Modeling, Executing and Monitoring IoT-Driven Business Rules with BPMN and DMN: Current Support and Challenges

Yusuf Kirikkayis, Florian Gallik, and Manfred Reichert

Institute of Databases and Information Systems, Ulm University, Germany
{yusuf.kirikkayis,florian-1.gallik, manfred.reichert}@uni-ulm.de

Abstract. The involvement of the Internet of Things (IoT) in Business Process Management (BPM) solutions is continuously increasing. While BPM enables the modeling, implementation, execution, monitoring, and analysis of business processes, IoT fosters the collection and exchange of data over the Internet. By enriching BPM solutions with real-world IoT data both process automation and process monitoring can be improved. Furthermore, IoT data can be utilized during process execution to realize IoT-driven business rules that consider the state of the physical environment. The aggregation of low-level IoT data into process-relevant, high-level IoT data is a paramount step towards IoT-driven business processes and business rules respectively. In this context, Business Process Modeling and Notation (BPMN) and Decision Model and Notation (DMN) provide support to model, execute, and monitor IoT-driven business rules, but some challenges remain. This paper derives the challenges that emerge when modeling, executing, and monitoring IoT-driven business rules using BPMN 2.0 and DMN standards.

Keywords: IoT · BPM · BPMN · DMN · Business Rules · Challenges

1 Introduction

As electronic components have become smaller, less expensive, and more powerful, the Internet of Things (IoT) has received an upswing [3]. Many embedded components are equipped with software, sensors, actuators, and network connectivity that enable the collection and exchange of data (sensors) as well as physical responses to events (actuators) [2]. Such physical objects can be embedded in everyday devices such as smartphones, wearable devices, washing machines, or refrigerators. They can be further found in large systems such as, smart cities, logistics or healthcare [4]. In general IoT refers to a network of physical objects populated by sensors and actuators that communicate and exchange data over the Internet [5]. While sensors are used to collect data about the real-world (e.g., temperature sensor, humidity sensor, heart rate sensor, or camera sensor), actuators are used control the physical world (e.g., watering systems, security systems, or air conditioner) [6]. Such interconnected IoT devices enable capturing the dynamic context of the physical world into the digital world.

While IoT enables exchanging and collecting data about the physical world over the Internet, BPM enables modeling, implementing, executing, monitoring, and analyzing business processes [7]. By enhancing business processes with IoT capabilities, process execution and monitoring as well as decision making can be enhanced. Furthermore, a more comprehensive view becomes possible for such IoT-aware business processes. Besides sensing the physical world, physical tasks such as moving a robot, as well as digital tasks, such as notifying a system, can be automated based on IoT devices [1]. By integrating the physical world as a key perspective in business processes, contextual information that was previously invisibly embedded in various environments can be continuously and automatically captured by IoT devices. IoT-aware business processes understand the dynamic context of the physical world, which makes them context-aware as well [8].

IoT has the ability to continuously and automatically support IoT-aware business processes with real-world IoT sensor data in real-time. IoT-driven decisions in business processes expose a need for context aggregation, context-awareness, and up-to-date (i.e. real-time) data, which are the key data source for dynamic decision making [9] [8]. To address this need, IoT sensor data collection should proceed as follows (I) sensing low-level data from the real-world (e.g., temperature, switch state, humidity, brightness), (II) combining low-level data and aggregating them into high-level information, and (III) enabling decision making based on the obtained information [10]. This means, **low-level data** are captured in the physical world and need to be aggregated and combined to process-relevant **high-level data** [11] [10]. Data from traditional repositories such as databases and data warehouses are not sufficient for IoT-aware decision making [1]. Decisions in IoT-aware business processes require up-to-date data about the physical environment [10]. For example, when using IoT devices such as temperature sensor, humidity sensor, and brightness sensor, the condition of the goods in a truck can be checked. By aggregating these low-level IoT data and combining them, decisions can be made in the course of a business process. Related to the example, the temperature and humidity value can be combined. If the maximum temperature and humidity are exceeded, the decision *start cooling system* can be made. We refer to this type of conditions *business rules*.

The integration of IoT in BPM has gained significant attention in literature, in particular several BPMN extensions and notations [19,33–35] have been proposed to integrate IoT in business processes in terms of resources. Consequently, IoT data is directly used without aggregating and combining it with other contextual process data. As a result, the possibility of generating high-level information is not exploited, which impairs the potential capability. In addition, decisions are traditionally hard-coded into business processes, which affects the ability to make dynamic decisions [8]. Current approaches mostly focus only on the integration of IoT into business processes to visually represent IoT involvement. The modeling, execution, and monitoring of IoT-driven business rules is neglected. Moreover, the integration of IoT and BPM is constrained due to the lack of a methodological framework for connecting the IoT infrastructure with the BPM system [8]. For modeling business rules, in turn, the Decision Model and Notation (DMN) [12] standard can be used in combination with BPMN. By using DMN, the decision logic can be separated from the process logic. Furthermore, DMN enables the aggregation of low-level data into high-level one. However, DMN does not provide official support for modeling IoT-driven business rules, which creates new challenges. In this paper, we derive and highlight research challenges that need to be tackled in order to properly model, execute, and monitor IoT-driven business rules.

This paper is structured as follows: Section 2 illustrates the support for modeling, executing, and monitoring IoT-driven business rules based on either BPMN or BPMN plus DMN. In Section 3 we derive challenges that need to be tackled when modeling, executing, and monitoring IoT-driven business rules. Finally, in Section 4 we summarize and discuss the results.

2 Current support for IoT-driven business rules in BPMN and BPMN + DMN

2.1 IoT-driven business rules in BPMN

BPMN 2.0 is a standardized graphical process modeling language that provides elements for modeling business processes and workflows [13]. However, BPMN 2.0 does not provide official support for modeling IoT involvement and capabilities, but provides different possibilities that can be used for representing IoT such as (i) tasks, (ii) events, and (iii) resources [14]. For IoT-driven business rules, different gateways may be used in the current BPMN 2.0 standard, these can be divided into the following categories (I) **exclusive**, (II) **inclusive**, (III) **parallel**, (IV) **complex**, and (V) **event-based** [13]. *Example 1* describes a business process with IoT-driven business rules. Note that the IoT-driven business rules are modeled exclusively with standard BPMN 2.0 elements.

Example 1: *Consider a medical system that monitors the health status of a patient who has been diagnosed with Chronic Obstructive Pulmonary Disease (COPD). COPD is a disease in which the lungs are permanently damaged and the airways (bronchi) are restricted. At anytime, the patient may experience unpleasant complications such as shortness of breath on exertion, coughing, sounds when breathing, fast heart rate, hyperactive muscle use, increased blood pressure, and a cold skin. Several studies [15] [16] have shown that the IoT-driven monitoring of sensor-equipped patients can improve their quality of life by identifying the severity of COPD disease and responding accordingly. In order to detect COPD, all required sensors are polled (cf. Figure 1). Based on the values provided by the IoT sensors and the defined IoT-driven business rule, either no treatment, treatment with an oxygen mask, or treatment with an inhaler is administered.*

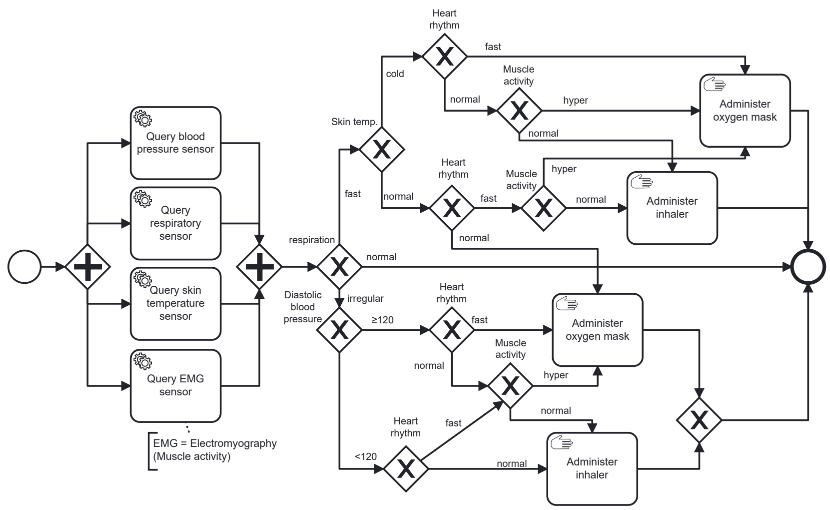

Fig. 1. Example of an IoT-driven business rules expressed in terms of BPMN 2.0

2.2 IoT-driven business rules in BPMN + DMN

The combined use of BPMN [13] and DMN [12] has already been studied in [17] and [18]. The interplay between process and decision logic plays a crucial role for business processes, as business rules are evaluated during process execution and may affect process outcomes [25]. DMN is a decision modeling standard that consists of two levels: The first one represents the decision requirements, where the dependencies between the elements involved in the decision model are captured [8]. The decision requirements are represented by DRDs (Decision Requirements Diagrams) and form the dependencies between the data and subdecisions. The input data for DRDs may be static or dynamic. The second level is the decision logic, which is usually modeled in terms of decision tables [8] [5]. To construct a DMN model, low-level data needs to be aggregated to higher-level one and enables consequently to aggregate contextual data [5] [12]. *Example 2* describes a decision-aware COPD process (cf. Figure 2). Note that the business process is modeled in terms of BPMN 2.0 and the business rules in terms of DMN using the elements provided by the two standards.

Example 2: *To identify the severity of COPD, the patient is equipped with several sensors. The severity of COPD is determined based on the defined business rules (cf. Figure 2 [6]), the data values provided by sensors in real-time (cf. Figure 2 [2]), and data from a database (cf. Figure 2 [3]) in DMN. The decision in DMN becomes evaluated when activating the Check COPD severeness business rule task in BPMN 2.0 (cf. Figure 2 [1]). After deciding whether treatment with oxygen mask or inhaler, or no treatment becomes necessary, the heart status is checked based on real-time sensor data (cf. Figure 2 [5]). Depending on the result, the patient is either not treated or treated with a defibrillator.*

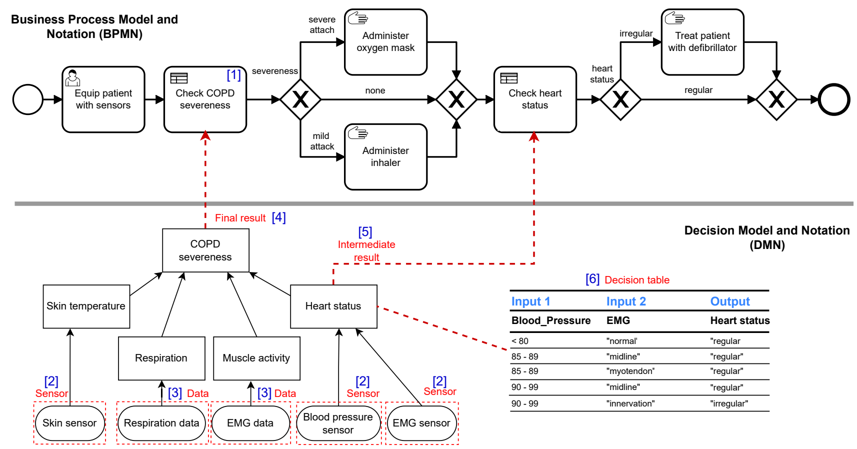

Fig. 2. Relationship between BPMN 2.0 and DMN

3 Challenges

Although the BPMN 2.0 and DMN allow expressing certain aspects of IoT-driven business rules, several challenges remain [5] [14]. We studied literature and IoT-driven business rules from different domains modeled in terms of either BPMN or BPMN + DMN. Moreover, we were able to identify additional challenges in the context of the two IoT-related projects BPMN Extension for IoT (BPMNE4IoT) [2] and IoT Decision Making for BPMN (IoTDM4BPMN) [10] we are involved in. We discuss the derived challenges and divide them along the modeling, execution, and monitoring of IoT-driven business rules. The following structure is applied for each challenge; we briefly describe the challenge, provide an example, and reference relevant literature that tries to address the research gaps described in the challenge. A summary of the challenges can be found in Table 1.

Table 1. Challenges for IoT-driven business rules in BPMN and BPMN + DMN.

Modeling Challenges
C1 - Modeling IoT-driven business rules in BPMN 2.0
C2 - Modeling IoT-driven business rules with BPMN 2.0 + DMN
C3 - Reducing the complexity of IoT-driven business rules
Execution Challenges
C4 - Extending process log with IoT data
C5 - Treatment of IoT data outliers
C6 - Treatment of defective IoT devices
Monitoring Challenges
C7 - Traceability of IoT-driven business rules
C8 - Fault monitoring in IoT-driven business rules
C9 - Real-time monitoring of IoT-driven business rules

3.1 Modeling Challenges

C1 - Modeling IoT-driven business rules in BPMN 2.0

Description: In Section 2.1, we discussed the current support of the BPMN 2.0 standard for incorporating IoT devices and the modeling of IoT-driven business rules. In order to express IoT involvement within business rules, it should be possible to model the involved IoT devices. Note that the returned data values of the IoT devices are used as basis for evaluating the IoT-driven business rule. Therefore, it is crucial to be able to properly capture IoT involvement.

Example: To describe the problem, Figure 3 illustrates the treatment of COPD. When modeling the business process and the corresponding IoT-driven business rules with the standard BPMN 2.0 elements, it remains unclear which tasks are IoT-related and which are not. Furthermore, it is unclear which sensors are actually used in the context of IoT-driven business rules (cf. Figure 3). To decide whether no treatment, a treatment with oxygen mask, or a treatment with inhaler is required, skin temperature (Task 2), respiration (Task 3), and EMG value (Task 4) are needed, whereas the ECG value (Task 5) is not needed for the treatment but for the alarm. Note that it is unclear which sensor is important for which business rule. The entire process model must be carefully read and understood in order to determine this. Furthermore, it is impossible to distinguish between sensors (Tasks 2-5) and actuators (6). In order to distinguish between sensors and actuators, the labels should reflect the involvement of IoT and the modeler needs to be familiar with IoT devices and their behavior. As another drawback, no visual difference between IoT-aware service tasks (Tasks 2-6) and BPMN service task (Tasks 1,9, 10) exists. Moreover, the complexity and thus, the comprehensibility of the business rules increases with growing number of involved IoT devices. This aggravates reading and understanding of the process models as well as the IoT-driven business rules. With increasing number of business rules and increasing complexity of the rule logic, the flexibility, scalability, and maintainability of the resulting process model and IoT-driven business rules is impaired. The complex nesting and ambiguous involvement of IoT makes any later extensions or changes difficult. As IoT-driven business rules are hard-coded in the business process in form of gateways, aggregation and combination of IoT low-level data into high-level one is not appropriate with BPMN 2.0. Obviously, the IoT-driven businesses rules cannot be reused in a different context. When using BPMN, both process and decision logic are defined in one and the same process model. As a result, the modeled logic is hard-coded and constrained to a local location. Therefore, reusability is impaired [5].

Possible solution: There exist several works [2, 19, 33, 34] that introduce extensions for representing IoT devices in the context of BPMN 2.0. These extensions enable the explicit modeling of IoT participation by introducing IoT specific elements. They propose a visual discrimination between regular BPMN elements and IoT elements in the modeling phase [14]. In [36], two approaches for modeling IoT-driven business rules are presented. The first one extends the BPMN

2.0 standard by providing specific IoT decision modeling elements. Note that BPMN 2.0 is a rather complex language and any extension constitutes a deviation from the standard [26] [14]. By extending BPMN with additional IoT elements complexity might increase. In turn, this might effect model comprehensibility. The second approach proposes an IoT-specific drag&drop modeler, which separates the business rules from the process logic. As the drag&drop modeler outsources the business rules from the BPMN process model, the structure of the IoT-driven business rule cannot be viewed in BPMN. This makes it difficult to extend, maintain, and troubleshoot the IoT-driven business rules.

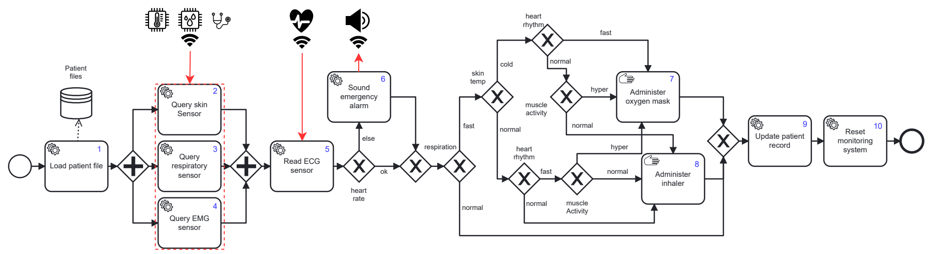

Fig. 3. IoT awareness in BPMN-based process model (adopted from [2]).

C2 - Modeling IoT-driven business rules with BPMN 2.0 + DMN

Description: Combining BPMN and DMN can solve some of the problems and gaps mentioned above. For example, DMN is suited for aggregating and combining business rules as it uses appropriate techniques such as decision tables. Since DMN does not provide any explicit elements for modeling IoT, the modeling of business rules based on IoT data constitutes a challenge.

Example: Consider Figure 4. The results of the queried IoT sensors are stored in data objects which then flow into the business rule task *Check COPD severeness* (cf. Figure 4). Representing the received IoT data as data objects increases the complexity and the number of modeling elements in the business process. If IoT data is not represented in terms of data objects, such as in the process model depicted in Figure 3, it will be unclear which IoT data actually concern the business rules in DMN. This, in turn, affects model readability and comprehensibility. In addition, it is impossible to distinguish between IoT data objects on the one hand and BPMN data objects on the other. Note that the *Check COPD severeness* business rule task represents the decision modeled and executed in DMN. As DMN outsources the decision logic from the BPMN process model, the structure of the IoT-driven business rule cannot be directly viewed in BPMN. Typically, the business rule task only provides the final decisions. In addition, DMN does not officially support the modeling of IoT-driven business rules. Consequently, it cannot be distinguished between IoT input data (cf. Figure 3 [2]) and, for example, input data from a database (cf. Figure 3 [3]). When using DMN, decision logic is captured in decision tables (cf. Figure 3 [4]). With increasing number of IoT devices, however, the complexity of the decision table increases as well. Accordingly, the error detection becomes more difficult.

Possible solution: Several authors have argued that DMN is capable of modeling IoT-driven business rules [5] [50]. For example, [5] shows how DMN elements can be used to model different IoT-driven business rules (e.g., smart transportation, smart ventilation, and smart healthcare). Thus, no discrimination between regular DMN elements (e.g. input data) and IoT-related DMN elements is present. One possible solution to close this gap would be to extend the DMN standard with IoT decision elements.

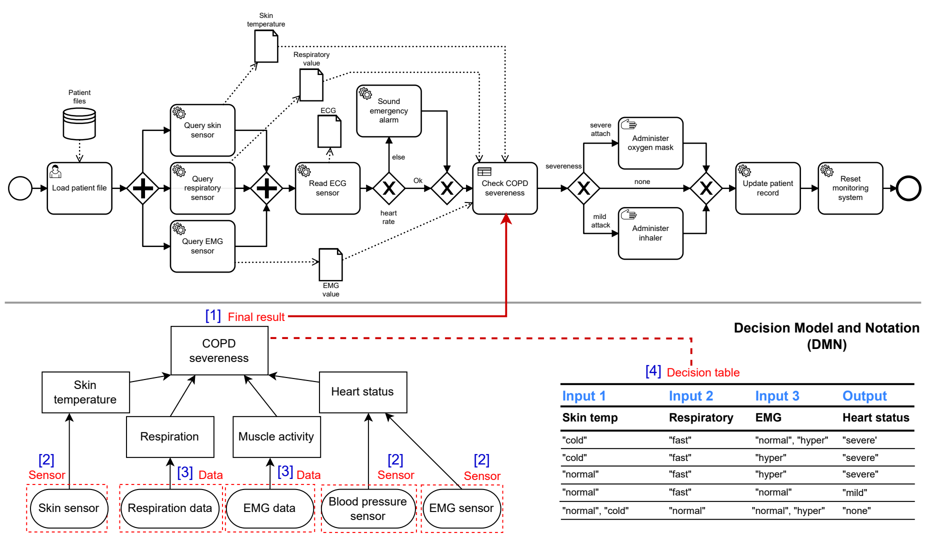

Fig. 4. Using BPMN 2.0 and DMN for modeling an IoT-driven business rule.

C3 - Reducing the complexity of IoT-driven business rules

Description: As discussed in the context of C1 and C2, the complexity of both the process and the decision model increases when involving IoT devices. Modeling IoT-awareness for a process and decision model is a complex undertaking, and the resulting model often turns out to be difficult to understand due to the potentially ambiguous use of modeling elements [2]. IoT-driven business rules become more complex when modeling them with BPMN 2.0 as the involvement of IoT is not supported by the standard. In turn, this has a negative repercussion on modeling IoT-aware processes and IoT-driven business rules.

Example: As processes running in an IoT setting are often data- and decision-intensive, the modeled process might be too extensive and, thus, too complex to be understandable. When modeling IoT-driven business rules in BPMN (cf. Figure 3), the number of gateways and control flow paths grows as additional business rules are introduced. This leads to a large number of branch conditions and control flow elements, resulting in a complex structure [14]. When combining BPMN and DMN we can encapsulate this complexity by defining the business rules in decision tables. This significantly reduces the number of gateways and sequence flows on one hand. On the other, the business rules are hidden in decision tables. At the BPMN level, it is impossible to see how the IoT-driven business rules are defined and how they depend on each other. In the following, we consider metrics proposed in literature to evaluate the complexity of the models described in the previous sections [27] [14]. The metrics are used for identical processes with different modeling approaches. The BPMN metrics NOA (number of activities), NOG (number of gateways), and NOF (number of flows) were defined in [27]. The metrics for DMN are taken from [28] and consist of TNR (total number of rules), NOD (number of decisions), and TNDO (total number of data objects). Table 2 shows that the complexity of modeling IoT-driven business rules in BPMN is larger compared to BPMN + DMN due to the higher number of sequence flows (NOF) and gateways (NOG). As opposed to BPMN, the complexity in BPMN + DMN is shifted to the decision tables (TNR).

Table 2. Evaluation of complexity through the application of metrics

Case	NOA	NOG	NOF	TNR	NOD	TNDO
BPMN	10	11	31	-	-	-
BPMN+DMN	11	6	23	17	5	5

Possible solution: A possible solution for reducing complexity related to IoT-aware processes is presented in [2]. The authors introduce new modeling elements that, for example, merge individual sensor artifacts into one sensor group artifact in order to increase the abstraction level. Another possible solution is the definition of guidelines for IoT-driven business rules. For example, [38] proposes seven process modeling guidelines (7PMG). However, these do not consider the modeling of IoT-driven business rules. Another approach is the definition of patterns for modeling IoT behavior. These patterns could, for example, reduce the number of message flows between the central pool and the IoT-aware pools by using the computing capacities of the IoT devices [51].

3.2 Execution Challenges

C4 - Extending process log with IoT data

Description: The sensors used in a business process record the physical world and transform it into the digital world. The data generated by IoT devices allows for the continuous monitoring and provision of opportunities for analysing and optimizing the performed processes, e.g., through process mining or real-time monitoring [42] [43]. Furthermore, as a data source IoT can improve the verification of the conformance between the actual execution of a business process in the physical world and its execution as recorded by the Business Process Management System (BPMS) based on a secondary log of sensor data [1]. Through the use of common business process engines (e.g. Camunda [20]), which are unaware of IoT involvement, extending the process log with IoT data is difficult and complex. As standard BPMN elements are used for modeling the IoT-driven business rules, the business process engines is unaware of the involvement of IoT, whereby the event log cannot be extended by the engine with IoT data.

Example: Process mining has become an important research area in Computer Science, which aims to extract knowledge from event logs to discover, monitor, and improve business processes [44] [45]. To allow for a finer grained discovery, monitoring, and improvement of IoT-aware business rules, the event log needs to be extended with IoT-related data collected from smart objects. Extending the event log to include IoT data requires an IoT-aware process engine and a suitable architecture. Most IoT infrastructures are based on isolated IoT devices and integrated with applications that are not necessarily process-aware. Furthermore, such applications are often based on proprietary control software with non-standard interfaces [43].

Possible solution: A possible solution to enhance a business rule log with IoT data is to use or develop an IoT-aware business rule engine as well as an embedding architecture. The IoT-aware engine should be able to detect IoT actions and record them in the log. Another way to extend the log with IoT data is to capture the IoT actions in a separate event log. Then the IoT event log may be merged with the process event log.

C5 - Treatment of IoT data outliers

Description: Outliers constitute irregularities or behavioral deviations of the IoT devices and the delivered IoT data. IoT sensors are responsible for capturing, collecting, and transmitting data. The data collected from the physical environment, however, might be prone to outliers [29]. The treatment of outliers is very important in relation to IoT-driven business rules to avoid erroneous decisions being made based on the faulty sensor data.

Example: The IoT is used in a wide variety of environments and scenarios, e.g. environmental monitoring, smart cities, disaster warning, and agriculture. In this context, sensors are often installed in harsh environments. As a consequence, the sensors are susceptible to malfunction, rapid wear, and tampering. This, in turn, can lead to outliers [29]. In Table 3, fault categorizations in IoT implementations are mentioned and summarized [24].

Table 3. IoT fault categorizations [24].

Fault	Definition
Short	An IoT data point deviates significantly from the expected temporal or spatial trend of the data.
Stuck-at	A series of data points has zero or almost zero variation for a period of time greater than expected.
Noise	Sensor data exhibiting an unexpectedly high amount of variation .

Illustrating example: Consider an environmental monitoring station that consists of temperature sensors, humidity sensors, and brightness sensors. If the brightness and temperature sensors are manipulated such that they are directly hit by the sun, the IoT sensor will provide distorted values. This, in turn, leads to the faulty execution of corresponding IoT-driven business rule.

Possible solution: There are different approaches [46–48] and techniques (e.g. machine learning) for detecting and treating of outliers. Most approaches, however, do not equip their IoT-aware business rule engine or architecture with the techniques for handling outliers. One possible solution is to equip the architecture with middleware that detects the IoT outliers and handles them accordingly.

C6 - Treatment of defective IoT devices

Description: Handling defective IoT devices constitutes another major challenge to be tackled in the context of IoT-driven business rules. As discussed in C5, IoT-driven business rules need real-time processing. In this context, IoT sensors must provide a result within an acceptable amount of time. The challenge is to detect and handle defective or non-reachable IoT sensors.

Example: As IoT devices constitute electronic components, they might suddenly fail and then no longer function [30]. Such an IoT device failure result in the evaluation of IoT-driven business rules with missing measured values or zero values. Note that this might lead to several runtime issues in the business process relying on these rules. In literature, such failures are referred to as binary failures [31]. The use of IoT devices in harsh environments and limited computing capacity can lead to failures as well. Other reasons include limited battery life, hardware failures, and human mistakes [32]. The failure of IoT devices involved in IoT-driven business rules might have dire consequences. For example, if a queried IoT sensor is not accessible, no decision can be made, which can lead to deadlocks as the workflow engine continuously checks whether the condition is met or not. Another possible sequence would be the execution of an incorrect business rule. If an IoT sensor suffers from a binary failure, i.e., it returns a zero value by default or the occurrence of an error, it might result in an incorrect business rule executed by mistake. Assume, for example, that the business rule "$temperature\_sensor < 25°C$" returns a zero value if the referred temperature sensor is defective; the condition would still be met.

Possible solution: Several techniques [30] [31] exist for detecting of defective IoT devices. However, there is no specific approach that deals with such failures in the context of IoT-driven business rules. One approach is to use a middleware that enables fault tolerance based on redundant IoT devices or the replacement of faulty IoT data by accessing historical records, depending on the duration of the outage. Another solution is to introduce a prioritization mechanism for IoT devices. The process modeler can assign priority levels for IoT devices. Depending on the priority level of the defective IoT device, the process execution may be aborted or the IoT devices be ignored for decision making.

3.3 Monitoring Challenges

C7 - Traceability of IoT-driven business rules

Description: When monitoring IoT-driven business rules (during both process and business rule execution) traceability constitutes a fundamental challenge. Traceability refers to the understanding of the decision resulting from the evaluation of an IoT-driven business rule. To understand what triggered an IoT-driven business rule, it is crucial to comprehend which IoT devices were queried how and why. A monitoring approach should address this challenge and present both the modeled and the executed IoT-driven business rules in a structured and understandable way.

Example: With increasing context-intensity of the environment in which the IoT-driven business rule is performed, the number of monitoring challenges increases. Moreover, an IoT sensor may be used by multiple business rules. Furthermore, the results of one IoT-driven business rule can be utilized by other rules, resulting in a complex nesting. Therefore, the traceability of IoT-driven business rules must be monitored in an appropriate manner during execution.

Possible solution: [10] introduced a BPMN 2.0 extension that represent business rules graphically in combination with a truth table. This approach further uses overlays and color highlighting to visualize the result of a business rule execution. Although it is possible to determine how the decision was reached, it is not possible to reconstruct the exact decision-making process of a business rule in retrospect, as detailed temporal information is missing, especially for time-critical sensor queries. One possible solution is to time-stamp the incoming data of the queried IoT devices and each evaluation of a business rule, and to visualize it accordingly in the process.

C8 - Fault monitoring in IoT-driven business rules

Description: Monitoring errors constitute another challenge. If IoT devices are used in business rules without receiving any feedback on faults, the IoT-driven business rule process might suffer. Detecting and monitoring IoT devices involved in business rules provides the visibility needed to understand exactly what went wrong and where it went wrong, to subsequently ensure that this error is avoided in the future.

Example: IoT sensors generate large amounts of data and operate automatically and continuously. In order to ensure that sensors properly work in the context of IoT-driven business rules, a precise monitoring system is needed to check the behavior and performance of the IoT sensors. As a key monitoring challenge faulty sensors need to be detected during runtime. Another challenge is to detect and monitor anomalies and outliers. Moreover, the monitoring of IoT devices supports the confidence of the data collected by the sensor and, thus, the quality of the business rules. The higher the confidence of the received IoT data is, the better and more precise the resulting IoT-driven business rule will be. For example, if four temperature sensors are used in a smart home to calculate the average temperature, but only two sensors provide a value as the other two are defective, the confidence of the data is compromised. As a consequence, the resulting output of the IoT-driven business rule will be not accurate and possibly an incorrect action be performed. Without a monitoring system detecting defective IoT devices, the discovery of such scenarios would be not possible.

Possible solution: [10] uses color highlighting (e.g., green, orange, and red) of IoT devices (sensor artifact) involved in the business rule in case an error such as a timeout occurs while polling sensor data. In addition, the corresponding error message is displayed in the execution log. However, the detection is limited to communication errors and errors in the source code. A possible solution is to realize a component that not only detects defective IoT devices, but outliers and insufficient data quality as well. Such a component can mark and visualize the respective errors and provide additional information about the kind of error.

C9 - Real-time monitoring of IoT-driven business rules

Description: Real-time monitoring of IoT-driven business rules enables continuously updated information streamed with low latency. In turn, the continuous streaming of up-to-date IoT data allows for the immediate detection of problems, i.e., based on the real-time monitoring of IoT-driven business rules alerts can be forwarded more quickly to systems for mitigation in the event of a failure of IoT devices.

Example: Monitoring IoT-driven business rules and relevant IoT devices in real-time constitutes another challenge. In particular, this monitoring shall provide additional information about the current processing state of the respective rule. For example, it needs to be monitored which IoT-driven business rules are currently running, in what state they are (e.g., are there faulty IoT devices?), and what will happen next. For the real-time monitoring of IoT-driven business rules, the monitoring system needs to communicate with all IoT devices involved in process and rule execution. Furthermore, the monitoring system should be extensible and scalable to be able to add IoT sensors and IoT-driven business rules on the fly.

Possible solution: Several works [10, 40, 41, 49] exist for monitoring IoT-driven business rules after their execution. In context, during execution it is only possible to monitor the final result of the IoT-driven business rules, but not how they are composed and which intermediate results (of sub-rule evaluation) exist. Moreover, it is not indicated in what state the rules are (e.g. ready, executing, or finish). One possible solution is to develop a suitable architecture that delivers all existing information about the IoT-driven business rules to the monitoring system in real-time. Note that this requires appropriate communication protocols and a real-time capable monitoring component in the architecture.

4 Conclusion

In this paper, modeling, execution, and monitoring IoT-driven business rules was examined by either exploring corresponding rules with BPMN 2.0 or BPMN in combination with DMN. The IoT adds value to BPM through its ability to transform the physical world to its digital twin. Integrating BPM with IoT capabilities should exploit the complete potential of IoT and cover all relevant use cases in this context. Current research related to the combination of IoT and BPM is concerned with the integration of IoT with BPM as a resource. Less attention is paid to the integration of IoT into BPM for decision making through IoT-driven business rules. As a result, several challenges exist with respect for the modeling, execution, and monitoring of IoT-driven business rules. In this paper, in addition to exploring the current support for IoT-driven business rules in BPMN and BPMN + DMN, we have derived these challenges through studying literature, real-world IoT-driven business rules, and hands-on experiences in our IoT-related projects BPMN Extension for IoT (BPMNE4IoT) [2] and IoT Decision Making for BPMN (IoTDM4BPMN) [10]. Existing solutions were described based on a literature review, including a discussion of their strengths and weaknesses. If no solution was found in literature, a possible solution approach was discussed.

The identified challenges should be addressed in future with the goal of enabling the integration of IoT and BPM for executing of IoT-driven business rules.

References

1. Janiesch et al.: The Internet of Things Meets Business Process Management: A Manifesto. In: Systems, Man, and Cybernetics Magazine, (2020)
2. Kirikkayis, Y., Gallik, F. and Reichert, M.: Towards a Comprehensive BPMN Extension for Modeling IoT-Aware Processes in Business Process Models. In: 16th Int Conf on Research Challenges in Inf Science (RCIS), (2022).
3. Ashton, K.: That 'Internet of Things' Thing. In: RFID journal, vol. 22, no. 7, pp. 97–114, (2009).
4. Chang, C., Srirama, S., Buyya, R.: Mobile Cloud Business Process Management System for the Internet of Things: A Survey. In: ACM Computing Surveys 49(4), pp. 1–42. (2016).

5. Hasić, F., Serral, E. and Snoeck, M.: Comparing BPMN to BPMN + DMN for IoT process modelling: a case-based inquiry. In 35th ACM/SIGAPP Symposium on Applied Computing, (2020).
6. Valderas, P., Torres, V. and Serral, E.: Modelling and executing IoT-enhanced business processes through BPMN and microservices. In: The Journal of Systems and Software 184, (2022).
7. Dumas, M., La Rosa, M., Mendling, J., Reijers, H.: Fundamentals of Business Process Management 2nd edn. Springer-Verlag GmbH, Germany (2018).
8. Song, R., Vanthienen, J., Cui, W., Wang, Y. and Huang, L.: Context-Aware BPM Using IoT-Integrated Context Ontologies and IoT-Enhanced Decision Models. In: Conf on Commerce and Enterprise Computing, (2019).
9. Koschmider, A., Mannhardt, F. and Heuser, T.: On the Contextualization of Event-Activity Mappings. In: Business Process Management Workshops, (2018).
10. Kirikkayis, Y., Gallik, F. and Reichert, M.: IoTDM4BPMN: A IoT Decision Making Framework for Business Processes in BPMN. In: Int Conf on Service Science, (2022).
11. Krishnamurthi et al.: An OVerview of IoT Sensor Data Processing, Fusion, and Analysis Techniques. In: Sensors, (2020).
12. OMG: Decision Model and Notation (DMN) 1.2, (2018).
13. OMG: Business Process Model and Notation (BPMN) 2.0, (2010).
14. Hasić, F. and Serral, E.: Executing IoT Processes in BPMN 2.0: Current Support and Remaining Challenges. In: 13th Int Conf on Service Science, (2019).
15. Zhou et al.: An Internet of Things based COPD managing system: Its development, challenges and first experiences. In: Clinical eHalth, (2019).
16. Guiling et al.: Clinical guidelines on the application of Internet of Things (IoT) medical technology in the rehabilitation of chronic obstructive pulmonary disease. In: Journal of thoracic disease, (2021).
17. Bazhenova et al.: From BPMN process models to DMN decision models. In: Information Systems 83, (2019).
18. Combi et al.: Seamless Design of Decision-Intensive Care Pathways. In: Int Conf on Healthcare Informatics (ICHI), (2016).
19. Yousfi et al.: uBPMN: A bpmn extension for modeling ubiquitous business processes. In: Information and Software Technology, (2016).
20. Camunda: Process Engine. In: https://docs.camunda.org/manual/7.8/user-guide/process-engine/, accessed: 2022-20-04.
21. SAP Signavio: SAP Signavio Process Governance In: https://documentation.signavio.com/suite/en-us/Content/workflow-accelerator/userguide/intro.htm, accessed: 2022-20-04.
22. Gruhn et al.: BRIBOT: Towards a Service-Based Methodology for Bridging Business Processes and IoT Big Data. In: Service-Oriented Computing: 19th Int Conf (ICSOC), (2021).
23. Torres et al.: Modeling of IoT devices in Business Processes: A Systematic Mapping Study. In: Conf on Commerce and Enterprise Computing (CEC), (2020).
24. Chakraborty et al.: Fall-curve: A novel primitive for IoT Fault Detection and Isolation. In: Embedded Networked Sensor Systems, (2018).
25. Bazhenova et al.: From BPMN process models to DMN decision models. In: Information Systemms, (2019).
26. Indulska, M., Muehlen, M., Recker, J.: Measuring Method Complexity: The Case of the Business Process Modeling Notation. (2009).
27. De Oca, IMM. and Snoeck, M.: Pragmatic guidelines for business process modeling, In: SSRN 2592983, (2014).

28. Hasic, F. and Vanthienen, J.: Complexity Metrics for DMN Decision Models, In: Computer Standards and Interfaces, (2019).
29. Gaddam et al.: Detecting Sensor Faults, Anomalies and Outliers in the Internet of Things: A Survey on the Challenges and Solutions. In: Electronics, (2020).
30. Pachauri, G., and Sharma, S.: Anomaly Detection in Medical Wireless Sensor Networks using Machine Learning Algorithms. In: Procedia Computer Science, (2015).
31. Ye, J-. Stevenson, G. and Dobson, S.: Detecting abnormal events on binary sensors in smart home environments. In: Pervasive Mob. Comput., (2016).
32. Choi et al.: Detecting and Identifying Faulty IoT Devices in Smart Home with Context Extraction. In: Conf on Dependable Systems and Networks, (2018).
33. Sungur et al.: Extending BPMN for Wireless Sensor Networks. In: Conf on Business Informatics, (2013).
34. Meyer, S., Ruppe, A., Hilty, L.: The Things of the Internet of Things in BPMN. In: Conf in Advanced Information Systems Engineering Workshops, (2015).
35. Cheng et al.: Modeling and Deploying IoT-Aware Business Process Applications in Sensor Networks, (2019).
36. Kirikkayis, Y., Gallik, F. and Reichert, M.: Visual Decision Modeling in IoT-Aware Processes. In: Central European Workshop on Services and their Composition, (2020).
37. Polak, P.: BPMN Impact on Process Modeling, (2013).
38. Mending, J., Reijers, H. and van der Aalst, w.: Seven Process Modeling Guidelines (7PMG), In: Information and Software Technology, (2020).
39. Gallik, F., Kirikkayis, Y. and Reichert, M.: Modeling, Executing and Monitoring IoT-Aware Processes with BPM Technology. In: Int Conf on Service Science, (2022).
40. R. Song, J. Vanthienen, W. Cui, Y. Wang and L. Huang: Context-Aware BPM Using IoT-Integrated Context Ontologies and IoT-Enhanced Decision Models. In: Conf on Commerce and Enterprise Computing, (2019).
41. R. Oliveira et al.: An intelligent model for logistics management based on geofencing algorithms and RFID technology. In: Expert Systems with Applications, (2015).
42. M. Pegoraro and W. M. P. van der Aalst: Mining uncertain event data in process mining. In 2019 Int Conf on Process Mining (ICPM), (2019).
43. Seiger et al.: Towards IoT-driven Process Event Log Generation for Conformance Checking in Smart Factories. In: Int Enterprise Distributed Object Computing Workshop, (2020).
44. van der Aalst: Process mining: Data Science in Action. Springer, (2016)
45. van der Aalst et al.: Process mining Manifesto, In: Lecture Notes in Business Information Processing vol 99, (2012).
46. Samara et al.: A Survey of Outlier Detection Techniques in IoT: Review and Classification. In: Journal of Sensor and Actuator Networks, (2021).
47. Jiang et al.: Outlier Detection Approaches Based on Machine Learning in the Internet-of-Things. In: Wireless Communications, (2020).
48. Bhatti et al.: Outlier detection in indoor localization and Internet of Things (IoT) using machine learning. In: Journal of Communications and Networks, (2020).
49. Celestrini et al.: An Architecture and Its Tools for Integrating IoT and BPMN in Agriculture Scenarios. In: Symposium on applied computing, (2019).
50. Song et al.: A DMN-Based Method for Context-Aware Business Process Modeling Towards Process Variability. In: Business Information Systems, (2019).
51. Domingos et al.: Automatic Decomposition of IoT Aware Business Processes - a Pattern Approach. In: Int Conf on ENTERprice Information Systems (CENTERIS), (2019).