

Sensibilität für Resilient Smart Farming (RSF) und seine Bedeutung in Krisenzeiten

RSF für eine nachhaltige, umweltgerechte und resiliente digitale Landwirtschaft

Daniel Eberz-Eder¹, Franz Kuntke² und Christian Reuter²

Abstract: Mit der globalen COVID-19-Pandemie und dem Hochwasser in West- und Mitteleuropa im Sommer 2021 hat unter anderem Deutschland in jüngster Vergangenheit zwei schwerwiegende Krisenszenarien erlebt. Die Auswirkungen auf die Gesellschaft und Wirtschaft sind verheerend. Parallel lassen sich Krisenereignisse im digitalen Raum, wie die Zunahme an Cyberkriminalität, beobachten. Es wird zunehmend deutlich, dass die Resilienz analoger sowie digitaler Prozesse wichtiger für die vollständige Betriebsfähigkeit wird. Die vorliegende Arbeit setzt sich mit der Bedeutung des Resilient Smart Farming (RSF) in Krisenzeiten als Möglichkeit für eine nachhaltige, umweltgerechte und resiliente digitale Landwirtschaft auseinander. Dazu wurden u. a. lokale Schadensmeldungen gruppiert und mögliche RSF-Gegenmaßnahmen aufgezeigt. Im Ergebnis zeigt sich eine Bewertung von Konzepten des RSF hinsichtlich der Krisenprävention und -bewältigung anhand aktueller realer Beispiele. Aufgrund zunehmender Bedrohungen durch Naturkatastrophen und Cyberkriminalität gehen wir davon aus, dass die Aufmerksamkeit von Gesellschaft und Politik für die Resilienz der Primärproduktion weiter steigen wird.

Keywords: Resilient Smart Farming, IoT, Ausfallsicherheit, Resilienz, Digitalisierung

1 Einleitung

Die Digitalisierung wird allgemein als ein Transformationsprozess für das gesellschaftliche und wirtschaftliche Leben beschrieben. Der digitale Wandel von analogen zu digitalen Prozessen hat sich im letzten Jahrzehnt durch zahlreiche technologische Innovationen rasant weiterentwickelt. Von dieser Entwicklung ist auch die Landwirtschaft als Primärsektor mit einem nicht unerheblichen Anteil betroffen. Einige der vormals rein analogen Planungs- und Umsetzungsprozesse wurden digitalisiert, z. B. durch den Einsatz von digitalen Schlagkarteien oder Farm Management Informationssystemen (FMIS). Die schnelle Umsetzung digitaler Prozesse in der Praxis birgt jedoch die Gefahr, dass gerade Sicherheitsaspekte vernachlässigt und hinten

¹ Dienstleistungszentrum Ländlicher Raum (DLR) Rheinhessen-Nahe-Hunsrück, Bad Kreuznach, daniel.eberz@dlr.rlp.de

² Technische Universität Darmstadt, Wissenschaft und Technik für Frieden und Sicherheit (PEASEC), 64289 Darmstadt, kuntke@peasec.tu-darmstadt.de,  <https://orcid.org/0000-0002-7656-5919>; reuter@peasec.tu-darmstadt.de,  <https://orcid.org/0000-0003-1920-038X>

angestellt werden. Da die Anwendungen im normalen Regelbetrieb jedoch unabhängig von der Sicherheit einer Anwendung funktionieren, wird oftmals nach der Einführung einer solchen digitalen Anwendung bzw. Lösung nicht nachgebessert. In Folge können gefährdete Systeme großflächig Einsatz finden. Diese können in erheblichen Schadenslagen auch großflächige Störungen in Wirtschafts- und Verwaltungsabläufen mit sich bringen.

Durch die globale COVID-19-Pandemie und das Hochwasser in West- und Mitteleuropa im Sommer 2021 hat unter anderem Deutschland in jüngster Vergangenheit zwei schwerwiegende Krisenszenarien erlebt. Dabei waren die Auswirkungen auf die Gesellschaft und Wirtschaft verheerend. Die Konsequenzen dieser Krisenszenarien haben sich dabei konkret auf die lokale und regionale Bevölkerung und Wirtschaft ausgewirkt. In dieser Krisenzeit wurde zunehmend deutlich, dass die Thematik der Resilienz analoger sowie digitaler Prozesse in Gesellschaft und Politik an Bedeutung gewinnt.

Das Konzept des Resilient Smart Farming (RSF) [Re18], welches im Innovationsprojekt GeoBox-I und GeoBox-II durch das Bundesministerium für Ernährung und Landwirtschaft (BMEL) gefördert wird, ist auf eine nachhaltige, umweltgerechte und resiliente digitale Landwirtschaft ausgerichtet. Durch die Einbindung von landwirtschaftlich relevanten öffentlichen georeferenzierten Daten und Fachinformationen wie z. B. Wetterdaten, Schaderregerauftreten oder Gewässerabstände können die digitalen Anwendungen als Entscheidungshilfe einen wichtigen Beitrag zur umweltgerechten Landwirtschaft leisten. Durch die Umsetzung in Form eines dezentralen Informationssystems mit Anspruch an Krisentauglichkeit soll die betriebliche Resilienz gestärkt werden. Der Wirtschaftsökonom Brunnermeier geht in seinem Buch „Die resiliente Gesellschaft“ 2021 davon aus, dass es immer wieder Krisen geben wird [Br21]. Daher ist es wichtig, sowohl die Gesellschaft als auch einzelne Sektoren resilienter zu machen und auf Krisenszenarien vorzubereiten. Die vorliegende Arbeit analysiert, inwieweit das Konzept des RSF sowie die technologische Umsetzung in konkreten Gefährdungslagen die landwirtschaftliche Produktion gesichert hätten, oder einen wichtigen Beitrag für den zivilen Schutz durch die Verwendung landwirtschaftlicher Infrastruktur geschaffen hätten.

2 Hintergrund – resiliente Technologie für die Landwirtschaft

Der Markt für digitale Anwendungen im Precision Farming sowie Smart Farming ist mittlerweile sehr umfassend. Die digitalen Anwendungen bieten vielfältige Chancen für die landwirtschaftliche Produktion und leisten einen wichtigen ökonomischen und ökologischen Beitrag durch betriebsindividuelle Entscheidungshilfen. Die derzeit auf dem Markt verfügbaren Dienstleistungen und Produkte sind dabei vordergründig durch die Funktionsweise des Cloud-Computings geprägt. Das bedeutet, dass Daten nicht mehr vor Ort gespeichert werden, sondern auf zentralen Servern in Rechenzentren ausgelagert werden. In der landwirtschaftlichen Praxis werden internetabhängige, u. a. vor allem

hochleistungsbasierte Anwendungen nicht selten durch unzureichende Bandbreiten und hohe Latenzzeiten eingeschränkt.

Eine Alternative zu zentralisierten Ansätzen in Form von Cloud-Computing ist, zumindest für gewisse Anwendungen ein eigenes dezentrales Netzwerk zu errichten und die Anwendungen mit einem „Offline-First“-Ansatz zu entwickeln. Bei einem solchen „Offline-First“-Ansatz geht es darum, dass Programme grundsätzlich ohne Internetanbindung nutzbar sind [RSE19]. Diese Idee setzen wir mit technologischen Konzepten um, die wir unter dem Begriff Resilient Smart Farming (RSF) sammeln. Die technologische Umsetzung des RSF ist zwischen Edge Computing [Sh16] und Fog Computing [Hu17] einzuordnen. Die Datenhoheit von landwirtschaftlichen Betriebsdaten spielt entsprechend bei der Akzeptanz digitaler Anwendungen eine wichtige Rolle. Durch das GeoBox-Projekt wird anhand des Resilient Edge Computing (REC) [Eb21] eine dezentrale Datenhaltung konzipiert und getestet, die wichtige Erkenntnisse zur resilienten, betrieblichen und lokalen Datenhaltung beinhaltet. Diese Testumgebung wird gemeinsam mit dem Projektvorhaben EF-Südwest auf der Open Data Farm Hofgut Neumühle aufgebaut. Die hierbei entstehende HofBox dient als lokaler Mini-Server mit Einsatz direkt im Betrieb, um Datenbanken vorzuhalten und auch IoT-Geräte anzubinden. Weiterhin kann die HofBox selbst auch Anwendungen bereitstellen, die beispielsweise per Browser aufrufbar sind. Weitere Konzepte aus dem RSF-Umfeld sind die Nutzung von LPWAN-Technologien für den Aufbau resilienter, drahtloser Datenkanäle, die in Notfällen eine infrastrukturlose Kommunikation unterstützen. Mit einem ähnlichen Ansatz können dabei auch Geräte drahtlos angebunden werden, die von sich aus keine LPWAN-Anbindung mitbringen [Ku21]. Grundgedanke im Umfeld des RSF ist stets, einen hohen Anteil an Autarkie der notwendigen Infrastruktur zu erreichen – sowohl software- als auch hardwareseitig – was neben dem Resilienzgedanken auch positive Effekte bzgl. Datenhoheit und Privatsphäre mit sich bringt. Durch diese Technologien zur Dezentralisierung und Absicherung von internetbasierten Anwendungen wird die Datenhaltung zurück in die Betriebe verlagert und sichert somit die initiale Datenhoheit den Landwirten zu.

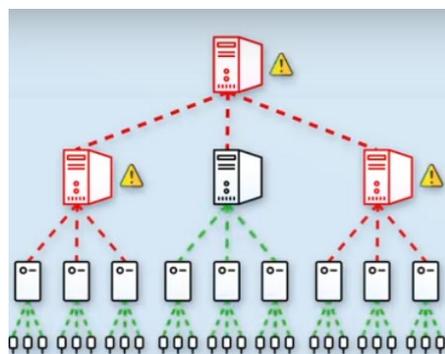


Abb. 1: Ausfall zentraler Dienste in der Hierarchie führt nicht zum Totalausfall des Systems

Im folgenden Kapitel wird eine Auswahl an Ereignissen dargestellt, um die Tauglichkeit der RSF-Entwicklungen theoretisch zu eruieren. Die Abbildung 1 zeigt schematisch den Aufbau des REC im landwirtschaftlichen Kontext mit einem zentralen Landesserver, einer regionalen Landkreisinstanz und die betrieblichen HofBoxen mit unterschiedlichen IoT-Sensoren. Ein Ausfall zentraler Dienste, z. B. Landesserver und die darunter liegenden Landkreisserver, führen bei einem Krisenereignis (z. B. Internetausfall) nicht zum Ausfall der betrieblichen HofBoxen.

3 Schadensereignisse in jüngster Vergangenheit

Eine systematische Recherche von Vorfällen in domänenspezifischen Nachrichtenportalen (agrارheute.com, topagrار.com, lz-rheinland.de) mit Stichworten (u. a. Hackerangriff, Defekte, Störungen, Stromausfall, Internetausfall, Ausfall, Hacker, Angriff, Cyber) hat zu einer Liste von Ausfällen einzelner Betriebe in der DACH-Region (Schwerpunkt Deutschland) geführt. Zum Zeitpunkt der Analyse im Jahr 2021 gab es sieben größere Vorfälle³, teils mit bezifferten erheblichen finanziellen Schäden im sechs- oder siebenstelligen Euro-Bereich.

Zwei der sieben Fälle können dabei eindeutig dem Bereich *Cyberattacke* zugeordnet werden. In beiden Fällen wurden dabei gezielt Großbetriebe attackiert und als Folge die Unternehmens-IT lahmgelegt. Da in den Berichten von „Lösegeld für die Wiederherstellung der Daten“ berichtet wird, handelte es sich vermutlich um Attacken auf Basis von Ransomware, bei denen Daten verschlüsselt werden. Für die Wiederherstellungsschlüssel wird i.d.R. ein Lösegeld gefordert. In der Vergangenheit ist eine Zunahme solcher Störungen in vielen Sektoren verstärkt zu beobachten. Ein Schadensereignis ist laut Nachrichtenportal auf einen technischen Defekt zurückzuführen, bei dem große Mengen Milch in ein Abwasserwerk flossen. Dabei wurde eine Verunreinigung eines benachbarten Flusses gefürchtet. Vier weitere Fälle beschreiben Brände in großen Ställen, wobei in zwei Fällen direkt technisches Versagen festgestellt wurde, bei zwei weiteren Fällen konnte allerdings keine direkte Brandursache erkannt werden. Die recherchierten Schadensereignisse von landwirtschaftlichen Betrieben sind statistisch nicht signifikant, sie verdeutlichen jedoch, dass der Ausfall von (Informations-)Technik zu erheblichen ökonomischen Verlusten sowie Tierleid führen kann.

³www.lz-rheinland.de/nachricht/detail/grossanlage-in-brand; www.agrarheute.com/tier/schwein/schon-brand-schweinmastbetrieb-580280; www.agrarheute.com/tier/technischer-defekt-huehnermobil-abgebrannt-581390; www.agrarheute.com/land-leben/stallbrand-800-1000-schweine-sterben-581626; www.agrarheute.com/management/hackerangriff-fleischgigant-jbs-schlachtbaender-stehen-still-581786; www.agrarheute.com/land-leben/technischer-defekt-25000-liter-milch-fliesen-klaeranlage-582538; www.agrarheute.com/management/agribusiness/hacker-legen-cyberangriff-molkerei-oesterreich-lahm-582644

4 Nutzung von RSF-Technologie

Obwohl der grundlegende Fokus der RSF-Thematik in der Stärkung der Resilienz liegt, könnten die angesprochenen technischen Lösungen einen wichtigen Beitrag in einzelnen Betrieben vor den Auswirkungen technischer Defekte oder Cyberangriffen leisten:

(a) *Redundante Datenhaltung*: Bei der Hauptapplikation wird die Datenhaltung sowohl auf Client (Smartphone, Tablet, oder Computer), als auch Server (HofBox) vorgehalten, sofern es der Speicher ermöglicht. Durch die Redundanz der Daten führt ein technischer Defekt eines einzelnen Gerätes nicht zu einem vollständigen Datenverlust – unabhängig von der Realisierung ordentlicher Backups, die in der Praxis leider zu selten anzutreffen sind.

(b) *Autarke Lauffähigkeit durch „Offline-First“-Ansatz*: Sind global angebundene Server nicht erreichbar, sei es durch eine größere Attacke⁴, einen Brand eines Rechenzentrums⁵ oder menschliches Versagen⁶, brechen auch die darauf angewiesenen Dienste zusammen. Die naheliegende Lösung sollte deshalb sein, bei kritischen bzw. krisenrelevanten Anwendungen nach Möglichkeit auf eine Internetabhängigkeit zu verzichten. Bei „Offline-First“-Anwendungen wird deshalb die Abhängigkeit reduziert, indem bereits bei der Entwicklung sichergestellt wird, dass die Funktionen so gut wie möglich auch offline, d. h. ohne Internetzugang, funktionieren. Dennoch können diese Anwendungen im „Normalbetrieb“ von einer funktionierenden Internetverbindung profitieren.

(c) *Datenhaltung des Farm Managements auf dedizierter Hardware*: Die Separierung der betrieblichen Datenhaltung von den Endgeräten macht das System weniger anfällig für häufige Angriffsmuster. Beispielsweise Schadcode, der per Mail-Anhang auf einem Endgerät Einzug erhält, ist somit bereits separiert von der Hardware mit den Daten für das Farm Management. Ebenso macht es die Spezialisierung der Hardware-Software-Kombination unwahrscheinlicher, zu den Zielen breitflächiger Angriffe zu gehören, durch den Verzicht auf breitflächig eingesetzte Software (z. B. Microsoft Windows), welche i.d.R. als Einfallstor solcher Attacken dient.

(d) *Integration einer IoT-Plattform zur einfachen Anbindung von Sensorik und Aktorik*: Aktuell ist der Einsatz und Aufbau von betrieblichen IoT-Umgebungen aufwändig und mit viel Recherche verbunden. Durch die Integration einer IoT-Plattform in die HofBox soll die Hemmschwelle für den Einsatz von IoT-Sensorik gesenkt werden, um beispielsweise schneller über kritische Zustände (Temperatur, Klimatisierung und Belüftung) in Ställen informiert zu werden.

4 <https://www.heise.de/news/Cyberangriff-auf-Anhalt-Bitterfeld-Landkreis-zeigt-sich-weiterhin-unerpressbar-6160917.html>

5 <https://www.faz.net/aktuell/wirtschaft/digitec/brand-bei-cloud-betreiber-millionen-von-webseiten-betroffen-17238989.html>

6 <https://www.zdf.de/nachrichten/digitales/facebook-ausfall-dns-konfigurationsfehler-100.html>

5 Abschluss und Ausblick

Im Hinblick auf die steigende Anzahl an Gefährdungen durch Naturereignisse und Cyberkriminalität müssen Schwachstellen verringert werden. Dies spricht für die Entwicklung resilienter Systeme. Ein Versuchsaufbau auf der Open-Data-Farm Neumühle zeigt bereits, dass das technologische Zusammenspiel aus „Open Horizon“ als Management-Framework (Cloud) für die Verwaltung und containerisierten Anwendungen auf der betrieblichen HofBox-Ebene (Edge-Device) funktioniert. Es können hierbei die HofBoxen mit aktuellen Softwarepaketen provisioniert und anschließend autark betrieben werden, auch wenn Teile der Infrastruktur vom Internet abgeschnitten sind. In Zukunft wird weiterhin analysiert, ob die im Krisenfall notwendigen Datenpakete auch über eine Notfallkommunikation z. B. durch LPWAN-Technologie (z. B. LoRa) kommuniziert werden können. Dafür steht die in den Projekten GeoBox-I/II und EF-Südwest aufgebaute digitale Infrastruktur auf der Open-Data-Farm Neumühle zur Verfügung und ermöglicht in den kommenden Monaten weitere Tests hinsichtlich resilienter digitaler Infrastruktur. Sowohl die großen Krisenereignisse in den letzten Monaten als auch die vielen kleineren, aber dennoch existenzgefährdenden Schäden haben dazu geführt, dass die Sensibilität für das Thema Resilienz in vielfältiger Weise gestiegen ist. Nach heutigem Stand und einer ersten Bewertung gehen wir davon aus, dass die Aufmerksamkeit innerhalb der Landwirtschaft, Wirtschaft, Gesellschaft und Politik zu Resilienz und Resilient Smart Farming in den nächsten Jahren steigen wird.

Literaturverzeichnis

- [Br21] Brunnermeier, M. K. et al. (Übers.): Die resiliente Gesellschaft: wie wir künftige Krisen besser meistern können. Berlin: Aufbau, 2021.
- [Eb21] Eberz-Eder, D. et al.: Technologische Umsetzung des Resilient Smart Farming (RSF) durch den Einsatz von Edge Computing. 41. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft, 2021.
- [Hu17] Hu, P. et al.: Survey on fog computing: architecture, key technologies, applications and open issues. In: Journal of Network and Computer Applications, Bd. 98, 2017.
- [Ku21] Kuntke, F. et al.: Low Power Wide Area Networks (LPWAN) für krisentaugliche Datenübertragung in landwirtschaftlichen Betrieben. 41. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft, 2021.
- [RSE19] Reuter, C.; Schneider, W.; Eberz, D.: Resilient Smart Farming (RSF) – Nutzung digitaler Technologien in krisensicherer Infrastruktur. 39. GIL-Jahrestagung: Informatik in der Land-, Forst- und Ernährungswirtschaft, 2019.
- [Re18] Reuter, C. et al.: Resiliente Digitalisierung der kritischen Infrastruktur Landwirtschaft – mobil, dezentral, ausfallsicher. Mensch und Computer 2018: Workshopband, 2018.
- [Sh16] Shi, W. et al.: Edge Computing: Vision and Challenges. In: IEEE Internet of Things Journal, Bd. 3, 2016.