er hat die „deutliche Erhöhung der Eigenproduktion" zum Ziel [16]. Bis 2030 sollen damit Investitionen von über 200 Mrd. $ ausgelöst werden. Auch die EU hat einen Chips Act beschlossen [17]. Er hat mit einem Fördervolumen von 42 Mrd. EUR die „Erhöhung des Weltmarktanteils auf 20%" zum Ziel. Ob dieses konkrete Ziel allerdings realistisch ist, bleibt angesichts der massiven Investitionen in China und USA, aber auch in Taiwan und Südkorea abzuwarten. Auch der Versuch, sich an die Spitze des Moore'schen Gesetzes zu bringen (z.B. durch den Bau einer 2 nm-Fab), scheint heute fragwürdig angesichts fehlender Absatzmärkte in der EU für eine solche Fab. Erfolgversprechender ist sicher, die heutige Expertise der EU im Chipdesign, bei Entwicklung und Produktion im Mixed-Signal-Bereich sowie im Fertigungs-Equipment weiter zu fördern.

VI. AUSBLICK

Im Bereich der Mixed-Signal-ICs, insbesondere für die Anwendungsgebiete Sensorik und Smart Power, die besonders für die Automobilindustrie relevant sind, ist die EU immer noch gut positioniert. Diese Position wird derzeit sogar gefestigt mit den neuen Fabs von Infineon, Bosch und Wolfspeed. Offenbar ist die EU ebenfalls noch interessant für Investitionen in das Chip-Design. So erweitert derzeit Apple sein Europäisches Zentrum für Chip Design in München für 1 Mrd. EUR für die Schwerpunkte HF (5G) und Power Management. Außerdem gründen Wolfspeed und ZF für 300 Mio. EUR ein F+E-Zentrum für SiC-Leistungselektronik in Nürnberg. Dies sind ermutigende Beispiele dafür, dass Chip-Design wieder eine bedeutendere Rolle auch in unserer Volkswirtschaft einnehmen könnte. In den USA haben sich entsprechende „fabless startups" wie z.B. Qualcomm oder Nvidia zu Multi-Milliarden-Konzernen entwickelt. Erfolgreiche Unternehmen, auch außerhalb der Elektrotechnik, haben systematisch Entwicklungsteams aufgebaut und entwickeln ihre ASICs zunehmend selbst (z.B. Apple, Google, Tesla). Gründe dafür sind Know-how-Anreicherung, Ausbau des technischen Vorsprungs (z.B. bessere Anpassung an die eigene Software und Minimierung des Energiebedarfs) und wirtschaftliche Unabhängigkeit. Dies sollte auch als Beispiel für europäische Unternehmen dienen, denn Elektronik und Software sind auch in ihren Produkten inzwischen wettbewerbsentscheidend. Insbesondere wird es zunehmend nötig sein, sicherheitskritische Infrastruktur selbst zu entwickeln.

Für die Hochschulen bietet sich damit auch in Zukunft (neben der Softwareentwicklung) ein weites Feld auf dem Gebiet des digitalen Systementwurfs, auch mit FPGA (zumindest im Prototyping). Vor allem wird auch zukünftig der Hardware-Entwurf für Mixed-Signal-Anwendungen entlang der gesamten Kette Sensorik – Frontend – A/D-Umsetzer – Signalverarbeitung – Aktorik unter besonderer Berücksichtigung der Konzepte für Low Power, Energy Harvesting, sensornahe KI und Smart Power eine wesentliche Rolle spielen. Der Einsatz von KI wird zukünftig auch im Design Flow eine bedeutsame Rolle spielen, denn wir kommen damit dem Ziel näher, die natürliche Sprache mit ihrem unbegrenzten Sprachumfang als Beschreibungssprache nutzen zu können.

Daraus erwachsen wiederum neue Chancen für die MPC-Gruppe. Sie kann ihre Attraktivität für KMU festigen bzw. ausbauen durch die Expertise ihrer Absolventinnen und Absolventen im HW-Entwurf und die Fähigkeit zur Hardwareentwicklung bis hin zum Chip, unter gezielter Nutzung der KI. Die MPC-Gruppe kann auch die Attraktivität gegenüber Studierenden aufrechterhalten durch interessante Studien mit aktuellem Bezug. Durch unsere herausragende Ausstattung sind wir in der Lage, auch künftig jederzeit interessante

Themen aus der Industrie aufzugreifen und bei Bedarf auch mit eigenen Mitteln zu bearbeiten. Auf diese Weise gelang es uns stets, auch sehr gute Studierende zu gewinnen. Selbst komplexe Designs können damit, wenn auch über mehrere Kohorten hinweg, bearbeitet werden, und inzwischen besteht ja das Promotionsrecht, mit dem sich ganz neue Zeithorizonte für die Projektbearbeitung auftun. Schließlich ist die MPC-Gruppe auch weiterhin attraktiv für Lehrende, nicht zuletzt aufgrund der eigenen Publikationsplattform. Vor diesem Hintergrund erscheint die Gründung der MPC-Gruppe vor 35 Jahren auch heute noch als Sternstunde in der Hochschulgeschichte, und die Chancen auf ein 50-jähriges Bestehen sind durchaus realistisch.

LITERATURVERZEICHNIS

[1] European Commission. *Remarks by Executive Vice-President Vestager on an Important Project of Common European Interest in microelectronics and communication technologies*. Brussels. 8. Juni 2023. URL: https://portal.ieu-monitoring.com/editorial/ipcei-eu-commission-approves-up-to-e8-1bn-of-public-support-to-support-research-innovation-and-%20the-deployment-of-microelectronics/409060 (besucht am 16.11.2023).

[2] F. Mrugalla, A. Erni und G. Forster. „Chipentwurf für einen 10-Bit-A/D-Umsetzer". In: *Tagungsband Workshop der Multiprojektchip-Gruppe* Ausgabe 38, Ulm (2007), S. 5–12. ISSN: 1872-7102. URL: https://www.mpc-gruppe.de/typo8/fileadmin/content/workshops-volums/MPC_Workshopband_38.pdf (besucht am 16.11.2023).

[3] Jack S. Kilby. „Miniaturized Electronic Circuits". 3,138,743. TX Texas Instruments Inc. Dallas. Feb. 1959. URL: https://www.dpma.de/docs/dpma/veroeffentlichungen/us3138743a_kilby.pdf.

[4] Robert N. Noyce. „Semiconductor Device-and-Lead Structure". 2,981,877. CA Fairchild Semiconductor Inc. Mountain View. Juli 1959. URL: https://www.dpma.de/docs/dpma/veroeffentlichungen/us2981877a_noyce.pdf.

[5] E. Haseloff und Texas Instruments Deutschland GmbH Applikationslabor. *Das TTL-Kochbuch: deutschsprachige TTL-Applikationen*. Technik Marketing, 1972. URL: https://books.google.de/books?id=OGJ0zQEACAAJ.

[6] Eike Jessen, Dieter Michel und Heinz Voigt. „Structure, Technology, and Development of the AEG-Telefunken TR 440 Computer". In: *IEEE Annals of the History of Computing* 32.3 (2010), S. 30–39. DOI: 10.1109/MAHC.2009.64.

[7] Statistisches Bundesamt. *Registrierte Arbeitslose und Arbeitslosenquote nach Gebietsstand*. URL: https://www.destatis.de/DE/Themen/Wirtschaft/Konjunkturindikatoren/Lange-Reihen/Arbeitsmarkt/lrarb003ga.html (besucht am 16.11.2023).

[8] Carver Mead und Lynn Conway. *Introduction to VLSI Systems*. USA: Addison-Wesley Longman Publishing Co., Inc., 1979. ISBN: 0201043580.

[9] K. Schmidt und A. Führer. „20 Jahre Multi-Projekt-Chip-Gruppe". In: *Die Multi-Projekt-Chip-Gruppe*. A. Führer, Hochschule Ulm, 2008, S. 7–10. ISBN: 978-3-9810998-1-2.

[10] D. Jansen und G. Albert. *Handbuch der Electronic-Design-Automation: mit 176 Tabellen*. Hanser-Verlag, München, 2001. ISBN: 9783446212886.

[11] C. Das. „Europractice: Supporting the European Academia in Microelectronics Design". In: *Tagungsband Workshop der Multiprojektchip-Gruppe* Ausgabe 50, Konstanz (2013), S. 11–16. ISSN: 1872-7102. URL: https://www.mpc-gruppe.de/typo8/fileadmin/content/workshops-volums/MPC_Workshopband_50.pdf (besucht am 16.11.2023).

[12] E. Sicard. „Eletromagnetic Compatibility of Integrated Circuits Measurement, Modeling and Design Techniques". In: *Tagungsband Workshop der Multiprojektchip-Gruppe* Ausgabe 50, Konstanz (2013), S. 5–10. ISSN: 1872-7102. URL: https://www.mpc-gruppe.de/typo8/fileadmin/content/workshops-volums/MPC_Workshopband_50.pdf (besucht am 16.11.2023).

[13] A. Vladimirescu. „Five Decades of SPICE – A Brief History". In: *Tagungsband Workshop der Multiprojektchip-Gruppe* Ausgabe 50, Konstanz (2013), S. 1–4. ISSN: 1872-7102. URL: https://www.mpc-gruppe.de/typo8/fileadmin/content/workshops-volums/MPC_Workshopband_50.pdf (besucht am 16.11.2023).

[14] G. Forster. *Mikroelektronik – Forschung und Lehre an Hochschulen für Angewandte Wissenschaften*. Hochschule Ulm, 2013. ISBN: 978-3-9810998-6-7.

[15] Nir Kshetri. „The Economics of Chip War: China's Struggle to Develop the Semiconductor Industry". In: *IEEE Computer* 56 (Juni 2023), S. 101–106. DOI: 10.1109/MC.2023.3263267.

[16] Semiconductor Industry Association 2022. *Chips for America Act & Fabs Act*. URL: https://www.semiconductors.org/chips/ (besucht am 01.08.2023).

[17] Pressemitteilung EU-Parlament vom 11. Juli 2023. *Halbleiter: Parlament nimmt Gesetz zur Stärkung der Chip-Industrie in der EU an*. URL: https://www.presseportal.de/pm/106967/5555777 (besucht am 01.08.2023).

Gerhard Forster studierte Physik mit dem Schwerpunkt Quantenelektronik an der Universität Heidelberg. Nach seinem Diplom-Abschluss 1977 befasste er sich als Wissenschaftlicher Mitarbeiter am damaligen Forschungsinstitut von AEG-Telefunken (später Daimler Forschungszentrum) mit der Entwicklung und Anwendung neuer Halbleiterprozesse. Zuletzt war er als Teamleiter zuständig für die Entwicklung und den Test anwendungsspezifischer Integrierter Schaltungen aus den Gebieten der Nachrichtentechnik und der Automobilelektronik. Von 1992 bis 2016 war er Professor für Elektronik und Mikroelektronische Schaltungen an der Hochschule Ulm. Seine Forschungsschwerpunkte lagen auf dem Gebiet des Entwurfs von Mixed-Signal-ASICs. Zwischen 2001 und 2010 hatte er die Leitung der Fakultät Elektrotechnik und Informationstechnik inne. Von 2007 bis 2016 war Prof. Forster Herausgeber des vorliegenden Tagungsbandes. Seit 2016 befindet er sich im Ruhestand.

Analog Computing for the 21$^{\text{st}}$ Century

Bernd Ulmann

Abstract—**Many people think of analog computing as a historic dead-end in computing. In fact, nothing could be further from the truth as analog computing – together with quantum computing – has the potential to bring computing to new levels with respect to raw computational power and energy efficiency. The following paper explains the limits of digital computers, gives a quick introduction to analog computing in general, and shows a number of recent developments that will change the way we think about computers in the next few years.**

Index Terms—**analog computing, unconventional computing**

I. Introduction

After many decades of extremely successful application of stored-program digital computers (just called *digital computers* here) two alternative computing paradigms are shifting into the limelight: Analog computing and quantum computing. Both hold much promise for the future. The reasons for this forthcoming paradigm shift away from digital computers, the basic ideas of analog computing, application areas, etc. are described here.

It should be noted here that *analog computing*, despite its long history (much longer than that of digital computers) is a very active and promising area of research. One should not think of large classic analog computers in a museum but instead of modern integrated circuits and high performance computing. The 21$^{\text{st}}$ century needs analog computers on integrated circuits as co-processors employing the current power efficient CMOS technology, so we are talking about cutting-edge technology, not some arkane relics of the past.

II. Why we should care about analog computing

Despite their incredible success and versatility, digital computers are about to hit fundamental physical limits and face a variety of other challenges thus shifting the focus of current research to different computational paradigms.

The first problem to mention is the high power consumption of our digital infrastructure, a large part of which is caused by the very digital computers at its heart. The overall ICT (*Information and Computing Technology*) sector is estimated to have consumed

Bernd Ulmann, ulmann@anabrid.com, anabrid GmbH, c/o DLR Innovationszentrum, Wilhelm-Runge-Straße 10, 89081 Ulm, Germany.

between 4% and 6% of the global electrical energy in 2020 with data centers accounting for about one sixth of that total number [1]. In particular the demand for CPU power for training deep artificial neural networks is growing at an ever increasing pace, thus further advancing the energy demands of our current computing infrastructure. Apart from the obvious implications for future systems and data centers with respect to energy consumption, this creates an additional problem – that of heat removal. Modern top performing CPUs such as members of AMD's *Ryzen Threadripper* family have TDP (*Thermal Design Power*) values of up to 250 Watt. Cooling large scale systems based on such chips is no easy task.

Interestingly, clock frequencies of digital computers have not increased much at all during the last two decades which is largely due to the fact that the overall power consumption of digital circuits increases super-linearly with clock frequency. Admittedly the energy efficiency of these systems has risen several times due to advances in computer architecture and a trend towards many-thread-architectures coupled with more and more specialised subsystems but these speedups are neither easy to implement nor applicable to all applications.

Generally, parallelism is rather hard to achieve in digital computers as observed and described by Gene Myron Amdahl as early as 1967. Even if Amdahl's *law*, derived in this seminal publication, is an oversimplification and does not take the structure of modern processors with their intricate caching systems, etc., into account, it turns out to be a rather good tool for estimating the maximum speedup achievable by parallelising a task [2]. Admittedly, there is a variety of tasks which benefit rather directly from parallel processing as described by Gustafson's *law* [3] but this is not a general rule. To get near the theoretical peak-performance of a given system with a real-world application is not a simple task, often leaving large parts of a CPU sitting idle.

Current technology nodes of 2 nm are about to hit fundamental boundaries of integration densities, and of the many billions of transistor functions in a modern CPU, typically only a small part is actually performing computations while the vast majority implements infrastructure such as high-speed caches, intricate control circuits ranging from out-of-order-execution to complex pipeline control, register renaming, a plethora of uncore functions, bus and memory interfaces, and many more. At the very heart of these systems are

comparatively few ALUs (*arithmetic logic unit*s) performing actual computations, which does not make really good use of the available silicon real estate.

A comparison of two state-of-the-art supercomputers might be interesting: Today's fastest digital supercomputer, *Frontier*, a HPE Cray EX system located at the Oak Ridge National Laboratory, achieves a staggering $1,194$ PFLOPS ($= 1.194 \cdot 10^{18}$ floating point operations per second, measured with the LINPACK benchmark) using $8,699,904$ cores and consuming about 22.7 MW of electrical power. This amounts to 52 GFLOPS per Watt which is really impressive but next to nothing compared with the contender, a human brain. The raw computational power of a brain is estimated to be in the ball park of 38 PFLOPS at an overall power consumption of about 20 Watt. This amounts to about 1.9 PFLOPS/W – many decades better than our current digital supercomputers.

How is that possible? What does nature do so differently from our classic approach to computation to achieve such an extraordinary high energy efficiency? It is mainly the fact that the brain does not execute an algorithm, i.e., there is no sequence of instructions to be executed in a step-by-step fashion. Instead a brain consist (vastly simplified) of billions of rather simple computing elements, neurons, which are interconnected in a suitable fashion to implement the many feats we are capable of. Thus, the *program* underlying a brain is not an algorithm but a directed graph describing the interconnection of neurons with their individual input weights etc. There is no central memory, no cache memory, no intricate control system, just a multitude of small computing elements all working in full parallelism.

From that perspective, a biological brain quite closely resembles an *analog computer* instead of a stored-program digital computer, as the interconnection of its computing elements is the actual program.

III. ANALOG COMPUTING

Now, what is an analog computer? In a nutshell, an analog computer consists of a number of computing elements, each capable of performing a basic mathematical operation such as summation, integration (this is a truly magic element), multiplication, etc., which are interconnected in a suitable way to form a model, an *analogue*, for a given problem to be solved. The term *analog computer* refers to the model building charactersitic and not to a certain representation of values.

Variables are typically represented by voltages or currents.[1] This representation simplifies the construction of an analog computer substantially since only a

single wire (or a pair of wires) is required to connect two computing elements. Nothing is more true in computer science than the saying "there is no such thing like a free lunch" which also holds true in the case of analog computers where this characteristic comes at a cost: An analog computer typically offers only limited precision with typical resolutions being of the order of 10^{-3} to 10^{-4}. Analog computers capable of a precision of 10^{-4} are often called *precision analog computers*.

As negative as this sounds it isn't much of a problem for many if not most applications. Engineering problems typically do not require more than a few decimal places for a useful solution, biological neural networks only feature very limited resolution for their synaptic weights which thus also holds true for artificial neural networks, etc. In cases where higher precision is required, results generated by an analog computer could be used as starting points for numerical algorithms executed on an attached digital computer which can then enhance these results to the required degree of precision.

Using voltages or currents to represent values not only removes much complexity from a computer but also adds significantly to the energy efficiency of the system since there is no need to flip zillions of signal lines between 0 and 1 billions of times per second, each time charging or discharging tiny parasitic capacitors. Furthermore this representation facilitates interfacing to the surrounding world making analog computers ideal for signal pre- and postprocessing, etc.

Analog computers are ideally suited for problems that can be described as (systems of coupled) differential equations (most problems relevant in science and engineering fall into this category). There are also suitable approaches to tackle partial differential equations on analog computers. They can even implement oscillator based *Ising machines* and thus solve problems which are normally attributed to adiabatic quantum computers [4][5].

The following simple problem shows the main difference between programming a classic digital computer and an analog computer. Here, $x = a(b + c)$ is to be computed. A classic digital computer requires six instructions to accomplish this as shown in figure 1. The two arithmetic operations at the core of the task are surrounded by four instructions to load data from memory and store the result back to memory. Of course, this ratio gets better with increasing problem complexity and with clever register allocation schemes, but it illustrates the nature of a digital computer quite well.

Solving the same problem on an analog computer requires two computing elements, one summer and one multiplier, and a few connection between these elements. The input values a, b, and c represented by voltages or currents are connected to these ele-

---

[1]It should be noted that there are even "digital analog computers" called *DDAs* (*Digital Differential Analyser*s) which represent values in a binary fashion but also rely on a set of computing elements which are interconnected with each other to implement a program.

anabrid
analog–digital hybrid computing

```
LOAD   A, R0
LOAD   B, R1
LOAD   C, R2
ADD    R1, R2, R1
MULT   R0, R1, R0
STORE  R0, ...
```

Figure 1. Computing $x = a(b + c)$ on a digital computer
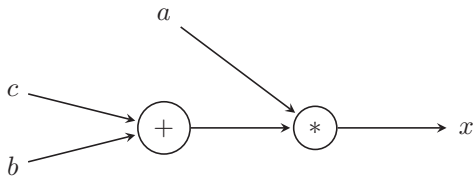

Figure 2. Analog computer setup for solving $x = a(b + c)$

ments, while the output of the summer is connected to one input of the multiplier. There is no algorithm in the classic sense of the word, instead the program resembles a directed graph describing how computing elements must be connected with each other to solve a given problem. Since there is no algorithm and no central memory storing instructions and values, all computing elements can work in full parallelism with no need for explicit synchronisation etc.

This leads to an interesting basic difference between digital and analog computers: In a digital computer it is always possible to trade problem complexity against solution time. The more complex a problem gets the longer it will take to solve it on a digital computer (always assuming there is enough memory to hold all instructions and variables for the problem). This often convenient tradeoff is not possible with an analog computer, which is a certain drawback. If the implementation of a problem requires more computing elements than a given analog computer contains, it cannot be solved (at least not directly) on this particular machine. On the other hand, the solution time for a problem on an analog computer does not increase with problem size, provided that there are enough computing elements available to implement the program.

Of course, there are some drawbacks of analog computers: In addition to the rather limited precision of analog computing elements, values have to be within the interval $[-1, 1]$.[2] Additionally, the generation of arbitrary functions as obtained by experiments or the like is also quite challenging for an analog computer especially when functions $f(x_1, \ldots, x_n)$ of more then one argument are required. Nowadays this can be easily

[2]It is best to always think in terms of this abstract interval instead of the actual minimum and maximum voltages or currents representing these values in order to simplify programming and scaling. Early vacuum tube based analog computers used voltages between ± 100 V to represent values. These voltages later dropped to ± 10 V in transistorised machines, while modern implementations use ± 1 V and even lower voltages at much increased bandwidths.

overcome by using lookup tables stored in some memory with attached analog-digital- and digital-analog-converters (*ADC*s and *DAC*s). Regarding integration, being a basic operation of an analog computer, only time is available as the free variable of integration; this constraint requires the use of advanced techniques to tackle PDEs (*partial differential equations*).

Modern analog computers typically will be part of a *hybrid computer*, i. e., a combination of a digital computer with an analog computer as a specialised, closely attached co-processor. This co-processor excels at the high-speed, energy efficient solution of (systems of) differential equations while the digital computer allows for storage, decision making, function generation, parametrisation of the analog computer, etc.

IV. PROGRAMMING

As arcane as analog computer programming may look to the uninitiated, it is much more straight forward than the algorithmic approach we were all taught and cherish. A simple example may show the basic approach which relies on an idea of Lord KELVIN who developed the KELVIN *feedback technique* [6]. in 1876 after the invention of a practical mechanical integrator by his brother [7, pp. 22 ff.].

This technique transforms a mathematical problem description into an analog computer program, i. e., a directed graph connecting suitable computing elements, in a series of five steps:

1) Organise the equation to isolate the highest derivative on the left hand side.
2) Assuming this derivative is known, all lower derivatives can be generated by repeated integrations.
3) Using summers, multipliers, and other computing elements, all terms on the right hand side of the equation obtained in the first step are derived.
4) These terms are now tied together to form the right hand side of the equation. Since this must be equal to the highest derivative this signal is then fed back into the circuit as the highest derivative which was assumed to be known in the second step.
5) This program typically needs scaling to ensure that no value lies outside the interval $[-1, 1]$. In addition to this, a good scaling process also ensures that ideally every variable will make best use of this interval, thus increasing the precision of the computation.

Suppose the 2nd-order differential equation $\ddot{y} + y = 0$ is to be solved with an analog computer. It first is solved for its highest derivative yielding $\ddot{y} = -y$. Starting from $\ddot{y}$ the lower derivatives $-\dot{y}$ and y are derived by a chain of two integrators. (Due to the actual implementation of such integrators, they typically perform an implicit sign flip. Summers behave similarly.) Since the right-hand side of $\ddot{y} = -y$ is negative, an
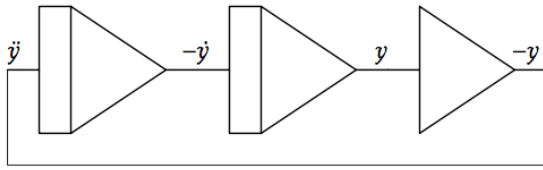
Figure 3. Basic analog computer setup for solving $\ddot{y} + y = 0$
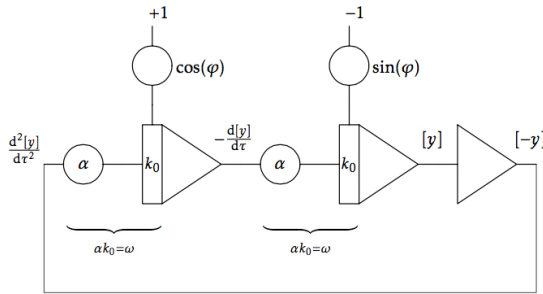
Figure 4. Analog computer setup for solving $\ddot{y} + \omega^2 y = 0$ with proper initial conditions

additional change of sign is required which is done by a summer with only one input, acting as an inverter. The output of this summer is then fed into the first integrator, thus completing a feedback loop as shown in figure 3. The triangular symbol on the right denotes a summer while the two symbols to its left represent integrators.

This program is missing one important detail – the initial conditions of the integrators, specifying which solution to obtain. A complete program for the solution of the equation $\ddot{y} + \omega^2 y = 0$ with initial conditions $y(0) = \sin(\varphi)$ and $\dot{y}(0) = \cos(\varphi)$ is shown in figure 4. The circles denote coefficients, k_0 denotes the *time-scale factor*[3] of the integrator with $\alpha k_0 = \omega$.

An analog computer typically features (at least) three modes of operation:

- *Initial Condition* mode (*IC*): The integrators are set to their respective initial condition values. This step must precede the following mode.
- *Operate* (*OP*): The integrators integrate with respect to time – the computer performs its actual computations.
- *Halt* mode (*HALT*): All integrators are halted, so that all variables within the program remain constant. This is typically used to read values when using slow ADCs. This mode may be followed by OP or IC.

Problems of a more realistic complexity can be transformed into analog computer programs employing the same rationale but typically need some (extensive) attention with respect to scaling. A recent and thorough

---

[3]This time-scale factor k_0 describes the speed at which an integrator runs. In the case of $k_0 = 1$ the output of an integrator will reach -1 with a constant input of $+1$ after one second. If $k_0 = 10^3$ this value will be reached after one millisecond, etc.

introduction to analog and hybrid computer programming can be found in [8].

V. PROBLEMS OF CLASSIC ANALOG COMPUTERS

While analog computers were the systems of choice when it came to the treatment of problems requiring real-time solutions of highly complex dynamic systems, they were basically replaced by digital computer in the early 1980s even though their digital rivals could not compete their computational power for another one or two decades to come.

The main reasons for this were that digital computer became quickly cheaper while analog computers continued to be rather expensive systems due to the required high precision components, etc. In addition to this, programming a classic analog computer required manually plugging hundreds and sometimes thousands of patch cables on a patch panel to implement a certain analog computer program, a time consuming and error prone process. Although such patch panels with their intricate maze of wires could be quickly replaced on medium to large scale analog computers, switching from one program to another still was a time consuming affair. Accordingly, most analog computers were used to treat a single problem for a prolonged time during which no other program could be run concurrently. In contrast to this digital computers offered time sharing access since the 1960s allowing many users to share the (limited) computing power of these machines. This characteristic alone often turned purchase decisions away from an analog computer.

Figure 5 shows a classic large scale analog computer installation at the German aerospace company Boelkow in 1960. This particular installation implemented a flight simulator for a vertical-takeoff-and-landing jet fighter. It shows clearly the fact that the analog computer's size must match the problem size. At its heart are three large Telefunken RA800 computers as well as a number of smaller scale table top analog computers, all being interconnected to form a single very large scale machine. It is quite impressive that it was possible to implement a realistic flight simulator controlling a hydraulic hexapod with a cockpit mounted on its top in 1960 using this approach, something digital computers needed many years to actually compete with.

At the same time this picture clearly shows how cumbersome programming these systems was back then. The patch panels are buried under heaps of patch cables connecting hundreds of computing elements with each other. Changes to such a complicated setup often required hours or even days and sometimes weeks of preparation and actual implementation. Changing parameters of a program required manually changing hundreds of precision 10-turn potentiometers, 300 of which are visible on the three large systems on the left in the figure with many more on the smaller machines on the right. A detailed history of analog computers can be found in [7].
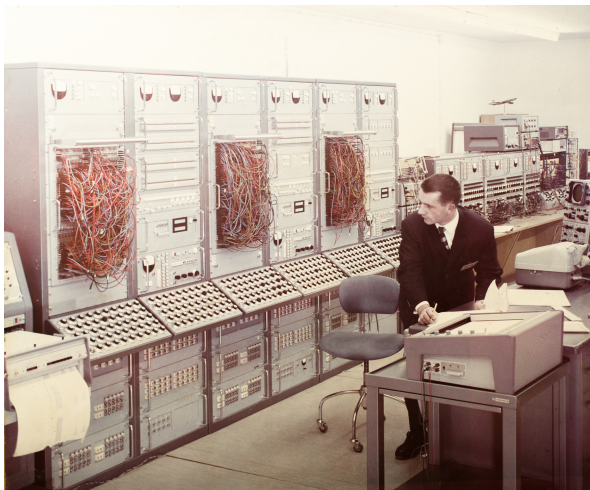
12

Figure 5. Classic large scale analog computer installation

VI. Areas of application

There is a wide variety of applications for modern analog computers. The most prominent of which are the implementation of artificial neural networks by means of analog electronic implementations of neurons, and high performance computing with applications such as molecular dynamics, computational fluid dynamics, Monte-Carlo simulations as often used in financial mathematics, optimisation tasks, and many more. These fields can benefit most from the high computational power of analog computers with their high energy efficiency in second place.

Another large application area where the high energy efficiency is of utmost importance are medical applications such as cardiac and brain pacemakers, blood sugar sensing and insulin pump control, in vivo instrumentation for cancer therapy, and many more. In some specialised applications it might be possible to power the implant by energy harvesting thus alleviating the need for bulky and inconvenient energy storage solutions, much to the benefit of the patient.

Since an analog computer does not execute an algorithm and has no traditional memory containing instructions or the like it is not prone to classic attack vectors, making it a worthwhile option for process control in critical environments and the like.

Used for signal processing, analog computers can perform trigger word detection for smart devices, vibration analysis, and other tasks for predictive and preventive maintenance, etc.

VII. Modern technology

Today, the main drawbacks of these classic systems can be overcome using modern CMOS technology. The patch panel is a thing of the past and belongs in a museum. Modern analog computers will be fully reconfigurable using large switch matrices (*crossbar switches*) under the control of an attached digital computer. Also the manual potentiometers have long since been replaced by digital potentiometers or multiplying DACs allowing the digital computer to change parameters in microseconds.

In addition to this, modern implementations of analog computers will offer much higher bandwidth computing elements, thereby allowing for much shorter solution times. Combined with automatic reconfiguration and reparametrisation this will make it possible to use an analog computer in a time-sharing like mode of operation.

One central problem that must be addressed in order to get widespread acceptance for analog and hybrid computing is the necessity of an abstract programming language, a *domain specific language* (*DSL*), that must hide most if not all of the underlying physical principles the analog computer relies on. The reason for this is the fact that programming analog computers requires a completely different mindset to writing an algorithm. Since the majority of programmers and IT professionals are trained to work in the algorithmic domain, the impedance mismatch between this approach and that of specifying the interconnection of individual computing elements must be minimised.

Furthermore, it is not that simple to tightly couple an analog computer with a digital system, especially since the analog computer offers solution times in the sub-microsecond range. This requires very short interrupt latencies on the digital computer so that it can keep up with its analog co-processor without forcing it to idle most of the time waiting for some interrupt to be processed.

VIII. Modern developments

This section gives a quick overview over recent developments in the field of analog and hybrid computing including academic and commercial projects.

Terminating a long hiatus in the field of analog computing, Glenn E. R. Cowan developed and implemented a reconfigurable analog computer on a VLSI chip in 2005 [9]. Its development showed the basic feasibility of CMOS based analog computers. This was then followed by an enhanced VLSI analog computer chip developed and implemented by Ning Gou in 2016 [10]. Unfortunately neither of these academic projects resulted in commercial developments. The bandwidth of the computing elements was rather limited with sometimes large phase shifts caused by the interconnect matrices. Also the software support was quite limited.

An early commercial development was due to *anadigm®* who developed and market *FPAAs* (*Field Programmable Analog Arrays*) consisting of a number of *Configurable Analog Block*s (*CAB*s) and a number of input/output interfaces. These can be used to imple-

ment a variety of signal pre- and postprocessing tasks such as filters, general audio signal conditioning, etc.[4]

Aspinity has developed two major technologies: The *RAMP*™[5] *Technology Platform*, a programmable analog neuromorphic processor, and the *AnalogML*™*Core*, a machine learning co-processor. Typical applications are trigger word detection for smart devices, glass break detection, acoustic event detection, and vibration monitoring. Due to the high energy-efficiency these devices can be applied in always-on sensing applications.

Another startup working towards analog computing for artificial intelligence is *Mythic* (https://mythic.ai/). They pioneer a *compute-in-memory* approach where memory cells are implemented as variable resistors in the form of flash memory cells. A matrix of such cells can perform typical operations of linear algebra by employing KIRCHHOFF's law, being fed row wise by DACs with ADCs reading out the results of the implicit additions and multiplications performed by the resistor array.

IBM, too, has developed an analog AI accelerator, which was unveiled in 2022.[6] It uses *Resistive RAM* (*ReRAM*) made from *Phase Change Memory* (*PCM*) cells the state of which is switched between an amorphous and a crystalline state. This experimental chip implements $35 \cdot 10^6$ such PCM cells.

A very interesting development is the implementation of artificial neural networks in a true three-dimensional topology. Stacking of chips has been done for many years in the digital domain but is inherently limited in its extent due to the high power consumption and the problems of removing the excess heat from such a stack of chips. The very high energy-efficiency of analog computing approaches will make large scale three-dimensional topologies feasible.[7]

One might ask about the application of Memristors as they are often mentioned being "ideal" devices for implementing synaptic weights in analog neural networks, etc.[8] It may be doubted that Memristors based on filament conduction would be a good choice for implementing synaptic weights due to their typically limited number of state changes as well as the necessity for a device forming period prior to their actual use in a circuit. Approaches to Memristors not relying on filament conduction are relatively new and seem to have not yet matured into integration-ready devices on a large scale. However, using Memristors in analog artificial neural networks might be interesting as they

might be able to implement self-learning systems based on assumptions such as "fire together, wire together".

Apart from these rather specialised and mostly AI centric analog computing applications and approaches, there is another startup, *anabrid* GmbH, based in Germany[9] pursuing general purpose analog computing with the ultimate goal of designing, implementing, and marketing a reconfigurable large-scale integrated analog processor. This device will act as a co-processor offloading compute intensive tasks from a classic digital processor but without being restricted to a narrow field of application, which is in contrast to the aforementioned developments.

Analog computing like quantum computing comes with the challenge that programming such machines is completely different to the classic algorithmic approach taught in schools and universities. Especially professional programmers have lots of difficulties adapting to a different computational paradigm like that of an analog computer. To bridge this gap at least two things are required: First, a cheap analog computer aimed at the educational market, at hobbyists, etc. Second, an abstract domain specific programming language which allows the seemless integration of analog co-processors into current digital computer systems. Ideally, a programmer should not have to think about the actual implementation of an analog computer or of intricacies such as scaling and the like.

Figure 6 shows *THE ANALOG THING*, an open hardware project[10] aimed at the educational market. This little analog computer contains enough computing elements for serious experiments in analog computing and can be easily interfaced to a digital computer, thus forming a hybrid computer.[11] It contains five integrators, four summers, four sign-inverters, two multipliers, two comparators, and eight manual coefficient potentiometers. Of this system more than 1000 have already been ordered showing a strong interest in analog computing in and for the 21ST century.

IX. CONCLUSION

It may be concluded that analog computing is making a comeback and will stay with us in the future. Analog computers, ranging from specialised devices to general purpose co-processors will substantially transform the way we compute in general. The following years will see huge leaps in analog computer implementations catching up with the developments in the digital domain during the last decades, eventually surpassing our classic computers for certain areas of application.

---

[4]A nice signal processing board based on such an FPAA was developed and is sold by NICOLAS STEVEN MILLER (https://zrna.org). These boards can be easily configured using a Python client.

[5]*Reconfigurable Analog Modular Processor*

[6]https://research.ibm.com/blog/the-hardware-behind-analog-ai

[7]See https://research.ibm.com/blog/vlsi-hardware-roadmap.

[8]ReRAM cells are typically not considered being Memristors due to their rather different behavior.

[9]The author is one of the founders of anabrid GmbH.

[10]See https://the-analog-thing.org and https://github.com/anabrid/the-analog-thing for schematics etc.

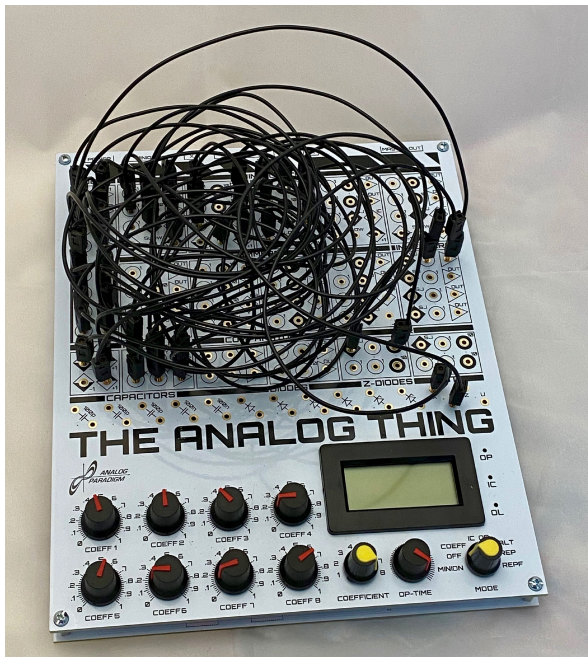[11]See https://the-analog-thing.org/wiki/Hybrid_Computer

Figure 6. THE ANALOG THING

Bernd Ulmann Bernd Ulmann is co-founder of anabrid GmbH and professor for business computer science at FOM University of Applied Sciences for Economics and Management. He studied mathematics with a minor in philosophy at the Johannes Gutenberg university Mainz. His main interests are analog and hybrid computing and the simulation of dynamic systems. He also collects and restores classic analog computers and has a soft spot for chaotic systems and their implementation on analog computers.

REFERENCES

[1] UK Parliament Post, "Energy Consumption of ICT", in *POST-NOTE*, Number 677, September 2022

[2] GENE M. AMDAHL, "Validity of the Single Processor Approach to Achieving Large-Scale Computing Capabilities", in *AFIPS Conference Proceedings*, 30, doi:10.1145/1465482.1465560, pp. 483–485

[3] JOHN L. GUSTAFSON, "Reevaluating Amdahl's law", in *Communications of the ACM*, Vol. 31, Issue 5, doi:10.1145/42411.42415, pp. 532–533

[4] JEFFREY CHOU, SURAJ BRAMHAVAR, SIDDHARTHA GHOSH, WILLIAM HERZOG, "Analog Coupled Oscillator Based Weighted Ising Machine", in *Scientific Reports, nature research*, 15 October 2019

[5] MOHAMMAD KHAIRUL BASHAR, ANTIK MALLICK, DANIEL S. TRUESDELL, BENTON H. CALHOUN, SIDDARTH JOSHI, NIKHIL SHUKLA, "Experimental Demonstration of a Reconfigurable Coupled Oscillator Platform to Solve the Max-Cut Problem", in *IEEE Journal on Exploratory Solid-State Computation Devices and Circuits*, 23 September 2020, pp. 116-121

[6] Sir WILLIAM THOMSON, "Mechanical Integration of linear differential equations of the second order with variable coefficients", in *Proceedings of the Royal Society*, Volume 24, No. 167, 1876, pp. 269–270,

[7] BERND ULMANN, *Analog Computing*, 2nd edition, DeGruyter, 2023

[8] BERND ULMANN, *Analog and hybrid computer programming*, DeGruyter, 2nd edition, 2023

[9] GLENN EDWARD RUSSELL COWAN, *A VLSI Analog Computer / Math Co-processor for a Digital Computer*, Columbia University, 2005

[10] N. GUO, Y. HUANG, T. MAI, S. PATIL, C. CAO, M. SEOK, S. SETHUMADHAVAN, and Y. TSIVIDIS, "Energy-Efficient Hybrid Analog/Digital Approximate Computation in Continuous Time", in *IEEE Journal of Solid-State Circuits*, vol. 51, no. 7, pp. 1514-1524, July 2016

HOCHSCHULE
RAVENSBURG-WEINGARTEN
UNIVERSITY
OF APPLIED SCIENCES

Evaluating encryption methods for the JTAG-debug port

Soham Sanjay Dekhane, Andreas Siggelkow

Abstract—Debug ports are one of the most important tools for designing, debugging, configuring and programming, however, they can be very vulnerable to a hacker with malicious intent. This project describes one of the many possible solutions to secure this debug port with the help of hardware based cybersecurity. This solution is demonstrated by designing a Pseudo-Random-Number-Generator (PRNG) using VHDL implemented on an FPGA and the seed exchange secured using the RSA algorithm.

Index Terms—FPGA, RSA, PRNG, VHDL, LFSR, Cryptography, JTAG, Debug

I. INTRODUCTION

Cyber threats present enormous risks to individuals, businesses, and even entire nations in today's connected world. Hardware cryptography is a vital defense against these threats. Strong key management and strong authentication are provided by cryptographic hardware modules. Only authorized individuals can access sensitive information and vital systems because of these hardware-based cryptographic solutions. Individuals and organizations can reduce the danger of unauthorized access, data leakage, and other criminal activity by utilizing hardware cryptography. Encryption is used in almost everyday life right from opening garage doors to credit cards. For such encryptions or cryptographic operations, generation of unique, random and secure keys is very important. Debug ports can be extremely helpful in designing embedded systems but they present a huge vulnerability. A hacker with malicious intent can get physical access of the system using this debug port can cause a huge damage. The obvious solution is securing the debug port by limiting the access to it by implementing some encryption algorithm. Hardware based cybersecurity; i.e. integrating cybersecurity measures in the processing unit of the embedded system itself can provide with various advantages; the biggest being that it is not at all vulnerable to cyber attacks unless the attacker has physical access to the hardware. In order to demonstrate such an example, this project focuses on designing a cryptographically secure Pseudo-Random-Number-Generator encrypting it using the RSA algorithm. Pseudo-Random-Number-Generators (PRNGs) are used for various applications

Soham Sanjay Dekhane, sohamdekhane@gmail.com, Andreas Siggelkow, andreas.siggelkow@rwu.de. Hochschule Ravensburg-Weingarten, Doggenriedstraße, 88250 Weingarten.

like Key Generation, Initialization Vectors, Nonces etc. This makes the output generated by this PRNGs very crucial. A perfect PRNG should have three main attributes: Integrity (prevent undesired modification to the output), Authenticity (allow access only to authentic users) and Confidentiality (prevent secrets from becoming known to the attackers). One has to make sure that the PRNG output is not illegally disturbed i.e. the random output of a PRNG should not become non-random/predictable. A PRNG could be vulnerable to plethora of cyber attacks such as Algebraic attack, State recovery attack, Clock attack etc. Implementing these attacks makes sure that the output of the PRNG could be predicated or tampered with by the attacker. The PRNG should be initialized using a seed value which will be fed to the PRNG via the debug port. This seed value should be first encrypted and then sent to the Device-under-Test (DUT) using the JTAG interface. This seed value is then decrypted in the DUT, the output of the PRNG is generated, encrypted and sent back to the debug interface via JTAG. This is done so as to secure the generated output of the PRNG during the exchange via the debug interface during which it is the most vulnerable. The data does not have to be secured for operations within the DUT but only during the exchange via the debug interface. The hardware consists of a MAX10 FPGA in which the PRNG as well as the encryption algorithm are implemented using VHDL.

II. PSEUDO-RANDOM-NUMBER-GENERATOR

A device used to generate a sequence of random numbers or symbols is called as a Random Number Generator. Random numbers have been historically used in many applications ranging from Cryptography, Simulations, Machine Learning Algorithms, Computing Applications etc. There are various methods and algorithms used to generate random numbers. The generators are called as Random Number generators as the symbols or numbers generated by them have no mathematical or statistical relation amongst the generated sequence of numbers. Once such random number generator is a Pseudo-Random-Number-Generator (PRNG). A PRNG is designed using a deterministic algorithm to produce the sequence of numbers. These generated sequences pass all the "Statistical pattern tests for Randomness" but can easily be predicted

once the seed value (initial condition) or the algorithm used to generate the PRNG is known. Hence the term "Pseudo" is used. A PRNG at best can generate a total of $(2^n - 1)$ number of random numbers and the same sequence then repeats itself. There are various algorithms used to build the PRNG namely: Xorshift, Inversive congruential generator, ISAAC (cipher) (indirection, shift, accumulate, add, and count), Blum Blum Shub, Multiply with carry, Lagged Fibonacci Generator, Linear Feedback Shift Register, Mersenne Twister, Linear congruential generator and the Well Equidistributed Long-period Linear. In this project, the Linear Feedback Shift register (LFSR) algorithm is used for designing the PRNG. For designing a PRNG, a seed value i.e. an initial condition has to be specified from which the next sequences of the random numbers are generated. This seed value determines the length of the PRNG (i.e. the total number of random symbols or sequences generated before the pattern is repeated). As discussed before, the maximum possible length of a PRNG is $(2^n - 1)$; n being the number of bits of the seed value. A seed value of Hamming Weigth of $n/2$ is usually desired, n being the total number of bits in the seed value. Taps are also set up at desired bits. The bit values where the taps are located are XORed and the result of this XOR is placed at the $(n-1)^{th}$ bit, the rest of the bits are shifted to the right, and the 0th bit is discarded or vice versa. PRNGs are vulnerable to various types of cyber attacks such as:

- Brute Force Attack: The attacker tries every possible seed value and checks if the observed sequence of numbers is obtained or not.
- Algebraic Attack: The output sequence of the LFSR can be described by a set of equations that an attacker can discover using algebraic methods. As a result, the attacker may be able to figure out the seed value and forecast future results.
- State Recovery Attack: If the attacker is aware of the previous results of the PRNG, they can predict the current as well as the future values of the PRNG.
- Clock Attack: The attacker forces the clock to skip or repeat certain states of the PRNG which will allow him to predict the future values of the PRNG.
- Side-Channel Attack: The attacker can use the leaked values of the electromagnetic emissions or the power consumption from the PRNG to determine the future values of the PRNG.
- Non-Linear Feedback Attack: An attacker could be able to create a set of equations that describe the LFSR's output sequence if it uses non-linear feedback. As a result, the attacker may be able to figure out the seed value and predict future results.
- Known Plaintext Attack: An attacker may be able to detect the state of the LFSR and anticipate future outputs if they have access to some of the

plaintext that was used to generate the pseudorandom sequence.
- Birthday Attack: An attacker might be able to perform a birthday attack to find collisions in the key space and recover the key if the LFSR is being used to create cryptographic keys.

III. THE RSA ALGORITHM

To encrypt the data during exchange or during debug, the RSA algorithm is implemented. RSA is the most well known Public Key Encryption method. It was developed by Ron Rivest, Leonard Adleman and Adi Samir in 1977 and is a type of asymmetric encryption method. Using such an algorithm is very advantageous as a key pair is always generated i.e. a public key and a private key. The public key is used for the encryption of the data while the private key which is used for decryption is kept a secret. The private key cannot be determined by using the public key and hence it can be distributed freely or even be published on websites. This is a pretty huge advantage of using asymmetric encryption method over a symmetric encryption method where the same key is used to encrypt and decrypt the data. The following steps illustrate the generation of the key for the RSA algorithm:

1) Select two distinct prime numbers; Assume they are p and q.
2) Compute their product "n" such that $n = p \cdot q$.
3) Calculate the Euler's totient function $\varphi(n) = (p-1) \cdot (q-1)$.
4) Select an "e" such that $0 < e < [\varphi(n)]$ and e & $\varphi(n)$ are coprime i.e $gcd(e, \varphi(n) = 1)$.
5) Calculate a "d" such that $d \mod \varphi(n) = 1$
6) (n, e) is the public key and is used for encryption while (n, d) is the private key and is used for decryption.

Once the public and private keys are calculated, the messages can be encrypted and decrypted as follows: Let x be the data and y be the encrypted data. Then, the encryption is done as $y = x^e \mod n$ while the decryption is done as $x = y^d \mod n$. Usually, x, y, n and d are 1024 bit or more. Security level of 80 bit is offered by RSA when 1024 bit keys are used while a security level of 128 bit is offered by RSA when 3072 bit keys are used. The RSA algorithm is vulnerable to cyber attacks as well. By knowing the product "n", attackers can try to factorize the product and try to find out the prime numbers p and q. This type of cyber attack is known as a factorization attack. Currently, it is believed that it will be possible to factor 1024 bit values within the next 10 to 15 years, and that intelligence agencies will likely be able to do it even sooner [1]. To minimize the risk of such an attack, it is recommended to choose the RSA parameters of 2048-4096 bits. The RSA algorithm is also vulnerable to Side-Channel attacks but for such an attack, the
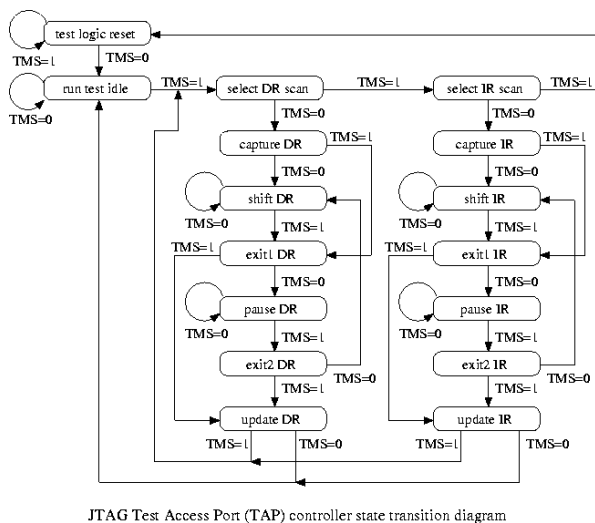
Figure 1. TAP-FSM

Figure 2. JTAG data register

Figure 3. ARM7 wrapped by JTAG data registers

Figure 4. 16 bit PRNG

attacker must have access to the RSA implementation. Attackers try to find leaked information about the private key through the timing behaviour or power consumption.

IV. JTAG

Almost all digital systems have a debug interface [2] with different possibilities to attack the system [3]. This debug logic connects all sub-blocks in the system by means of a shadow bus system in order to test or debug it. This could act as a back door which is not secured. To equip this back door and all connection points of the debug bus with a lock, is the focus of the system introduced in the following. It is just the base system for different cypher/debug pairs, it is the base of a system evaluation.The lock can be a cypher system. Parallel to the debug problem is the update over the air possibility in such systems, especially modern cars and IoT. Also this back door can be secured by cyphering. An emulator of this kind has been presented in [4].

The back door itself is the well known JTAG (Joint Test Action Group) port [5]. The element, which accesses all logic on chip is the JTAG port together with the test access port (TAP) controller. The TAP-Controller is implemented as a finite-state-machine (Figure 1).

The signal timing is defined as follows: The **test mode select (TMS)** will be captured with every rising edge of **test clock (TCK)**. Also **test data in (TDI)** will be taken with the rising edge of TCK. Contrary to this, **test data out (TDO)** will be driven with the falling edge of TCK. So, the wiring to a second chip, which receives the output of the actual SoC, could be allowed a delay of one half of the period of TCK.

The FSM has 16 states. Two general states (test logic reset and run test idle) and seven states for the instruction register and seven for the data register. Changing from one state to the other, it is required to
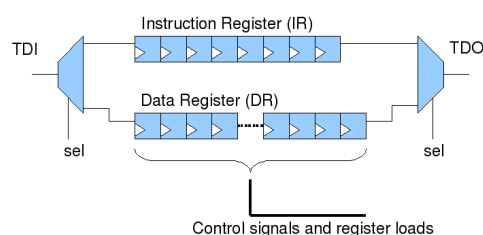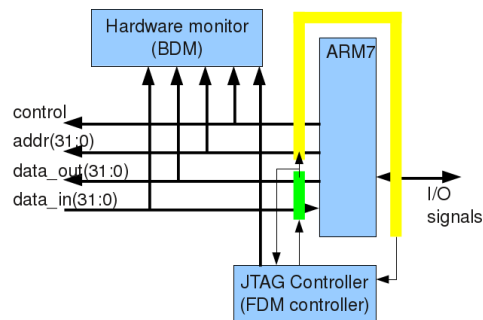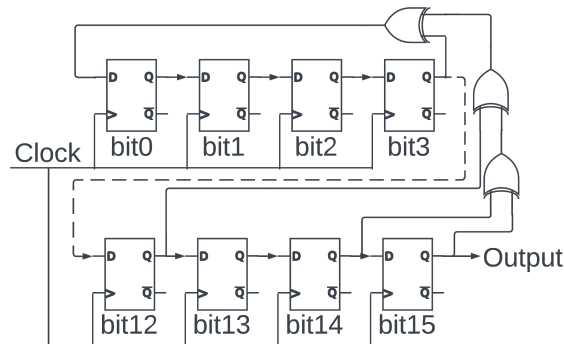
change TMS with the rising edge of TCK according to the diagram (Figure 1). According to the IEEE specification many tests will be predefined but for the debug purpose, the data register (Figure 2) is the important element. With the data register every design element in the system-on-chip (SoC) can be encapsulated (all inputs can be read and written, all outputs can be read and written) and is under total control of the TAP controller (Figure 3). Additionally, all flip-flops in the design are chained up to the so called scan chain, which is also a JTAG data register.

This is needed for debugging a SoC, but is obviously also a serious security threat.

To solve this security problem, different cypher methods on the data stream (TDI to TDO) will be researched.

V. Implementation

A. PRNG

The Pseudo-Random-Number-Generator is designed such that it produces 16 bit pseudo random number sequences by taking a seed value to initialize the sequence and XORing the bits of the last output by placing taps at certain bits. When the VHDL program is reset, the first input is taken as the seed which is taken through the testbench and that would be the first output produced by the PRNG. The 16 bit seed is carefully chosen keeping the Hamming weight of the seed as 8 in order to get a proper sequence of outputs. Taps are then placed at bits 4, 13, 15 and 16 i.e. from the previous output, the bit are positions 4, 13, 15 and 16 are XORed, the most significant bit from the previous out is removed, the remaining bits are shifted to the left and the result of XOR is placed at the position of the least significant bit. This 16 bit number will be the new output of the PRNG. As this is a 16 bit PRNG, we will have such $(2^{16} - 1)$ i.e. 65535 unique pseudo random outputs. As mentioned in this paper previously, these outputs can be used for applications like Key Generation, Initialization Vectors, Nonces etc. and hence need to be secured during the debug phase.

B. Encryption during the debug phase

The debug phase for a PRNG is the most critical phase and also the most vulnerable at the same time. The seed exchange as well as the exchange of the outputs is done between the test interface and the DUT over the debug interface. During this exchange, both the seed and the generated outputs are vulnerable to a hacker with malicious intent. To prevent this, in this project, the seed value and the generated outputs are secured using the RSA algorithm. For the RSA algorithm, a set of 64 bit public and private keys are generated. The seed value is first encrypted using the public key in the the testbench itself and transmitted over the debug interface to the DUT. This is then decrypted in the DUT using the private key and then given as an input to the PRNG. This is then processed by the PRNG and the output that is to be transmitted is again encrypted using the public key and transmitted over the debug interface.

VI. Conclusion and Future Work

In this project, the first steps have been taken to securing the debug interface. It has been demonstrated how the seed exchange over the debug interface can be encrypted in order to secure the leak of information due to a potential cyber attack. Further steps would include integrating a JTAG Tap controller with the PRNG and test the encryption using an ASIC tester. The complete ecosytem for the RSA algorithm also needs to be created such as a public key and private key infrastructure including a database for the keys that can be used for encryption and decryption purposes.

References

[1] Christof Paar and Jan Pelzl. *Understanding Cryptography*. Springer, 2010. ISBN: 978-3-642-04101-3.

[2] C.F. Kao and H.M. Chen. *Hardware-Software Approaches to In-Circuit Emulation for Embedded Processors*. IEEE Design and Test, 25 (5): 462 - 477, 2008.

[3] Swarup Bhunia, Sandip Ray, and Susmita Sur-Kolay (Editors). *Fundamentals of IP and SoC Security: Design, Verification, and Debug*. Springer, Cham, Switzerland, 2017. ISBN: 978-3-319-50055-3.

[4] Gregor Benz and Andreas Siggelkow. *Implementation of a GPS and GSM module into a Zynq Z7 SoC based emulator tracking system*. Workshop der Multiprojekt-Chip-Gruppe Baden-Württemberg, 2020.

[5] *IEEE Standard for Test Access Port and Boundary-Scan Architecture*. IEEE Std 1149.1-2013 (Revision of IEEE Std 1149.1-2001), pp.1-444, 2013. ISBN: doi: 10.1109/IEEESTD.2013.6515989.

Soham Sanjay Dekhane received his B.Tech. degree in Electronics and Telecommunication Engineering from Symbiosis International (Deemed) University, India in July 2021. Since September 2021, he is pursuing his Master's degree in Electrical Engineering and Embedded Systems at Hochschule Ravensburg-Weingarten.

Andreas Siggelkow received the academic degree Dipl. -Ing. in 1988 from the University of Karlsruhe. In 1996, he obtained his doctorate at the University of Stuttgart for Dr. -Ing. From 1996 to 2007 he worked for Infineon on specifications for base-band processor ASICs. Since 2007, he is a professor for ASIC-Design and Computer Architecture at the Hochschule Ravensburg-Weingarten.

On the Influence of Line Routing and EMC Noise Sources on high-speed Data Transmission and Signal Integrity

Lennart Stark, Michael Engelbrecht, Bernhard M. Rieß

Abstract—The aim of this work was to investigate the effect of routing on signal transmission on printed circuit boards in the frequency range of up to 16 GT/s. For this purpose, various boards with different attributes were designed, manufactured and evaluated. In particular, the effects of single and multiple vias, X-vias, microstrip lines, and plane coupling on data transfer were analyzed. Moreover, the effect of interfering signals on the maximum data rate was investigated. For our investigations we use Peripheral Component Interconnect Express, a well-known and frequently used high-speed serial computer expansion bus standard. The examinations include simple benchmarks with regard to the effective data throughput as well as measurement of the signal integrity with an oscilloscope. In total, the eye pattern during signal transmission was measured on ten boards with respect to eye width and eye height. Our results show that modern signal transmission technologies are very mature and robust, and that routing has a surprisingly small influence. Nevertheless, the goal in PCB design should still be a high quality layout, taking best practice routing rules into account.

Index Terms—Printed Circuit Boards, Signal Routing, Data Transmission, Signal Integrity, Interference, Vias, Microstrips, Plane Coupling, Noise, Eye Pattern, PCIe

I. INTRODUCTION

In the automotive industry, analog and power but also high-performance components are widely used to evaluate and process incoming data from sensors like cameras, radar, and lidar. This generates extremely large amounts of data for which very powerful hardware is required. For processing, the data is forwarded to servers via various interfaces on the internet and stored on local SSD hard drives. Due to the high data throughput required for processing data in deep neural networks, corresponding powerful interfaces are needed. Many devices currently rely on the use of Peripheral Component Interconnect Express (PCIe) Gen 4 [1], a serial interface that can also be extended in parallel from an architectural point of view. The individual serial connections are called lanes and work independently of each other. A lane consists of a differential line pair. The gross data throughput of

such a lane is up to $16\,\mathrm{GT/s}$, that is, 16 billion bits transmitted in one second. This results in an effective data throughput of roughly $1.8\,\mathrm{GB/s}$. Since one piece of information is transmitted with each clock edge, the effective frequency is $8\,\mathrm{GHz}$. Therefore, the system can only be examined in consideration of line theory, and the laws related to waves apply [2]. Furthermore, this results in various requirements that apply to the development of suitable printed circuit boards (PCBs). Wave properties must also be taken into account in terms of measurement technology, since any measurement influences the signal to be measured [3]. Moreover, the transmission of ideally rectangular, digital signals results in various harmonics. These are subject to strong damping, for example, in the case of impedance jumps. The measurement difficulty then is that the harmonics must also be measured correctly in order to represent the signal correctly. This requires a measurement technique with very high time resolution (sample rate), and measurement adapters and cables that do not attenuate the signal too strongly [4]. In the following, the aim is to understand and describe the physical conditions. We will derive corresponding rules, based on the specifications, for physical implementation, which will then be examined in various specific cases of use.

II. FUNDAMENTALS

This Chapter covers the relevant basics that are required for the analysis and measurements of this work. In Chapter II-A, transmission lines are examined with a focus on the telegraph equation (1). Next, the properties in the very high frequency range are considered, and finally the model is extended to a three-wire system, as it is used in practice for differential (balanced) lines on PCBs. Chapter II-B then addresses the problems and challenges in applications. Assumptions regarding the development of PCBs will be examined and discussed in Chapter II-C.

A. Transmission Line

1) Real Lines and Wave Impedance: In theory, a wire establishes an electrical connection between two points. For most simple electrical circuits, this model is quite sufficient. To complete an electric circuit, a

Lennart Stark, lennart.stark.xr@renesas.com, Michael Engelbrecht, michael.engelbrecht@renesas.com, Renesas Electronics Germany GmbH, Düsseldorf, Germany.

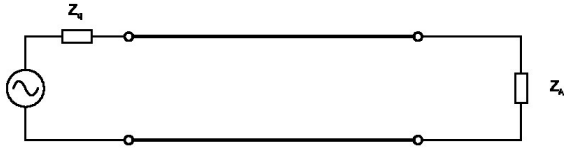Bernhard Rieß, bernhard.riess@hs-duesseldorf.de, University of Applied Sciences Düsseldorf, Germany.

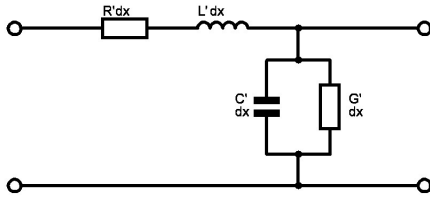Figure 1. Ideal electric connection.

Figure 2. Equivalent circuit diagram of a real line [6].

Figure 3. Cross section of a microstrip line [6] [7].

forward and a return conductor are needed. This is shown in Figure 1.

Now we begin to differentiate between ideal connections and real lines. First, we will look in detail at the line segment shown in bold in Figure 1. It is obvious that a line has an ohmic resistance, comparable to the filament of a light bulb. Accordingly, losses and thus a voltage drop occur on a line. They depend primarily on three factors: The length of the cable, the cross-section of the cable, and the specific conductivity of the material used. Furthermore, the conductance of the insulator between the lines is subject to the same dependencies as the specific line resistance. With a DC application we could end our investigations here, but this is not the case with RF transmission lines.

Figure 2, for example, shows that there is an - admittedly small - capacitor between two lines. Accordingly, a pair of lines has shunt self capacitance which, in addition to the ohmic properties of a conductor, also leads to a change in the signal depending on the frequency. With PCBs, there is no analytical method to determine these. This is due to the geometric shape of the conductor lines [5] [6]. Finally, there is a less descriptive property in this model: The series inductance of a line. To make this tangible, we imagine a line as an unwound coil. The self inductance is not lost in the physical model of a coil either.

In order to keep these different properties manageable for technical applications, wave impedance Z_l is introduced to model the equivalent circuit shown in Figure 2. It is calculated according to the Telegraph Equation (1). The apostrophes illustrate that we are not dealing with discrete components, but with conduction properties.

$$Z_l = \sqrt{\frac{R' + j\omega L'}{G' + j\omega C'}} \qquad (1)$$
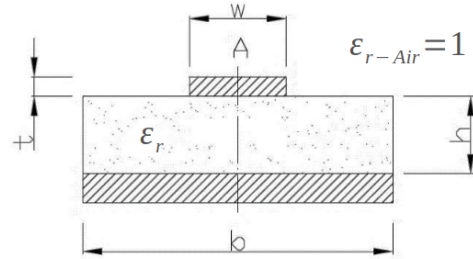
Wave impedance facilitates the calculation of high-frequency signals. Even if the skin effect increases the series resistance as the frequency increases, the real-value series resistances are so small that they are negligible. The same holds for the shunt conductance: At a sufficiently high frequency, it is negligible. Thus, Equation (1) can be simplified as follows:

$$Z_l \approx \sqrt{\frac{L'}{C'}} \qquad (2)$$

If the wave impedance changes from one section of the line to another, this leads to reflections. That results in a loss of wave energy and therefore also to an attenuation of the signal. The reflection factor r can be calculated according to Equation (3).

$$r = \frac{Z_{l2} - Z_{l1}}{Z_{l2} + Z_{l1}} \qquad (3)$$

2) Transverse Electromagnetic Modes and Waveguide Properties: We will now focus in greater detail on the wave properties. Signals with a sufficiently high frequency only need to be considered on the basis of their wave properties. An ideal, lossless wave that travels only with transverse amplitudes in the direction of propagation is generally called a transverse electromagnetic mode (TEM) or TEM wave in the context of propagation. Thus, a guided, progressive wave is formed between two conductors. In the strict physical sense, such a wave does not exist, since each conductor has losses and therefore the voltage drops by a very small amount. However, this effect is so small that further treatment takes place at an ideal wave. Classic examples of such two-wire lines are parallel lines (twisted pair), coaxial lines and microstrip lines. The latter can be easily and cheaply implemented on PCBs and therefore enjoy very frequent use.

As shown in Figure 3 it is important that the width b of the ground plane is considerably wider than the width w of the microstrip. Furthermore, the height of the trace is described by t and the thickness of the insulator with the dielectric constant ϵ_r by h. However, the entire conductor is not surrounded by a shield as would be the case with a coaxial cable, for example. The electromagnetic field propagates differently
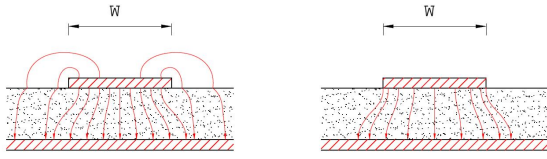
Figure 4. The electric field of the microstrip line at low (left) and high frequencies (right) [6] [7].

Figure 5. Cross-section of a coplanar waveguide [10] [7].

depending on the frequency, which also leads to a change in the conductor track impedance. Therefore, it is a great challenge to apply microstrip lines for a wide frequency range [7]. Figure 4 shows that the electromagnetic field does not propagate in a constant dielectric but in a layered dielectric consisting of air and substrate, the dielectric constant values of which differ from each other.

As a result, the behavior is described by an effective dielectric constant $\epsilon_{r,eff}$, which can be calculated according to [7] [2] [3] [8]:

$$\epsilon_{r,eff} = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2} \cdot \left(\frac{1}{\sqrt{1 + 12(h/w)}}\right) \quad (4)$$

There are three main factors that characterize the impedance Z_l of a line: First, the effective dielectric constant $\epsilon_{r,eff}$ calculated with Equation (4). Second, the width of the microstrip w and third, the height of the dielectric h. Depending on the ratio between width and height, the dependencies as stated in Equation (5) arise [7].

$$Z_l = \begin{cases} \frac{Z_0}{2\Pi\sqrt{\epsilon_{r,eff}}} \ln\left(8\frac{h}{w} + \frac{w}{4h}\right) & \text{when } \frac{h}{w} \leq 1 \\ \frac{Z_0}{\sqrt{\epsilon_{r,eff}}[\frac{w}{h} + 1.393 + 0.667\ln(\frac{w}{h} + 1.444)]} & \\ & \text{when } \frac{h}{w} \geq 1 \end{cases}$$

$$(5)$$

However, it should be noted that this is not an analytical calculation of the impedance but only an approximation. Influencing factors arising from manufacturing can only be taken into account to a limited extent. For example, manufacturing techniques may result in the microstrip no longer being rectangular but being given a V-shape, for example, due to under-etching. Wave impedance can be tested and measured using a time domain reflectometer (TDR). Here, an edge of known amplitude at the open end of the source is propagated down the line to be tested. Since the wave impedance at the feed is known, the characteristic impedance Z_l can be determined from the reflected signal at the open end. Here v is the injected signal, a the reflected signal and Z_s the impedance of the source [9].
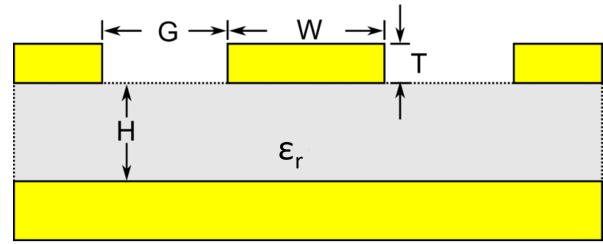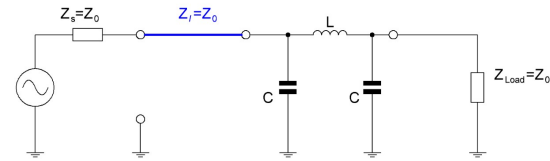

Figure 6. Asymmetric single ended transmission line [6].

$$Z_l = Z_s \frac{a/v}{1 - a/v} \quad (6)$$

3) Differential Signaling: For applications requiring high frequency stability, coplanar waveguides can be used. These are transmission lines having a ground plane on the same layer as the signal line. The signal line is located between the surrounding ground planes and separated by a gap. A ground plane is also located under the substrate and a thin topcoat is applied over the circuit. Such a line is shown in Figure 5. The biggest benefit is good suppression of crosstalk between several microstrip lines [9] [7].

The speed of wave propagation ϑ_p of a TEM wave depends on the effective dielectric constant $\epsilon_{r,eff}$ of the transmitting medium and can be calculated as follows [7]:

$$\vartheta_p = \frac{c_0}{\sqrt{\epsilon_{r,eff}}} \quad (7)$$

We will now consider the previously introduced line as an unbalanced single ended (SE) system, also called a two-wire system. This is because one line always has the ground function and circuits are therefore designed asymmetrically. For example, an unbalanced low-pass filter is shown schematically in Figure 6.

This design is very popular in applications because it is easy to calculate. However, it is subject to some disadvantages, namely that interference has an unbalanced effect on the signal. Therefore, digital applications require signal levels with a sufficiently high amplitude so that the signal can be correctly detected at the line end. Due to the capacitive behavior of a line, a sufficiently strong driver is therefore required. This leads to many other issues; for example, the currents for high frequencies, which are equivalent to high data rates, are associated with high magnetic field strengths,

Hochschule Düsseldorf
University of Applied Sciences

HSD

ON THE INFLUENCE OF LINE ROUTING AND EMC
NOISE SOURCES ON HIGH-SPEED DATA
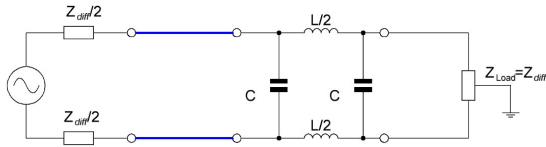TRANSMISSION AND SIGNAL INTEGRITY

Figure 7. Symmetric three wire differential signaling transmission line [6].
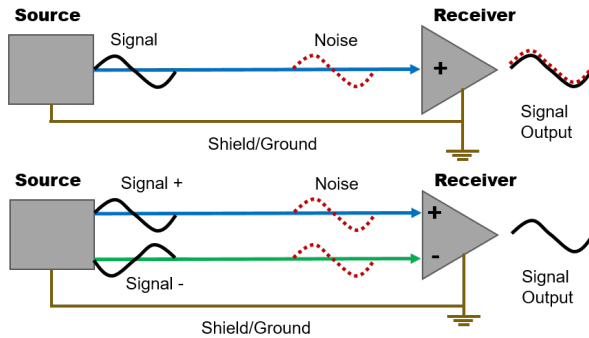
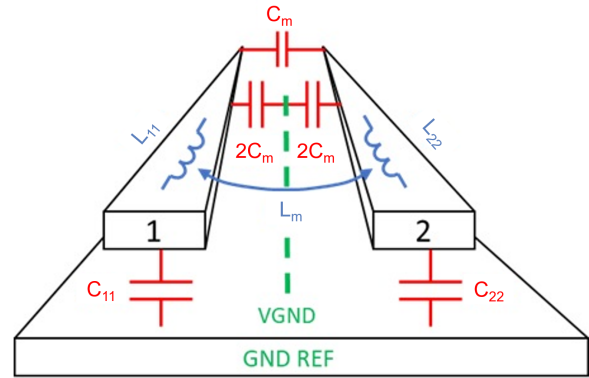Figure 8. Noise on single ended vs. differential transmission line [11].

Figure 9. Pair of microstrip traces showing self-loop inductance (L_{11}, L_{22}), self-capacitance (C_{11}, C_{22}) mutual capacitance (C_m) and mutual inductance (L_m) when line 1 and line 2 are driven differentially [12].

which have a disruptive effect on neighboring circuit parts. In addition, corresponding powerful driver transistors need, correspondingly, more space on the wafer and lead to high heat dissipation. All these problems are avoided by introducing a symmetrical three-wire system. The same filter as in Figure 6 is shown in Figure 7 using a symmetrical three-wire system. The contact in the center of the load resistor represents the reference to the ground potential.

What at first glance looks like a considerably greater amount of extra effort offers several advantages. As can be seen in Figure 8, coupled interference has the same effect on both lines.

While the signal at the top of Figure 8 is superimposed by the noise at the output, this effect disappears in the line shown in the lower part of Figure 8 after both transmitted signals have been subtracted from each other. This enables a reduction in the required voltage swing at which the signal can still correctly be recognized at the receiver. Since the transmitted signals are equal but have opposite polarity, the driver only needs an additional inverter, which does not impose significant extra effort on a chip. Due to the symmetrical design, injected currents induce a counter-current on the complementary line, which again reduces susceptibility to errors as well as emitted radiation. Thus, the cost is only a single additional line, with the condition that both lines have the same length, are close together, and have the same dimensions so that the wave impedances match and no reflections occur [9] [6].

The physical properties as well as the calculation of these are similar to the single ended (SE) line. However, the electromagnetic fields interact with each other due to coupling, which can be described by introducing a virtual ground (VGND). This is illustrated schematically in Figure 9.

The special thing about determining the impedance is that two modes, even and odd, can propagate on a differential pair of lines. The odd mode, in which the signal on both lines has an inverted polarity, is preferred. With the even mode, this is not inverted, which is why the electromagnetic fields interact differently with each other and therefore also have an effect on the differential wave impedance. This results in a new parameter for the SE line, named Z_{odd}. With $L_S = L_{11} = L_{22}$ and $C_S = C_{11} = C_{22}$ the impedance can be calculated according to Equation (8) [12] and Equation (9) [13].

$$Z_{odd} = \sqrt{\frac{L_S - L_M}{(C_S + 2C_M)}} \qquad (8)$$

$$Z_{diff} = 2 \cdot Z_{odd} \qquad (9)$$

As with the microstrip line, there is also an equation to approximate the differential wave impedance. It is based on the dimensions of the line as shown in Figure 10 and is calculated according to Equation (10) [13].

$$Z_{diff} = \frac{174}{\sqrt{\epsilon_r}} ln\left(\frac{5.98 \cdot h}{0.8 \cdot w + t}\right) \cdot (1 - 0.48 \cdot e^{(-0.96\frac{d}{h})}) \qquad (10)$$

B. PCB Construction and Connection Technology

Like a sandwich, a PCB consists of different layers. Conductive layers, where the signal routing is located, are pressed between electrical insulating layers. This way, components that are physically separated from each other can be connected on conductive layers.
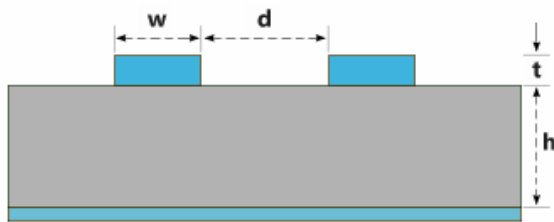
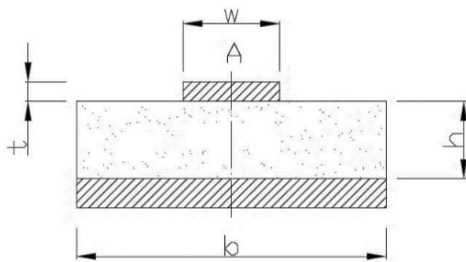Figure 10. Cross section of a differential microstrip [13].

Figure 11. Microvia compared to Plated Through-Hole (PTH) [14].

Figure 12. Via stub [17].

Figure 13. 3W rule (left) and 5W rule (right) horizontal on a PCB.

It makes sense to take a systematic approach here. For example, with two-layer PCBs, it is common to lay only vertical connections on one layer and only horizontal connections on the other. Even components whose lines cross in the circuit diagram can thus be connected to each other. With more complex layer structures, it is possible to bring more structure into the design as well as to implement more technology in physical form.

A typical example is the connection of microcontroller chips. It is common to bring their pins quite close together, which has the distinct advantage of reduced hardware dimensions but requires more complexity in terms of design. Therefore, multi-layer PCBs with more than 4 layers use the inner layers for routing Power Delivery Networks (PDN) and ground. The use of the central ground layer improves signal integrity. Due to the separation in terms of conductivity, the electric field cannot crosstalk from the two outer layers and thus influence the signal path on the opposite line. This is particularly advantageous for signals that operate at high data rates. Connections between different layers are made by drilling a hole which is then plated with copper through a galvanization process. This simplest type is called Plated Through Hole (PTH) shown in Figure 11 on the right. In another process, a laser is used to burn a hole through the outermost prepreg layer, an insulating composite made of a glass fiber mat soaked in synthetic resin, and then electroplated. Such a structure is called microvia and shown in Figure 11 on the left.
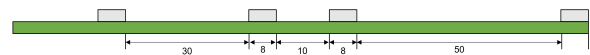
Microvias are more expensive compared to standard vias but offer two advantages: First, they save space, and second, they improve signal integrity for higher frequency signals. This is due to the absence of a stub as shown in Figure 12, which is a loose wire end that causes reflections that impair signal integrity.

Considering signal integrity means that the layout and routing of a signal line from the transmitter to the receiver are implemented in such a way that data transmission quality is maintained. At a data rate of 16 GT/s, the length of the via stub is in the range of 10% of the wavelength, and an impact on the signal is therefore to be expected. With through-hole vias, integrity can be improved further by removing unconnected residual rings on the intermediate layers and setting up a larger area without copper around the pad of the vias, the so-called anti-pad. However, it is not only the vias that have an impact on signal integrity but also the routing. The higher the applied frequency, the more likely it is that kinks in the line should be avoided. Instead, directional changes are accomplished through the curved course of the conductor paths. To avoid crosstalk on neighboring lines, the distance from neighboring lines can be increased. Usually, the $5W$ rule applies, where the next line should be at least five times the conductor width W away. However, it is even better to surround the line with a ground plane that is well connected to the other ground layers. The $3W$ rule, which means a distance between the line and the ground plane of three times the width of the conductor, is sufficient here [1].

When developing a PCB, it may be necessary to route a PDN on a layer neighboring the microstrip line due to space. This is problematic because there is a jump in the wave impedance at this point. This can be compensated by coupling capacitors such as those in Figure 14, which guarantee the correct routing of the return current.
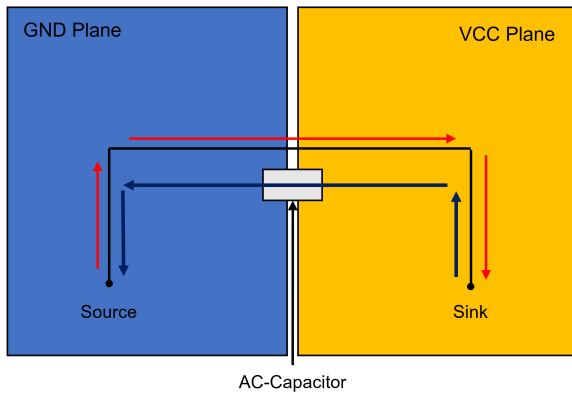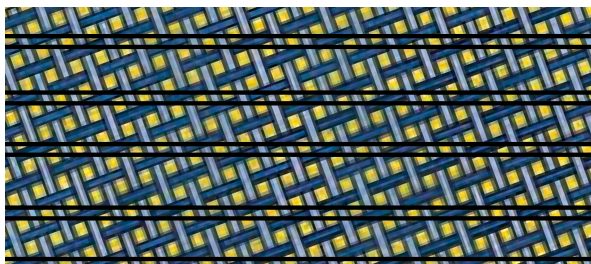
Figure 14. AC-Coupling capacitor.

Figure 15. Rotation of the underlaying PCB fiber weave [15].

Figure 16. Link definition for two components [16].

If a line is routed inside a PCB, it is also called a stripline. This has the advantage that there is even better shielding against interfering signals and better electrical coupling. As described above, the insulating layers are made of a woven glass fiber mat impregnated with epoxy resin. Due to this structure, this material offers no completely homogeneous properties. The glass fiber has a different relative dielectricity to the resin. To avoid any potential problems, either the prepreg can be pressed at a different angle during production or the entire design can be rotated by an angle of 20°, for example, when creating the production data. Figure 15 shows a typical example, where the prepreg is tilted relative to the lines.

C. Peripheral Component Interconnect Express

1) Constraints and Hardware Specifications: The physical properties and requirements discussed above are taken for granted in the specifications for PCIe. A consortium founded by various companies, the PCI-Special Interest Group (PCI-SIG), takes responsibility for publishing complete specifications containing all the necessary information to establish a securely functioning data connection between a host and its peripherals. The characteristics of the PCIe specifications are discussed below.

The PCIe bus is a high-speed bus with point-to-point topology and independently operating serial links. A link is an established data connection implemented on one lane. A lane consists of one differential line pair.
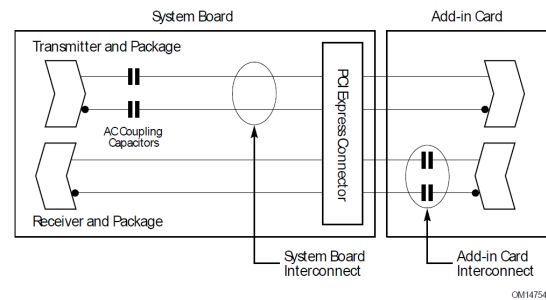
The bus width can range from one to typically sixteen lanes. A bus width of 32 lanes is also envisaged but is not yet common in practice. Each lane can perform upstream and downstream data transfer as discussed in Chapter II-A3. The first pair is the sending lane, also called TX (transmit). On this lane the data is sent from the root complex to the endpoint. The latter pair of lines is used to send data from the endpoint to the root complex, which is why it is referred to as RX (receive) from the root complex perspective. Since the frequency is proportional to the applied data rate, which is in the range of Giga Hertz, it is essential to consider the wave characteristics introduced in Chapter II-A. The differential wave impedance used was set to the range of 72.5 Ω to 97 Ω. If there is a mechanical connector between the root complex and the endpoint, it is recommended that the SE impedance for auxiliary signals is in the range of 42.5 Ω or 50 $\Omega \pm 7\%$. This is because there must not be a ground layer in the area surrounding the contacts, which can lead to crosstalk from the RF signals to the auxiliary signals. In addition, it is recommended that these signals are connected to plug-in cards with a CR element consisting of a capacitor with a capacitance of 1 pF and a resistor of 42.5 Ω or 50 Ω with a tolerance of 2 Ω.

AC coupling capacitors with a capacity of 220 nF are located in the lanes. Since the wave impedance changes at the connection pad, ceramic capacitors of size 0201 are recommended as shown in Figure 16 [1] [16].

The polarity of the differential line pair may be swapped in routing as desired, which simplifies the routing effort and therefore also has a positive effect on signal integrity. However, the difference in length between the individual lines due to routing must not be greater than 0.064 mm. The specifications do not limit the maximum number of vias. Various manufacturers use different numbers in the range of 1 to 6 vias. Via stubs are not permitted, however.

The thickness of plug-in cards is specified as 1.57 mm, with a tolerance of 0.13 mm. The exact dimensions from plug-in area to card edge are given, as well as the height and width for different module sizes. The edge for the insertion area should be milled
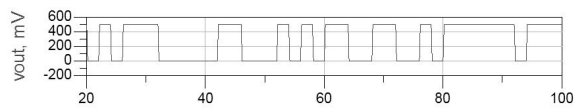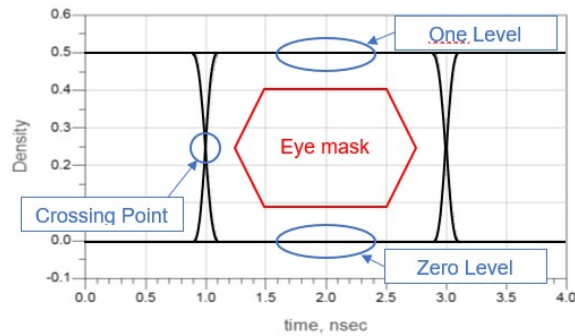
Figure 17. Example of a signal over time [5].

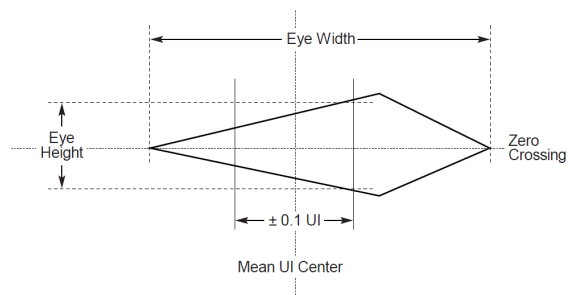Figure 18. Eye pattern [5] [4].

Figure 19. Minimal requirements at the receiver, illustrated in the mask with eye height and eye width [1].

Table I
16.0 GT/s CHANNEL TOLERANCING EYE MASK VALUES FOR [1].

Symbol	Parameter	Value	Units
UI	Unit Interval	62.48125 (min) 62.51875 (max)	ps
$V_{RX-CH-EH-16G}$	Eye height	15 (min)	mVPP
$T_{RX-CH-EH-16G}$	Eye width at zero crossing	0.3 (min)	UI
$T_{RX-DS-OFFSET-16G}$	Peak eye height offset from UI center	$\pm$ 0.1	UI

with a 20° angle to protect board and socket during the insertion process [1] [16].

2) Eye Pattern, Jitter and Bit Error Rate: Figure 17 shows a signal over time.

In order to assess signal integrity, the shortest time unit between two edges is measured. An internal trigger signal is derived from this, and all edges are superimposed on the same point. Later, this time period is used as a unit interval (UI). The result then becomes a signal curve as shown in Figure 18. This representation is commonly referred to as "eye pattern" or "eye diagram".

Signal integrity can now be analyzed based on the eye pattern. The central opening is the reason for the name of this type of representation. The so-called mask is shown in red in the center of Figure 18. This area must remain blank according to the specifications for any signal. Depending on the protocol, the mask may look different. The Bit Error Rate (BER) is a measure of the frequency with which the mask is violated. It is defined as the ratio between the incorrectly transmitted bits and the correctly transmitted bits. Ideally, it is 0 or as low as possible. If the error rate becomes higher than 10^{-12}, the link is cancelled and renegotiated. The procedure for this will be presented in the following Chapter II-C3.

Besides the BER, many other parameters can be quickly read from an eye diagram: The eye height is the vertical difference between the zero and one level, also named the vertical eye opening. Ideally, the eye crossing point is exactly 50% of the eye height. The temporal distance between the two crossing points is the eye width. Another important feature is the jitter. This is determined by displaying the spread of the crossings at the crossing point using histograms. The rise time is the time it takes for the signal to rise from 20% to 80% signal level, while the fall time is exactly the opposite.

3) Link Initialization and Training: According to the PCIe specifications, the binary states 1 and 0 are represented by voltage values. None of them correspond to 0V, which is why we speak of non-return-to-zero (NRZ). To ensure that only the AC mode exists during data transmission, the 8b10b coding is used for PCIe Gen 1 and 2. Here, no bytes but only 8 bit symbols are transmitted, with a maximum parity difference of ± 2. The other 2 bits are used to compensate the odd parity. Therefore, 20% of the transmitted data contains no information but overhead bits. In contrast to this, PCIe generations 3 and 4 use 128b/130b coding. Here the sequence starts with a 0-1 toggle and is followed by a 128 bit long data packet. It is assumed that the signal no longer has a DC component on time average. For the receiver, the PCI-SIG provides a mask for the eye diagram in a diamond shape as shown in Figure 19. The most important characteristic limit values can be found in Figure II-C3.

Due to the characteristic properties of a trace, edges are strongly attenuated by the inductive behavior. This can be compensated by applying the following three countermeasures as illustrated in Figure 20.

First, de-emphasis at the beginning of an edge alternation is achieved by applying a higher signal level for a short period of time. Second, if a signal state is present for a longer period of time, the signal level
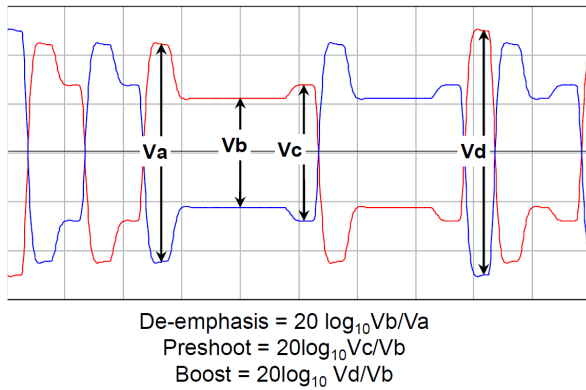
Hochschule Düsseldorf
University of Applied Sciences

HSD

ON THE INFLUENCE OF LINE ROUTING AND EMC
NOISE SOURCES ON HIGH-SPEED DATA
TRANSMISSION AND SIGNAL INTEGRITY

$$\text{De-emphasis} = 20 \log_{10} Vb/Va$$
$$\text{Preshoot} = 20\log_{10} Vc/Vb$$
$$\text{Boost} = 20\log_{10} Vd/Vb$$

Figure 20. Definition of Tx voltage levels and equalization ratios [1].

Figure 21. Flow chart of the test setup.

can be slightly increased by a preshoot before the state transitions. This increases the steepness of the falling edge. Third, a boost is applied especially for 010 or 101 state changes. For link training, eleven different presets of these individual equalization ratios are specified.

When setting up a link, the root complex and the endpoint synchronize via the reference clock after the power supply is applied to all components involved. In the next step, the receiver starts with the RX detect to check on which input a line is located, then the devices, individually on each lane, start sending serial data at a rate of 2.5 GT/s. This is the absolute minimum speed at which the devices can send data according to the original PCIe Gen 1 specifications that must be supported by any PCIe device.

After the physical connection has been recognized, polling begins. Training sequences at PCIe Gen 1 speed are sent from the root complex to the endpoint. Meanwhile, the receiver tries to synchronize itself with the known sequences. This is performed until the bits are correctly recognized first, then the endpoint tries to decode the transmitted 1-0-bit symbols. The last step is to compensate for the different line lengths of the individual lanes. Once this is complete, the system is in L0 state, which means normal mode.

Link training for PCIe Gen 2 is the same as for GEN 1, except that different symbols are sent during polling.

To establish a Gen 3 or Gen 4 link, an L0 state link must already exist. Starting with this, the equalization phase begins. Here, training sequences with the different presets are sent and the receiver tells the transmitter at which preset the data is best received and again the L0 state is reached. Gen3 L0 state is negotiated first before the negotiation of Gen 4 is started. There is an option to start the training of the equalization connection for a Gen 4 connection directly. However, this only makes sense for embedded systems with known and defined modules.
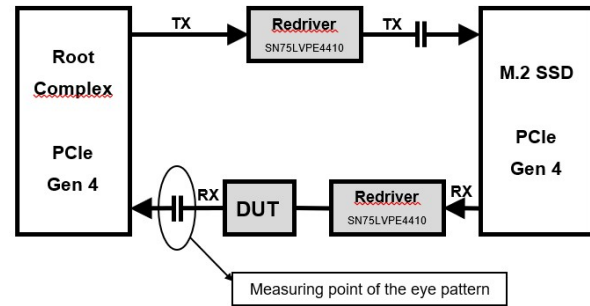
III. INTRODUCTION TO THE INVESTIGATED HARDWARE

A. Research Concept

To assess the effects of routing on signal integrity, a system available on the consumer market is used. The root complex consists of a CPU on a mainboard, which meets the required PCIe 4.0 specifications. The endpoint is a compatible peripheral device. We use a latest generation M.2 solid state drive. Various plug-in cards are to be plugged in between to evaluate the effects of signal routing. They will be presented and discussed in greater detail in Figure III-B. In order to keep the impact of the plug-in connections as low as possible, a redriver ensures that the signal is reprocessed. However, this is pure signal amplification without any combinatorial logic. In addition, this component increases comparability among the evaluated PCBs. On the RX line, namely the line on which data is transferred from the hard disk to the root complex, different types of line routing implemented on the plug-in cards are to be investigated. In Figure 21, this is the device under test (DUT).

In theory, a link will work if all the rules of the PCIe specifications are met. To evaluate the effect of signal routing, the requirements of the specifications were systematically violated by implementing various design alternatives. This means that, as far as possible, one rule was broken for each board examined. The subject of the investigation was initially subject to a simple pass or fail. Data transmission performance is then examined in greater detail. For this purpose, there is a tool "performance test" that is already included in the operating system used, Linux Ubuntu 22. The signal characteristics of the AC coupling capacitors are to be measured and examined with an oscilloscope.
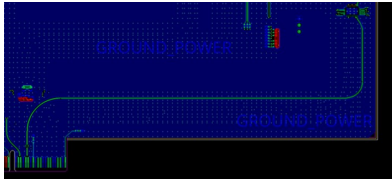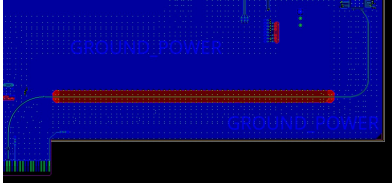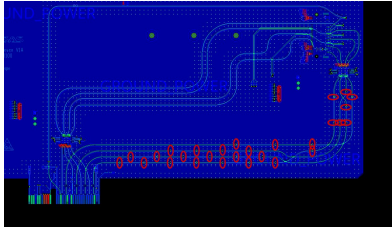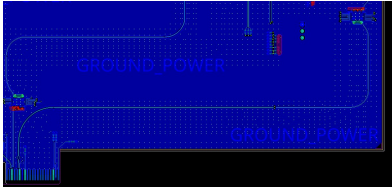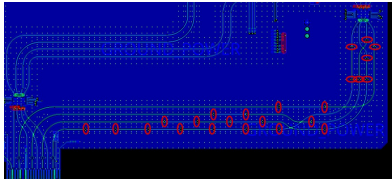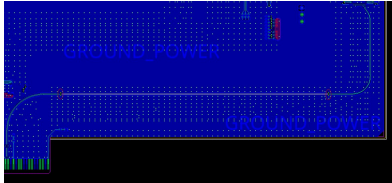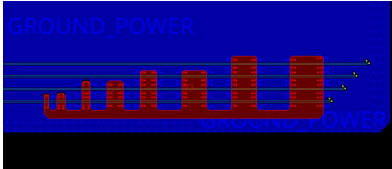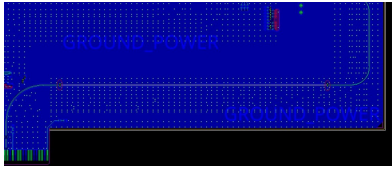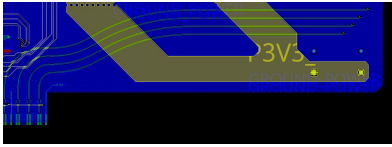
B. Plug-in Cards

For the examinations carried out in this work, a total of ten plug-in cards were developed. Figure 22 and Figure 23 provide an overview of one of these plug-in cards, which is used as reference for further analysis.

The reference plug-in card, as well as the nine other designed and investigated plug-in cards are contained and described in Figure III-B.

Table II
OVERVIEW ON THE 10 DESIGNED AND EVALUATED PLUG-IN CARDS.

| Board name	Test subject	Board name	Test subject
No via	This board is the reference for all following investigations. It is a PCB with exactly one lane on which all the rules of the specifications are observed.	Plane Coupling	The design is the same as the "No via" board, except that part of the trace is routed on another plane. In this region, this transmission line is not coupled to the ground potential. This should have an influence on the wave impedance and lead to reflections. However, it is possible to couple the reference plane to ground power, as shown in Figure 14.
Even via count (x4)	The effects of vias on the signal path and data throughput are to be tested. For this purpose, 4 (lane 1) to 10 vias (lane 4) per lane are on the board. Via locations are marked in red.	Single via	The design is the same as the "No via" board, except that a via conducts the signal from the top to the bottom.
Odd via count (x4)	The effects of vias on the signal path and data throughput are to be tested. For this purpose, 3 (lane 1) to 9 vias (lane 4) per lane are on the board. Via locations are marked in red.	Single X-via	The design is the same as the "Single via" board, except that the via has a 90° bend.
Micro-stripline	The design is the same as the "No via" board, except that part of the trace is routed as a stripline on an inner layer. The intermediates have been marked in red.	Plane Coupling V2	This design is a step up from the board "Plane Coupling": The aim is to investigate the effect of multiple uncoupled line segments.
Micro-stripline Microvia	Just like the board "Microstripline", except that the stubs are eliminated by the use of microvias.	EME	The effect of an interference source is to be investigated on this board. For this purpose, the lanes are crossed by a PDN on an inner layer through which a high, pulsating current flows.
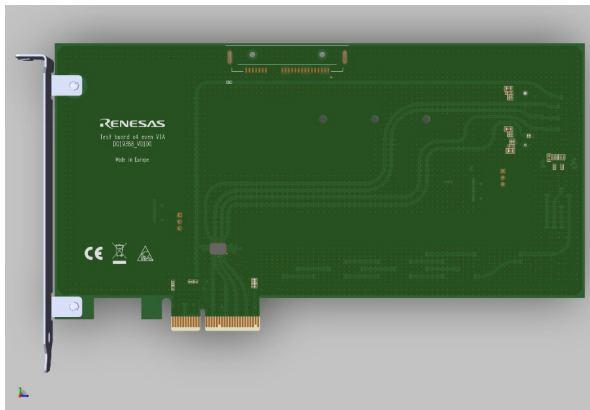
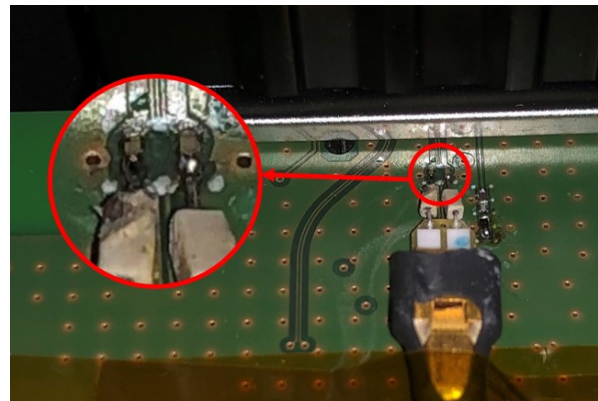Figure 22.   Top view of the reference plug-in card.

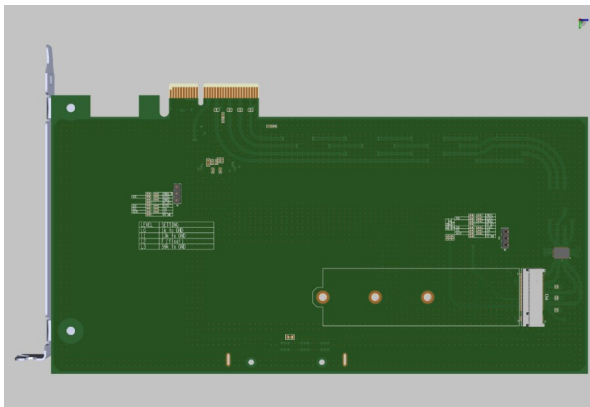Figure 23.   Bottom view of the reference plug-in card.

Figure 24.   Used oscilloscope with test system.
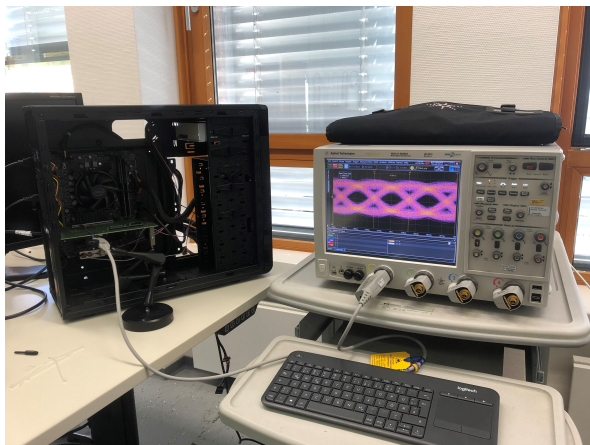

Figure 25.   Differential probe tip.

Figure 26.   Eye pattern of a line without vias.

C. Measurement Setup

The signal integrity is measured with an oscilloscope as shown in Figure 24. This device has a resolution of up to 80 GS/s and is therefore fast enough for a measurement of PCIe Gen 4. An active differential probe is used, which was specially developed for the measurement of Low Voltage Differential Signals (LVDS).

The actual measuring tip as shown in Figure 25 is soldered onto the plug-in card.

This is the best option without distorting the signal. The location was chosen so that the signal is detected as close to the receiver as possible. This is to capture as many of the effects of the routing as possible. Due to the equalization introduced in Chapter II-C3, it is not possible to measure the signal in the condition in which it later arrives at the receiver. For this purpose, the oscilloscope has a continuous time linear equalizer (CTLE) that reverses the influences of the link training and the signal is interpolated in such a way that it is most likely directed at the receiver.

IV. EVALUATION OF THE MEASUREMENT RESULTS

In this Chapter, the results of all measurements on the 10 designed plug-in cards are presented and discussed. For this purpose, the eye diagrams were measured with the oscilloscope presented in Chapter III-C for all cards and analyzed with regard to signal integrity.

A. No Via

Figure 26 shows the measured results of a PCIe lane.

This card was developed with full consideration of the PCIe specifications and serves as a reference for the
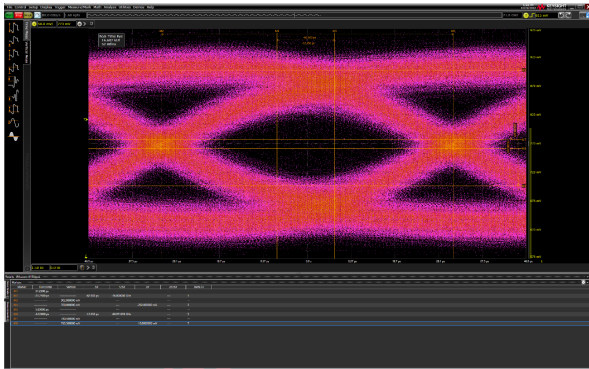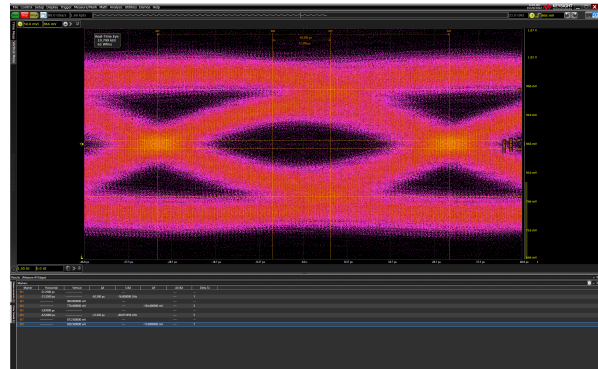
Figure 27. Eye pattern of lane 4.

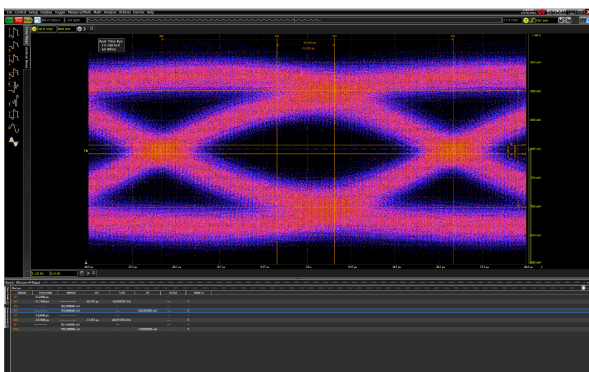Figure 29. Eye pattern of a stripline with via stubs.

Figure 28. Eye pattern of lane 4.

following measurements. Peak-to-peak, the maximum signal level is about 300 mV. The eye height is about 90 mV. The crossing point is at 50% and the inside of the eye is a little noisy. The eye width is 36 ps and the mean UI center is in the middle of the eye. Apart from a few dots inside the eye, the mask is rarely violated, which indicates good signal integrity and corresponds to the result from the data throughput measurements.

B. Even Via (x4)

Figure 27 shows the measurement result of lane 4 which was modified to have 10 vias.

Peak-to-peak, the maximum signal level is about 350 mV, while the eye height is about 150 mV. The crossing point for this measurement is 50%. Horizontally, the eye width is about 37 ps and the mean UI center is right in the middle. The inside of the eye is a little noisier than in Figure 26, but the aperture is still easily recognizable, and the mask is rarely violated. In comparison to Chapter IV-A, it is noted that the amplitudes of this card are 1.3 dB higher. This is probably due to the link training, which is intended to compensate for the influence of the layer changes.

C. Odd Via

Figure 28 shows a measurement result of lane 4, but this time there is an odd number, 9, of vias.

The maximum signal level is about 300 mV, while the eye height is about 110 mV. The crossing point is again at 50% and the center is exactly in the middle. At this lane, the eye width is about 40 ps, which is a bit wider compared to the two cards discussed above. The inside of the eye is only minimally noisy, and the mask is almost not violated at all. At first glance, this result does not match the performance in terms of data throughput, but it can be explained by the performance of the hard disk or the solder joints.

D. Microstripline

Figure 29 shows a measurement result of lane 1. In one section the line is routed as a stripline on an inner layer.

The maximum signal level is again around 300 mV and the eye height is 70 mV. Again, the crossing point is at 50%, and the UI center is in the middle. The eye width is about 32 ps. Looking at the eye, it is noted that it is much noisier in this measurement than in the previous measurements. This can be explained by reflections at the via stub. These seem to have a considerable effect on signal integrity.

E. Microstripline Microvia

Figure 30 shows the measurement result of lane 1 and, as in Chapter IV-D, the line is routed on a section as a stripline on an inner layer.

In this measurement, however, microvias without stubs were used instead of through-hole vias. This leads to a smaller maximum signal level, which is only about 250 mV here. The eye height, on the other hand, is considerably higher than in the previous measurement, at about 100 mV. The crossing point is at 50%, the center is in the middle and the eye width is 38 ps. This diagram exhibits almost no noise at all, and the mask is only very rarely violated. This demonstrates very clearly the difference of the via used. The signal level is -1.6 dB lower than with via stubs, which can be attributed to better signal integrity and adjusted link training.

Hochschule Düsseldorf
University of Applied Sciences

HSD

ON THE INFLUENCE OF LINE ROUTING AND EMC
NOISE SOURCES ON HIGH-SPEED DATA
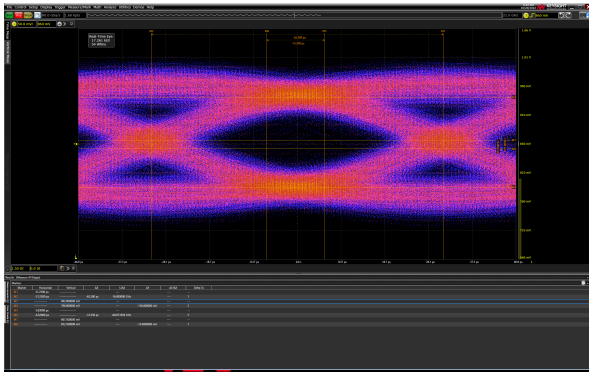TRANSMISSION AND SIGNAL INTEGRITY

Figure 30. Eye pattern of a stripline without via stubs through the use of microvias.
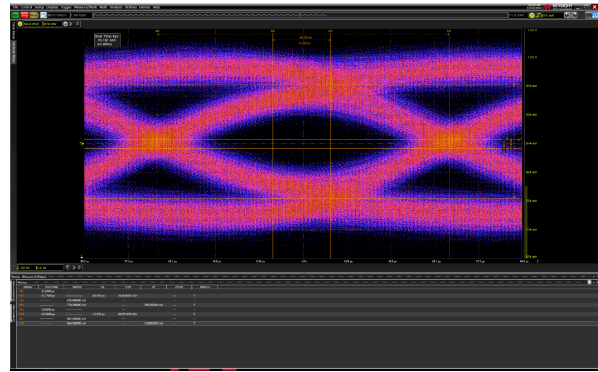

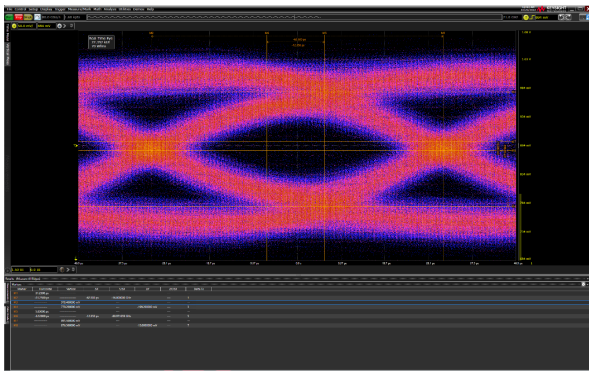Figure 32. Eye pattern planecoupling with 2x 220nF coupling on each side.

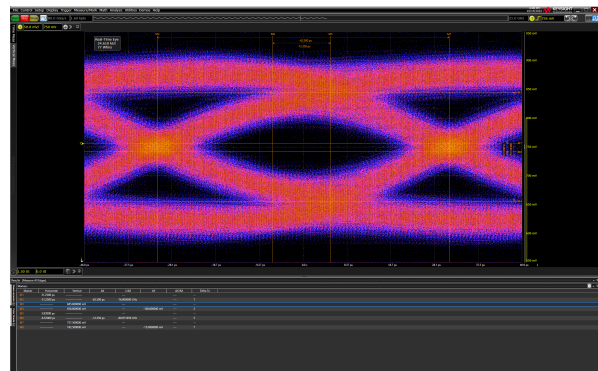Figure 31. Eye pattern planecoupling without coupling capacitors.

Figure 33. Eye pattern of a PCIe lane with one via.

F. Plane Coupling

Figure 31 shows the results of the first of two measurements on lane 1 where a line segment on the adjacent inner layer was coupled with a power delivery network (PDN). However, in the case shown here, the coupling capacitors are not populated.

The maximum signal level of this measurement is again about 300 mV. The eye height is about 100 mV and the crossing point is at 50%. The center is slightly to the right and the eye slightly resembles a diamond shape. The eye width is 38 ps. There is slight noise inside the eye, but the mask is barely violated.

In the results shown in Figure 32 the measurement was carried out again, now with equipped coupling capacitors.

With regard to the measurement results, hardly any differences from the pattern without coupling capacitors can be seen. Maximum signal level and eye height and width are similar to Figure 31. However, the eye is still a little bit less noisy.

G. Single Via

The measurement corresponding to the results shown in Figure 33 was carried out on lane 1.

The card is the same as the reference card, except for a layer change from top to bottom. The maximum signal level is again around 300 mV. The eye is a

little narrower with a eye height of about 80 mV. The mean center is again in the middle of the eye and the crossing point is at 50%. The eye width is 38 ps. The eye interior shows little noise, and the mask is subject to little violation.

H. Single X-Via

Figure 34 shows a measurement result on lane 1 that is basically the same as the measurement result shown in Figure 33. However, here an "X-via" was used here to bend the lane at a 90-degree angle in the course of the layer change and to swap the polarity instead of routing a bend shape.

This modification has no effect on the maximum signal level. The eye width is slightly higher at about 100 mV. It is particularly noteworthy, however, that the inside of the eye is somewhat noisier compared to the results shown in Chapter IV-G.

I. Plane Coupling V2

This card featured several PDNs on the reference layer. Figure 35 shows the measurement results.

First of all, it is noted that the maximum signal level, which in all previous measurements on the cards discussed above had settled between 250 mV and 350 mV, is now close to 400 mV. The eye height is also
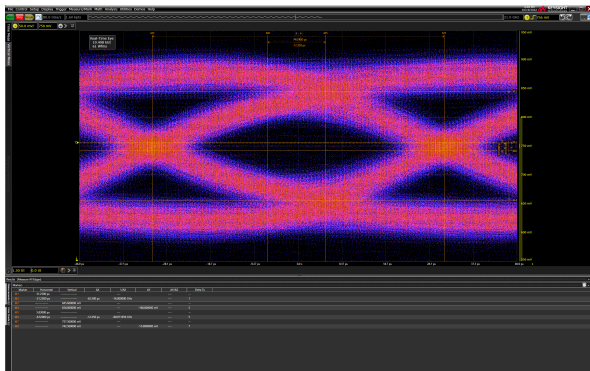
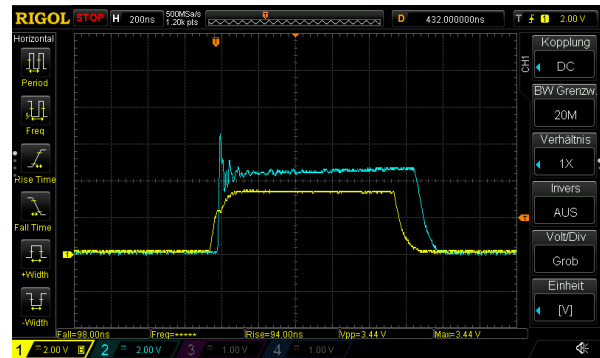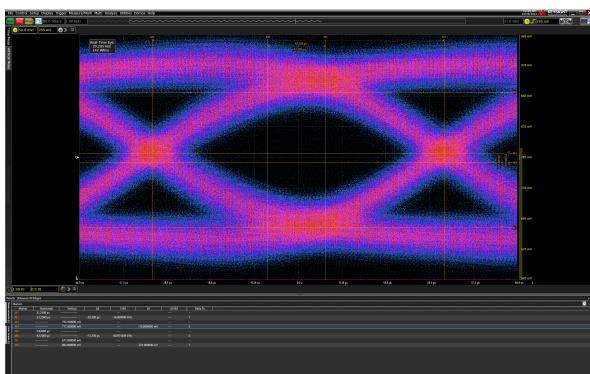Figure 34. Eye pattern of a PCIe line with a 90° turn in a via.

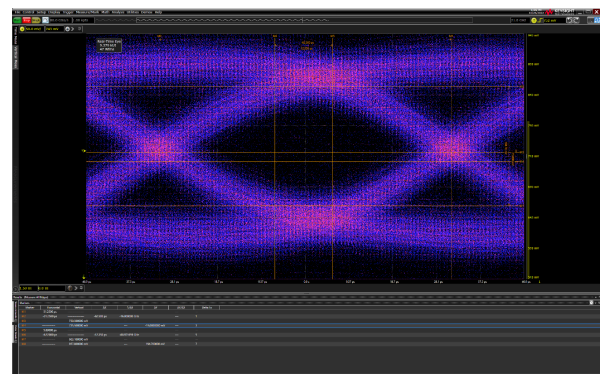
Figure 35. Eye pattern plane coupling V2 lane 4 uncoupled.

Figure 36. Eye pattern plane coupling V2 lane 4 coupled.

Figure 37. Signal of the noise source.

Figure 38. Eye pattern of a disturbed PCIe lane by EM-noise.

considerably higher than in the previous measurements, with a maximum opening of about 180 mV. The crossing point is at 50%, but the central UI center is shifted to the right and again resembles the diamond shape. The eye width is 42 ps. The eye is visibly noisy, even though the mask is found to be very clean in the eye. The higher voltage can be explained by a different preset in link training, which also automatically leads to steeper edges. The horizontal shift indicates inductive behavior, probably due to the disturbed return path.

Figure 36 shows results where the aforementioned PDNs were also connected to the ground reference via coupling capacitors in terms of wave properties.

With regard to the maximum signal level and the eye height and width, there are no differences from the results shown in Figure 35. However, it is noted that the eye in this measurement is visibly less noisy than in the first measurement. In addition, the mask has moved a little closer to the center.

J. EME 500 kHz

In this test case, an electromagnetic emission (EME) interferer was installed on an internal layer during measurement, which is supposed to represent the use of neighboring circuit parts. Under certain circumstances, this can produce noise comparable to that of a real application. Figure 37 shows the characteristics of the noise source in blue while the corresponding control signal, which is generated by a frequency generator, is shown in yellow.

Figure 38 shows the eye diagram for the corresponding measurement.

Here, the maximum signal level is again relatively high at about $400\,\mathrm{mV}$. The eye height is about $150\,\mathrm{mV}$ and the eye width is $40\,\mathrm{ps}$. The crossing point is at $50\,\%$ and the center of the mask is in the middle. All the curves are highly diffused, and the eye is visibly noisy due to the interfering transmitter in this measurement. The mask is also frequently violated. This is consistent with the fact that data throughput

Table III
EYE CHARACTERISTICS AND RESULTS OF SPEED AND LINK STATUS

Board name	max. peak-to-peak signal level	eye height	crossing point	eye width	Payload bandwidth	Lane count	Link type
No via	300 mV	90 mV	50 %	36 ps	1.8 GB/s	×1	Gen 4
Even via (×4)	350 mV	150 mV	50 %	37 ps	6.5 GB/s	×4	Gen 4
Odd via (×4)	300 mV	110 mV	50 %	40 ps	5.9 GB/s	×4	Gen 4
Microstrip line	300 mV	70 mV	50 %	32 ps	1.8 GB/s	×1	Gen 4
Microstrip line Microvia	250 mV	100 mV	50 %	38 ps	1.8 GB/s	×1	Gen 4
Plane Coupling	300 mV	100 mV	50 %	38 ps	1.8 GB/s	×1	Gen 4
Single via	300 mV	80 mV	50 %	38 ps	1.8 GB/s	×1	Gen 4
Single X-via	300 mV	100 mV	50 %	38 ps	1.8 GB/s	×1	Gen 4
Plane Coupling V2	400 mV	180 mV	50 %	42 ps	5.2 GB/s	×4	Gen 4
EME	n.a.	n.a.	n.a.	n.a.	5.4 GB/s	×4	Gen 4
EME 500kHz	400 mV	150 mV	50 %	40 ps	4.8 GB/s	×4	Gen 4

is significantly reduced as soon as the source of interference is switched on.

K. Evaluation Summary

The measurement results of all 10 cards are summarized in Figure IV-J with respect to maximum peak-to-peak signal level, eye height, crossing point, eye width, payload bandwidth, lane count, and link type.

To classify the results: The theoretical maximum payload bandwidth of PCIe without protocol overhead is $1.97\,\text{GB/s}$ on a single lane and $7.88\,\text{GB/s}$ on four lanes.

As shown in Figure IV-J, all the plug-in cards worked with a Gen 4 link. The measured payload bandwidths for all plug-in cards with one lane are very close to the theoretical maximum. Only the plug-in cards with 4 lanes cause the measurement results to become scattered. If signal integrity declines and more faulty packets arrive at the receiver, the receiver notices this and requests them again. Since the information now has to be retransmitted, the effective data rate decreases. This may not necessarily be due to signal integrity issues, however, but might also be related to the maximum performance of the SSD hard drive.

V. CONCLUSION

The key question considered during this work was the effect of signal routing on signal integrity and thus payload bandwidth or data throughput. The PCBs developed for this investigation incorporate a wide range of different influences. These include various designs and numbers of vias, outer and inner layer behavior, wave impedance effects and, finally, provoked EM interference.

The physical fundamentals of data transmission were first addressed and related to an application, the PCIe bus. This is subject to very broad specifications when taking the principles of line theory into account. However, if the necessary knowledge is adapted, it provides an excellent working basis for a PCB developer.

Through link training, the PCIe protocol is surprisingly well equipped and tolerant of minor layout errors. Nevertheless, the most important point is still that there must be enough space on the PCB for the individual lanes. The EME test has shown that neighboring circuit parts can have such a disruptive effect that significant performance losses occur, which are expressed metrologically by strong noise and a diffuse signal curve. Also, if the ground reference is changed several times, lower data rates have to be accepted. On a physical level, this is shown by more inductive behavior on the part of the data line. Layer changes are unproblematic, but attention must be paid to the choice of via used, as stubs have a negative effect on signal integrity.

The use of redrivers and retimers should be considered by the PCB designer, especially for longer lines or multiple connectors.

In terms of implementation it is easiest if data lines are routed on the outer layer, which is perfectly fine in terms of signal integrity. As expected, the stripline, with its internally routed lines, performs slightly better. On one hand, however, this does not help if interference signals are coupled in by high currents on adjacent layers. On the other hand, it can help with external radiation and long signal lines.

As robust as PCIe is, a good product does not stop at the board layout. The manufacturer should be consulted on the dimensioning of the tracks with regard to wave impedance, particularly in respect of the production of boards. It also makes sense to machine assemble the components as poor solder joints have a negative effect on overall stability and performance, and this may not necessarily be measurable.

REFERENCES

[1] PCI-Sig, *PCI Express® Base Specification Revision 4.0 Version 1.0* 2017.

[2] H. Wheeler, *Transmission-Line Properties of Parallel Strips Separated by a Dielectric Sheet* IEEE Transactions on Microwave Theory and Techniques, vol. 13, no. 2, pp. 172 - 185, March 1965.

[3] H. Wheeler, *Transmission-Line Properties of a Strip on a Dielectric Sheet on a Plane* IEEE Transactions on Microwave Theory and Techniques, vol. 25, no. 8, pp. 631 - 647, Aug 1977.

[4] Anritsu, *Understanding Eye Pattern Measurements* Anritsu, 2010.

[5] F. Gustrau, *Hochfrequenztechnik: Grundlagen der mobilen Kommunikationstechnik* München: Hanser Verlag, 2019.

[6] H. Heuermann, *Hochfrequenztechnik* Aachen: Springer Vieweg, 2018.

[7] L. Stark, *Development of simulation models for circuits and PCB layouts* Düsseldorf, 2020.

[8] E.Hammerstad and Ø.Jensen, *Accurate Model for microstrip computer-aided design* in 5th European Microwave Conference, Hamburg, Germany, Germany, 1975.

[9] H. Johnson and M. Graham, *HIGH-SPEED SIGNAL PROPAGATION ADVANCED BLACK MAGIC* Upper Saddle River, NJ 07458: PRENTICE HALL, 2003.

[10] *Cross Section of Coplanar Waveguide Transmission Line.png* Wikipedia, https://de.wikipedia.org/wiki/Datei:Cross_Section_of_Coplanar_Waveguide_Transmission_Line.png [Accessed 25.08.2020].

[11] C. Anet, *QSC* QSC, LLC, 27 March 2020. https://blogs.qsc.com/live-sound/what-are-the-differences-between-balanced-unbalanced-and-loudspeaker-cables/. [Accessed 17.11.2022].

[12] L. Simonovich, *What is Differential Impedance and Why do We Care?* Signal Integrity Journal, 14 April 2020.

[13] everythingRF, *everythingRF* 2020. https://www.everythingrf.com/rf-calculators/differential-microstrip-impedance-calculator. [Accessed 17.11.2022].

[14] *Microvias* NCAB GROUP.

[15] K. Ritz, *Spezielle Multilayer: Ein Buch für Designer, Hersteller und Anwender* Eugen G. Leuze Verlag, Bad Saulgau, Germany, 2013.

[16] PCI-Sig, *PCI Express Card Electromechanical Revision 4.0, Version 1.0* 2019.

[17] B. Simonovich, *Bert Simonovich's Design Notes* 15 February 2011. https://blog.lamsimenterprises.com/tag/via-stub/. [Accessed 19.11.2022].

[18] Keysight Technologies, *InfiniiMax III Probes User's Guide* Keysight Technologies, Colorado Springs, 2021.

[19] CalPlus GmbH, *CALPLUS* CalPlus GmbH, https://www.calplus.de/rigol-ds1054z.html. [Accessed 23.11.2022].

Lennart Stark was born in Duisburg, Germany in 1995. In 2016, he completed his vocational training as an electronics technician for automation technology at Henkel AG & Co KGaA. He earned his bachelor's degree in Microelectronics in 2020 at University of Applied Sciences Düsseldorf, Germany, and has since pursued his studies with the goal of earning a master's degree. In 2022, he joined Renesas Electronics Germany GmbH in Düsseldorf where he is developing Hardware for the latest MCUs.

Michael Engelbrecht was born in Nashua, NH, USA, in 1976. He has been living in Germany since shortly after. He received the Dipl.-Ing. degree in electrical engineering and information technology from the Technical University of Darmstadt, Germany, in 2001. In 2001, he joined NEC Electronics in Düsseldorf, Germany. NEC Electronics merged into Renesas Electronics in 2010. He started designing digital circuits for MCUs and their emulators. Later he also modeled circuits and developed early prototyping systems using FPGAs in large scales. Besides designing, he also has the focus on verification and simulation, electrically and functionally. For completed designs he implements automated tests and accompanies manufacturing processes.

Bernhard Rieß was born in Würzburg, Germany in 1966. He received the Dipl.-Ing. degree in Electrical Engineering and Information Technology from the Technical University of Munich, Germany in 1992. From 1992 to 1996, he was a Research Assistant at the Institute for Electronic Design Automation, Technical University of Munich, where he received his Dr.-Ing. degree in 1996. In 1997, he joined Infineon Technologies in Munich, Germany. Since 2012, he has been a Professor of Microelectronics at the University of Applied Sciences Düsseldorf, Germany. His research interests include design and electronic design automation of integrated digital circuits.

Hochschule Reutlingen
Reutlingen University

A Digitally Configurable ASIC for Sensorless Control of a Switched Reluctance Motor

Bekir Djanklich, Sven Korb, Samuel Lotfey, Maximilian Wiendl, Eckhard Hennig

Abstract—**The current paper presents a digitally configurable ASIC for sensorless control of 8/6 switched reluctance motors. Building on a previous implementation [1], the work in this paper provides improved control capabilities. The main improvement is a current controller with a variable hysteresis, which allows the machine to operate over a wider voltage range. In addition, an improved method for determining the initial rotor position is proposed. The integration of a serial interface allows all parameters of the ASIC to be programmed by the user. As a result, the ASIC can be used to control any 8/6 SRM.**

Index Terms—**Sensorless control, switched reluctance motor, current control, application-specific integrated circuit (ASIC)**

I. INTRODUCTION

Switched reluctance motors (SRMs) work without permanent magnets. The resulting cost advantage can be increased even further by not relying on a position sensor to control the machine.

A suitable sensorless control method has been developed in [2]. The main idea is to energize two phases of the motor simultaneously: To build up torque, a high current is fed through the first phase, which is called the *working phase*. Meanwhile, a second phase, called the *sensing phase*, receives a small ripple current which is used to measure its inductance to determine the rotor position. The assignments of working and sensing phases are shifted around periodically to follow the rotor's movement.

Figure 1 visualizes this sensorless method of position detection. The current i_{P3} in the sensing phase (P3, green) is controlled by an on-off controller. While the rotor turns to align with the working phase (P1, red), its alignment with the sensing phase P3 decreases. This causes the inductance L_{P3} of the sensing phase to decrease as well, which leads to reduced rise and fall times of the sensing current i_{P3}.

As a result, the switching frequency of the current controller is increasing, which can be read from the PWM signal d_{P3}. This frequency increase is exploited to detect the alignment of the rotor: once the PWM frequency f_{P3} reaches the programmed threshold value

Bekir Djanklich, bekir.djanklich@icloud.com, Sven Korb, sven-korb@web.de, Samuel Lotfey, samuel.lotfey@icloud.com, Maximilian Wiendl, maximilian.wiendl@gmail.com, Eckhard Hennig, eckhard.hennig@reutlingen-university.de. Reutlingen University, Alteburgstraße 150, 72762 Reutlingen.

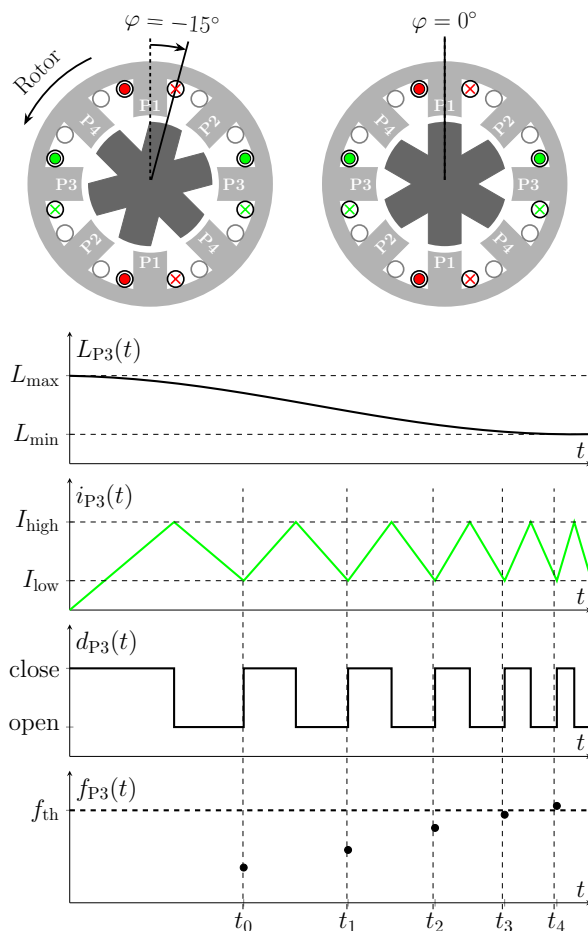

Figure 1. Working principle of the SRM.

f_{th}, the rotor is assumed to be aligned with the working phase, and the working and sensing phases are switched forward one position.

By shortening the time between switching cycles, the granularity of the frequency measurement is increased and the rotor's position can be detected more accurately. Consequently, higher frequencies of the current controller enable more precise phase switches, allowing the motor to turn more smoothly.

Figure 2 shows the circuitry used to control one motor phase, where R_P is the phase resistance and L_P is the phase inductance. The current i_P is fed into the coil by switching the two MOSFETs T_1 and T_2 simultaneously.
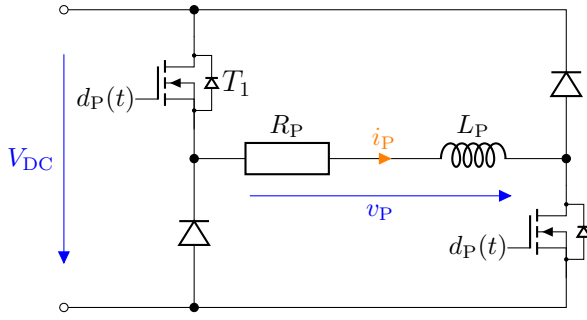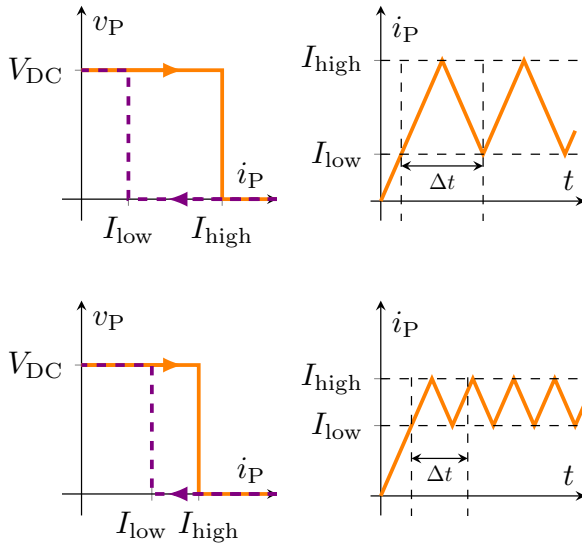
Figure 2. Asymmetric half-bridge topology.

Figure 3. Influence of current hysteresis on the switching frequency of the current controller.
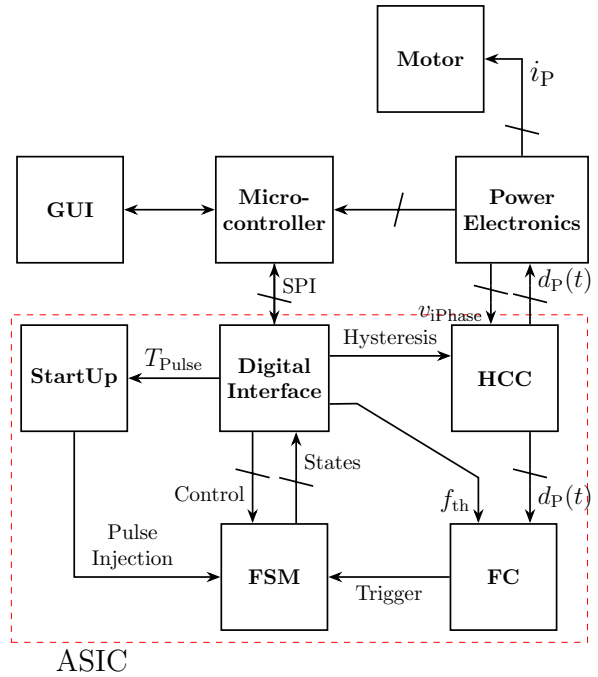

Figure 4. System block diagram.

A further improvement compared to the previous work is the addition of a digital serial interface for configuration and control purposes. It facilitates a fast and automated commissioning process through a large number of configuration parameters.

II. IMPLEMENTATION

A. System Architecture

Figure 4 shows a block diagram of the system.

B. Finite State Machine (FSM)

The FSM is the digital logic that controls if a phase is idling, sensing or working, depending on internal signals and external configuration parameters.

C. StartUp

Since the phase inductances depend on the rotor's orientation, applying consecutive voltage pulses to all phases will cause different currents according to $u = L \cdot \frac{\mathrm{d}i}{\mathrm{d}t}$. By measuring and comparing the occurring phase currents, the rotor's orientation can be determined. This approach, called *Pulse Injection*, was previously used in [3].

Figure 5 shows the improved method that was implemented for the current paper. By applying the voltage pulse to all motor phases simultaneously, instead of consecutively, the time needed for position detection is reduced.

In the example shown, the yellow current rises the least in response to the voltage pulse applied during the Pulse Injection process. Therefore, the yellow inductance (L_{P2}) is the highest, indicating that the yellow

The ASIC developed in the prior work [1] used a current controller with fixed hysteresis. This resulted in low positional resolution in certain working points, causing poorly timed phase switches.

Figure 3 demonstrates how a reduction in hysteresis width increases the current controller's switching frequency, allowing a more accurate measurement of the rotor's position. switching cycles. The work at hand aims to utilize this principle to obtain improved rotational control by implementing a current controller with configureable hysteresis.

With the previous method for sensorless SRM control, it is not possible to determine the initial rotor position before start-up. In the prior work [1], the rotor was moved into a defined starting position by energizing a single phase. During this alignment process, the direction of rotation was not defined. Furthermore, the machine's rotation had to be stopped to perform the alignment process. For the work at hand, a sensorless method for determining the rotor position at standstill was developed and implemented in the ASIC. The new method allows a smooth start-up to be performed even while the machine is still turning.

Hochschule Reutlingen
Reutlingen University

Figure 5. Pulse injection process.

Figure 6. Structure of the digital interface.
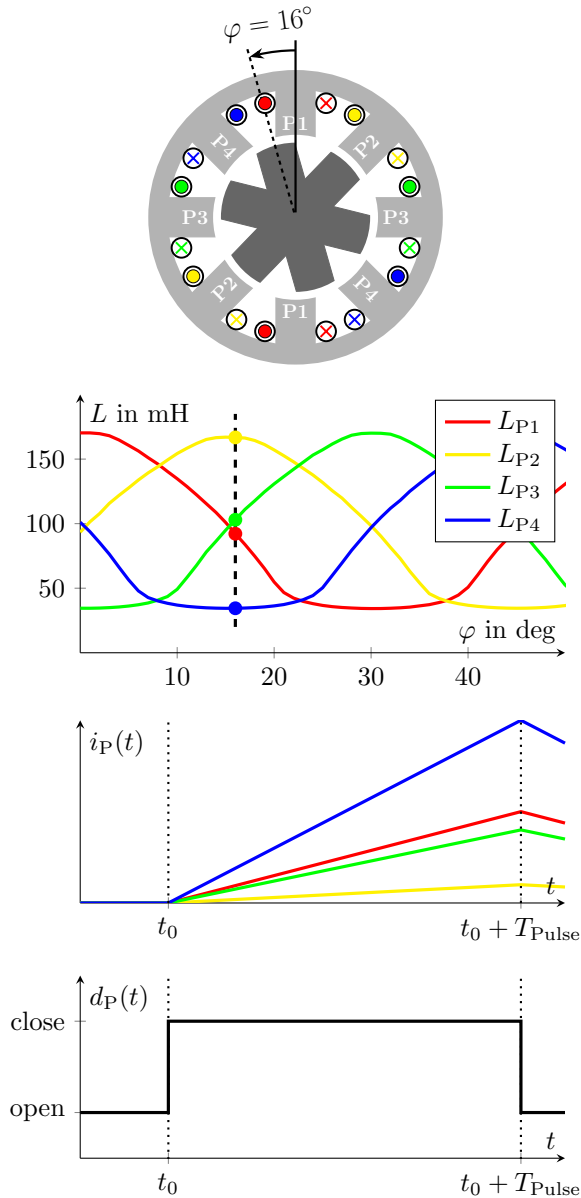
phase (P2) is the most aligned. This information is passed on to the FSM, which uses it to select the correct initial state. Depending on the direction of rotation, either P1 or P3 will be powered next.

D. Digital Interface

The ASIC is equipped with a SPI interface based on [4]. The interface provides 18 registers with 8 bits each, and can be used to read and write configuration and measurement data.

Some 10-bit signals had to be split up into two 8-bit registers, which created the need to read or write multiple registers simultaneously. This requirement is fulfilled through an intermediary buffer memory.
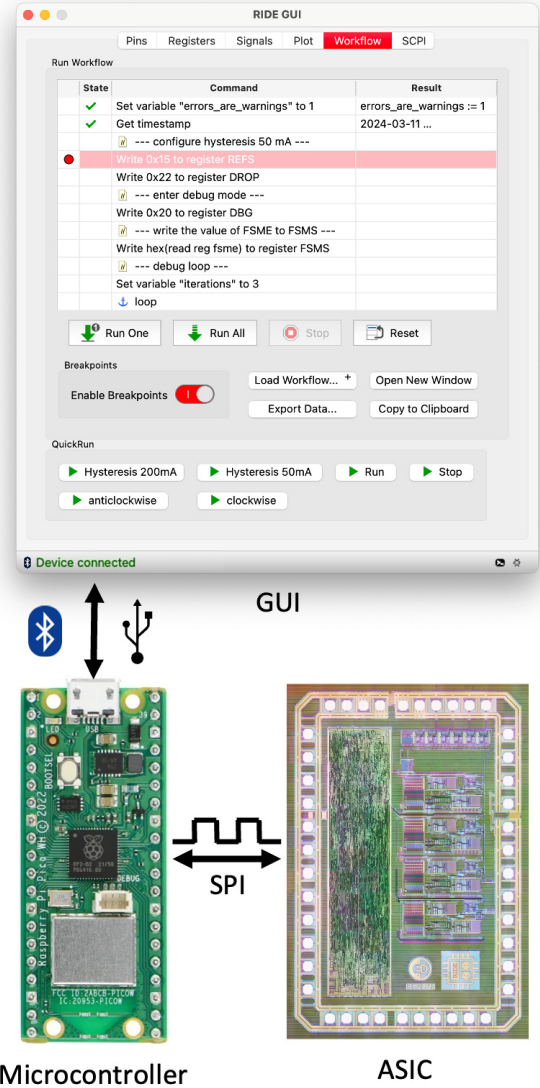
A microcontroller is used to make the functions of the ASIC's SPI interface available via USB or Bluetooth.

User interaction takes place through a custom graphical user interface (GUI), which provides a number of measurement automation, control and data visualization functions. A back-to-back overview of the digital interface is pictured in Figure 6.

E. Hysteresis Current Controller (HCC)

The circuit topology of the HCC, as shown in Figure 7, is the result of rapid prototyping with a focus on using standard library components, instead of a full-custom solution. A configurable hysteresis is implemented through a switched adjustable current sink: When S_5 is switched on, a voltage drop V_{R1} occurs across R_1. The magnitude of the voltage drop depends on the amount of current $n \cdot I_0$ sunk by the
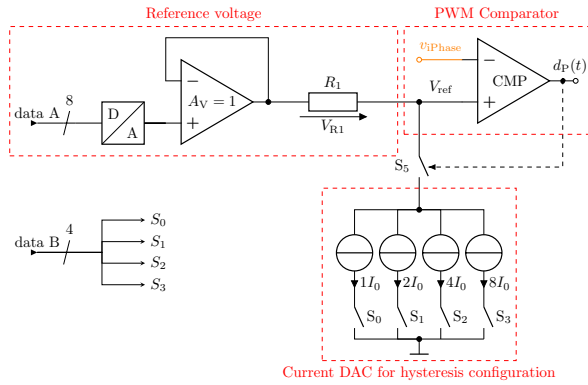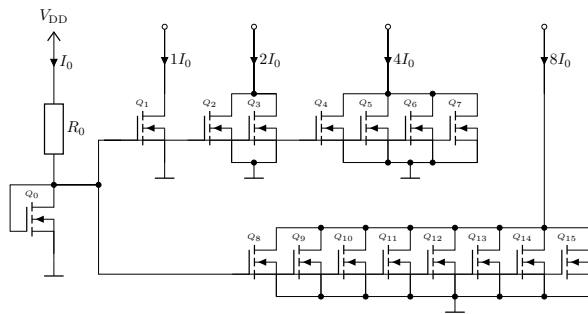
Figure 7. HCC block diagram for one phase.

Figure 8. Current mirror circuit

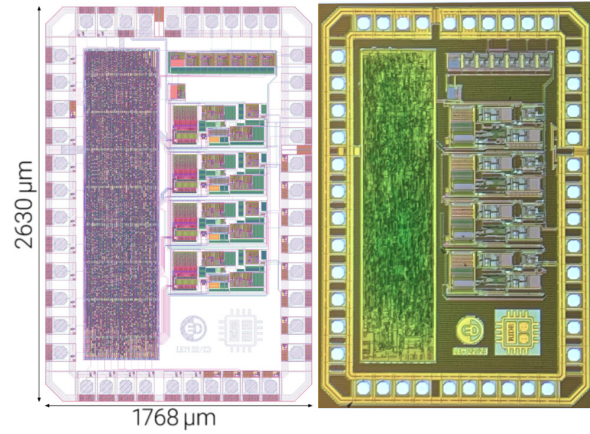
Figure 9. ASIC layout design (left) in comparison to a microscope image of the manufactured die (right).

Figure 10. Smart power electronics system

current DAC. By setting S_1 through S_4 with a 4-bit word *data B*, any multiple of I_0 can be sunk up to a maximum of $15 \cdot I_0$. An 8-bit word *data A* is used to define the reference voltage.

Using this circuit topology, a variable hysteresis of $10\,\mathrm{mV}$ to $150\,\mathrm{mV}$ around a reference point between $0\,\mathrm{V}$ and $3.3\,\mathrm{V}$ can be configured. PWM control signals for each phase's asymmetric half-bridge are generated by comparing the output voltage v_{iPhase} of the phase's current sensor to V_{ref}.

To improve accuracy, the current sinks consist of unit transistors in a current mirror topology, as shown in Figure 8. In the layout, the transistors were matched using the common-centroid method.

F. Frequency Comparator (FC)

The FC measures the switching frequency of the HCC using a digital counter. Once the frequency surpasses a configurable threshold f_{th} (see Figure 1), a trigger signal is sent to the FSM.

G. ASIC Layout

Figure 9 shows the resulting ASIC layout. It is divided into a digital part on the left and an analog part on the right half, which contains the StartUp block at the top and the four HCC instances in the center. The ASIC is surrounded by an ESD frame with pads. It was designed and manufactured using $350\,\mathrm{nm}$ technology with three metal layers.
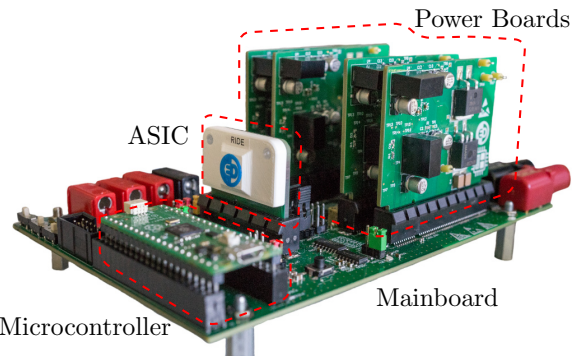
III. COMMISSIONING

For commissioning, the ASIC is placed in the smart power electronics system shown in Figure 10. The ASIC - directly bonded onto an adapter PCB - is plugged into the Mainboard together with four Power Boards. The Mainboard is directly connected to the SRM. Each Power Board contains one asymmetric half-bridge circuit to control the current in one motor phase. This modular design makes it easier to replace components should the ASIC or a Power Board become damaged.

To test the StartUp functionality, the initial rotor position is set to $30°$ as shown in Figure 12. In this position, the inductance in P3 is the highest because it is aligned with a rotor tooth, whereas the inductance in P1 is the lowest. The resulting currents during motor start-up can be seen in Figure 11 (color coding as in Figure 12). The measurement is split into three time frames T_1, T_2 and T_3. Figure 13 shows a separate close-up of the current curves in T_1. During Pulse Injection, the highest current rise can be observed in P1, while the lowest occurs in P3, due to the different phase inductances.

The ASIC correctly determines the rotor alignment based on these currents. Once Pulse Injection is fin-
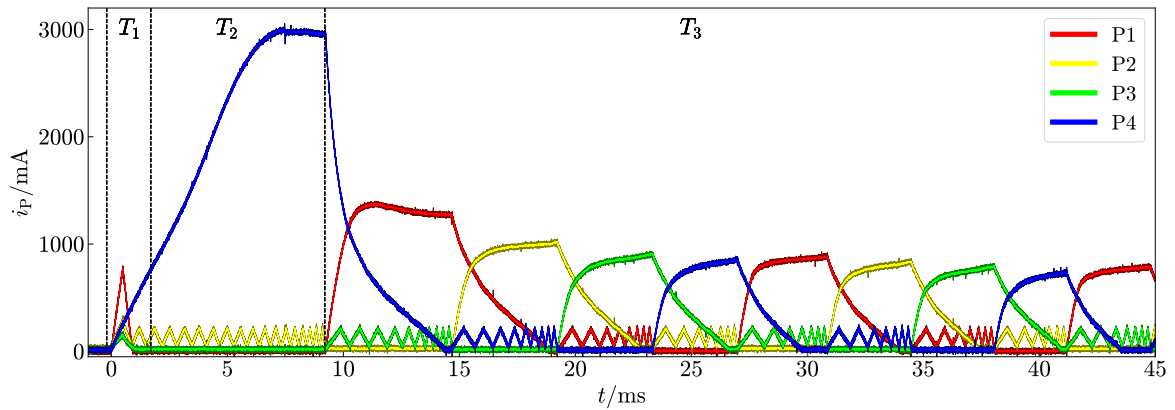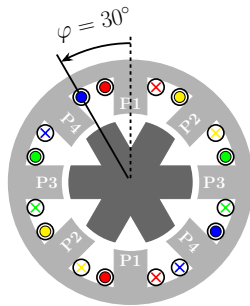
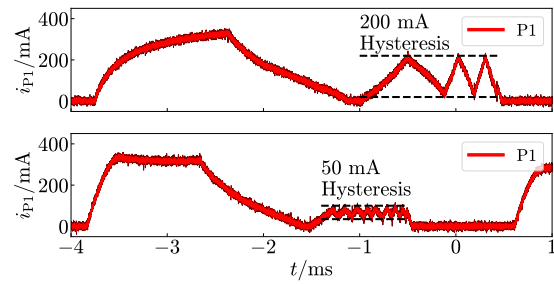Figure 11. Motor phase currents during start-up

Figure 12. Rotor 30° aligned

Figure 14. Hysteresis configuration for higher sensing granularity
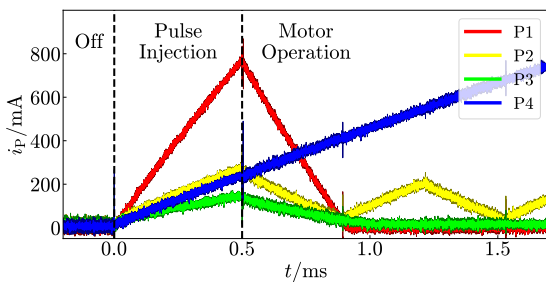
Figure 13. Motor phase currents during T_1

Figure 15. Effect of different switching thresholds

ished after $T_{\mathrm{Pulse}} = 0.5\,\mathrm{ms}$, P4 is selected as working phase and P2 as sensing phase for counterclockwise rotation.

During the time period T_2, a high current is visible in Figure 11. Due to the correlation $M \sim i_{\mathrm{P}}^2$ [5] between torque M and phase current i_{P}, the motor draws a high current building up high torque to overcome the moment of inertia.

In time period T_3, the continuous motor operation can be seen. The ASIC energizes the working phases (W) and sensing phases (S) in the following chronological order:

$$(\texttt{W1, S3}) \rightarrow (\texttt{W2, S4}) \rightarrow (\texttt{W3, S1}) \rightarrow$$
$$(\texttt{W4, S2}) \rightarrow (\texttt{W1, S3}) \rightarrow \ldots$$

To test the HCC, the current hysteresis is reduced through the digital interface, increasing the granularity of the frequency measurement as shown in Figure 14. The smaller hysteresis also leads to power loss savings due to smaller currents in the sensing phase.

Next, the threshold frequency f_{th} is changed from $18.9\,\mathrm{kHz}$ to $9.9\,\mathrm{kHz}$, resulting in earlier phase switching and thus faster rotation as pictured in Figure 15.

Altogether, the measurements prove the correct function of the adjustable hysteresis controller, the StartUp position detection and the serial interface.

IV. CONCLUSION

The paper at hand introduces improvements to previous ASIC developments for sensorless SRM control which allow the control of any 8/6 SRM. Additionally, the ASIC offers rotor position detection supporting a soft start of the machine, as well as convenient configuration options via an SPI interface.

ACKNOWLEDGEMENTS

REFERENCES

[1] Erik John, Till Moldenhauer, Zong Xern Sim, and Eckhard Hennig. "Design of an ASIC for Sensorless Control of a Switched Reluctance Motor". In: (June 2022).

[2] Annika Walz-Lange and Gernot Schullerus. "Sensorless Control of a Switched Reluctance Machine Based on Switching Frequency Evaluation". In: *IEEE Transactions on Industry Applications* 58.4 (2022), pp. 4768–4777. DOI: 10.1109/TIA.2022.3173595.

[3] Hai-Jin Chen, Long-Xing Shi, Rui Zhong, and Wei-Ping Jing. "A robust non-reversing starting scheme for sensorless switched reluctance motors". In: *2009 International Conference on Mechatronics and Automation*. 2009, pp. 2297–2301. DOI: 10.1109/ICMA.2009.5246744.

[4] Erik John. "Entwurf einer adaptierbaren digitalen Konfigurations- und Testschnittstelle für anwendungsspezifische integrierte Schaltungen". In: (Reutlingen University, 2023).

[5] Annika Walz-Lange. "Entwicklung einer leistungselektronischen Baugruppe zur Ansteuerung einer geschalteten Reluktanzmaschine". In: (Reutlingen University, 2020).

Bekir Djanklich received his Bachelor degree in Mechatronics in 2022 from Reutlingen University. Currently he pursues his Master degree in Power- and Microelectronics at Reutlingen University. Recent activities include the ASIC development for switched reluctance motors.

Sven-Stefan Korb Soldado received his Bachelor degree in Mechatronics in 2022 from Reutlingen University. Currently he pursues his Master degree in Power- and Microelectronics at Reutlingen University. Recent activities include the ASIC development for switched reluctance motors.
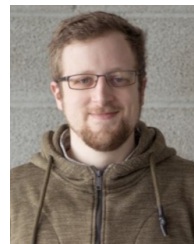
Samuel Lotfey received his Bachelor degree in Mechatronics in 2022 from Reutlingen University. Currently he pursues his Master degree in Power- and Microelectronics at Reutlingen University. Recent activities include the ASIC development for switched reluctance motors.

Maximilian Wiendl received his Bachelor degree in Automotive Engineering from Esslingen University of Applied Sciences. Currently he pursues his Master degree in Power- and Microelectronics at Reutlingen University. Recent activities include the ASIC development for switched reluctance motors.

Eckhard Hennig received the Dipl.-Ing. degree in Electrical Engineering from the Technical University of Braunschweig, Germany, in 1994 and the Dr.-Ing. degree from the University of Kaiserlautern, Germany, in 2000. He is a Professor of digital and integrated circuits with Reutlingen University, Germany. His research interests include low-power CMOS circuit design for smart-sensor applications and electronic design automation.

Intelligente Lasten

Dominik Stolte

Zusammenfassung—Ziel dieser Arbeit war die Entwicklung einer elektronischen Last, die auf einem FPGA als Regler basiert. Die Verwendung von FPGAs ermöglicht es, die Leistungsfähigkeit und Flexibilität elektronischer Lasten zu verbessern. In dieser Arbeit werden die für das Design der elektronischen Last relevanten Theorien ausführlich dargestellt und deren Implementation näher erläutert. Zudem wird ein Algorithmus auf Basis der Zustandsraumdarstellung vorgestellt, der es ermöglicht, beliebiges lineares Lastverhalten in einem FPGA zu simulieren.

Schlüsselwörter—FPGA, Regelungstechnik, Filter

I. Motivation

Eine elektronische Last ersetzt eine konventionelle ohmsche Last beim Test einer elektrischen Quelle. Sie kann – je nach Einstellung – als ohmscher Widerstand, als Konstantstromsenke, Konstantleistungssenke, oder Konstantspannungssenke betrieben werden.

Komplexeres Zweipolverhalten kann mithilfe einer PC-Schnittstelle zur Fernsteuerung erzeugt werden. Hierfür ist es erforderlich, dass die aktuelle Spannung der Last abgefragt wird und aus dieser abgetasteten Spannung einen Stromsollwert bestimmt wird. Die Latenzzeiten dieser Schnittstelle sind typischerweise nicht vorhersagbar und liegen im Millisekundenbereich. Aufgrund der fehlenden Echtzeitfähigkeit ist eine präzise Regelung nicht möglich. Die Bandbreite einer Regelung wird durch die hohe Latenz begrenzt.

Abbildung 1 beschreibt die grundsätzliche Funktionalität der entwickelten Last mit einer abgetasteten Spannung, die in einem FPGA in einen Stromsollwert gewandelt wird. Zur Spannungsquelle hin verhält sich die Last nun wie ein komplexer zeit- und zustandsabhängiger Zweipol.

Die Arbeit enthält als Neuerung zu erhältlichen Lasten eine Implementierung, die interne Zustände enthält, welche genutzt werden können, um ein zustandsabhängiges Verhalten zu erzeugen. Eine mögliche Last ist z.B. ein Motor, dessen interner Zustand die Rotationsgeschwindigkeit des Rotors ist, deren Integral die Position des Rotors ist. Die Position wird in einer realen Anwendung genutzt, um die Rotationsgeschwindigkeit zu bestimmen und diese dann zu regeln.

Als Leistungssenke wurde ein DCDC-Konverter genutzt, der elektrische Leistung aufnimmt. Das Pulsbreitenverhältnis des Konverters bestimmt die aufgenommene Leistung.

Dominik Stolte, stolte@vh-s.de. Von Hoerner & Sulger GmbH, Schlossplatz 12, 68723 Schwetzingen.
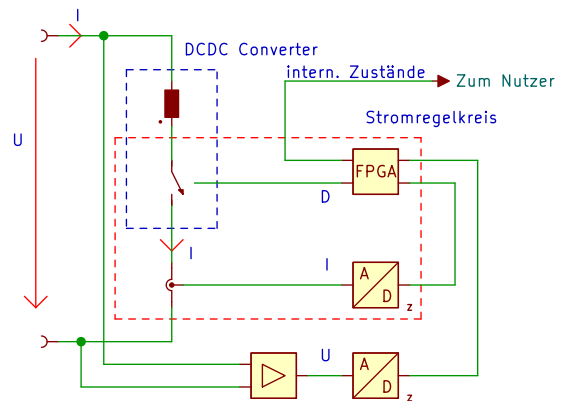
Abbildung 1. Blockschaltbild der entwickelten Last.

II. Elektrische Zweipole

Als elektrischen Zweipol bezeichnet man ein elektrisches Bauelement mit 2 Anschlüssen. Das Verhalten an den Klemmen dieses Bauelements wird durch seine Eigenschaften bestimmt. So haben resistive Zweipole eine Spannung/Strombeziehung ohne ein Zeitverhalten. Induktive und kapazitive Zweipole hingegen haben ein Zeitverhalten. Aus Sicht einer angeschlossenen Quelle erscheint eine elektronische Last als Zweipol.

III. Zustandsraumdarstellung

Die Zustandsraumdarstellung von Systemen ist eine von mehreren Möglichkeiten, ein System zu beschreiben. Sie wurde in den 1960er Jahren von Rudolf E. Kálmán entwickelt und ermöglicht es, dynamische Systeme zu beschreiben und zu analysieren. Sie wird häufig in der Regelungstechnik verwendet, um Regelungsstrategien zu entwickeln und die Stabilität und Leistung von Regelungssystemen zu überprüfen. Die Zustandsraumdarstellung setzt nicht voraus, dass das System linear und zeitinvariant ist. Sie eignet sich allerdings am besten für die Analyse von Systemen, die diese Voraussetzungen erfüllen.

A. Einführung

Das Verhalten eines dynamischen Systems wird durch eine Differenzialgleichung n-ter Ordnung beschrieben, wobei n die Anzahl voneinander unabhängiger Speicher ist. Die Differenzialgleichung beschreibt die Abhängigkeit des dynamischen Systems vom Zustandsvektor $\vec{x}$ der Speicher und vom Eingangssignalvektor $\vec{u}$.

In Zustandsraumdarstellung wird das System n-ter Ordnung, in ein Gleichungssystem von n Differenzialgleichungen erster Ordnung überführt. Sie beschreibt Systeme mit den beiden folgenden Vektordifferenzialgleichungen in Matrizenform:

$$\dot{\vec{x}}(t) = \boldsymbol{A}(t)\vec{x}(t) + \boldsymbol{B}(t)\vec{u}(t) \qquad (1)$$

$$\vec{y}(t) = \boldsymbol{C}(t)\vec{x}(t) + \boldsymbol{D}(t)\vec{u}(t). \qquad (2)$$

Mit der Systembeschreibung im Zustandsraum ist es möglich, single-input-single-output (SISO), wie auch multiple-input-multiple-output (MIMO) Systeme zu beschreiben. Weiterhin ermöglicht die Zustandsraumdarstellung, die Beschreibung von nichtlinearen Systemen. Lineare Systeme haben keine Zeitabhängigkeit in den systembeschreibenden Matrizen – aus $\boldsymbol{A}(t)$ wird $\boldsymbol{A}$ etc.

B. Übertragungsfunktion

Ist die Übertragungsfunktion gesucht, so kann diese allgemein durch den folgenden Zusammenhang, mit $\boldsymbol{I}$ als der Einheitsmatrix, ermittelt werden:

$$\boldsymbol{\Phi} = (s\boldsymbol{I} - \boldsymbol{A})^{-1}; \; G(s) = \boldsymbol{C} \cdot \boldsymbol{\Phi} \cdot \boldsymbol{B}. \qquad (3)$$

Ist das System ein MIMO System mit n Eingängen und m Ausgängen, so ist G eine $m \times n$ Matrix. Es gilt:

$$\vec{y}(s) = \boldsymbol{G}\vec{u}(s). \qquad (4)$$

C. Beobachtbarkeit und Steuerbarkeit

Eine der grundlegenden Eigenschaften von dynamischen Systemen sind Steuerbarkeit und Beobachtbarkeit [1, S. 37]. Ein Zustand eines Systems ist steuerbar, wenn ein Steuersignal u_t existiert, das dazu führt, dass dieser Zustand in finiter Zeit einen gewünschten Endzustand erreicht. Trifft dies auf jeden Zustand des Systems zu, so ist dieses System „vollständig steuerbar" [2, S. 483]. Ein System ist vollständig steuerbar, wenn folgendes gilt:

$$\mathrm{rang}(\boldsymbol{Q}_\mathrm{s}) = n \text{ mit } \boldsymbol{Q}_\mathrm{s} = [\boldsymbol{B}|\boldsymbol{AB}|\boldsymbol{A}^2\boldsymbol{B}|\ldots|\boldsymbol{A}^{n-1}\boldsymbol{B}]. \qquad (5)$$

$\boldsymbol{Q}_\mathrm{s}$ wird hierbei als Steuerbarkeitsmatrix bezeichnet. Diese ist bei der Transformation in eine andere Darstellungsform wichtig.

Ein Beispiel für ein nicht steuerbares System ist das Pendel. Ohne einen Mechanismus, um Energie in das System zu einzuleiten, ist die Position zu einer Zeit t nur über die Länge des Pendels, die Auslenkung zur Zeit t_0 und die Schwerkraft bestimmt. Ein steuerbares System hingegen ist das LC-Glied. Die Zustände sind über die Eingangsspannung beeinflussbar.

Ein Zustand ist beobachtbar, wenn ein Zustand aus Messungen der Ausgangssignale zu jeder Zeit ermittelbar ist. Trifft dies auf jeden Zustand des Systems zu, so ist dieses System „vollständig beobachtbar". [2, S. 487]

Ein System ist vollständig beobachtbar, wenn folgendes gilt:

$$\mathrm{rang}(\boldsymbol{S}_\mathrm{b}) = n \text{ mit } \boldsymbol{S}_\mathrm{b} = \begin{pmatrix} \boldsymbol{C} \\ \boldsymbol{AC} \\ \boldsymbol{A}^2\boldsymbol{C} \\ \vdots \\ \boldsymbol{A}^{n-1}\boldsymbol{C} \end{pmatrix}. \qquad (6)$$

$\boldsymbol{S}_\mathrm{b}$ wird hierbei als Beobachtbarkeitsmatrix bezeichnet. Auch diese kann für die Transformation des Systems in eine andere Darstellungsform genutzt werden. Nicht beobachtbare Systeme ergeben sich bei der Parallelschaltung mehrerer Systeme. Es lässt sich nicht feststellen, wie groß der Anteil der einzelnen Systeme am Ausgang ist, ohne die einzelnen Zustandsgrößen zu messen.

D. Transformation von Zustandsdarstellungen

Die Zustandsraumdarstellung ist nicht eindeutig, da zu einem System unendlich viele Zustandsraumdarstellungen existieren. Ein Satz Zustände $\vec{x}$ kann in einen anderen Darstellungsraum zu einem neuen Satz $\vec{z}$ transformiert werden. Hierfür muss eine Transformationsmatrix $\boldsymbol{P}$ gefunden werden, bei der folgendes gilt:

$$\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \boldsymbol{D} \rightarrow \boldsymbol{PAP}^{-1}, \boldsymbol{PB}, \boldsymbol{CP}^{-1}, \boldsymbol{D}; \; \vec{z} = \boldsymbol{P}\vec{x}. \qquad (7)$$

Die neue Zustandsdarstellung beschreibt dasselbe System, weshalb alle Systemeigenschaften nach der Transformation unverändert sind.

Die Transformation von Zustandsdarstellungen kann aus verschiedenen Gründen sinnvoll sein. Ein möglicher Grund ist, dass die Transformation zu einer vereinfachten oder übersichtlicheren Darstellung des Systems führt. Diese Darstellungen können bestimmte Eigenschaften des Systems, wie die Beobachtbarkeit, die Steuerbarkeit, oder die Eigenwerte des Systems hervorheben.

E. Reglernormalform

Für diese Arbeit ist die Reglernormalform von besonderer Bedeutung. Die allgemeine Übertragungsfunktion eines SISO Systems n-ter Ordnung hat die folgende Form:

$$G(s) = \frac{a_0 + a_1 s + \ldots + a_{n-1}s^{n-1}}{b_0 + b_1 s + \ldots + b_{n-1}s^{n-1} + s^n}. \qquad (8)$$

Abbildung 2 zeigt den Signalfluss für ein beliebiges SISO System.

hochschule mannheim
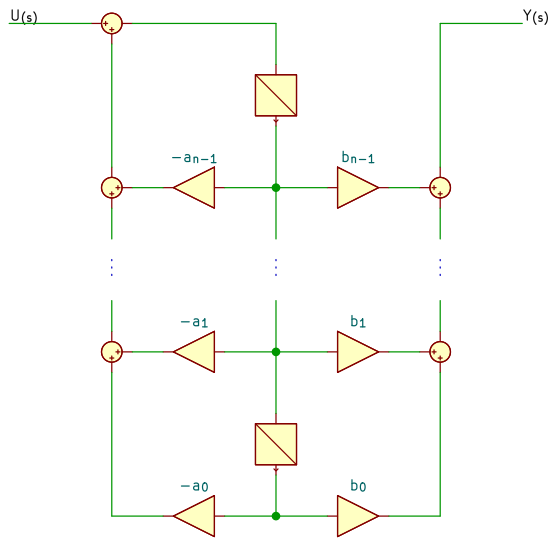
Signalfluss SISO

Abbildung 2. Signalfluss für ein SISO System in Reglernormalform.

Tabelle I
DESIGNPARAMETER DES ANALOGFRONTENDS

Symbol	Parameter	Wert
U_{ein}	Eingangsspannung	$0\,\text{V} - 40\,\text{V}$
U_{aus}	Ausgangsspannung	$0\,\text{V} - 4{,}096\,\text{V}$
R_{ein}	Eingangswiderstand	$1\,\text{M}\Omega$
B_{ein}	Wortbreite	$12\,\text{Bit}$
f_{s}	Abtastrate	$>200\,\text{ksps}$

F. Übertragung in den zeitdiskreten Bereich

Für die Berechnung der Zustände in einem FPGA ist es notwendig, das zeitkontinuierliche System in den zeitdiskreten Bereich zu übertragen. Hierfür müssen die $\boldsymbol{A}$ und $\boldsymbol{B}$ Matrizen über ein festes Zeitintervall T_{s} diskretisiert werden. Dabei gelten folgende allgemeine Zusammenhänge:

$$\boldsymbol{A}_{\text{d}} = \mathrm{e}^{\boldsymbol{A}T_{\text{s}}} \tag{14}$$

$$\boldsymbol{B}_{\text{d}} = \int_0^{T_{\text{s}}} \boldsymbol{A}_{\text{d}}\boldsymbol{B}\mathrm{d}t. \tag{15}$$

Für die Echtzeitberechnung im FPGA kann das Matrixexponential linear angenähert werden. Die Gleichungen vereinfachen sich dann zu:

$$\boldsymbol{A}_{\text{d}} = \boldsymbol{A}T_{\text{s}} + \boldsymbol{I} \tag{16}$$

$$\boldsymbol{B}_{\text{d}} = T_{\text{s}}\boldsymbol{B}. \tag{17}$$

Es ergibt sich eine zeitdiskrete Zustandsraumdarstellung mit folgender Form:

$$\vec{x}_{k+1} = \boldsymbol{A}_{\text{d}}\vec{x}_k + \boldsymbol{B}_{\text{d}}\vec{u}_k \tag{18}$$

$$\vec{y}_{k+1} = \boldsymbol{C}\vec{x}_k + \boldsymbol{D}\vec{u}_k. \tag{19}$$

Diese Methode wird als „Euler-Vorwärts" Methode bezeichnet und sie führt zu einer sprunginvarianten Diskretisierung eines Systems.

Diese Darstellung hat für ein SISO System n-ter Ordnung die folgende Form:

$$\boldsymbol{A} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ -a_0 & -a_1 & -a_2 & \dots & -a_{n-1} \end{pmatrix} \tag{9}$$

$$\boldsymbol{B} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \tag{10}$$

$$\boldsymbol{C} = \begin{pmatrix} b_0 & b_1 & \dots & b_{n-1} \end{pmatrix}. \tag{11}$$

Die Zustände $\vec{x}$ des Systems sind nun nicht mehr direkt verfügbar, können aber über die Transformationsmatrix $\boldsymbol{P}$ aus dem Zusammenhang der Gleichung 7 aus dem transformierten Zustandsvektor $\vec{z}$ bestimmt werden:

$$\vec{z} = \boldsymbol{P}\vec{x} \rightarrow \vec{x} = \boldsymbol{P}^{-1}\vec{z}. \tag{12}$$

Für die Bestimmung der Transformationsmatrix wird die Steuerbarkeitsmatrix $\boldsymbol{Q}_{\text{s}}$ in Gl. 5 genutzt. Für die Transformationsmatrix gilt dann:

$$\boldsymbol{P} = \begin{pmatrix} \boldsymbol{q}_{\text{s}}^\top \\ \boldsymbol{q}_{\text{s}}^\top \boldsymbol{A} \\ \boldsymbol{q}_{\text{s}}^\top \boldsymbol{A}^2 \\ \vdots \\ \boldsymbol{q}_{\text{s}}^\top \boldsymbol{A}^{n-1} \end{pmatrix}; \text{ mit } \boldsymbol{q}_{\text{s}} = (0,\dots,0,1)\boldsymbol{Q}_{\text{s}}^{-1}. \tag{13}$$

IV. ANALOGFRONTEND

Die Eingangsspannung der elektronischen Last liegt im Intervall von $0\,\text{V}$ bis $40\,\text{V}$. Diese Spannung muss für die A/D Wandlung herunter geteilt und gefiltert werden, um das Nyquist-Theorem für bandpassbegrenzte Systeme einzuhalten.

Zu diesem Zweck wird ein gepuffertes Butterworth Filter verwendet. Das Butterworth Filter wird durch einen Operationsverstärker von einem hochohmigen Eingangsspannungsteiler getrennt.

Die Wortbreite des Analogfrontends beträgt $12\,\text{Bit}$, welche durch Truncating im FPGA verkleinert werden kann, sollten im Laufe der Entwicklung die Routingressourcen nicht ausreichen, um das Filter zu implementieren.

Tabelle I beschreibt die Designparameter des Analogfrontends für die Spannungsmessung.

Als A/D-Wandler wurde ein LTC1420 gewählt, dessen Kennwerte in Tabelle II dargestellt sind.
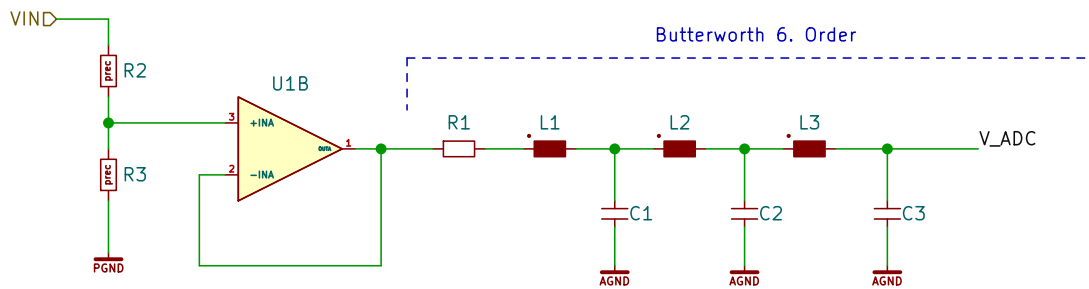
Abbildung 3. Eingangsbeschaltung des Analogfrontends.

<table>
<tr><td colspan="3" align="center">Tabelle II
A/D-WANDLER KENNWERTE</td></tr>
</table>

Symbol	Parameter	Wert
f_s	Abtastrate	10 Msps
f_{nutz}	Nutzsignalbandbreite	100 MHz
U_{ein}	Eingangsspannungsbereich	$0\,V - 4{,}096\,V$
B_{ein}	Wortbreite	12 Bit
$SINAD$	Signal zu Rauschen/Verzerrung	71 dB

Ein LSB (kleinst wertigstes Bit) hat an diesem ADC eine Wertigkeit von $1\,mV$ oder $-60\,dB$. Für eine exakte Abtastung des Signals muss der kumulierte Fehler kleiner als ein halbes LSB sein. Um dies zu erreichen, muss die Amplitude einzelner Signalbestandteile der Störsignale kleiner als $-66\,dB$ sein. Aufgrund auftretender Mess- und Bauteileungenauigkeiten wird im Folgenden mit einer maximalen Amplitude von $-70\,dB$ für alle Störungen gerechnet.

Die erforderliche Filterordnung ergibt sich aus der nachstehenden Gleichung (20) mit:

$$n = \frac{\delta_s}{20 \cdot (\log_{10}(f_0) - \log_{10}(f_s))}. \tag{20}$$

Mit f_0 als der Grenzfrequenz in Hz, f_s als der Frequenz des Stoppbandes und δ_s als der Dämpfung im Stopband. Es ist eine Filterordnung von mindestens 5 notwendig. Die Eingangsbeschaltung des LTC1420 fordert einen Kondensator am Eingang. Daher wird die Filterordnung auf 6 erhöht.

Abbildung 3 zeigt die Filterschaltung des Analogfrontends. Die Widerstände $R2$ und $R3$ bilden einen Spannungsteiler, der die Verstärkung und den Eingangswiderstand des Frontends bestimmt. Die Verstärkung wurde so gewählt, dass die Eingangsspannung einen Bereich von 0 bis $50\,V$ abdeckt, da diese in der Leistungselektronik durch eine Zenerdiode auf $47\,V$ begrenzt wird. Die 0 - $50\,V$ werden auf den Eingangsspannungsbereich des ADC von 0 bis $4{,}096\,V$ herunter geteilt und vom Operationsverstärker U1 gepuffert. Der Verstärkungsfaktor G_{AFE} beträgt somit $\frac{4095}{50}\,\frac{1}{V}$ und kann mittels Trimmpotentiometer genau eingestellt werden. Eine Spannung von $1\,V$ am Eingang des Analogfrontends entspricht somit einem ADC Wert von 82. Das Netzwerk bestehend aus dem Widerstand $R1$

<table>
<tr><td colspan="4" align="center">Tabelle III
BAUTEILPARAMETER DER FILTERKOMPONENTEN</td></tr>
</table>

Bauteil	Wert	Bauteil	Wert
$L1$	$1{,}236\,\mu H$	$C1$	$4{,}021\,nF$
$L2$	$5{,}737\,\mu H$	$C2$	$8{,}238\,nF$
$L3$	$8{,}400\,\mu H$	$C3$	$8{,}238\,nF$

und den nachfolgenden Induktivitäten und Kapazitäten bildet ein passives Butterworth Filter mit der Ordnung n von 6.

[4, S. 104] beschreibt die Bestimmung der Bauteilwerte für passive LC-Netzwerke. Die normierten Werte des Filters bestimmen sich nach folgenden Gleichungen:

$$a_k = \sin\left(\frac{\pi}{2}\frac{2k-1}{n}\right); \quad k = 1, 2, \ldots, n \tag{21}$$

$$c_k = \cos^2\left(\frac{\pi k}{2n}\right); \quad k = 1, 2, \ldots, n \tag{22}$$

$$g_1 = a_1; \quad g_k = \frac{a_k a_{k-1}}{c_{k-1} g_{k-1}}; \quad k = 2, 3, \ldots, n. \tag{23}$$

Die ungeraden Indices k der Reihe g_k enthalten hierbei die normierten Bauteilwerte der Kapazitäten und die geraden Indices, die der Induktivitäten. Durch Denormalisierung lassen sich die konkreten Bauteilwerte aus der Grenzkreisfrequenz ω_c und dem Eingangswiderstand $R1$ ableiten:

$$L_k = \frac{R1 \cdot \omega'}{R' \cdot \omega_c} L'_k \quad C_k = \frac{R' \cdot \omega'}{R1 \cdot \omega_c} C'_k. \tag{24}$$

Für ein einseitig terminiertes Butterworth Filter mit dem Eingangswiderstand von $30\,\Omega$ und einer Grenzfrequenz von $1\,MHz$, sowie den Skalierungsfaktoren $R' = 1\,\Omega$ und $\omega' = 1\,Hz$ ergeben sich nach Anwendung der obigen Formeln die in Tabelle III aufgeführten Bauteilparameter.

Da Bauelemente nicht in beliebigen Nennwerten verfügbar sind und Induktivitäten parasitäre Effekte aufweisen, wurde die Einhaltung der Spezifikation durch eine Simulation verifiziert.

Abbildung 5 zeigt die Abweichungen aufgrund der Nutzung real verfügbarer Bauelemente. Die Verstärkung an der Stellen $100\,kHz$ und $5\,MHz$ sind in Tabelle IV angegeben.
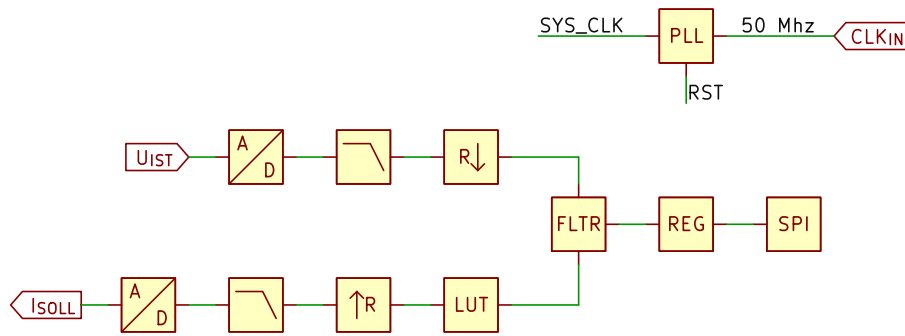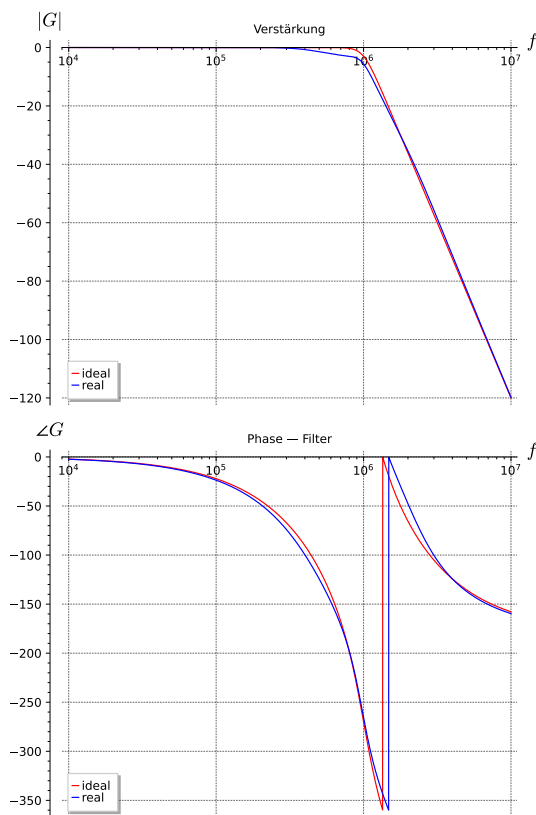
Abbildung 4. FPGA Systemebene.

Abbildung 5. Bode Diagramm des realen und idealen Filters.

Tabelle IV
VERSTÄRKUNGEN BEI 100 kHz UND 5 MHz

Frequenz	$|G(f)|$		
	ideal	real	Spezifikation
100 kHz	$-2{,}13\,\mu$dB	$-2{,}2\,$mdB	$-2{,}75\,$mdB
5 MHz	$-83{,}88\,$dB	$-83{,}07\,$dB	$-70{,}00\,$dB

Tabelle V
TAKTFREQUENZEN DER MODULE

Modul	Clock	Teiler
ADC	10,0 MHz	4
DAC	20,0 MHz	2
CIC-Dezimator	10,0 MHz / 312,500 kHz	4 / 128
CIC-Interpolator	10,0 MHz / 312,500 kHz	4 / 128
Filter	312,500 kHz	128
Register	20,0 MHz	2
Look-Up-Table	312,500 kHz	128
SPI Controller	20,0 MHz	2

V. DESIGN DES FPGA

Die Abbildung 4 beschreibt das Design des FPGA. Ein SPI Master wird genutzt, um mit dem FPGA zu kommunizieren. Über die SPI Schnittstelle kann ein beliebiger Master eine Verbindung mit dem FPGA aufbauen und Daten mit diesem austauschen. Die SPI Schnittstelle kann genutzt werden, um die A und B Parameter vorzugeben und damit die Funktion des Filters zu beeinflussen. Weiterhin ist es möglich, die Zustände $\vec{z}$ des Filters abzurufen.

A. Clock-Management-Unit

Die Clock-Management-Unit besteht aus einer PLL Zelle im FPGA und einem Zähler, welcher es ermög-licht den PLL Takt durch Exponenten von 2 zu teilen. Der Ausgang der einzelnen Takte ist phasengleich und es werden Takte mit einem Teilungsfaktor von bis zu 128 erzeugt. Tabelle V zeigt, welche Takte in welchem Modul benötigt werden.

Nach dem Power-On-Reset des FPGA wird der PLL Takt erzeugt und die Takte für die einzelnen Module werden durch den Timer erzeugt. Die PLL Zelle erzeugt ein „Locked" Signal, sobald die PLL stabil ist. Das Inverse Signal wird genutzt, um global den Reset der einzelnen Module zu aktivieren. Der Reset wird asynchron aktiviert und bleibt bestehen, bis der PLL Takt stabil ist. Der Reset wird dann synchron mit dem jeweiligen Takt deaktiviert.

B. ADC Ansteuerung

Abbildung 6 beschreibt die Takterzeugung inner-halb des FPGA. Zur Ansteuerung des Analog-Digital-Konverters ist eine Taktrate von 10 MHz erforderlich. Diese wird von einem Frequenzteiler aus dem System-takt des FPGA gewonnen, sodass die Abtastung des Analog-Digital-Konverter synchron zum Systemtakt, bei der steigenden Flanke des ADC Taktes, möglich ist. Der Analog-Digital-Konverter Takt wird direkt nach
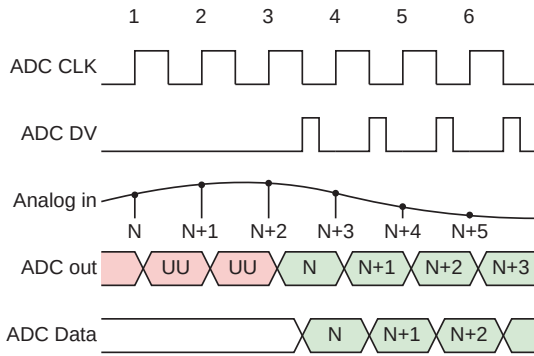
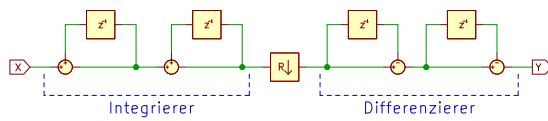Abbildung 6. FPGA ADC Datenerfassung.
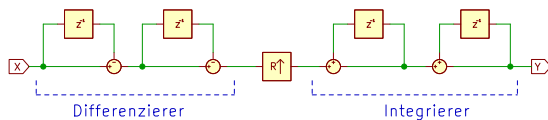

Abbildung 7. CIC Dezimationsfilter.

Abbildung 8. CIC Interpolationsfilter.

dem Reset des FPGA erzeugt. Die Architektur des AD-Konverters führt nach dem Start des AD-Konverters zu 2 falschen Datenworten [3]. Diese werden nach dem Reset des FPGA verworfen und erst ab dem dritten Datenwort, wird der richtige Messwert am Ausgang sichtbar.

C. Dezimationsfilter

Das Dezimationsfilter ermöglicht es, die Rechenoperationen auf die Eingangsdaten mit einer kleineren Taktfrequenz, als der Abtastrate durchzuführen. Dies ermöglicht es mit kleineren Registerbreiten zu rechnen, da die Koeffizienten nun einen größeren Wert annehmen. Das Dezimationsfaktor R beträgt 32, was zu einem Filtertakt von nur noch 312,500 kHz anstatt 10,0 MHz führt.

Es wurde ein Dezimationsfilter 2. Ordnung in CIC Struktur implementiert. Das CIC Filter nutzt ausschließlich Additionen und Register, was es ermöglicht, die Dezimation schnell und ressourcensparend durchzuführen. Die Abb. 7 zeigt die implementierte Struktur. Das Dezimationsfilter führt die Dezimation durch, indem es von den integrierten Werten nur jeden R-ten Wert ausliest.

D. Interpolationsfilter

Das Interpolationsfilter ist erforderlich, da das Filter mit einer kleineren Taktfrequenz betrieben wird, als die Stromregelung. Dies würde zu starken Sprüngen in den
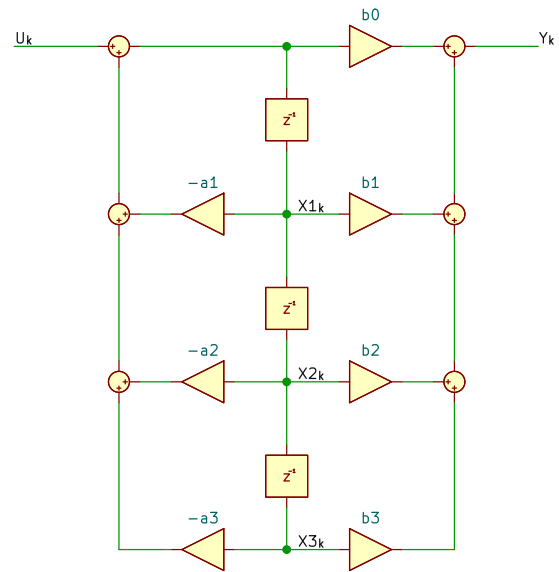

Abbildung 9. FPGA-Filter in Direktform II.

Ausgangssignalen führen, wenn das Filter einen neuen Wert errechnet hat. Um dieses Verhalten zu vermeiden, wird ein Interpolationsfilter in CIC Topologie analog zum Dezimationsfilter im vorigen Abschnitt genutzt.

Es wurde erneut ein Filter 2. Ordnung in CIC Struktur implementiert. Abbildung 8 zeigt die implementierte Struktur.

E. Speicher

Der Speicher ist als 16 Bit breites Register implementiert und dient der Speicherung der aktuellen Mess- und Ausgangswerte der verschiedenen Module, sowie der Speicherung der aktuellen Filterkoeffizienten. Die Inhalte der Register lassen sich per SPI Schnittstelle lesen und schreiben. Hierbei ist es nicht möglich, die Ausgaben der Module zu überschreiben, um undefiniertes Verhalten zu vermeiden.

F. Filter

Abbildung 9 beschreibt die implementierte Filterstruktur im FPGA. Es handelt sich um ein diskretes Filter in Direktform II, dessen A und B Parameter sich aus den Gleichungen in Abschnitt III direkt ergeben. Die Implementation des Filters ist die digitale Entsprechung der zeitkontinuierlichen Filterdarstellung in Abbildung 2.

VI. AUSWERTUNG

A. Filter

Um die Funktion des Digitalteils im FPGA im Zeitbereich zu überprüfen, wurde ein Rechtecksignal an den Filtereingang gelegt. Die Filterantwort wurde über einen am FPGA angeschlossenen DAC in ein
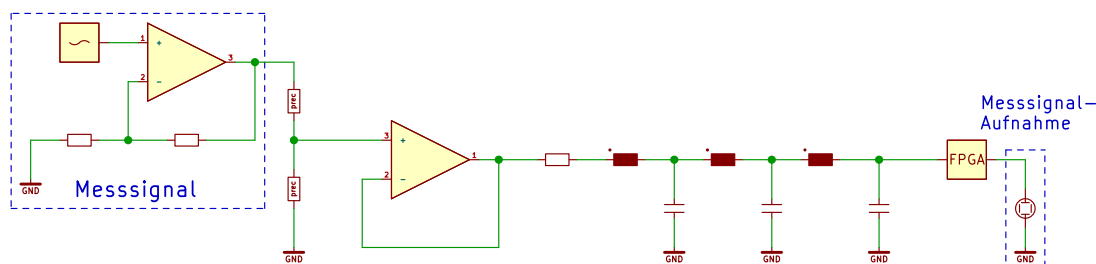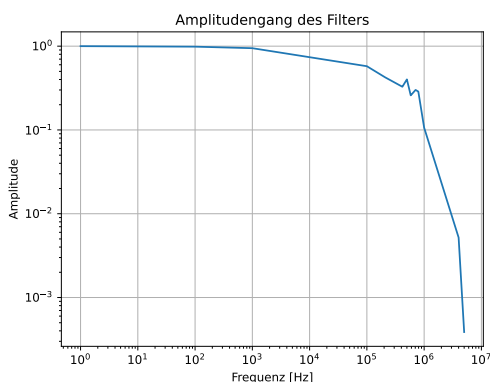
Abbildung 10. Messaufbau der Filtermessung.

Abbildung 11. Amplitudengang des Analogfrontends.

Abbildung 12. Das LR-Glied.

Analogsignal gewandelt und dann gemessen. Dies ermöglicht es, das Zeitverhalten des Filters direkt am Oszilloskop abzubilden, ohne dass zusätzliche Debuglogik synthetisiert werden muss. Der Messaufbau ist in Abbildung 10 dargestellt.

Um den Aussteuerbereich des Analogfrontends abzudecken ist es notwendig, das Ausgangssignal eines Signalgenerators zu verstärken.

Die Messung des Amplitudengangs ergab eine Abweichung vom simulierten Amplitudengang. Dies ist auf die Ungenauigkeit der verwendeten Bauteile zurückzuführen. Die Abweichung ist in Abbildung 11 dargestellt.

B. Modelltests

Die Messung in Abbildung 10 konnte genutzt werden, um die Funktion des Filters zu validieren.

Zu diesem Zweck wurde das Modell des LR-Glieds (Abb. 12) verwendet.

Das LR-Glied ist als Zweipol ein Tiefpass 1. Ordnung. Es speichert Energie im magnetischen Feld einer Spule. Dem Anstieg des Stroms wirkt hier ein Widerstand entgegen.

Die Übertragungsfunktion des LR-Glieds lautet:

$$G(s) = \frac{I_{\mathrm{LR}}}{U_{\mathrm{in}}} = \frac{1}{Ls + R}. \tag{25}$$

Die systembestimmende Gleichung lautet:

$$\frac{\mathrm{d}i_{\mathrm{LR}}}{\mathrm{d}t} = \frac{1}{L}(u_L - I_L R). \tag{26}$$
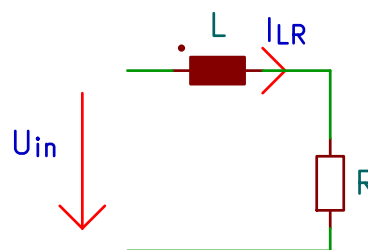
In Zustandsraumdarstellung wird das System so beschrieben:

$$(\dot{i}_L) = \left(-\frac{R}{L}\right) \cdot (i_L) + \left(\frac{1}{L}\right) \cdot (u_L) \tag{27}$$

$$(i_L) = (1) \cdot (i_L) + \mathcal{O} \cdot (u_L). \tag{28}$$

Mit den Gleichungen 27 und 28 lassen sich die A und B Parameter des Filters bestimmen. Daraufhin wurde mit dem Funktionsgenerator eine Sprungfunktion erzeugt und die Sprungantwort aufgenommen.

Die Abbildung 14 zeigt die Systemantwort auf einen Eingangssprung von 0 V auf 7 V.

Die Abbildungen 15 bis 17 zeigen die Systemantwort auf eine Sinusanregung mit 200 kHz, der Grenzfrequenz 1590 kHz und 22 kHz. In diesen Abbildungen sind das Frequenzverhalten des Filters erkennbar.

VII. ZUSAMMENFASSUNG UND FAZIT

Abbildung 13 zeigt die entwickelte Schaltung mit Converter und Frontend. In dieser Arbeit wurden mehrere Ergebnisse erzielt. Es wurde ein Analogfrontend entwickelt, welches eine präzise Spannungsmessung ermöglicht.

Darüber hinaus wurde eine Filtertopologie entwickelt und in einem FPGA implementiert, welche eine Simulation von Systemen bis zur dritten Ordnung ermöglicht. Die Filtertopologie ist erweiterbar, solange entsprechende Ressourcen im FPGA zur Verfügung stehen.

Ein weiteres Ergebnis der Arbeit ist die Entwicklung von Modellen für verschiedene Lasten und die Erstellung der Berechnungsvorschriften für diese Lasten. Dadurch wird es ermöglicht, die Koeffizienten für diese Lasten einfach zu bestimmen, was die Anwendung vereinfacht.
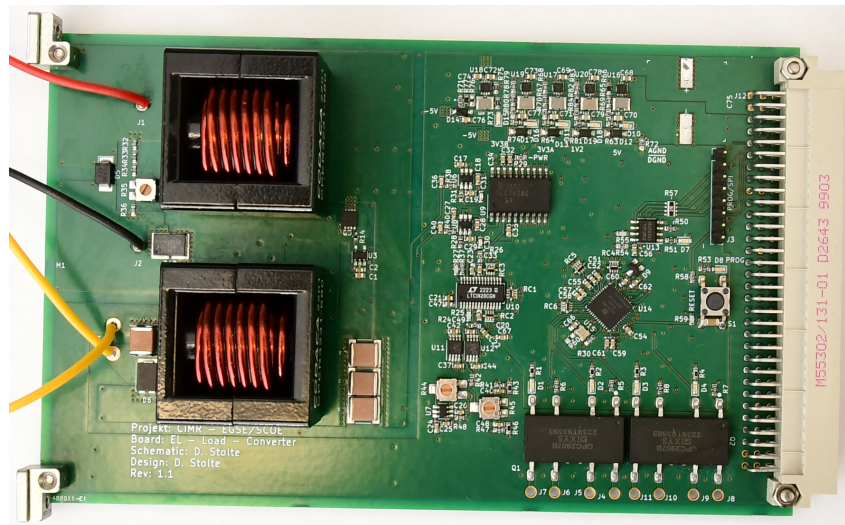
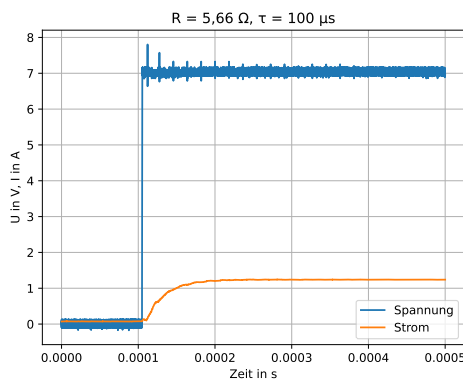Abbildung 13. Entwickelte Schaltung mit Converter und Frontend.

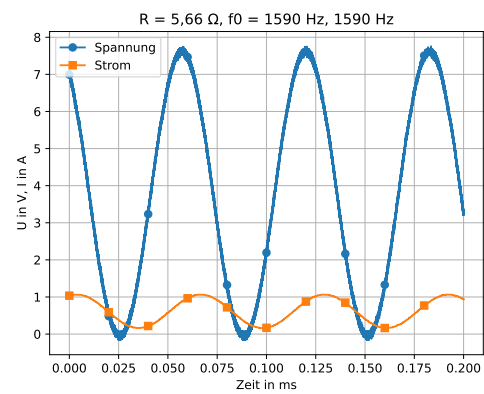Abbildung 14. Sprungantwort R = 5,66 Ω und $\tau = 100\,\mu$s.

Abbildung 16. R = 5,66 Ω und $f_c = 1{,}59\,$kHz, 1590 Hz.
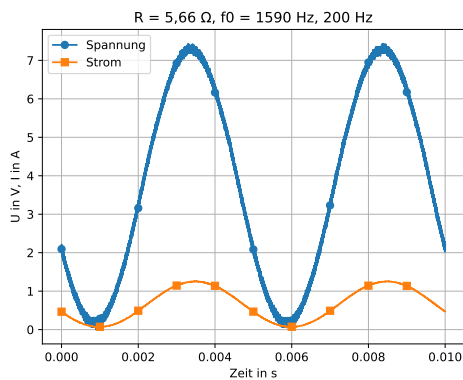
Abbildung 15. R = 5,66 Ω und $f_c = 1{,}59\,$kHz, 200 Hz.
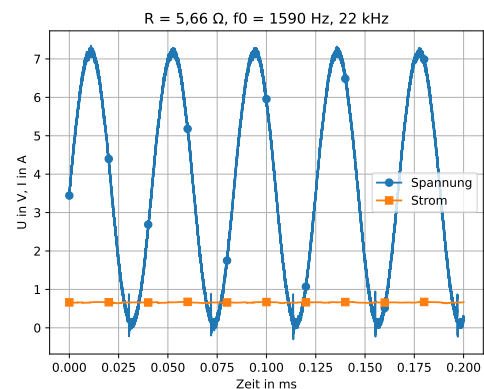
Abbildung 17. R = 5,66 Ω und $f_c = 1{,}59\,$kHz, 22 kHz.

VIII. AUSBLICK

Auf Basis dieser Arbeit ergeben sich weitere mögliche Entwicklungsrichtungen:

- Leistungselektronik: Im Rahmen der Arbeit wurde ein DC DC-Konverter in SEPIC Topologie

genutzt, um elektrische Leistung aufzunehmen. Die Nutzung eines DCDC-Konverters verursacht besonders bei großen aufgenommenen Strömen Störungen im Analogfrontend. Alternativ zu geschalteten DCDC-Konvertern ist die Verwendung

hochschule mannheim

von Verstärkern im Linearbereich möglich. Diese wandeln die aufgenommene Energie direkt in Wärme um.

- Analogfrontend: Die Nutzung eines Sigma/Delta ADC erlaubt es die Dezimation bereits im ADC durchzuführen. Dies würde das Filter im Analogfrontend vereinfachen.

- Lastquadranten: Die entwickelte Last erlaubt nur die Verarbeitung positiver Spannungen und Ströme. Dies kann durch die Entwicklung eines Analogfrontends, welches positive und negative Spannungen erfassen kann, auf andere Lastquadranten erweitert werden.

- Digitalfilter: Durch die Dezimation im FPGA ergibt es sich, dass Ressourcen im Filter frei werden. So können mehrere Multiplikationen von einem Multiplikator durchgeführt werden.

- FPGA: Die Multiplikatoren und Speicherressourcen des FPGA wurden im Laufe dieser Arbeit voll ausgenutzt. Dieses Problem könnte durch die Nutzung eines anderen FPGA gelöst werden. Die verwendete Toolchain unterstützt neben Lattice ICE40 FPGA, auch die größere ECP5 Familie, sowie Typen von Xilinx. Ein Grund für die Verwendung des ICE40 war die Verfügbarkeit der Bauteile und die Handlötbarkeit des Bauelements.

LITERATURVERZEICHNIS

[1] Walter Hildebrand. *Zustandsregelung*. Wiesbaden, Springer Vieweg, 2019.

[2] R.E. Kalman. „On the general theory of control systems". In: *IFAC Proceedings Volumes* 1.1 (1960). 1st International IFAC Congress on Automatic and Remote Control, Moscow, USSR, 1960, S. 491–502.

[3] Linear Technologies. *LTC1420 12-Bit 10Msps Sampling ADC*. 1999.

[4] G. L. Matthaei, L. Young und E. M. T. Jones. *Microwave Filters, Impedance-Matching Networks, and Coupling Structures*. ARTECH HOUSE. Artech House Microwave Library, 1964.

Dominik Stolte erhielt den akademischen Grad des Master of Science in Informationstechnik von der Hochschule Mannheim im Jahr 2023. Aktuell arbeitet er als Entwicklungsingenieur bei der von Hoerner und Sulger GmbH im Bereich der Hardwareentwicklung für Raumfahrtsysteme.

Development, Simulation, and Validation Environment for Autonomous Driving Algorithms Based on a ROS Architecture

Constantin Blessing, Reiner Marchthaler

Abstract—Virtual environments for development, simulation, and validation of robot applications are indispensable, constituting a cheap, safe, and often faster alternative to working with real-world vehicles. Consequently, the scope of this paper covers the design and implementation of such an environment geared to the needs of smaller scaled autonomous driving applications based on a robot operating system architecture.

Index Terms—Autonomous Driving, Simulation, Robot Operating System, Vehicle Dynamics, Robotics

I. INTRODUCTION

In an era of rapid technological advancements, the quest for autonomous driving (AD) has emerged as a pivotal challenge in the realm of computer engineering. With the aim of increasing vehicle safety, optimizing traffic flow, and revolutionizing transportation systems, researchers and engineers have turned their attention toward developing intricate algorithms capable of enabling vehicles to navigate and operate autonomously. But achieving autonomy comes at the cost of increasing algorithmic complexity and corresponding validation.

While the commercial automotive industry offers extensive and powerful ecosystems for developing and validating AD algorithms — often advertised for their certification capabilities — their feature set and complexity are often excessive for smaller scaled projects where such aspects are less relevant.

Therefore, the objective of this paper is to investigate the feasibility of a practical, functional, and easy-to-use framework that supports the efficient development, simulation, and validation of AD algorithms for smaller scaled applications.

The resultant environment is presented in the context of the autonomous model vehicle depicted in Figure 1. This vehicle's software stack is built on top of the robot operating system (ROS) and its sensor suite encompasses a stereo RGB camera for lane and object detection, two reflectance sensors to measure the wheel speeds of the front left-hand and front right-hand

Constantin Blessing, constantin.blessing@hs-esslingen.de, Reiner Marchthaler, reiner.marchthaler@hs-esslingen.de. Esslingen University of Applied Sciences, Flandernstraße 101, 73732 Esslingen, Germany.
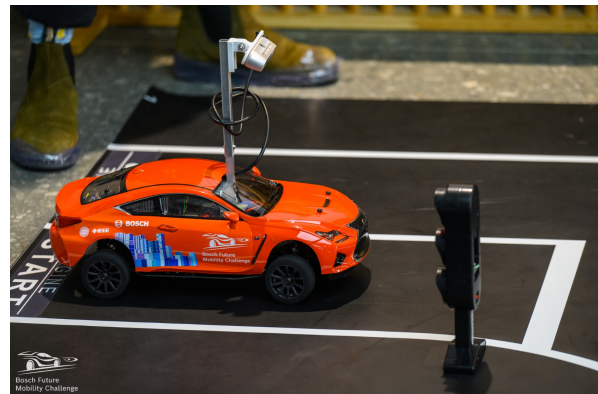
Figure 1. The real-world vehicle serving as the basis for the digital counterpart. Source: [1]

wheels, respectively, and an inertial measurement unit (IMU) capturing rotation and acceleration [2].

The remainder of this paper is structured as follows: Section II investigates currently available simulation and development frameworks relevant to the objective of this work, and section III outlines the driving factors behind the development, simulation, and validation environment presented in this paper. The environment's goals and objectives are subsequently highlighted in section IV. Continuing with Section V, the conceptual ideas behind the environment are discussed, followed by the actual implementation in section VI. An overview of the resultant environment can be found in section VII. Finally, section VIII and IX will conclude the paper and provide an outlook, respectively.

II. RELATED WORK

J. Collings et al. provide an overview of numerous physics-based simulators for robotics applications [3]:

The AirSim simulator features simulated environments powered by Unreal Engine and is focused on the simulation of aerial vehicles such as drones, but also features support for wheeled vehicles [4]. Due to being built on top of Unreal Engine, AirSim can portray environments with a high degree of realism, lending itself well to generating camera-based training data for machine vision applications. In addition to cameras, sensors such as IMU, GPS, and barometer

are part of its supported sensor suite [4]. AirSim can serve as a simulation and development environment on all major operating systems, i.e. Linux, Windows, and MacOS. First published in 2017, it is scheduled to be archived in 2024 and will be replaced by Project AirSim [5].

Arguably the most well known simulator is Gazebo. Being maintained by Open Robotics, Gazebo possesses good integration with ROS. The Gazebo simulator incorporates an accurate physics simulation and a wide range of sensors, such as IMU, LiDAR, and camera [6, 3], although its suitability for high-fidelity image generation is limited compared to Unity- or Unreal Engine-based simulations [3]. In addition, if the existing array of sensors is insufficient, Gazebo features a plugin system through which new sensors can be implemented. In terms of cross-platform functionality, Gazebo is best suited for a Linux-based operating system (OS). Windows operating systems are only supported by the community, hence full functionality is not officially guaranteed [7].

A popular alternative to Gazebo is CoppeliaSim, a versatile and scalable robot simulation framework [8]. Worth mentioning is CoppeliaSim's capability to embed functionality directly within its environment using Lua scripting, additionally making it a powerful development environment. Moreover, like Gazebo, it features a large array of preimplemented sensors but also lacks sophisticated realistic rendering [3]. Noteable is the inclusion of a path planning module that can handle non-holonomic vehicles like cars. Similarly to AirSim, this simulation framework supports all major operating systems, although with the disadvantage of not being free for commercial use.

Alternatively, NVIDIA Isaac Sim is a high-fidelity robotics simulator built on Omniverse, offering PhysX-powered physics and ray-traced rendering for realistic sensor simulation [9]. Unlike Gazebo and CoppeliaSim, it excels at photorealistic perception data generation, making it ideal for AI-based applications. However, it requires NVIDIA GPUs for optimal performance and is primarily optimized for Linux, limiting its versatility compared to cross-platform alternatives.

Lastly, [10] derives a framework for vehicle control and simulation based on ROS and Unity, leveraging ROSBridge for cross-communication between the two tools. Through two validation use cases, [10] details their framework's support for non-holonomic robots and sensors such as LiDAR. Also described in the paper is a quite extensive manual setup process for the proposed framework. Finally, it is not immediately clear whether the introduced framework is cross-platform.

III. MOTIVATION

The motivation underpinning this research stems from several key challenges that pervade the landscape of embedded development, specifically the development of autonomous driving algorithms:

1) **Limited Hardware Availability:** The tangible constraints of time, resources, and safety considerations impede the expansive deployment of autonomous vehicles for rigorous real-world validation and testing.
2) **Demands of AI-based Algorithms and Training Data:** The potency of AI-based autonomous driving algorithms hinges on the acquisition and use of substantial training data. However, generating such data manually through the physical vehicle proves to be an arduous undertaking.
3) **Cumbersome Iterative Development Process:** The iterative process of coding, deployment, observation, and data retrieval with a physical vehicle can be cumbersome and time-consuming.

IV. GOALS

The goals defining the environment's scope are the following:

1) **Minimal Setup:** The creation of a user-friendly standalone desktop application with as few dependencies as possible and a minimal setup.
2) **Cross-Platform:** Whether a user or developer works on Windows or Linux operating systems, cross-platform capability ensures that they can harness the environment irrespective of their OS.
3) **Extensible and Modular Architecture:** A flexible, modular design, allowing easy integration of new components and features, is an essential objective of the environment. This ensures adaptability and simplifies future enhancements.
4) **Testing and Validation of Vehicle Software:** An important goal is to provide a platform for rigorous testing and validation of the vehicle software stack. The vehicle software stack should be testable as-is to the extent feasible.
5) **Iterative Prototyping of Vehicle Algorithms:** Rapid modification, implementation, and evaluation of new algorithmic approaches foster an environment that encourages innovation and experimentation.

V. CONCEPT

Figure 2 illustrates the high-level architecture of the development, simulation, and validation environment derived in this work. Focusing on the simulation aspect, the structure can be roughly divided into two parts.

The first part is realized by the Unity game engine which is responsible for simulating the vehicle and its surroundings. Additionally, to create an easily extensible and modular architecture, an operating system framework, residing inside the simulator itself, has been conceptualized. Besides controlling the simulator
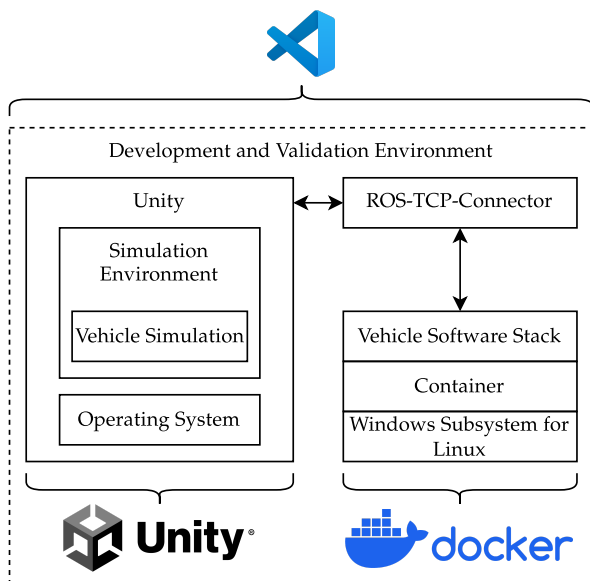
HOCHSCHULE
ESSLINGEN

Figure 2. The architecture of the environment on a Windows OS. On a Linux OS the block "Windows Subsystem for Linux" is not present.
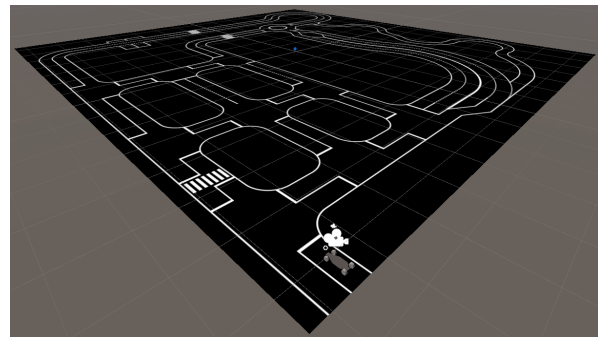

Figure 3. The simulator as visible inside Unity's scene view.

Surrounding the simulation component is the development and validation environment. The former is largely enabled by Visual Studio Code and its Docker integration, whereas the latter relies on the well-established suite of validation and analysis tools provided by ROS itself to enable testing and verification of vehicle algorithms.

VI. IMPLEMENTATION

The simulated environment (simulator) comprises a flat plane with a basic road network consisting of city streets, a roundabout, pedestrian crossings, as well as a highway and a country road section mapped on top, as seen in figure 3. This constitutes the static world of the simulated environment. Environmental effects such a rain, wind, or fog are not taken into account. Located within the static world is the simulated vehicle depicted in the lower center.

A. Operating System

Figure 4 shows a simplified class diagram of the operating system. Its user interface (UI) is implemented using Unity's UI Toolkit. The entry point is the singleton `OperatingSystem` which possesses the capability to instantiate new applications via its application programming interface (API):

Depending on the generic type parameter, the singleton dynamically constructs an appropriate application instance, injecting the `arguments` parameter passed into `OpenWindow<TApplication>(...)`, using C# reflection. Following the setup of the application, it is embedded into a new `Window` instance, and a `TaskbarItem` object is created. The latter two components serve distinct roles:

- **The `TaskbarItem` Class:** When clicked via the mouse, a taskbar item toggles the visibility of the associated window and causes it to fire an `OnWindowEvent`, transmitting the appropriate `WindowEvent` value.
- **The `Window` Class:** Windows are the containers for started applications. They can be minimized, maximized, closed, resized, and moved freely within the limits of the desktop environment.

and managing the communication with the vehicle software stack, its purpose is to offer a common, homogeneous interface for future extensions while avoiding some common pitfalls with a potentially ever-growing set of features:

The user interface can become cluttered and difficult to navigate. Icons, buttons, and menus can start competing for screen space, making it harder for users to find the functions they need. Moreover, new features can potentially introduce performance bottlenecks, especially if they require extensive processing power or memory usage. Finally, users may also become overwhelmed by the sheer number of features, not knowing where to start or how to use the software effectively.

The second part uses Docker to containerize the vehicle software stack. This ensures cross-platform readiness and also automates the installation of the vehicle software stack and its dependencies.

Under the hood, communication between the simulated environment and the ROS-based vehicle software stack operating inside the Docker container is achieved by Unity's ROS-TCP-Connector. Through it, sensor data will be channeled into the software stack and actuator data will, in turn, be captured and applied to the vehicle simulation by leveraging ROS' topic-based communication. Notably, this connector employs a separate TCP socket through which binary data is transceived, making it substantially faster than ROS-Bridge's JSON-based approach [11]. Finally, it's worth mentioning that any vehicle software stack that is compatible with the simulator's ROS topics can be integrated.

Figure 4. Simplified class diagram of the operating system.

Figure 5. The wheel forces from left to right: Suspension force F_S, Rolling force F_R, Turning Force F_T

B. Vehicle Simulation

The simulated vehicle is integrated into Unity's physics system. Its sensor sensor and actuator suite encompasses the sensors (camera, IMU, and wheel speed sensors) and the actuators (steering, motor, and wheels).

The camera was implemented using a Unity camera component with asynchronous GPU read-back to mitigate frame drops. To read back the depth texture, a custom shader pass, separating the depth element from the camera render into a separate texture, is executed prior. The color and depth frames are consequently published via the ROS-TCP-Connector at a rate of 30 Hz.

The IMU's acceleration is measured via Unity's `Rigidbody.GetPointVelocity(...)` API and the orientation is retrieved through the GameObject's transform component. Subsequently, the information is published on the ROS network at a rate of 70 Hz.

Similarly, the wheel speed sensors also use the same rigidbody API to retrieve the velocity at the respective wheels and publish it with a frequency of 100 Hz.

The simulated vehicle uses front-wheel steering with an Ackermann geometry. There is no dedicated motor simulation. Instead, the torque is applied directly to a custom wheel component that applies the forces shown in Figure 5. The implementation of the wheel component is largely based on [12]. The suspension force F_S (seen on the left) emulates the suspension of
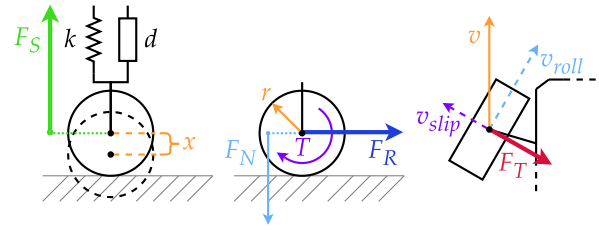
the wheel and is modeled as a spring-damper system by

$$F_S = k \cdot x - \dot{x} \cdot d \tag{1}$$

whereas x refers to the spring's displacement from rest, and k and d the spring and damper stiffnesses, respectively. Depicted in the center, the rolling force F_R converts the applied torque into a force through the radius of the wheel. Additionally, friction is taken into account by applying a force proportional to the normal force and directed against the rolling direction. c_{rr} in the equation 2 refers to the coefficient of rolling resistance, and the normal force F_N can be computed using equation 1.

$$F_R = \frac{T}{r} - \text{sign}(v_{roll}) \cdot F_N \cdot c_{rr} \tag{2}$$

While not implemented, one could adaptively adjust c_{rr} based on the contact surface to simulate various surface conditions.

Lastly, the turning force F_T originates from the fact that a wheel prefers to rotate around its mounting axle. Any movement parallel to this axle results in the wheel slipping or scraping along the surface and is therefore opposed. Equation 3 models this behaviour by applying a force opposite to the slip velocity of the wheel.

$$F_T = -m \cdot \frac{v_{slip}}{t} \tag{3}$$

One critical aspect is to ensure that the aforementioned equations are calculated with sufficient frequency. If the forces are computed too sporadically, the wheel simulation breaks down due to instability. The computational frequency is largely governed by Unity's physics time step, which has been set to 200 Hz.

C. Simulator-Aware ROS Nodes

One of the objectives of the simulator is to test the software in its unaltered state. However, achieving this objective encounters limitations, particularly regarding features that interface with real-world hardware embedded within the vehicle such as sensors and actuators. In light of this, it becomes clear that the environment must incorporate mechanisms that enable ROS nodes to detect the simulator.

HOCHSCHULE
ESSLINGEN

Table I
MECHANISMS FOR SIMULATOR-AWARENESS.

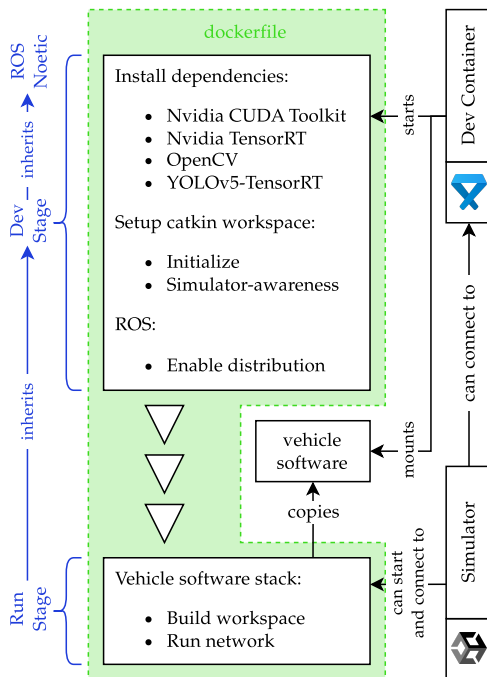| Language	Mechanism

CMake	```if(DEFINED SIMULATOR)```
	``` # ...```
	```endif()```

C/C++	```#ifdef SIMULATOR```
	``` // ...```
	```#endif```

Python	```import rospy```
	```name = "SIMULATOR"```
	```if rospy.has_param(name):```
	``` # ...```

Figure 6. The multi-stage `dockerfile` and its dependents.

Table I presents the mechanism implemented for each language. The CMake and C/C++ mechanisms are enabled by passing the appropriate CMake arguments via `catkin config --cmake-args` during setup of the catkin workspace. Python utilizes the ROS parameter server to make nodes simulator-aware.

D. Docker Container

The Docker container is set up using the multi-stage `dockerfile` seen in figure 6. As visible, there are two stages:

1) **Dev Stage:** Based on ROS' official Noetic image, various dependencies are installed, most of them required for the image processing logic of the vehicle. Additionally, the catkin workspace is set up, and the mechanisms for simulator-awareness are enforced here.

2) **Run Stage:** This stage inherits its contents from the dev stage. Its main purpose is to copy the
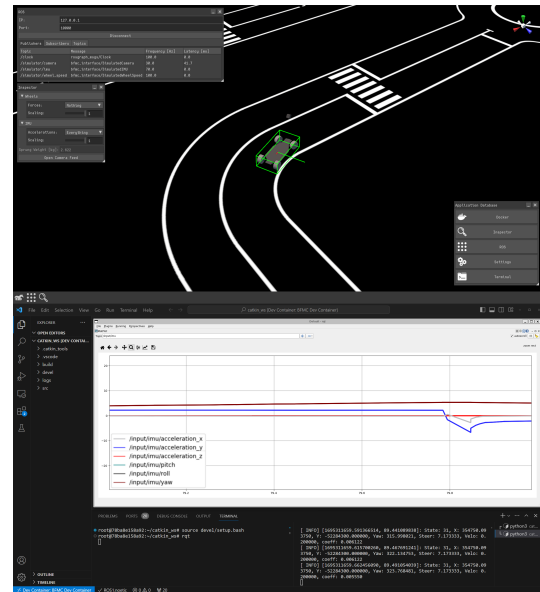

Figure 7. The development, simulation, and validation environment.

vehicle software, build it, and run the resulting ROS network.

VII. RESULTS

Figure 7 shows the development, simulation and validation environment in which the existing ROS toolkit is used to analyze the IMU messages published.

The upper half of the figure is taken up by the simulator itself. The lines originating from the center of the vehicle visualize the accelerations perceived by the vehicle. The two applications seen in the upper left-hand corner are, from top to bottom, ROS which manages the connection established over Unity's ROS-TCP-Connector, and the inspector which can show custom information about objects present in the simulated environment. The latter application currently displays information about the simulated vehicle. Lastly, the application in the bottom right-hand corner is used to launch any of the available applications implemented within the simulator's operating system.

The lower half of the figure depicts Visual Studio Code operating from within the docker container detailed in section VI. Embedded in the lower right-hand corner is a terminal that runs the vehicle software stack, and right next to it another terminal is used to run the `rqt` application whose GUI is placed in the center of the integrated development environment (IDE). `rqt` itself harnesses the `rqt_plot` plugin to visualize the individual IMU messages published by the simulator topic over time.

VIII. CONCLUSION

This paper detailed a comprehensive development, simulation, and validation environment for ROS-based autonomous driving algorithms.

Initially, the conceptual ideas behind the environment were presented. Through the use of Docker and OS-agnostic software, it could be demonstrated that a single unified architecture can support developers and researchers across multiple operating systems. The simulator was designed with extensibility, modularity, and ease of use in mind, aspects largely facilitated by the introduced operating system. Additionally, the custom vehicle simulation ensures complete control over the vehicle's driving dynamics.

Lastly, the development and validation qualities of the environment were presented, highlighting the synergy between the simulator and the existing ROS tools. Practical experience has shown that new users were able to familiarize themselves with the environment and be productive within days. Additionally, a noticeable speedup in development of the underlying vehicle software could be observed.

IX. FUTURE WORK

Although the development, simulation, and validation environment already accelerates the development of the underlying ROS software tremendously, the general workflow could be further improved by removing the need to recompile the ROS network after each modification. This could be accomplished by employing a scripting environment inside the simulator that harnesses the ROS-TCP-Connector to publish data directly into the ROS network, circumventing the need for a recompile.

REFERENCES

[1] Robert Bosch SRL. *Welcome to the Challenge*. URL: https://boschfuturemobility.com/.

[2] Jakob Häringer and Noah Köhler. *Neuartiger Software-Stack für ein autonom fahrendes Fahrzeug*. University of Esslingen, Feb. 2023. URL: https://gitlab.hs-esslingen.de/itmoves-masters/BFMC/-/wikis/uploads/dc65f1260898899e479baa7f70c7398b/Bericht_Forschungprojekt_1_Koehler_Haeringer.pdf.

[3] Jack Collins, Shelvin Chand, Anthony Vanderkop, and David Howard. "A Review of Physics Simulators for Robotic Applications". In: *IEEE Access* 9 (2021), pp. 51416–51431. DOI: 10.1109/ACCESS.2021.3068769.

[4] Shital Shah, Debadeepta Dey, Chris Lovett, and Ashish Kapoor. "AirSim: High-Fidelity Visual and Physical Simulation for Autonomous Vehicles". In: *Field and Service Robotics*. 2017. eprint: arXiv:1705.05065. URL: https://arxiv.org/abs/1705.05065.

[5] Microsoft AI & Research. *AirSim*. URL: https://github.com/microsoft/AirSim#readme (visited on 09/22/2023).

[6] N. Koenig and A. Howard. "Design and use paradigms for Gazebo, an open-source multi-robot simulator". In: *2004 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) (IEEE Cat. No.04CH37566)*. Vol. 3. 2004, 2149–2154 vol.3. DOI: 10.1109/IROS.2004.1389727.

[7] Open Source Robotics Foundation. *Gazebo : Tutorial : Windows*. URL: https://classic.gazebosim.org/tutorials?tut=install_on_windows&cat=install (visited on 09/22/2023).

[8] E. Rohmer, S. P. N. Singh, and M. Freese. "CoppeliaSim (formerly V-REP): a Versatile and Scalable Robot Simulation Framework". In: *Proc. of The International Conference on Intelligent Robots and Systems (IROS)*. www.coppeliarobotics.com. 2013.

[9] NVIDIA. *NVIDIA Isaac Sim*. URL: https://developer.nvidia.com/isaac-sim (visited on 01/30/2025).

[10] Ahmed Hussein, Fernando García, and Cristina Olaverri-Monreal. "ROS and Unity Based Framework for Intelligent Vehicles Control and Simulation". In: *2018 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*. 2018, pp. 1–6. DOI: 10.1109/ICVES.2018.8519522.

[11] Dr. Martin Bischoff. *Differences between Unity Robotics Hub and ROS*. URL: https://github.com/siemens/ros-sharp/wiki/Ext_RosSharp_RoboticsHub#differences-between-unity-robotics-hub-and-ros (visited on 08/18/2023).

[12] Toyful Games. *Making Custom Car Physics in Unity (for Very Very Valet)*. URL: https://www.youtube.com/watch?v=CdPYlj5uZeI (visited on 08/17/2023).

Constantin Blessing received his Bachelor of Engineering in Computer Engineering in 2020 at Esslingen University of Applied Sciences. Staying at the same university, he is currently pursuing his Master of Science in Applied Computer Science.

Prof. Dr.-Ing. Reiner Marchthaler is a professor of embedded systems with a specialty in autonomous systems at Esslingen University of Applied Sciences.

MULTI PROJEKT CHIP GRUPPE

Hochschule Aalen
Prof. Dr. Bürkle, (07361) 576-2103
heinz-peter.buerkle@htw-aalen.de

Hochschule Albstadt-Sigmaringen
Prof. Dr. Gerlach, (07571) 732-9155
gerlach@hs-albsig.de

Hochschule Esslingen
Prof. Dr. Lindermeir, (0711) 397-4221
walter.lindermeir@hs-esslingen.de

Hochschule Furtwangen
Prof. Dr. Benyoucef, (07723) 920-2342
bed@hs-furtwangen.de

Hochschule Heilbronn
Prof. Dr. Gessler, (07940) 1306-184
gessler@hs-heilbronn.de

Hochschule Karlsruhe
Prof. Dr. Ng, (0721) 925-1520
Herman-Jalli.Ng@hs-karlsruhe.de

Hochschule Konstanz
Prof. Dr. Schick, (07531) 206-657
cschick@htwg-konstanz.de

Hochschule Mannheim
Prof. Dr. Giehl, (0621) 292-6860
j.giehl@hs-mannheim.de

Hochschule Offenburg
Prof. Dr. Mackensen, (0781) 205-4770
elke.mackensen@hs-offenburg.de

Hochschule Pforzheim
Prof. Dr. Kesel, (07231) 28-6567
frank.kesel@hs-pforzheim.de

Hochschule Ravensburg-Weingarten
Prof. Dr. Siggelkow, (0751) 501-9633
siggelkow@hs-weingarten.de

Hochschule Reutlingen
Prof. Dr. Hennig, (7121) 271-7129
eckhard.hennig@reutlingen-university.de

Technische Hochschule Ulm
Prof. Dr. Terzis, (0731) 96537-627
anestis.terzis@thu.de

www.mpc-gruppe.de